Vertrag zur Auftragsverarbeitung gemäß Art. 28 der Datenschutzgrundverordnung (DSGVO)

zwischen b2 Internetservice, Inhaber Dirk Petermann, Triftweg 2a 15741 Bestensee

- nachfolgend Auftragnehmer genannt -und - nachfolgend Auftraggeber genannt

-1. Gegenstand und Dauer des Auftrags

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

[1a] Die in diesem Dokument enthaltenen Punkte, beziehen sich auch auf folgende Dienstleistungen:

- IT-Office (Arbeiten an IT-Systemen, Einrichtung von Soft- und Hardware)
- PC-Nodienst
- Einweisungen, Erklärungen, Beratungen und Schulungen

(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 und der Administration von Serversystemen 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 Absatz (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 zwischen den Parteien geschlossenen Vertrag konkretisieren die Vertragsparteien mit vorliegendem Auftragsverarbeitungsvertrag die gegenseitigen Pflichten im generellen Umgang mit den Daten des Auftraggebers.

2. Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten

Der Umfang, die Art und der Zweck einer etwaigen Erhebung, Verarbeitung oder Nutzung der Daten ergeben sich aus dem zwischen den Vertragsparteien bestehenden Vertrag. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

3. Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit.c DSGVO)

(1) Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er trifft dabei technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten vor Missbrauch und Verlust, um den Anforderungen der DSGVO zu entsprechen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 Satz 2 lit.c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen.

(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.

4. Berichtigung, Sperrung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den

Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Pflichten des Auftragnehmers

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

- Soweit seitens des Auftragnehmers eine Erhebung, Verarbeitung oder Nutzung der Daten erfolgt, ist dies nur zulässig im Rahmen der vertraglichen Vereinbarungen zwischen Auftraggeber und Auftragnehmer. Soweit der Auftragnehmer Zugriff auf Daten des Auftraggebers hat, verwendet er diese nicht für vertragsfremde Zwecke, insbesondere gibt er diese an Dritte nur weiter, soweit hierzu eine gesetzliche Verpflichtung besteht. Kopien von Daten dürfen nur mit Zustimmung des Auftraggebers erstellt werden. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder Erfüllung vertraglicher oder gesetzlicher Verpflichtungen erforderlich sind.

- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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.

- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechen Art. 28 Abs. 3 Satz 2 lit. c, 32 DSGVO und der Anlage (Technische und organisatorische Maßnahmen nach Art. 32 DSGVO).

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

- 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.

- 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.

- 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.

6. Unterauftragsverhältnisse

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen, insbesondere, aber nicht ausschließlich, für die Bereiche Wartung und Installation der Rechenzentrumsinfrastruktur, Telekommunikationsdienstleistungen und Benutzerservice, verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt.

(2) Der Auftraggeber kann eine aktuelle Liste der eingesetzten Unterauftragnehmer jederzeit beim Auftragnehmer anfordern.

(3) Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Auftragsverarbeitungsvertrag dem Unterauftragnehmer zu übertragen.

7. Pflichten und Kontrollmöglichkeiten des Auftraggebers

(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.

(4) Der Auftraggeber hat das Recht, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

(5) Dem Auftraggeber steht hierzu die durch den Auftragnehmer erstellte, regelmäßig überarbeitete und den gesetzlichen Anforderungen entsprechende Dokumentation über die vorhandenen technischen und organisatorischen Maßnahmen zur Verfügung.

(6) Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach Art. 28 Abs. 1 DSGVO vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass der Auftraggeber sich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann.

