VERTRAG ZUR AUFTRAGSVERARBEITUNG GEMÄSS ART. 28 DSGVO

Zwischen der Firma

sprintfish communication gmbh & co. kg
kapellenhof 6A
91207 Lauf an der Pegnitz

– nachfolgend „Auftragnehmer" genannt –

und der Firma

_____

_____

_____

– nachfolgend „Auftraggeber" genannt –

HINWEIS: Dieser Auftragsverarbeitungsvertrag regelt die Verarbeitung der Daten des Auftraggebers durch den Auftragnehmer im Sinne des Art. 28 der EU DatenschutzGrundverordnung (DSGVO) sowie im Sinne des Art. 9 des Schweizerischen Bundesgesetzes über den Datenschutz (DSG).

sprintfish

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

1.1 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).

*1.2 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.*

1.3 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.

1.4 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.

*1.5 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)

2.1 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.

2.2 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.

2.3 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.

2.4 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

2.5 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

2.6 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.

2.7 Der Vertrag beginnt, wenn beide Parteien den Vertrag unterschrieben haben. Die Dauer richtet sich nach Dauer der Dienstleistung zwischen Arbeitgeber und Arbeitnehmer. Eine Mindestdauer besteht nur bei anderweitig geschlossenen Verträgen.

2.8 Bei gravierenden Vertragsverletzungen kann der Vertrag sofort aufgelöst werden.

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

3.1 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.

3.2 Soweit seitens des Auftragnehmers eine Erhebung, Verarbeitung und / oder Nutzung der Daten erfolgt, geschieht dies im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in Drittländern, sofern die besonderen Voraussetzungen der DSGVO eingehalten werden.

3.3 Bei Konkurs des Auftragnehmers werden keine Daten des Auftraggebers in die Hände Dritter fallen.

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

4.1 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!)

-Personenstammdaten
-Kommunikationsdaten (z.B. Telefon, E-Mail)
-Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
-Vertragsabrechnungs- und Zahlungsdaten

4.2 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	

5. Pflichten des Auftragnehmers

5.1 Allgemeine Pflichten Art. 28-33 DSGVO

5.1.1 Der Auftragnehmer (sprintfish communication gmbh & co. kg) ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Der Ansprechpartner beim Auftragnehmer ist Jörg Schmidt, Kapellenhof 6A, 91207 Lauf an der Pegnitz, info(a)sprintfish.de oder telefonisch unter 09123 / 80 90 730 erreichbar.

5.1.2 Soweit seitens des Auftragnehmers eine Erhebung, Verarbeitung und / 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.

5.1.3 Der Auftragnehmer stellt die Wahrung der Vertraulichkeit entsprechend Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO sicher. Alle Personen, die auftragsgemäß auf die unter Punkt 4.1 aufgeführten

Daten des Auftraggebers zugreifen könnten, müssen auf die Vertraulichkeit verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

5.1.4 Der Auftragnehmer stellt die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Art. 32 DSGVO sicher.

5.1.5 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.

5.2 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

5.2.1 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.

5.2.2 Die Parteien sind sich einig, dass die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der Weiterentwicklung unterliegen. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Er muss den Auftraggeber hierüber auf Anfrage informieren und sicherstellen, dass das Sicherheitsniveau der festgelegten Maßnahme nicht unterschritten wird. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 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. Wesentliche Änderungen sind zu dokumentieren.

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

6.1 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. Der Auftragnehmer behält sich vor, gemäß Ziffer 3.2 dieser Vereinbarung Subunternehmer in den dort genannten Regionen einzusetzen.

