Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Zwischen

Rico Rothenburger
Haydnstr. 2
30659 Hannover

- nachfolgend „**Auftragnehmer**“ genannt –

und der Firma

Firmenname:

Straße, Nr.:

PLZ: Ort: Land:

- nachfolgend „**Auftraggeber**“ genannt –

besteht / bestehen unter

Kundennummer:

ein / mehrere von dem Auftraggeber genutzte(r) Vertrag / Verträge.

1. Gegenstand des Vertrages, Gegenstand dieses Auftragsverarbeitungsvertrages (Art. 28 Abs. 1 DSGVO)

(1) Gegenstand des Vertrages ist die Bereitstellung von Webhosting-Dienstleistungen bzw. eines (oder mehrerer) dedizierten/dedizierter Webserver(s) sowie der damit im Zusammenhang stehenden Leistungen wie z.B. E-Mail, Domainregistrierung, etc. Im Rahmen dieses Vertrages hat der Auftraggeber – je nach Tarif und vereinbartem Leistungsumfang – unter Nutzung u.a. z.B. eines Webservers, FTPServers oder SSH-Zugangs die Möglichkeit, Daten zu verarbeiten (zu speichern, zu verändern, zu übermitteln und zu löschen).

(2) Gegenstand des Vertrages ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Im Zuge der Leistungserbringung des Auftragnehmers als zentraler IT-Dienstleister im Bereich des Hostings, des Supports bzw. der Administration von Server-Systemen des Auftraggebers, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden.

(3) Die Einzelheiten ergeben sich aus dem Hauptvertrag / den Hauptverträgen, die unter der benannten Kundennummer zusammengefasst sind. Die Vereinbarung zur Auftragsverarbeitung findet Anwendung auf das gesamte Dienstleistungsverhältnis, sofern die in Punkt 1.1 beschriebenen Dienstleistungen betroffen sind.

(4) Soweit nachfolgend von Daten die Rede ist, handelt es sich ausschließlich um personenbezogene Daten im Sinne der DSGVO. Die nachfolgenden Datenschutz- und Datensicherheitsbestimmungen finden Anwendung auf alle Leistungen der Auftragsverarbeitung i.S.d. Art. 28 Abs. 1 DSGVO, die der Auftragnehmer gegenüber dem Auftraggeber erbringt und auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

(5) In Ergänzung zu dem/den zwischen den Parteien geschlossenen Vertrag/Verträgen konkretisieren die Vertragsparteien mit vorliegendem Auftragsverarbeitungsvertrag die gegenseitigen Pflichten im generellen Umgang mit den Daten des Auftraggebers.

2. Laufzeit, Beendigung, Löschung von Daten (Art. 28 Abs. 1 DSGVO)

(1) Die Laufzeit des Vertrages richtet sich nach der Dauer der Erbringung von Hosting-Leistungen des Auftragnehmers an den Auftraggeber. Der Auftrag endet, wenn der Auftraggeber keine Hosting-Leistungen des Auftragnehmers, entsprechend den Leistungsvereinbarungen/Angeboten der einzelnen Auftragsbestätigungen für Hosting-Leistungen des Auftragnehmers, mehr in Anspruch nimmt.

(2) Die Rechte der durch den Datenumgang bei dem Auftragnehmer betroffenen Personen, insbesondere auf Berichtigung, Löschung und Sperrung, sind gegenüber dem Auftraggeber geltend zu machen. Er, der Auftraggeber, ist allein verantwortlich für die Wahrung dieser Rechte.

(3) Nach Ende des Auftrags oder auf schriftliche Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche Daten des Auftraggebers vollständig datenschutzgerecht zu löschen (einschließlich der verfahrens- oder sicherheitstechnisch notwendigen Kopien) oder an den Auftraggeber zurückzugeben. Das gleiche gilt auch

für Test- und Ausschussmaterial, das bis zur Löschung oder Rückgabe unter datenschutzgerechtem Verschluss zu halten ist. Dies gilt nicht für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen oder soweit z.B. rechtliche Regelungen, gesetzliche Pflichten oder gerichtliche Verfügungen dem entgegenstehen. Entstehen durch eine Löschung vor Vertragsbeendigung zusätzliche Kosten, so trägt diese der Auftraggeber.

(4) Der Auftragnehmer ist verpflichtet, im Rahmen seiner Tätigkeit für den Auftraggeber an ihn gerichtete Ersuchen Betroffener zur sachgerechten Bearbeitung unverzüglich an die Auftraggeber weiterzuleiten. Er ist nicht berechtigt, diese Ersuchen ohne Abstimmung mit dem Auftraggeber selbständig zu bescheiden.

(5) Der Auftragnehmer hat den Auftraggeber bei der Umsetzung der Rechte der Betroffenen nach Kapitel III der DSGVO, insbesondere im Hinblick auf Berichtigung, Sperrung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen der technischen Möglichkeiten, insbesondere hinsichtlich des Charakters der geschuldeten Dienstleistung, zu unterstützen.