(7) Der Auftragnehmer verpflichtet sich, den Auftraggeber auf Anforderung die zur Wahrung seiner bei der Verarbeitung der oben genannten Daten bestehende Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und Nachweise zu führen. Dies gilt auch, soweit der Auftragnehmer die Kontrolle seiner Unterauftragnehmer für den Auftraggeber durchführt.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei von ihm oder der bei ihm beschäftigten Personen begangenen Verstößen gegen Datenschutzvorschriften. Gleiches gilt im Falle schwerwiegender Störungen des Betriebsablaufs oder anderen Unregelmäßigkeiten im Umgang mit Daten des Auftraggebers. Soweit den Auftraggeber Pflichten nach Art. 32 und 33 DSGVO treffen, hat der Auftragnehmer ihn hierbei zu unterstützen. Soweit den Auftraggeber Pflichten nach Art. 32-36 DSGVO

treffen, z.B. im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten durch Dritte, hat der Auftragnehmer ihn hierbei im Rahmen des Charakters der durch den Auftragnehmer erbrachten Dienstleistung zu unterstützen.

9. Weisungsbefugnis des Auftraggebers

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

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Der Auftragnehmer gibt dem Auftraggeber auf Anfrage hin Auskunft zur Natur und dem Zeitpunkt der Löschung.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Sonstige Vereinbarungen

(1) Entgelte Ein Entgelt für diesen Auftrag wird nicht gefordert. Soweit der Auftraggeber Unterstützung nach Ziffer 4 für die Beantwortung von Anfragen Betroffener benötigt, hat er die hierdurch entstehenden Kosten zu erstatten. Soweit der Auftraggeber nach Ziffer 7 Kontrollmöglichkeiten ausüben wird, orientiert sich die vorab zu vereinbarende Höhe des Entgelts an einem festzulegenden Stundensatz des für die Betreuung vom Auftragnehmer
C2 General abgestellten Mitarbeiters. Erteilt der Auftraggeber dem Auftragnehmer Weisungen nach Ziffer 9, so hat er durch diese Weisung entstehende Kosten zu erstatten.

(2) Vertragsdauer Diese Vereinbarung ist abhängig vom Bestand eines Hauptvertragsverhältnisses gemäß Ziffer 1. Die Kündigung oder anderweitige Beendigung des Hauptvertragsverhältnisses gemäß Ziffer 1 beendet gleichzeitig diese Vereinbarung. Das Recht zur isolierten, außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte konkret für die Vereinbarung bleiben hierdurch unberührt.

(3) Rechtswahl Es gilt das Recht der Bundesrepublik Deutschland.

(4)Gerichtsstand Die Parteien vereinbaren als Gerichtsstand den Sitz des für Bestensee zuständigen Gericht

Anlage: Technische und organisatorische Maßnahmen durch notwendige Dritte, die zur Umsetzung des Vertrages notwendig sind

Anlage: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Zutrittskontrolle

- DIN ISO/IEC 27001 zertifiziertes Rechenzentrum:
- elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um den gesamten Datacenterpark
- dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Racks
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen

2. Zugangskontrolle

- Passwort, welches nach erstmaliger Inbetriebnahme nur vom Auftraggeber selbst geändert wird und dem Auftragnehmer nicht bekannt ist
- Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien (z.B. Mindestlänge) erfüllen.

3. Zugriffskontrolle

- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
- Tägliche Datensicherung aller Kundendaten, verschlüsselt auf Backup-Server untergebracht

4. Weitergabekontrolle

- Alle Mitarbeiter sind i.S.d. Art. 32 Abs. 4 DSGVO 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.

5. Eingabekontrolle

- Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst
- Änderungen der Daten werden, sofern technisch möglich, protokolliert.

6. Auftragskontrolle

- Alle Mitarbeiter sind i.S.d. Art. 32 Abs. 4 DSGVO unterwiesen und vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers
- Die AGB enthalten detaillierte Angaben über Art, Umfang und Zweckbindung der personenbezogenen Daten des Auftraggebers.

7. Verfügbarkeitskontrolle

- Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanter Daten je nach gebuchten Leistungen des Hauptauftrages
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter)
- Einsatz von Festplattenspiegelung bei allen relevanten Servern
- Einsatz unterbrechungsfreier Stromversorgung
- Dauerhaft aktiver DDoS-Schutz

8. Trennungsgebot

•Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.

•Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.