Auftragsverarbeitungsvertrag („Vertrag“, „Auftrag“, „Vereinbarung“) gemäß Art. 28 DS-GVO

Naherholungs- und Kulturverein Großensee e.V.

Norbert Paech (1. Vorsitzender)

Brookwisch 6a

22946 Großensee

– nachstehend „für die Verarbeitung Verantwortlicher“ und „Verantwortlicher“ genannt –

und

Febas, Roman Baumgärtner
Ostlandstr. 5
49565 Bramsche

– nachstehend „Auftragsverarbeiter“ genannt –

schließen zur Kundennummer 8185 und die darunter geführten Webhosting-, vServer- und Domainmietverträge (=“Hauptvertrag“, „Hauptverträge“) nachfolgenden ergänzenden Auftragsverarbeitungsvertrag („Auftrag“, „Vertrag“, „Vereinbarung“) über die Verarbeitung von Daten des Verantwortlichen durch den Auftragsverarbeiter.

Dieser Auftrag ist zur sprachlichen Vereinfachung und Klarheit nicht gegendert. Wenn die männliche Form für eine Person verwendet wird (z.B. „Besucher“, „Mitarbeiter“) ist damit auch die weibliche Form gemeint (z.B. „Besucherin“, „Mitarbeiterin“).

1. Gegenstand und Dauer der Vereinbarung

(1) Der Hauptvertrag umfasst Webhosting-Dienstleistungen, d.h. Vermietung von Speicherplatz im Internet zum Betrieb von Websites und Computerprogrammen auf diesen Websites. Der genaue Leistungsumfang ist in den Webseiten des Auftragsverarbeiters für die jeweils vom Verantwortlichen gemietete Dienstleistung konkretisiert. Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten im Auftrag des Verantwortlichen im Sinn von Art. 4 Nr. 2 und Art. 28 DS-GVO.

(2) Die Laufzeit dieses Auftrags entspricht der Laufzeit des Hauptvertrages. Für den Fall, dass Leistungen auch darüber hinaus erbracht werden, gelten die Regelungen dieses Auftrags solange fort, bis die tatsächliche Zusammenarbeit endet.

(3) Der Verantwortliche kann diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragsverarbeiter eine Weisung des

Verantwortlichen nicht ausführen kann oder will oder der Auftragsverarbeiter Kontrollrechte des Verantwortlichen vertragswidrig verweigert. Das Recht zur Ausübung eines gesetzlichen Rücktrittsrechts für diese Vereinbarung bleibt hierdurch unberührt.

2. Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung

(1) „Datenverarbeitung“ oder „Verarbeitung“ meint in diesem Auftrag die Verwendung von personenbezogenen Daten, insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung, Löschung, Anonymisierung, Pseudonymisierung, Verschlüsselung oder sonstige Nutzung der Daten.

(2) Verarbeitungsgegenstand sind alle Daten, die im Rahmen des Hauptvertrages vom Verantwortlichen in seinen Websites, Datenbanken und E-Mail-Postfächern gespeichert oder verarbeitet werden, von Nutzern der Websites des Verantwortlichen auf dessen Websites eingegeben werden, per E-Mail an ihn gesendet werden oder vom Verantwortlichen per E-Mail versendet werden.

Insbesondere sind folgende Datenarten Verarbeitungsgegenstand (angekreuzt):

- ☒ Adressdaten
- ☒ Abrechnungsdaten (Rechnungsdaten)
- ☒ Archivdateien
- ☒ Bank- und Kontodaten
- ☒ Bestelldaten
- ☒ Bilder/Fotos
- ☒ E-Mails und E-Mail-Anhänge
- ☐ Mitarbeiterdaten
- ☒ Vertragsdaten
- ☒ Stammdaten
- ☒ Statistiken (Nutzungsdaten, Protokolle)
- ☒ Texte
- ☒ Videos
- ☐
- ☐
- ☐

Kreis der Betroffenen (angekreuzt):

- ☐ Kunden
- ☒ Nutzer
- ☐ Lieferanten
- ☐ Mitarbeiter
- ☐ Bewerber
- ☐ Interessenten
- ☐ Geschäftspartner
- ☒ Mitglieder
- ☐ Dienstleister
- ☐ Praktikanten
- ☐
- ☐
- ☐

(3) Die Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verarbeitung in einem Drittland darf nur erfolgen, wenn die Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind und bedarf der vorherigen Zustimmung des Verantwortlichen.

3. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

(1) Die technischen und organisatorischen Maßnahmen sind in der Anlage „Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO“ zu diesem Auftrag geregelt.

(2) Der Auftragsverarbeiter beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Die Datensicherheitsmaßnahmen bei dem Auftragsverarbeiter können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind von dem Auftragsverarbeiter mit dem Verantwortlichen schriftlich abzustimmen.

4. Regelungen zur Erhebung, Berichtigung, Löschung und Sperrung von Daten

(1) Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder zu sperren, wenn der Verantwortliche dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragsverarbeiters dem nicht entgegenstehen. Der Auftragsverarbeiter wird Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig löschen oder deren Verarbeitung einschränken.

(2) Für den Fall, dass sich eine betroffene Person an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter das Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

5. Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen. Die Kosten, die durch Weisungen des Verantwortlichen, die den vertraglich vereinbarten Leistungsumfang des Hauptvertrages übersteigen, bei der Auftragsnehmerin entstehen, sind vom Verantwortlichen zu tragen.

(2) Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien werden nur zum Zwecke der Datensicherung oder Servermigration, kurzzeitig temporär von Software, die zur Datenverarbeitung eingesetzt wird, für das Erreichen des Verarbeitungszwecks, wenn es technisch für die ordnungsgemäße Funktion der Serversoftware notwendig ist, darüber hinaus aber ohne Wissen des Verantwortlichen nicht erstellt.

(3) Der Auftragsverarbeiter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Verantwortlichen das Datengeheimnis zu wahren.

(4) Der Auftragsverarbeiter dokumentiert die Umsetzung der technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO hinsichtlich der konkreten Auftragsdurchführung und übergibt die Dokumentation dem Verantwortlichen. Bei Annahme durch den Verantwortlichen werden die dokumentierten Maßnahmen wesentlicher Bestandteil des Auftrags. Als hinreichend umfangreiche und genaue Dokumentation wird zwischen beiden Parteien die Anlage „Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage“ dieses Auftrags vereinbart.

(5) Der Auftragsverarbeiter hat über die gesamte Abwicklung der Dienstleistung für den Verantwortlichen insbesondere folgende Kontrollen in seinem Bereich durchzuführen:

- Regelmäßige Serverwartung einschließlich notwendiger Sicherheitsupdates der Serversoftware
- Regelmäßige Datensicherung gemäß Leistungsbeschreibung des Hauptvertrages

(6) Der Auftragsverarbeiter wird den Verantwortlichen bei der Durchführung von Kontrollen durch den Verantwortlichen unterstützen und an der zügigen und vollständigen Kontrolle mitwirken. Sofern der Verantwortliche sein Kontrollrecht ausübt, steht dem Auftragsverarbeiter eine Vergütung dafür zu, die in Abschnitt (8.4) dieses Auftrags näher geregelt ist.

(7) Der Auftragsverarbeiter gestaltet seine Betriebsabläufe so, dass die Daten, die er im Auftrag des Verantwortlichen verarbeitet, so wie erforderlich gesichert und von der Kenntnisnahme unbefugter Dritter geschützt sind.

(8) Der Auftragsverarbeiter arbeitet auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung derer Aufgaben zusammen.

(9) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Datenschutz-Folgeabschätzungen und Meldepflichten bei Datenpannen. Dazu gehören u.a.

- Technische und organisatorische Maßnahmen, die eine zügige Feststellung bedeutender Verletzungsereignisse ermöglichen und dabei die Umstände und Zweck der Verarbeitung und vermutete Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen.
- Meldung von Verletzungen des personenbezogenen Datenschutzes an den Verantwortlichen.
- Unterstützung des Verantwortlichen im Rahmen der Informationspflicht der Auftragsnehmerin gegenüber Betroffenen und zügige Bereitstellung aller bedeutenden Informationen.
- Unterstützung des Verantwortlichen bei dessen Datenschutz-Folgeabschätzung.
- Unterstützung des Verantwortlichen bei Vorab-Beratungen mit der Aufsichtsbehörde.

Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Hauptvertrages enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, bezahlt der Verantwortliche eine dem tatsächlichen Aufwand angemessene Vergütung an den Auftragsverarbeiter, die sich am Stundensatz des für die Unterstützungsleistung durch den Auftragsverarbeiter abgestellten Mitarbeiters und dem Zeitaufwand für die Unterstützung orientiert.

(10) Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine vom Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Verantwortlichen bestätigt oder geändert wird.

(11) Der Auftragsverarbeiter informiert den Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, wenn sie sich auf diesen Auftrag beziehen. Dies gilt auch dann, wenn eine zuständige Behörde im Rahmen eines Straf- oder Ordnungswidrigkeitsverfahrens in Bezug auf die Verarbeitung personenbezogener Daten der Auftragsverarbeitung bei dem Auftragsverarbeiter ermittelt und diese Ermittlungstätigkeit oder Strafverfolgung dadurch nicht behindert wird.

(12) Der Auftragsverarbeiter teilt dem Verantwortlichen unverzüglich Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf

Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Informationspflichten des Verantwortlichen nach §§ 32 und 33 BDSG sowie § 15a TMG. Der Auftragsverarbeiter sichert zu, den Verantwortlichen bei seinen Informationspflichten nach §§ 32 und 33 BDSG zu unterstützen.

(13) Der Auftragsverarbeiter hat an der Erstellung der Verfahrensverzeichnisse durch den Verantwortlichen mitzuwirken wie folgt: Er hat dem Verantwortlichen auf konkrete Nachfrage des Verantwortlichen die jeweils notwendigen Angaben konkret angefragter Verfahren in geeigneter Weise mitzuteilen.

(14) Der Auftragsverarbeiter kann dem Verantwortlichen Person(en) nennen, die berechtigt sind, Weisungen des Verantwortlichen zu empfangen.

(15) Ein betrieblicher Datenschutzbeauftragter ist bei dem Auftragsverarbeiter nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt. Sollte der Auftragsverarbeiter später zur Bestellung eines Datenschutzbeauftragten verpflichtet sein, wird er einen Datenschutzbeauftragten im Sinne § 38 BDSG bestellen und ihn dem Verantwortlichen in Textform benennen. Bis dahin wird die Rolle eines Datenschutzbeauftragten durch den Geschäftsinhaber des Auftragsverarbeiters hinreichend erfüllt, ohne dass es dazu einer gesonderten Bestellung bedarf.

6. Unterauftragsverhältnisse

(1) Unterauftragsverhältnisse sind solche Dienstleistungen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht dazu gehören Nebenleistungen, die der Auftragsverarbeiter zur Sicherung von Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hardware und Software seiner Datenverarbeitungsanlagen in Anspruch nimmt, insbesondere Telekommunikationsleistungen, Post- und Transportdienstleistungen, Wartung, Support und Benutzerservice.

(2) Der Auftragsverarbeiter kann zur Erfüllung der vertraglichen Leistungspflichten des Hauptvertrages verbundene Unternehmen des Auftragsverarbeiters heranziehen oder Dritte unterbeauftragen. Der Verantwortliche erklärt sich damit einverstanden. Der Auftragsverarbeiter muss dafür Sorge tragen, dass er den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 28 DS-GVO sorgfältig auswählt.

7. Pflichten des Verantwortlichen

(1) Der Verantwortliche ist verantwortliche Stelle für die Verarbeitung von Daten im Auftrag durch den Auftragsverarbeiter im Sinne § 46 Abs. 7 BDSG. Für die Beurteilung der Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Verantwortliche verantwortlich. Alle sich aus datenschutzrechtlichen Anforderungen ergebenden Pflichten liegen beim Verantwortlichen. Dazu gehört zum Beispiel die Führung eines öffentlichen Verfahrensverzeichnisses.

(2) Der Verantwortliche ist verantwortliche Stelle für die Wahrung der Betroffenenrechte. Betroffenenrechte sind gegenüber dem Verantwortlichen wahrzunehmen. Falls eine Mitwirkung der Auftragsverarbeiter zur Wahrung von Betroffenenrechte durch den Verantwortlichen notwendig ist – insbesondere der Rechte auf Auskunft, Berichtigung, Sperrung oder Löschung – wird der Auftragsverarbeiter die notwendigen Maßnahmen gemäß Weisung des Verantwortlichen treffen. Der Mehraufwand des Auftragsverarbeiters ist in solchen Fällen durch den Verantwortlichen an den

Auftragsverarbeiter angemessen zu vergüten. Die Vergütung orientiert sich an den auf der Website des Auftragsverarbeiters veröffentlichten Stundensätzen für Softwareentwicklung.