(6) Zu einem Datenträgeraustausch gemäß Art. 28 Abs. 3 lit. g DSGVO zwischen den Beteiligten dieser Auftragsverarbeitung kommt es nicht. Insoweit ist eine Rückgabe nicht zu regeln.

3. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten

(1) Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten ergeben sich aus dem zwischen den Vertragsparteien bestehenden Vertrag.

Der Auftragnehmer ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden. Dem Auftragnehmer ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikatsdateien zur leistungsgemäßen Erhebung, Verarbeitung und / oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt. Dem Auftragnehmer ist nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Daten aus Adressbüchern und Verzeichnissen dürfen nur zur Kommunikation im Rahmen der Auftragserfüllung mit dem Auftraggeber verwendet werden. Eine anderweitige Nutzung und Übermittlung für eigene oder fremde Zwecke, einschl. Marketingzwecke, ist nicht gestattet.

(2) Soweit seitens des Auftragnehmers eine Erhebung, Verarbeitung und / oder Nutzung der Daten erfolgt, geschieht dies ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Jede Verlagerung in ein anderes Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 DSGVO erfüllt sind.

4. Art der Daten und Kreis der Betroffenen (Art. 28 Abs. 3 S. 1 DSGVO)

(1) Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung der Daten des Auftraggebers gem. Ziff. 1.2 Satz 2 sind folgende Datenarten:

(durch den Auftraggeber vollständig und richtig auszufüllen/anzukreuzen!)

- ☐ Pseudonymisierte Nutzungsdaten und -profile aus dem Webtracking z.B. im Web Analytics-System des Auftragnehmers aufgezeichnete Nutzungsdaten, insbesondere IP-Adressen der Nutzer
- ☐ Vertrags- und Kontaktdaten von Kunden und Interessenten, Name, Adresse, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Lieferadresse, Zählernummer, Informationen zum Auftragsstatus, sowie die Zahlung betreffende Daten der Kunden des Auftragnehmers
- ☐ Kontaktdaten der betroffenen Mitarbeiter und Dienstleister des Auftraggebers, Name, Adresse und E-Mail-Adresse
- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail) Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten Planungs- und Steuerungsdaten Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

☐ Sonstige Daten:

(2) Kreis der Betroffenen

Der Kreis der durch den Umgang mit den Daten gem. Ziff. 1.2 Satz 2 Betroffenen umfasst:

(durch den Auftraggeber vollständig und richtig auszufüllen/anzukreuzen!)

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner

☐ Sonstige Betroffene:

5. Pflichten des Auftragnehmers

5.1 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der

konkreten Auftragsdurchführung, zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit eine Prüfung bzw. ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5.2 Qualitätssicherung und sonstige Pflichten des Auftragnehmers (Art. 28-33 DSGVO)

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr Rothenburger, Rico, +49 511 - 219 568 76, datenschutz@enerspace.de benannt.

(2) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

(4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(5) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde

im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(6) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
(7) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(8) Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 9 dieses Vertrages.

6. Unterauftragsverhältnisse (Art. 28 Abs. 2 u. 4 DSGVO)

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Die Auftragnehmer trägt dafür Sorge, dass dem Auftraggeber eine aktuelle Liste der eingesetzten Unterauftragnehmer die unter https://www.enerspace.de/unterauftragnehmer stets zum Abruf zur Verfügung steht. Bei Änderung dieser Liste in Bezug auf die Hinzuziehung oder Ersetzung von weiteren Auftragnehmern ergeht hierüber eine Information an den Auftraggeber.

(3) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

7. Pflichten des Auftraggebers (Art. 24 DSGVO und Art. 13 und 14 DSGVO)

(1) Der Auftraggeber ist für die Einhaltung der für ihn einschlägigen datenschutzrechtlichen Regelungen verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er Verstöße des Auftragnehmers gegen datenschutzrechtliche Bestimmungen feststellt.

(3) Den Auftraggeber treffen die sich aus Art. 24 DSGVO und Art. 13 und 14 DSGVO ergebenden Informationspflichten.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO oder die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO; aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI- Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

9. Weisungsbefugnisse, Berichtigung, Löschung und Sperrung, Rechte Betroffener (Art. 29 i.V.m. 28 DSGVO sowie Kapitel III der DSGVO)

(1) 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. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

(2) 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. 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 soweit notwendig 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.

10. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.:

(a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
(b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
(c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
(d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
(e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

11. Sonstiges, Allgemeines

(1) Sollten die personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den personenbezogenen Daten des Auftraggebers bei dem Auftraggeber liegt.

(2) Unbeschadet des Weisungsrechts des Auftraggebers gemäß Absatz 11 dieser Vereinbarung bedürfen Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf diese Formerfordernis.

(3) Die Regelungen dieser Vereinbarung gelten auch nach einer Beendigung des primären Leistungsverhältnisses bis zur vollständigen Vernichtung oder Rückgabe aller personenbezogenen Daten des Auftraggebers an den Auftraggeber fort.

12. Salvatorische Klausel, Gerichtsstand

(1) Sollte eine Bestimmung dieses Vertrages ungültig oder undurchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieses Vertrages hiervon unberührt. Die Parteien vereinbaren, die ungültige oder undurchsetzbare Bestimmung durch eine gültige und durchsetzbare Bestimmung zu ersetzen, welche wirtschaftlich der Zielsetzung der Parteien am nächsten kommt. Das Gleiche gilt im Falle einer Regelungslücke.