6.2 Der Auftragnehmer trägt dafür Sorge, dass dem Auftraggeber eine aktuelle Liste der eingesetzten Unterauftragnehmer im Kundenportal, als Anhang zu dieser Vereinbarung oder aus sonstige Weise stets zum Abruf und Einsicht zur Verfügung steht, diese ist fester Bestandteil der vorliegenden Vereinbarung. Der Auftraggeber stimmt dem Einsatz der dort genannten Subunternehmer zu. Bei Änderung dieser Liste in Bezug auf die Hinzuziehung oder Ersetzung von weiteren Subunternehmern ergeht hierüber eine Information an den Auftraggeber. Die Änderungen gelten als vom Auftraggeber akzeptiert, wenn dieser nicht innerhalb von 4 Wochen nach Veröffentlichung widerspricht.

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

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

7.1 Der Auftraggeber ist für die Einhaltung der für ihn einschlägigen datenschutzrechtlichen Regelungen verantwortlich.

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

7.3 Den Auftraggeber treffen die sich aus Art. 24 DSGVO und Art. 13 und 14 DSGVO ergebenden Informationspflichten.

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

8.1 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.

8.2 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.

8.3 Weisungbefugte Personen des Arbeitnehmers sind: Jörg Schmidt, Kapellenhof 6A, 91207 Lauf an der Pegnitz.

9. Kontrollrechte des Auftraggebers

9.1 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.

9.2. Dem Auftraggeber steht hierzu die durch den Datenschutzbeauftragten des Auftragnehmers erstellte, regelmäßig überarbeitete und den gesetzlichen Anforderungen entsprechende Dokumentation über die vorhandenen technischen und organisatorischen Maßnahmen zur Verfügung.

9.3. Der Auftraggeber hat das Recht, die Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, nach rechtzeitiger vorheriger Anmeldung (3 Wochen) zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in seinem Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem

Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Kosten, die dem Auftragnehmer durch seine Unterstützungshandlung entstehen, sind ihm im angemessenen Umfang zu erstatten.

9.4 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.

9.5 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.

9.6 Der Auftragnehmer verpflichet, sich auch nach Vertragsende, die Geheimhaltungspflicht zu wahren.

10. Haftung

Der Auftragnehmer haftet nur für Schäden, die durch die Verarbeitung verursacht wurden, in Bezug auf welche der Auftraggeber (1) den Pflichten nach der DSGVO, die sich speziell auf die Auftragsverarbeiter beziehen, nicht nachgekommen ist oder (2) den rechtmäßigen schriftlichen Weisungen des Kunden zuwider gehandelt hat. In diesen Fällen gilt die in der Vereinbarung enthaltene Haftungsregelung.

Wenn der Auftragnehmer und der Auftraggeber an einer Verarbeitung gemäß dieser Vereinbarung beteiligt sind, die bei der betroffenen Person Schaden verursacht hat, übernimmt der Auftraggeber beim ersten Mal die volle Entschädigung (oder einen anderen Ausgleich), die der betroffenen Person zusteht, und beim zweiten Mal, fordert der Auftraggeber vom Auftragnehmer den Teil der Entschädigung der betroffenen Person, der der Verantwortung vom Auftragnehmer für den Schaden entspricht, zurück, vorausgesetzt, dass jede in der Vereinbarung enthaltene Haftungsbeschränkung Anwendung findet.
Bei Vertragsverstößen erfolgt die Haftung nach Art. 82 DSGVO.

11. Salvatorische Klausel, Gerichtsstand

11.1 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.

11.2 Als Gerichtsstand wird Hersbruck vereinbart.

_____ *, den* _____

_____
Auftraggeber

Auftragnehmer sprintfish communication gmbh & co. kg

_____ *, den* _____ ***(Vertragsbeginn)***

_____
Auftragnehmer

Anlage: Technische und organisatorische Maßnahmen, Liste der Subunternehmer

DOKUMENTATION DER TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN

gem. Anlage zu Art. 32 DSGVO

V 1.4

Host Europe GmbH

c/o WeWork

Friesenplatz 4

50672 Köln

1. Präambel

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, treffen der Auftraggeber und der Auftragnehmer die nachfolgenden technischen und organisatorischen Maßnahmen (TOM). Diese gelten für die im Hauptvertrag definierten IT-Leistungen, welche in den unter Ziffer 2 definierten Rechenzentren erbracht werden.