(3) Der Verantwortliche arbeitet auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung derer Aufgaben zusammen.

(4) Der Verantwortliche erteilt alle Aufträge oder Teilaufträge in der Regel in Textform. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(5) Sämtliche bei dem Auftragsverarbeiter verarbeitete Daten werden in der Regel sofort, aber spätestens 30 Tage nach Beendigung des Hauptvertrages gelöscht, wenn dem keine gesetzlichen Zurückbehaltungspflichten des Auftragsverarbeiters entgegenstehen. Der Verantwortliche wird Daten vor Beendigung des Vertrages umziehen oder davon eine Sicherungskopie anfertigen. Er hat selbst Zugriff auf seine Daten, deshalb ist der Auftragsverarbeiter nicht verpflichtet, sie herauszugeben. Davon unberührt bleibt die Pflicht des Auftragsverarbeiters, während der Vertragslaufzeit Datensicherungen gemäß Leistungsbeschreibung des Hauptvertrages anzufertigen.

(6) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten feststellt.

(7) Der Verantwortliche kann dem Auftragsverarbeiter Person(en) nennen, die berechtigt sind, dem Auftragsverarbeiter Weisungen zu erteilen.

8. Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche hat das Recht, gemeinsam und nach Abstimmung mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelnen zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichproben, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter zu überzeugen.

(2) Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf konkrete Nachfrage die notwendigen Auskünfte zu erteilen und die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann wahlweise durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO, aktuelle Testate, Berichte oder Auszüge aus solchen Berichten unabhängiger Einrichtungen (z.B. Revision, Wirtschaftsprüfer, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Qualitäts- oder Datenschutzauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erfolgen. Solche Zertifizierungen, Berichte, Testate u.a. wie vorstehend beschrieben sind auch dann hinreichend, wenn sie nicht für den Auftragsverarbeiter selbst, sondern für den Unterauftragnehmer des Auftragsverarbeiters bestehen, an den die Auftragsverarbeitung durch den Auftragsverarbeiter ganz oder teilweise ausgelagert wird.

(4) (4) Für die Durchführung solcher Kontrollen des Verantwortlichen und die Mitwirkung des Auftragsverarbeiters daran zahlt der Verantwortliche dem Auftragsverarbeiter eine angemessene Vergütung (Die Vergütung orientiert sich an den auf der Website des Auftragsverarbeiters

veröffentlichten Stundensätzen für Softwareentwicklung) und ersetzt dem Auftragsverarbeiter allen ihm dadurch entstehenden Mehraufwand (z.B. Arbeitszeitkosten, Materialeinsatz, Reise-, Übernachtungs- und Verpflegungskosten und den Aufwand, der der Auftragsverarbeiter durch Unterauftragnehmer für solche Kontrollen in Rechnung gestellt wird).

9. Datengeheimnis

(1) Der Auftragsverarbeiter ist zur Wahrung des Datengeheimnisses im Sinne des § 53 BDSG verpflichtet, wenn er Daten für den Verantwortlichen verarbeitet. Er beachtet dabei die gleichen Geheimschutzregeln, die dem Verantwortlichen obliegen.

(2) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften des BDSG bekannt sind.

(3) Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und sie auf das Datengeheimnis schriftlich verpflichtet. Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

(4) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder an Betroffene darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Weisung oder Zustimmung durch den Verantwortlichen erteilen.

(5) Beide Vertragsparteien verpflichten sich, alle Informationen, die sie in Verbindung mit der Vertragsdurchführung des Hauptvertrages und dieser Vereinbarung erhalten, zeitlich unbegrenzt vertraulich zu behandeln und ausschließlich zur Vertragsdurchführung zu verwenden. Keine Vertragspartei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den in diesem Vertrag genannten Zwecken zu nutzen oder Dritten zugänglich zu machen. Diese Pflicht gilt nicht für Informationen, die eine der Parteien von Dritten erhalten hat, ohne einer Geheimhaltungspflicht zu unterliegen, oder die öffentlich bekannt sind.

10. Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags

(1) Spätestens 30 Tage nach Beendigung des Hauptvertrages hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dieser Vereinbarung und Hauptvertrag stehen, datenschutzgerecht zu löschen bzw. zu vernichten. Davon unberührt bleiben gesetzliche Aufbewahrungs- und Zurückbehaltungspflichten (z.B. im Fall eines laufenden polizeilichen Ermittlungsverfahrens oder Strafverfahrens oder steuerrechtlicher Aufbewahrungsfristen, sofern diese Fristen des Auftragsverarbeiters betreffen).

11. Vergütung

(1) Der Abschluss dieses Auftrags ist entgeltfrei.

(2) Wenn der Verantwortliche Unterstützung bei der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Datenschutz-Folgeabschätzungen und Meldepflichten bei Datenpannen benötigt im Sinne von Abschnitt (5.) dieses Auftrags oder wenn der Verantwortliche Unterstützung für die Beantwortung von Anfragen Betroffener benötigt im Sinne von Abschnitt (7.) dieses Auftrags, hat er die hierdurch entstehenden Kosten zu erstatten. Wenn der Verantwortliche Kontrollrechte ausübt, orientiert sich das vorab zu vereinbarende Entgelt an dem festzulegenden Stundensatz des für die Betreuung von dem Auftragsverarbeiter und Unterauftragnehmern abgestellten Mitarbeiter zuzüglich aller dem Auftragsverarbeiter entstehenden Mehrkosten gemäß Abschnitt (8.) dieses Auftrags. Wenn der Verantwortliche dem Auftragsverarbeiter Weisungen erteilt, hat er die durch die Weisungen entstehenden Kosten zu erstatten. Darüber hinaus können Vergütungsansprüche des Auftragsverarbeiters gegen den Verantwortlichen entstehen, wenn diese in anderen Abschnitten dieser Vereinbarung als Folge von Handlungen oder Unterlassungen angekündigt sind. Solche Vergütungsansprüche orientieren sich an den auf der Website des Auftragsverarbeiters veröffentlichten Stundensätzen für Softwareentwicklung.

12. Schlussbestimmungen

(1) Für den Fall, dass das Eigentum des Verantwortlichen bei dem Auftragsverarbeiter durch Maßnahmen Dritter (z.B. Pfändung, Beschlagnahme), durch ein Insolvenzverfahren oder sonstige Ereignisse gefährdet wird, wird der Auftragsverarbeiter den Verantwortlichen unverzüglich informieren. Der Auftragsverarbeiter wird die Gläubiger informieren, dass es sich um Daten handelt, die im Auftrag verarbeitet werden.

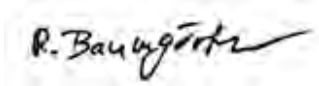
(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Die Einrede des Zurückbehaltungsrechts im Sinne des § 273 BGB wird hinsichtlich der für den Verantwortlichen verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(4) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Bersenbrück.

(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht.

(6) Änderungen und Ergänzungen am Vertragstext abseits der einleitenden Angaben zur Person und Kundennummer des Verantwortlichen und der in Abschnitt (2.) möglichen Ergänzungen sind unwirksam.

Ort, Datum	Bramsche, 18.07.2018
	
(Verantwortlicher) Unterschrift	(Auftragsverarbeiter)

Anlage zum Auftrag gemäß Art. 28 DS-GVO: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage

Die technischen und organisatorischen Maßnahmen betreffen den Auftragsverarbeiter und seine Unterauftragnehmer, insbesondere die Hetzner Online GmbH, 91710 Gunzenhausen, bei der der Auftragsverarbeiter Server in mehreren Rechenzentren betreibt. Der Auftragsverarbeiter hat mit der Hetzner Online GmbH einen Auftrag gemäß Art. 28 DS-GVO abgeschlossen, deren technische und organisatorische Maßnahmen nach Art. 32 DS-GVO mindestens dem in dieser Anlage wiedergegebenen Standard entsprechen.

I. Vertraulichkeit

Zutrittskontrolle

Rechenzentren:

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um den gesamten Datacenterpark
- dokumentierte Schlüsselvergabe
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
- Der Zutritt für betriebsfremde Personen (z.B. Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Mitarbeiters des Auftragsverarbeiters oder des Unterauftragnehmers.

Verwaltung der Rechenzentren:

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Videoüberwachung an den Ein- und Ausgängen

Kaufmännische Verwaltung:

- Keine Zugangsmöglichkeit für betriebsfremde Personen
- Räumliche Trennung vom technischen Betriebsteil

Zugangskontrolle

Rechenzentren und Server:

- Das Passwort zur Administrationsoberfläche wird vom Verantwortlichen selbst gesteuert und muss vordefinierte Sicherheitsrichtlinien erfüllen. Zusätzlich steht dem Verantwortlichen dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Kundenzugangs zur Verfügung.
- Der Zugang ist passwortgeschützt; Zugriff besteht nur für berechtigte Mitarbeiter der Auftragsverarbeiterin; verwendete Passwörter müssen Mindestlänge und eine Mindestkomplexität haben.
- Zugang ausschließlich für wenige, mit der Serverwartung betraute Mitarbeiter.

- Zeitliche Befristung und funktionelle Beschränkung für Mitarbeiter von Support-Unternehmen, insbesondere zur Wartung der Webspace-Control-Panel Software im Fehlerfall.

Kaufmännische Verwaltung:

- Zugang zu Netzwerk, Geräten, Betriebssystem und Warenwirtschaftssystem ist mehrstufig passwortgeschützt.
- Zugang ausschließlich für die mit der kaufmännischen Verwaltung betrauten Mitarbeiter.

Zugriffskontrolle

- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragsverarbeiter sicher, dass unberechtigte Zugriffe verhindert werden.
- Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Unterauftragnehmers.
- Passwortgeschütztes Warenwirtschaftssystem mit mehreren Berechtigungsstufen.
- Passwortgeschützte Datenbanken und Bürosoftware-Dokumente, z.B. Excel-Tabellen.
- MAC-Adressen gebundene Zugriffsbeschränkungen auf alle Bürosysteme.
- Für übertragene Daten und Software in dem Webspace des Hauptvertrages ist einzig der Verantwortliche in Bezug auf Sicherheit und Updates zuständig.

Datenträgerkontrolle

- Festplatten von Host-Systemen, auf denen sich Kundenkonten befinden, werden nach Stilllegung oder Austausch wegen eines Defekts mit einem vorgeschriebenen Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
- Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum zerstört (geschreddert).

Trennungskontrolle

- Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
- Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

Pseudonymisierung

Für die Pseudonymisierung ist der Verantwortliche verantwortlich

II. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

- Alle Mitarbeiter beim Auftragsverarbeiter und Unterauftragnehmer sind im Sinn des Art. 32 Abs. 4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
- Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.

Eingabekontrolle

Interne Verwaltungssystemen des Auftragsverarbeiters mit öffentlichen Schnittstellen (insbesondere Website und Bestellformular):

- Die Daten werden vom Verantwortlichen selbst eingegeben bzw. erfasst.

Interne Verwaltungssysteme des Auftragsverarbeiters ohne öffentliche Schnittstellen (insbesondere Warenwirtschaftssystem, Abrechnungssystem, Büro-Programme):

- Die Daten werden von Mitarbeitern des Auftragsverarbeiters eingegeben und bearbeitet.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter)
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage
- Dauerhaft aktiver DDoS-Schutz
- Brute-Force-Erkennung und IP-Sperren
- Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages
- Einsatz von Festplattenspiegelung
- Einsatz von Softwarefirewall und Portreglementierungen
- Ständige selbsttätige Überwachung der Server- und Diensteverfügbarkeit durch interne und externe Überwachungssysteme
- Selbsttätige Benachrichtigung verantwortlicher Mitarbeiter im Fehlerfall auf mehreren Kommunikationswegen

Zügige Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

- Bei dem Auftragsverarbeiter: Die Administratoren haben Zugriff auf Datensicherungen, um das System daraus schnellstmöglich wiederherzustellen.
- Beim Unterauftragnehmer: Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).

Auftragskontrolle:

- Alle Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sind vertraut mit den Anweisungen und Richtlinien für die Datenverarbeitung im Auftrag sowie dem Weisungsrecht des Verantwortlichen.
- Der Unterauftragnehmer und Rechenzentrumsbetreiber Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und ein Informationssicherheitsmanagementsystem in die bedeutenden betrieblichen Prozesse eingebunden.