(2) Als Gerichtsstand wird Hannover vereinbart.

Ort/Datum	Unterschrift / Stempel des Auftraggebers
Hannover, 24.05.2018	
Ort/Datum	Auftragnehmer Rico Rothenburger

Anlage 1: Technische und organisatorische Maßnahmen

TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN

gem. Anlage zu Art. 32 DSGVO

der Organisation

enerSpace Webhosting
Rico Rothenburger
Haydnstr. 2
30659 Hannover

Stand
22.05.2018

enerSpace Webhosting vermietet die Datenverarbeitungsanlage an den Kunden. Dies beinhaltet die Vermietung von Hard- und Software, sowie die Bereitstellung von Anbindungen an das Internet sowie weitere Dienste entsprechend der jeweiligen Vereinbarung. Der Kunde entscheidet allein und ausschließlich darüber, welche personenbezogene Daten in welcher Weise verarbeitet werden („Herr der Daten“). Die hierfür erforderlichen Programme zur Datenverarbeitung werden durch den Kunden erstellt und eingesetzt. enerSpace Webhosting sorgt für die technische Einsatzbereitschaft des Systems entsprechend den vertraglichen Vereinbarungen und führt Buch darüber, welche Anlagen durch den Kunden in welchem Umfang genutzt werden. Die Datenverarbeitung erfolgt durch den Kunden. enerSpace Webhosting hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die og. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Sicherheitsschlösser	☒ Schlüsselregelung / Liste
☒ Manuelles Schließsystem	☒ Empfang / Rezeption / Pförtner
☒ Türen mit Knauf Außenseite	☒ Besucher in Begleitung durch Mitarbeiter

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.
Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Anti-Viren-Software Server	☒ Allg. Richtlinie Datenschutz und / oder Sicherheit
☒ Anti-Virus-Software Clients	☒ Zentrale Passwortvergabe

☒ Intrusion Detection Systeme	☒ Richtlinie „Sicheres Passwort“
☒ Firewall	☒ Richtlinie „Löschen / Vernichten“
☒ Automatische Desktopsperre	☒ Anleitung „Manuelle Desktopsperre“
☒ W-LAN-Verschlüsselung	☐

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Aktenschredder (mind. Stufe 3, cross cut)	☒ Einsatz Berechtigungskonzepte
☒ Physische Löschung von Datenträgern	☒ Minimale Anzahl an Administratoren
☐	☒ Verwaltung Benutzerrechte durch Administratoren

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Test-umgebung	☒ Datensätze sind mit Zweckattributen ver-sehen
☒ Mandantenfähigkeit relevanter Anwendungen	☒ Festlegung von Datenbankrechten

1.5. Anonymisierung / Pseudonymisierung / Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Anonymisierung, Pseudonymisierung oder Verschlüsselung von Daten des Auftraggebers sind grundsätzlich nicht Gegenstand der von enerSpace Webhosting zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Weitergabekontrolle

Maßnahmen, die 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, und dass überprüft und festgestellt

werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von VPN	☒ Weitergabe in anonymisierter oder pseudonymisierter Form
☒ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen	☒ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☒ Strenge administrative Aufgabentrennung	☐

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
☒ Manuelle oder automatisierte Kontrolle der Protokolle	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
☐	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☐	☒ Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	☒ Tägliche inkrementelle Datensicherung
☒ Feuerlöscher Serverraum	☒ Wöchentliche vollständige Datensicherung

☒ Serverraumüberwachung Temperatur und Feuchtigkeit	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ Serverraum klimatisiert	☒ Getrennte Partitionen für Betriebssysteme und Daten
☒ Unterbrechungsfreie-Stromversorgung (USV)	☒ Trennung von Anwendungs- und Administrationszugängen
☒ Schutzsteckdosenleisten Serverraum	☒ Überwachung und Protokollierung allgemeiner Benutzeraktivität
☒ RAID System / Festplattenspiegelung	☒ Protokollierung von administrativen Änderungen
☒ Videoüberwachung Serverraum	☐
☒ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	☐
☒ Schutz der Infrastruktur durch Hardware-Firewalls und Software-Firewalls	☐
☒ Antivirus-Software auf allen Systemen	☐

3.2. Belastbarkeit der Systeme

enerSpace Webhosting unternimmt die unter Ziffer 3.1. dargestellten Maßnahmen um eine Belastbarkeit der ITSysteme sicherzustellen. Penetrationstests der IT-Systeme des Auftraggebers sind grundsätzlich nicht Gegenstand der von enerSpace Webhosting zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☐	☒ Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
☐	☒ Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Formaler Prozeß und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☐
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☐
☒ Intrusion Detection System (IDS)	☐
☒ Intrusion Prevention System (IPS)	☐

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☐
☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	☐

4.4. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	Organisatorische Maßnahmen
☐	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
☐	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
☐	☒ Regelung zum Einsatz weiterer Subunternehmer
☐	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags