Vertrag über die Auftragsverarbeitung personenbezogener Daten

Stand 06/2018

zwischen

Firmenname inkl. Rechtsform:	
Straße:	
PLZ:	Ort:

- Auftraggeber -

und der

bluechip Computer AG
Geschwister-Scholl-Str. 11a
04610 Meuselwitz

- Auftragnehmer -

1. Einleitung, Geltungsbereich, Definitionen

1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien" genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
2. Bei etwaigen Widersprüchen zu anderen vertraglichen Vereinbarungen der Parteien, insbesondere denjenigen des Hauptvertrages, gehen die Regelungen dieser Vereinbarung zum Datenschutz den sonstigen zwischen den Parteien getroffenen Vereinbarungen vor.
3. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.
4. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung (DSGVO) zu verstehen. Soweit Erklärungen im Folgenden „schriftlich" zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst die Bereitstellung, Missbrauchskontrolle und Abrechnung der folgenden Dienste:

- Cloud Services (Iaas/SaaS/Storage)
- Hosting
- Housing

2.2 Dauer

1. Die Verarbeitung beginnt am _____ und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrages oder des Hauptvertrages durch eine Partei.
2. Der Vertrag ist mit einer Frist von drei Monaten zum Quartalsende kündbar.
3. Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

3. Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

3.1 Art und Zweck der Verarbeitung

In Abhängigkeit des gebuchten Dienstes, ist die Verarbeitung folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung, Bereitstellung, Abgleich, Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten

Der Zweck der Datenverarbeitung richtet sich nach dem gebuchten Dienst. Welche Zwecke mit dem entsprechenden Dienst verfolgt werden, kann aus Anlage 2 entnommen werden.

3.2 Art der Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Bestandsdaten – Begründung der Einzel- und Gesamtvertragsverhältnisse
- Nutzungsdaten – zur Abrechnung der Nutzung der Produkte und Dienste
- Verbindungsdaten – zur Erkennung und Abwehr von Störungen der Infrastruktur und des Missbrauchs der Dienste
- Inhaltsdaten – zum Sicherstellen der Funktion der Produkte und Dienste

3.3 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Auftraggeber samt Mitarbeiter
- Auftragnehmer samt Mitarbeiter
- Kunden des Auftraggebers

4. Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
2. Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
3. Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.
4. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
5. Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.
6. Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.
7. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistung im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.
8. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.
9. Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden.

Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit. Die Kontaktdaten des Datenschutzbeauftragten sind stets unter *https://www.bluechip.de/datenschutz* einsehbar.

10. Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers ist nur mit Zustimmung des Auftraggebers zulässig. Die Verarbeitung von Daten im Sinne dieses Vertrages erfolgt grundsätzlich auf Servern der bluechip Computer AG, die im Rahmen eines Colocation-Vertrages in den Rechenzentren der Hetzner Online GmbH stationiert sind.
11. Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.
12. Ist der Auftragnehmer nicht in der Europäischen Union niedergelassen, bestellt er einen verantwortlichen Ansprechpartner in der Europäischen Union gem. Art. 27 Datenschutz-Grundverordnung. Die Kontaktdaten des Ansprechpartners sowie sämtliche Änderungen in der Person des Ansprechpartners sind dem Auftraggeber unverzüglich mitzuteilen.

5. Technische und organisatorische Maßnahmen

1. Die in Anlage 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.
2. Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Die zur Aufrechterhaltung der Informationssicherheit erforderlichen Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.
3. Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es im Verantwortungsbereich des Auftragnehmers Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer dem Auftraggeber darüber informieren. Für die technischen und organisatorischen Maßnahmen des Auftraggebers gegenüber dessen Kunden trägt der Auftragnehmer keine Verantwortung.
4. Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten organisatorisch von sonstigen Datenbeständen strikt getrennt werden.
5. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
6. Die Verarbeitung von Daten in Privatwohnungen ist nur im Zuge der Homeoffice-Tätigkeiten der weisungsempfangsberechtigten Personen gemäß Kapitel 10 (3) dieses Vertrages gestattet. Die Verarbeitung von Daten in Privatwohnungen, deren Umfang über das für Homeoffice-Tätigkeiten erforderliche Maß hinausgeht, ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit eine Verarbeitung in Privatwohnungen erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.
7. Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.
8. Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber spätestens alle 12 Monate unaufgefordert und sonst jederzeit auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

6. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

1. Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
2. Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.
3. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Löschung oder Sperrung seiner Daten wenden sollte, wird der Auftragnehmer den Auftraggeber unverzüglich hiervon benachrichtigen.

7. Unterauftragsverhältnisse

1. Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.
2. Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die mit denen in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.
3. Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmen durchzuführen oder durch Dritte durchführen zu lassen.
4. Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.
5. Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.
6. Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation auf Anfrage zu übermitteln.
7. Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Kapitel 4 (10) und (11) dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.
8. Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber auf Anfrage zu übermitteln.
9. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.
10. Der Auftragnehmer wird alle bestehenden Unterauftragsverhältnisse, die zur Bereitstellung der Infrastruktur im Rahmen dieser Vereinbarung unerlässlich sind, angeben. Eine stets aktuelle Liste aller Unterauftragsverhältnisse ist im bluechip Cloud Kundencenter einsehbar.
11. Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8. Rechte und Pflichten des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.
3. Regelungen über etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.
4. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.
5. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.
6. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9. Mitteilungspflichten

1. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
    a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl

der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

2. Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
3. Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
4. Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10. Weisungen

1. Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
2. Der Auftraggeber benennt die zur Erteilung von Weisungen ausschließlich befugten Personen in elektronischer Form durch Vergabe von entsprechenden Rechten im bluechip Cloud Kundencenter.
3. Der Auftragnehmer benennt dem Auftraggeber die Personen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Eine stets aktuelle Liste von weisungsempfangsberechtigten Personen des Auftragnehmers ist im bluechip Cloud Kundencenter einsehbar.
4. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
5. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
6. Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11. Beendigung des Auftrags

1. Bei Beendigung des Auftragsverhältnisses oder eines unter diesen Vertrag fallenden Einzelvertrages (je nachdem welches Ereignis früher eintritt) oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder an den Auftraggeber zu übergeben oder mit einer Frist von drei Monaten zu vernichten. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.
2. Der Auftragnehmer ist verpflichtet, die Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.
3. Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber auf Anforderung vorzulegen.
4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12. Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

13. Haftung

1. Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

14. Sonderkündigungsrecht

1. Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung"), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will, oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.
2. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
3. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

15. Sonstiges

1. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln. Keine Partei ist berechtigt, die erlangten Kenntnisse ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Informationen Dritten zugänglich zu machen.
2. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.
3. Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.
4. Für Nebenabreden ist die Schriftform erforderlich.
5. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
6. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge von Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.
7. An Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame oder durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahe kommt. Gleiches gilt bei Vertragslücken.
8. Diese Vereinbarung beruht auf den ab 25.05.2018 geltenden Regelungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzrichtlinie). Die Vertragsparteien sind sich einig, dass bis zur Geltung der Datenschutzgrundverordnung die entsprechenden Regelungen des Bundesdatenschutzgesetzes in der Fassung der Bekanntmachung vom 14.01.2003 (Bundesgesetzblatt 1 Seite 66) anstelle der hier in Bezug genommen Regelungen der DSGVO entsprechend gelten sollen.
9. Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftraggebers.

Ort, Datum, Unterschrift – Auftraggeber

Ort, Datum, Unterschrift – Auftragnehmer

Vertrag über die Auftragsverarbeitung personenbezogener Daten

Stand 06/2018

Anlage 1 – Technische und organisatorische Maßnahmen

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

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Das Gelände des Rechenzentrumsbetreibers ist eingezäunt und wird rund um die Uhr videoüberwacht. Es existiert zudem eine Alarmanlage samt Wachschutz. Der Zutritt auf das Gelände des Rechenzentrums erfolgt mit Hilfe eines physikalischen Tokens. Die Tore lassen entsprechend mit einem Lichtschrankensystem Fahrzeuge nur vereinzelt nach einer erfolgreichen Authentifizierung durch. Das Token wird durch die bluechip Computer AG verwaltet und befindet sich räumlich getrennt vom Rechenzentrum. Die Herausgabe des Tokens an definierte Mitarbeiter der bluechip Computer AG mit Zutrittsberechtigung wird strengstens protokolliert. Der Zutritt zum Rechenzentrum wird videoüberwacht und protokolliert. Es werden zudem die Bilder der Videoüberwachung beim Betreten des Rechenzentrums an ausgewählte Mitarbeiter der bluechip Computer AG als Mitteilung gesendet. Bei einem begründeten Verdacht besteht die Möglichkeit, die Videoaufzeichnungen des gesamten Aufenthaltes zu sichten und auszuwerten. Der Zutritt zu den 19“ Schränken der bluechip Cloud Services erfolgt zudem mit einem separaten Schlüssel pro Rack.

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Alle Hosting- und Software-as-a-Service-Server sowie die Infrastructure as a Service-Hosts besitzen keinen direkten administrativen Zugang aus Kundennetzwerken oder aus dem Internet. Definierte Administratoren der bluechip Cloud Services erhalten ausschließlich Zugriff auf diese Systeme über sogenannte speziell abgeschottete Jump Server, die ausschließlich per VPN erreichbar sind. Alle Server, die von bluechip verwaltet werden, wurden zudem besonders unter dem Sicherheitsaspekt gehärtet. Die Zugänge sind gesichert und haben hohe Anforderungen an die Passwortlänge und -kompläxität. Hosting- und SaaS-Dienste sowie die einzelnen Virtual Private Server werden dabei von redundanten, virtuellen Firewalls gesichert, die über separate VLANs mit dem Internet kommunizieren. Hierbei erlaubt die bluechip Computer AG nur die Verwendung von bestimmten Ports und überwacht die Firewalls ständig. Im Bereich Virtual Private Cloud bieten die bluechip Cloud Services dem Partner/Kunden die Verwendung eigener Firewalls zur Sicherung der eigenen virtuellen Infrastruktur. Hierbei haben die bluechip Mitarbeiter keinen administrativen Zugang zu den Firewalls des Kunden. Die bluechip weist zudem ausdrücklich darauf hin, dass der Datenschutz für Übertragungen in offenen Netzwerken, wie dem Internet, nach dem derzeitige Stand der Technik, nicht umfassend gewährleistet werden kann. Für die Sicherheit der im Internet übertragenen sowie bei der bluechip Cloud Services gespeicherten Daten ist der Partner/Kunden vollumfänglich verantwortlich. Der Partner/Kunde weiß, dass ausgewählte Mitarbeiter der bluechip Computer AG oder Ihrer eventuell bestellter Subunternehmer im Rahmen von Wartung und Administration der Infrastruktur, in Support-Fällen oder bei Beseitigungen von Störungen technisch gesehen die Möglichkeit besitzen, die gemieteten Dienste sowie eventuell die dort abgelegten Daten einsehen zu können. Andere Teilnehmer im Internet sind unter Umständen technisch in der Lage in die Netzsicherheit einzugreifen und so Zugriff auf bestimmte Daten zu erhalten oder den Nachrichtenverkehr zu kontrollieren. Aus diesem Grund ist es auch für Partner/Kunden umso wichtiger, entsprechende Zugangspunkte (egal ob in der bluechip Cloud oder im lokalen Netzwerk) abzusichern, starke Passwörter zu verwenden sowie jeden Verdacht auf Missbrauch in jeglicher Form der bluechip Computer AG unverzüglich anzuzeigen.

Im Bereich der E-Mail-Dienste, die durch bluechip verwaltet werden, kommt zudem ein separates Cluster aus Antispam- und Antivirus Gateways zum Einsatz. Hierbei übernimmt bluechip nicht die Verantwortung dafür, dass alle Viren und Spam-Nachrichten erfolgreich erkannt werden. Die Regeln werden zwar mehrmals täglich aktualisiert, allerdings besteht aus technischer Sicht die Möglichkeit, entsprechende Viren zu verschleiern und erst auf Kundenseite auszuführen. Beim Einsatz einer automatisierten Antispam- und Antivirus-Lösung kommt es auch manchmal vor, dass E-Mails, die keine Viren oder keinen Spam enthalten von den Gateways abgewiesen werden. Hierbei bieten die bluechip Cloud Services dem Partner/Kunden an, die eigenen Whitelisten selbst zu verwalten, um die Erkennung in einem solchen Falle zu vermeiden.

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.

Es liegt ein anwenderbezogenes Konzept der Berechtigungen der jeweiligen Dienste vor, welches im administrativen Bereich auf Basis eines Active Directory umgesetzt wurde und dort entsprechend schriftlich dokumentiert ist. Anwender, die für die Bestellabwicklung, Erfassung und Änderung der laufenden Aufträge sowie der dazugehörigen Kundendaten, sowie für die Abwicklung und Beantwortung der Tickets und dazugehörigen E-Mails zuständig sind, werden separat in einer Datenbank verwaltet und besitzen entsprechend Ihrer Tätigkeit abgestuften Berechtigungsprofile. Sämtliche Zugriffe der Benutzer werden protokolliert. Da die verschiedenen Netzwerke physikalisch voneinander getrennt sind, erhalten die Anwender ohne administrative Berechtigungen keinen Zugriff auf das Management-Netzwerk, auf das Hardware-Management sowie auf die administrativen Konsolen der Infrastruktur. Kundenpasswörter in allen Bereichen werden in verschlüsselter Form gespeichert und liegen den Mitarbeitern der bluechip Cloud Services sowie Ihrer eventuell beauftragter Subunternehmer niemals im Klartext vor.

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Das Trennungsgebot wird mit Hilfe von VLANs in der gesamten Infrastruktur der bluechip Cloud Services umgesetzt. Zudem existieren mehrere voneinander physikalische getrennte Netzwerke, die speziell zu dem jeweiligen Zweck über separate Netzwerk-Komponenten und separate Verkabelung realisiert wurden. Softwareseitig existiert eine logische Mandantentrennung beim Einsatz von Hosting und SaaS-Dienste. Bei IaaS-Diensten (speziell bei Virtual Private Cloud) wird die Trennung der einzelnen Kunden-Netzwerke über VLANs vorgenommen.

II. Integrität gem. Art. 32 Abs. 1 lit. b DSGVO

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.

Die verschiedenen Netzwerke sind durch VLANs voneinander getrennt. Im Bereich Virtual Private Cloud wird jedem Kunden ein eigenes VLAN zugeordnet. Eine Doppeltvergabe ist ausgeschlossen. Die Zuteilung von öffentlichen IP-Adressen verwaltet der Partner/Kunde selbst im Admin-Portal, je nach Kontingent. Die Pflege der VLANs und öffentlichen IPs erfolgt durch die Mitarbeiter der bluechip Cloud Services. Alle Angebote im Bereich Hosting, SaaS und Virtual Private Server werden hierbei von Firewalls durch unbefugten Zugriff gesichert. Bei der optionalen Migrationsunterstützung in oder aus der bluechip Cloud werden etwaige Datenträger nach Absprache mit dem Partner/Kunden ausschließlich durch sorgfältig ausgewähltes Personal behandelt und entsprechend vor Weitergabe geschützt. bluechip empfiehlt dabei beim Transport der Datenträger eine Verschlüsselung einzusetzen und den Schlüssel zur Entschlüsselung auf einem anderen Wege zu übertragen.

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.

Die Einwahl in das Management-Netzwerk sowie Konfigurationsänderungen wird protokolliert. Die Änderungen an den Aufträgen und den Partner-/Kundendiensten werden separat protokolliert und gespeichert. Dafür werden die von den Softwareherstellern zur Verfügung gestellten Log- und Transaktionsprotokolle zur Gewährleistung der Eingabekontrolle benutzt. Änderungen an den Inhaltsdaten des Kunden werden nicht protokolliert.

III. Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs. 1 lit. b DSGVO

1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die Bereitstellung der bluechip Cloud Services setzt auf ein durchgängig redun-

dantes Konzept für alle Dienste. Alle Komponenten der Kern-Infrastruktur (Netzwerk, Server, Storage) sind redundant ausgelegt und miteinander in Clustern verbunden, so dass der Ausfall einer Komponente nicht die Verfügbarkeit der Infrastruktur beeinträchtigt. Die Anbindung an das Internet erfolgt dabei redundant über zwei dedizierte Leitungen pro Rack, die an zwei Router des Anbieters gekoppelt sind. Der Ausfall einer Leitung beeinträchtigt nicht die Verfügbarkeit der Dienste. Jedes Rack in einem speziell dafür vorgesehenen Gebäude verfügt jeweils über zwei getrennte Stromkreise, die an getrennte USVs angeschlossen sind und diese wiederum von zwei getrennte Diesel-Generatoren gespeist werden, falls der Stromausfall über die Kapazitätsgrenze der USVs andauern sollte. Die Tanks der Diesel-Generatoren können den Ausfall des Stroms für bis zu eine Woche überbrücken, bis diese nachgefüllt werden müssen. Die USV-Anlagen samt Diesel-Generatoren werden regelmäßig auf Ihre Funktionalität geprüft. Es existieren zudem Klimaanlagen zur Kühlung des gesamten Rechenzentrums über einen Doppelboden, um die optimale Kühlung jedes einzelnen Schranks/Servers zu gewährleisten. Feuer- und Rauchmeldeanlagen sowie spezielle Feuerlöschgeräte zur Brandbekämpfung sind in allen kritischen Räumen vorhanden. Die Rauchmeldeanlage ist an die örtliche Feuerwehr angeschlossen und löst automatisch einen Alarm aus, falls ein Brand oder eine Rauchentwicklung erkannt wird. Zutritte zum Rechenzentrum von befugten als auch von unbefugten Personen mit Hilfe der bluechip Zutrittsmittel werden protokolliert und es wird automatisch eine Mitteilung an ausgewählte bluechip Mitarbeiter versendet. Unbefugte Zutritte werden durch die Zutrittskontrolle des gesamten Geländes schon vor dem Einfahrtstor nicht zugelassen. Neben der redundanten Infrastruktur kommen bei den bluechip Cloud Services zudem redundante Hosted Exchange-Cluster, Firewall-Cluster sowie Anti-Spam/Anti-Virus Gateway-Cluster zum Einsatz, um die Verfügbarkeit als auch die Performance der Dienste noch weiter zu steigern. Alle geschäftskritischen bluechip Dienste werden dabei durch ein Backup- und Recovery-Konzept vor Datenverlust gesichert. Welche Dienste in welchem Rahmen gesichert werden ist der jeweiligen Leistungsbeschreibung „bluechip Cloud Services – Datensicherung“ zu entnehmen, die in der aktuellsten Fassung im Downloadbereich des bluechip Cloud Kundencenters eingesehen werden kann. Dies ersetzt jedoch nicht die Pflicht des Partners/Kunden zur eigenen Datensicherung, da eine vom Kunden angeforderte Wiederherstellung aufgrund versehentlicher Löschung von Daten oder falscher Bedienung seitens des Partners/Kunden nach Aufwand berechnet wird. Zudem ist es technisch nicht möglich die Backup-Daten auf externen Datenträgern zur Verfügung zu stellen, da diese unter Umständen auch Daten anderer Kunden beinhalten könnten.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d DSGVO; Art. 25 DSGVO

1. Datenschutz-Management

Die bluechip Computer AG hat einen internen Datenschutzbeauftragten ernannt, der sowohl zum Zeitpunkt der Festlegung der Mittel für eine Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung das Vorhandensein geeigneter technischer und organisatorischer Maßnahmen kontrolliert und gegebenenfalls beratend eingreift. Darüber hinaus führt bluechip sowohl in der Rolle des Verantwortlichen als auch als Auftragsverarbeiter gemäß Art. 30 DSGVO ein Verzeichnis von Verarbeitungstätigkeiten. Eine regelmäßige – mindestens jährliche – Überprüfung der technischen und organisatorischen Maßnahmen auf ihre Wirksamkeit und darauf, ob unter Berücksichtigung des Standes der Technik unter Umständen Optimierungspotentiale vorhanden sind, wird ebenso praktiziert, wie die regelmäßige Schulung und Sensibilisierung aller Mitarbeiter zum Thema Datenschutz.

2. Incident-Response-Management

Innerhalb der bluechip Cloud Services steht ein dediziertes Ticket-System für etwaige Kundenanfragen zur Verfügung. Mit Hilfe dieses Systems wird jede Anfrage des Kunden sowie die Antwort des jeweiligen bluechip Mitarbeiters für beide Seiten dokumentiert. Telefonische Anfragen, die Änderungen an einem bestimmten Dienst oder an bestimmten Daten zur Folge haben oder die Weisungen eines Kunden enthalten, werden nicht angenommen. Diese werden schriftlich im Ticket-System durch einen bluechip Mitarbeiter dokumentiert und der Kunde wird aufgefordert, der dokumentierten Vorgehensweise schriftlich zuzustimmen, bevor mit der Durchführung der Maßnahmen begonnen wird. Der Kunde ist zudem verpflichtet die bluechip Computer AG unverzüglich über das Ticket-System zu unterrichten, sobald er Kenntnis von einem Sicherheitsvorfall erlangt, unabhängig davon wodurch dieser Vorfall verursacht wurde.

Intern verwendet die bluechip Computer AG im Rahmen der bluechip Cloud Services zudem ein Monitoring- und Benachrichtigungssystem, wodurch qualifizierte bluechip Mitarbeiter über automatisiert erkannte Vorfälle benachrichtigt werden und entsprechende Maßnahmen rechtzeitig ergreifen zu können.

3. Datenschutzfreundliche Voreinstellungen gem. Art. 25 Abs. 2 DSGVO

Die bluechip Portale sind entsprechend so konzipiert, dass nur die Daten erhoben werden, die zur Abrechnung, Installation, Bereitstellung, Durchführung und oder Wartung der Dienste benötigt werden.

4. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Die bluechip Computer AG arbeitet streng nach der ISO9001 Norm. Das eingesetzte Qualitätsmanagementsystem ermächtigt die bluechip Produkte und Dienstleistungen bereitstellen zu können, die den Kundenerwartungen genügen. Zudem existiert ein bestellter Datenschutzbeauftragter.

Anlage 2 – Zweck der Datenverarbeitung in Abhängigkeit der gebuchten Dienste

- **Desktop-as-a-Service:** Der Dienst ermöglicht das Arbeiten durch einen oder mehrere Endanwender per Remotedesktopverbindung auf einer dedizierten, kundeneigenen virtuellen Maschine in der bluechip Cloud. Eine mögliche Datenspeicherung erfolgt sowohl lokal auf der virtuellen Festplatte der virtuellen Maschine in der bluechip Cloud, als auch per Netzwerkfreigabe auf dem bluechip Cloud Storage Dienst, je nach Präferenz und Konfiguration durch den Kunden. Die Administration der virtuellen Maschine obliegt dem Kunden.
- **Hosted Exchange:** Der Dienst ermöglicht hauptsächlich die Kommunikation per E-Mail. Es ist zudem unter anderem dem Endanwender möglich Kontakte, Aufgaben und Notizen zu speichern. Die ankommenden und ausgehenden E-Mails werden durch redundante Anti-Spam und Anti-Viren-Gateways auf Basis von Mailcleaner automatisiert gefiltert. Es ist dem Endanwender zudem möglich seine eigene Spam-Quarantäne einzusehen und die E-Mails innerhalb 60 Tagen freizugeben, falls entsprechend konfiguriert. Die Datenspeicherung erfolgt dabei auf den Servern in der bluechip Cloud. Zur automatisierten Prüfung von möglichen Spam-Nachrichten können Informationen aus den Headern einer E-Mail an weitere Server gesendet werden (z.B. Verwendung von Blacklisten oder anderen Spam-Datenbanken).
- **REDDOXX MailDepot:** Der Dienst ermöglicht das Archivieren von E-Mails sowohl von der eigenen Organisation im bluechip Hosted Exchange Dienst als auch von externen E-Mail-Servern. Die Speicherung der Log-Dateien und der noch nicht archivierten E-Mails erfolgt lokal in der virtuellen Festplatte der für einen Kunden dedizierten virtuellen Maschine. Die Speicherung der Archiv-Container erfolgt auf dem bluechip Cloud Storage Dienst. Der Kunde hat zudem die Möglichkeit bei Anlage ein Passwort für jeden Archiv-Container zu vergeben. In manchen Konfigurationsfällen kann es notwendig sein, sogenannte Reverse Proxy Server des in Deutschland ansässigen Unternehmen REDDOXX GmbH zu verwenden, um Kunden den Zugriff auf die in der bluechip Cloud liegenden virtuellen Maschinen und entsprechende Archiv-Container zu ermöglichen. Die Administration der virtuellen Maschine obliegt dem Kunden.
- **Infrastructure-as-a-Service (Virtual Private Server / Virtual Private Cloud):** Der Dienst ermöglicht das Installieren und Konfigurieren von virtuellen Maschinen, die direkt oder hinter einer eigenen, virtuellen Firewall direkt im Internet erreichbar sind. Bei dem Virtual Private Server Dienst ist dabei die virtuelle Maschine direkt im Internet erreichbar. Bei dem Virtual Private Cloud Dienst hat Kunde die Möglichkeit ein eigenes virtuelles Netzwerk auf VLAN-Basis zu benutzen, um mehreren virtuellen Maschinen die Kommunikation innerhalb dieses Netzwerks miteinander zu ermöglichen. Die Datenspeicherung erfolgt hierbei in/auf den Servern der bluechip Cloud Services. Die Administration der virtuellen Maschinen obliegt dem Kunden.
- **Cloud Storage:** Der Dienst ermöglicht die Speicherung von Daten auf einem zentralen Storage-Bereich in der bluechip Cloud. Der Zugriff ist je nach Konfiguration durch Kunden mit einem Berechtigungskonzept sowohl extern im Internet als auch in Kombination mit manchen Diensten in der bluechip Cloud intern möglich.
- **Veeam Cloud Connect:** Der Dienst ermöglicht die Auslagerung von Backups, die von einer lokalen Kundeninfrastruktur mit unterstützten Produkten des Herstellers Veeam erstellt worden sind. Die Datenspeicherung erfolgt hierbei auf den Servern der bluechip Cloud Services. Auf Grund von Lizenzprüfung und Abrechnung kann es notwendig sein, dass Lizenzinformationen an den Hersteller Veeam oder seine Distributoren übertragen werden.
- **Microsoft Lizenzen in der bluechip Cloud (SPLA):** Viele bluechip Cloud Dienste erfordern die richtige Lizenzierung der entsprechenden Produkte bei Microsoft. Aus diesem Grund kann es notwendig sein, die entsprechenden Lizenzinformationen an den Hersteller Microsoft oder seine Distributoren zu übertragen.
- **Gehostete Organisation:** Dieser Dienst ermöglicht eine Benutzer- und Gruppenverwaltung der Kunden in der bluechip Cloud. Diese Verwaltung kann für manche bluechip Cloud Dienste notwendig sein, damit die Funktionsfähigkeit der entsprechenden Dienste gewährleistet werden kann.
- **Webserver:** Dieser Dienst ermöglicht Kunden die Bereitstellung von Webseiten, die öffentlich im Internet abrufbar sind. Für die Inhalte der öffentlich zur Verfügung gestellten Webseiten ist Kunde verantwortlich. Die Speicherung erfolgt auf den Servern der bluechip Cloud Services. Bedingt durch die Internet-Technologie können jedoch beliebige Personen Kopien dieser Inhalte anfertigen, wenn diese nicht explizit durch die Webseite selbst geschützt werden.
- **FTP-Server:** Dieser Dienst wird benötigt, um Inhalte der jeweiligen Webseite Kunden zu pflegen. Der Zugriff erfolgt hierbei direkt auf den Speicherbereich des jeweiligen Webservers.
- **Datenbanken:** Um Dienste wie z.B. Webserver bereitstellen zu können, kann die Speicherung von Daten des jeweiligen Dienstes in einer Datenbank erfor-