Bei der Auswahl der Maßnahmen wurden die vier Schutzziele des Art. 32 Abs. 1 b) DSGVO, namentlich die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, berücksichtigt. Eine rasche Wiederherstellung nach einem physischen oder technischen Zwischenfall ist gewährleistet. Alle technischen und organisatorischen Maßnahmen werden regelmäßig gemäß Art. 32 Abs. 1 d) DSGVO auf ihre Wirksamkeit hin geprüft.

Generell gilt es folgendes zu beachten:

Die Host Europe GmbH 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. Host Europe 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. Host Europe hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

2. Fähigkeit der Vertraulichkeit

Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.

Maßnahmen
Festgelegte Sicherheitsbereiche
Individuelle Zutrittsberechtigungsvergabe
Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den Zutritt zum jeweiligen Data Center nur für autorisierte Personen
Dokumentationen von Zutrittsberechtigungen
Zutrittsdokumentation
Autorisiertes Wachpersonal[1] - Während der Geschäftszeiten - 24/7 - Sichtkontrollen
Rollenabhängige Zutrittsregelungen für die Mitarbeiter (Administratoren, Hilfskräfte, Reinigungspersonal, etc.)
Besucher-Regulierungen
Regelmäßige Kontrollgänge durch das Sicherheitspersonal außerhalb des RZ-Bereiches
Automatisches Zuziehen und Verschließen von Türen
Schließung aller Gebäudeeingänge, wie Fenster und Türen
Zusätzliche mechanische Schutzmaßnahmen für das Erdgeschoss
Büroräume außerhalb der Arbeitszeit sind verschlossen
Schutz und Beschränkung der Zutrittswege
Transponder- oder schlüsselkartenbasierte Schließanlage
Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes
Alarmmeldungen können von vor Ort befindlichem Personal eingesehen werden
Eingezäuntes Gelände inkl. Videoüberwachung
Zutrittskontrollsystem mit Zutrittskarten
Zusätzliche Zugangsbeschränkung der Serverräume

[1] Nicht RZ Köln (CGN1)

Maßnahmen
Änderung der Standardkennwörter aller System- und Infrastrukturkomponenten
Protokollierung von Benutzer relevanten Aktivitäten (Anmeldung, Abmeldung, Zugangsverweigerungen, etc.)
Demilitarisierte Zonen
Schutz der Infrastruktur durch Alarmmeldungen an Fenstern und Türen
Zugangsbeschränkungen für bestimmte IP-Adressbereiche
VPN-Beschränkungen
Sperrung von nicht erforderlichen Ports
Externer Zugang nur über sichere Verbindungen (VPN, RDP oder vergleichbar)
W-LAN-Verschlüsselung
Regelmäßige Software-Updates
Benutzerauthentifizierung für Systemzugang- und/oder Anwendungszugriff erforderlich
Einschränkung der zeitlichen Gültigkeit der Benutzerkonten
Automatische Deaktivierung von Benutzern nach mehreren fehlgeschlagenen Logins
Zwangs- oder Pflicht-Änderung der Kennwörter nach der ersten Anmeldung
Ablauf von Benutzerpasswörtern
Erforderliche Mindestkomplexität für Kennwörter
Passwort-Historie zur Verhinderung der Mehrfachnutzung desselben Passwortes
Angemessene Gestaltung der Benutzeraccount-Wiederherstellung im Falle eines verlorenen oder vergessenen Authentifizierungsdatensatzes
Verschlüsselte Speicherung von User-Passwörtern
User-Login-Verlauf
Vernichtung von physikalischen Medien nach DIN 66399
Nutzung eines Aktenvernichters (gem. DIN 66399)

3. Fähigkeit der Integrität (Gilt für alle RZ-Standorte)

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.

Maßnahmen
Rollenbasiertes Berechtigungskonzept (Lesen / Schreiben / Ändern / Kopieren / Löschen)
Dokumentation der Vergabe von Zugriffsrechten
Strenge administrative Aufgabentrennung
Protokollierung von externen Support-Prozessen
Dokumentation der Weitergabe von physischen Speichermedien
Logische Datentrennung: Separate Datenbanken oder strukturierte Dateiablage
Separate Instanzen für Entwicklungs- und Produktivsysteme (Sandboxes)
Spezifische Genehmigungsregelung für die Datenbank und den Anwendungszugriff / Berechtigungskonzept

4. Fähigkeit der Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Maßnahmen
Schutz der Infrastruktur durch Hardware-Firewalls
Software-Firewall
Antivirus-Software
Überwachung und Protokollierung von administrativen Systemzugang und von Konfigurationsänderungen
Kontrollierter Zugang zu E-Mails und Internet
Trennung von Anwendungs- und Administrationszugängen
Überwachung und Protokollierung allgemeiner Benutzeraktivität
Protokollierung von externen Support-Prozessen
Protokollierung von administrativen Änderungen

Maßnahmen
Zugriffsregelungen und Zugriffsverwaltung
Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag
Unterbrechungsfreie-Stromversorgung (USV)
Feuer und/oder Rauchmelder verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr bzw. bei lokalem Sicherheitspersonal
Kühlsystem im Rechenzentrum / Serverraum
Automatische Brandlöschanlage
Disaster-Recovery-Mechanismen für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust
Tägliche inkrementelle Datensicherung
Wöchentliche vollständige Datensicherung
Wöchentliche Backups auf separat gespeicherten physischen Medien oder auf physikalisch getrennten Systemen
Der Kraftstoffvorrat ist für mindestens 16 Stunden bei Volllast ausreichend. Eine Auftankung ist während des laufenden Betriebs des Generators möglich
Geräte zur Überwachung der Temperatur und Feuchtigkeit in den Data Centern
Notfallplan
Externe Audits und Sicherheitstests
Klar definierte Verwaltungsaufgaben für Auftraggeber und Auftragnehmer

5. Verfahren zur regelmäßigen Überprüfung (Gilt für alle RZ-Standorte)

Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?

Maßnahmen
Regelmäßige Überprüfung der Systemzugangsberechtigungen
Interne- und externe Audits
Disziplinarmaßnahmen im Falle einer Datenschutzverletzung
Regelmäßige Sicherheitsprüfungen

Maßnahmen
Regelmäßige Kontrolle externer Dienstleister
Regelmäßige Besprechungen mit den bestellten Datenschutzbeauftragten in Bezug auf Betriebsprozesse, welche die Verarbeitung von personenbezogenen Daten betreffen

6. Schutz vor unrechtmäßigem Zugang zu personenbezogenen Daten (Gilt für alle RZ-Standorte)

Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?

Maßnahmen
Kontrollierter Zugang zu E-Mails und Internet
Trennung von Anwendungs- und Administrationszugängen
Regelmäßige Sicherheits-Updates
Überwachung und Protokollierung allgemeiner Benutzeraktivität
Verbot der Nutzung von privaten Datenträgern
Rollenabhängige Zugriffsbeschränkungen
Applikationsbasierte Überprüfung der Eingabeberechtigung

7. Verarbeitung personenbezogener Daten nur nach Anweisung (Gilt für alle RZ-Standorte)

Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?

Maßnahmen
Vertraulichkeitserinnerungen
Schriftliche Verpflichtung aller Mitarbeiter auf die Wahrung der Vertraulichkeit
Regelmäßige Datenschutz-Unterweisung der Mitarbeiter
Geregeltes Löschen / Entsorgen von Datenträgern wie Festplatten, CDs, DVDs, USB-Sticks
Datentransfer und -weitergabe in Übereinstimmung mit den Anweisungen des Auftraggebers
Schriftliche Richtlinien für die Datenübertragung und -weitergabe
Verbindliche Regeln für die Offenlegung von sensiblen Daten

Maßnahmen
Datenschutzkonforme Löschung aller Datenkopien und Datensicherungen nach Abschluss des Auftrags
Verarbeitung personenbezogener Daten erfolgt ausschließlich entsprechend den Weisungen des Auftraggebers
Festgelegte Ansprechpartner für Änderungsanfragen
Kontrollrechte der Auftraggeber bei der Auftragsdatenverarbeitung
Subunternehmer werden auf die gleichen Regelungen und Bestimmungen verpflichtet wie Host Europe selbst

8. Anonymisierung / Pseudonymisierung / Verschlüsselung

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

9. Belastbarkeit der Systeme

Host Europe unternimmt die unter Ziffer 4 dargestellten Maßnahmen, um eine Belastbarkeit der IT-Systeme sicherzustellen. Penetrationstests der IT-Systeme des Auftraggebers sind grundsätzlich nicht Gegenstand der von Host Europe zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.

Annex 1:
“Subunternehmerliste”

Wir nutzen die folgenden externen Dienstleister für die Vertragserfüllung:

Name des Unternehmens	Land der Eintragung	Beschreibung der Verarbeitung	Verarbeitete Kategorien
Acronis International GmbH	Schweiz	Kunden Back-Ups.	Backup-Snapshots.
Amazon Web Services	Vereinigte Staaten	Anbieter von Cloud-Rechenzentren und Netzwerken. Dienstleister für Infrastrukturplattformen, Produkte und Servicebereitstellungen.	Produktinhalte und Kundenkontoinformationen, die für die Bereitstellung von Produkten und Dienstleistungen benötigt werden.
Arbor Networks, ARBOR Technology Company Ltd	Vereinigte Staaten	Überwacht den Netzwerkverkehr und stellt Informationen für Forensik und DDoS-Erkennung/Abschwächung bereit.	IP-Adressen, Zeitstempel, Netzwerkverkehr, Ports und Protokolle.
Audriga GmbH	Deutschland	Migrationsservice für gehostete E-Mail- und Groupware-Lösungen.	Alle Kundenkontoinformationen, die für die Bereitstellung benötigt werden, sowie E-Mail-Daten.
Automattic Inc	Vereinigte Staaten	WooCommerce Plugin und Addons innerhalb von Ecommerce WordPress.	WordPress-Benutzerprofile von Kunden (einschließlich des Name und der E-Mail-Adresse) und Mitarbeitern/Auftragnehmern.
Basekit Platform Ltd	Vereinigtes Königreich	Website Builder für Kunden.	Alle Kundenkonto-Informationen, die für eine WebsiteBuilder-Website benötigt werden, sowie alle Kundendaten, die auf einer gehosteten Website gespeichert sind.
Cisco International Limited, Cisco Solutions GmbH, Cisco Systems Inc	Vereinigtes Königreich, Deutschland	Bereitstellung und Verwaltung von Netzwerklösungen als Teil unseres Netzwerks.	Verarbeitet Metadaten von IP-Adressen, Timestamps und Netzwerkverkehr.
Cloudflare Inc	Vereinigte Staaten	CDN (Content Delivery Network), WAF (Web Application Firewall) and SSL (Secure Sockets Layer) für Managed Wordpress.	Website Traffic Inspektion. Metadaten von IP-Adressen, Zeitstempel und Netzwerkverkehr.
Cloudmark Inc	Vereinigte Staaten	E-Mail Anti-Spam Schutz, ansässig in den Niederlanden.	Endanwender E-Mail Header und Inhalt.
cPanel Inc	Vereinigte Staaten	cPanel Control Panel für VPS und Dedicated Servers.	Alle Kundendaten, die im Control Panel bearbeitet werden.
Epages GmbH	Deutschland	Hosted E-Commerce Software für Kunden.	Alle Kundenkonto-Informationen.

Equinix Netherlands BV	Niederlande	Rechenzentrums-Colocation-Einrichtungen.	Eine Verarbeitung von persönlichen Daten ist nicht vorgesehen.
GlobalSign GMO Internet Group	Vereinigtes Königreich	SSL-Zertifikate.	Alle Kundendaten, die für ein SSL-Zertifikat notwendig sind.
Juniper Networks Inc	Vereinigte Staaten	Bereitstellung und Verwaltung von Netzwerklösungen als Teil unseres Netzwerks.	Verarbeitet Metadaten von IP-Adressen, Timestamps und Netzwerkverkehr.
LivePerson Inc	Vereinigte Staaten	Live-Chat zu Support-Zwecken.	Chat-Abschriften, automatisierte Informationen wie IP-Adresse, Betriebssystem und Art des Geräts.
LvivIT	Ukraine	Bereitstellung von operativer Plattformunterstützung.	Produktinhalte und Kundenkontoinformationen, die für die Bereitstellung von Produkten und Dienstleistungen benötigt werden.
Microsoft Corporation	Vereinigte Staaten	Hosted Exchange Mailboxen und Groupware-Lösungen für Kunden.	Kundenkontodaten und E-Mail-Adressen.
Open-Xchange AG	Deutschland	Software- und Hosting-Anbieter für E-Mail-Produkte.	Alle Inhalte, Logdateien und Anwendungsdaten für die Bereitstellung und den Support des Produkts.
OVH Groupe SAS	Frankreich	Rechenzentrums-Colocation-Einrichtungen in Deutschland, Wiederverkauf von Server-Produkten.	Vom Kunden gehostete Daten, einschließlich, aber nicht beschränkt auf Websites, Anwendungen und Daten von Kunden des Kunden. Dazu kann auch Netzwerkverkehr gehören.
Plesk International GmbH	Deutschland	Plesk Control Panel für VPS und Dedicated Server und Website Builder Plus.	Alle Kundendaten, die sich im Plesk Control Panel befinden, sowie Kundendaten, die auf einer gehosteten Webseite gespeichert sind.
SiteLock LLC	Vereinigte Staaten	Sichern der Kundenwebseiten vor Schadsoftware.	Alle Kontoinformationen, die für die Bereitstellung der Webseite benötigt werden, sowie Kundendaten, die auf der gehosteten Webseite gespeichert sind.
Teamviewer GmbH	Deutschland	Fernwartung des Kunden-Desktop zu Support-Zwecken.	Hostname und IP-Adresse des Kundencomputers. Es werden keine privaten Daten gesammelt.
Virtuozzo International GmbH	Schweiz	Software für Containerisierungs-Plattform.	Alle Kundendaten, die in einem Container gespeichert sind.

Darüber hinaus können personenbezogene Daten insbesondere zur Vertragserfüllung an verbundene Unternehmen der GoDaddy-Gruppe weitergegeben werden:

Name des Unternehmens	Land der Eintragung	Beschreibung der Verarbeitung	Verarbeitete Kategorien
123 Reg Ltd	Vereinigtes Königreich	Bereitstellung eines E-Mail-Marketingtools, das von unseren Teams genutzt wird.	Kundenkontodaten, E-Mail-Adresse.
Datadock SARL	Frankreich	Rechenzentrums-Colocation-Einrichtungen.	Eine Verarbeitung von persönlichen Daten ist nicht vorgesehen.
GoDaddy Media Temple Inc d/b/a Sucuri	Vereinigte Staaten	SAAS Produkt: Schutz der Kundenwebseiten vor Schadsoftware.	Alle Kontoinformationen, die für die Bereitstellung der Webseite benötigt werden, sowie Kundendaten, die auf der gehosteten Webseite gespeichert sind.
GoDaddy Media Temple Inc d/b/a Sucuri	Vereinigte Staaten	Web Application Firewall auf Websites und in Kunden-Control-Panels zum Schutz der IT und von Kundendaten.	Website Traffic Inspektion. Metadaten von IP-Adressen, Zeitstempel und Netzwerkverkehr.
GoDaddy Operating Company LLC	Vereinigte Staaten	Dienstleister für interne Plattformen und Rechenzentren. Ausgewählte Produkte und Dienstleistungen werden aus den Niederlanden, Singapur und den USA unterstützt. (z. B. Hosting- und Serverprodukte, E-Mail, Authentifizierung, CRM, Netzwerk- und DNS-Dienste).	Produktinhalte und Kundenkontoinformationen, die für die Bereitstellung von Produkten und Dienstleistungen benötigt werden.
Mesh Digital Ltd	Vereinigtes Königreich	Domain Registrierungsdienste.	Alle Kontoinformationen, die für die Bereitstellung der Domain notwendig sind.
Starfield Technologies LLC	Vereinigte Staaten	SSL-Zertifikate.	Alle Kundendaten, die für ein SSL-Zertifikat notwendig sind.

UNTERAUFTRAGSVERARBEITER, DIE AN DER VERARBEITUNG PERSONENBEZOGENER DATEN DURCH OVH AUF WEISUNG DES KUNDEN BETEILIGT SIND

Im Rahmen der Erbringung der Dienstleistungen setzt OVH Unterauftragsverarbeiter ein, die sich an den von OVH auf Weisung des Kunden durchgeführten Verarbeitungen beteiligen können. Diese Unterauftragsverarbeiter können **(A)** Verbundene Unternehmen von OVH und **(B)** Nicht-Verbundene Unternehmen von OVH sein.

A. Verbundene Unternehmen von OVH

Name des Verbundenen Unternehmens	Standort des Verbundenen Unternehmens	Dienstleistungen, die von dem Verbundenen Unternehmen erbracht werden können
OVH Hispano	Spanien	Sämtliche Dienstleistungen (ungeachtet des Standorts des Rechenzentrums, wo sich die Dienstleistung befindet)
OVH SRL	Italien	
OVH GmbH	Deutschland	
OVH Hosting Limited	Irland	
OVH Hebergement INC	Kanada	
OVH Sp. Zo.o.	Polen	
OVH Hosting Sistemas informaticos unipessoal	Portugal	
OVH BV	Niederlande	
OVH SAS	Frankreich	
OVH Limited	Vereinigstes Königreich	
OVH Singapore PTE Ltd	Singapur	Dienstleistungen, (i) die im Rechenzentrum / in Rechenzentren im asiatisch-pazifischen Raum gehostet werden, oder (ii) für die die anwendbaren Besonderen Geschäftsbedingungen vorsehen, dass diese Verbundenen Unternehmen von OVH an der Erbringung solcher Dienstleistungen teilnehmen können.
OVH Australia PTY Ltd	Australien	
OVH Tech R&D Private Limited	Indien	
DCD Data Center Deutschland GmbH	Deutschland	Wartung des entsprechenden Rechenzentrums
Data Center Ozarow spółka z ograniczoną odpowiedzialnością	Polen	
Data Center Erith Ltd	Vereinigstes Königreich	
Altimat Data Center Singapore PTE. Ltd	Singapur	
Data Center Sydney PTY Ltd	Australien	

B. Nicht-Verbundene Unternehmen von OVH

Wenn OVH im Rahmen der Erbringung einer Dienstleistung Nicht-Verbundene Unternehmen von OVH einsetzt, die sich an den von OVH auf Weisung des Kunden durchgeführten Verarbeitungen beteiligen können, ist dies in den jeweils gültigen Besonderen Dienstleistungsbedingungen festgelegt.