derlich werden. Hierbei werden die Daten auf den Servern der bluechip Cloud Services gespeichert. Es obliegt der Applikation oder Webseite des Kunden den Zugriff auf die Daten in der Datenbank zu regeln.

- **DNS-Server:** Um die korrekte Namensauflösung von Domains im Internet zu gewährleisten, betreibt bluechip eigene DNS-Server. Bei bestimmten Diensten, z.B. bei der Domainverwaltung, kann es notwendig sein, die entsprechend notwendigen Informationen zu hinterlegen und öffentlich im Internet verfügbar zu machen.
- **Domains:** Eine Domain-Registrierung oder ein Domain-Transfer innerhalb der bluechip Cloud Services ist grundsätzlich jederzeit möglich. Um den Auftrag ausführen zu können, müssen Informationen über den Domain-Inhaber und eventuell über den Partner an Dritte übertragen werden (z.B. an Registrare und/ oder Domain-Provider). Diese können die übertragenen Informationen entsprechend zwecks Authentifizierung und Nachverfolgung öffentlich zur Verfügung stellen.
- **SSL- und S/MIME Zertifikate:** Als Händler bietet bluechip den Erwerbe von SSL- und S/MIME Zertifikaten. Hierbei kann es notwendig werden, dass Daten, die zur Prüfung der Echtheit der jeweiligen Person oder Organisation an Dritte (z.B. an Zertifizierungsstellen und/oder an weitere Zertifikatshändler) übertragen werden. Dem Kunden obliegt es, in welcher Form und auf welchen Systemen die Zertifikate verwenden und gespeichert werden.
- **Microsoft Cloud und Microsoft Cloud Deutschland:** Bei allen Microsoft Cloud und Microsoft Cloud Deutschland Diensten fungiert die bluechip Computer AG als direkter Microsoft-Vertriebspartner. Die übertragenen Daten werden hierbei auf den jeweiligen Servern von Microsoft gespeichert und unterliegen nicht der Kontrolle durch bluechip. Hierbei gelten die entsprechenden Vereinbarungen zwischen Microsoft und dem Kunden selbst. bluechip überträgt hierbei die zur Abrechnung und Erstellung der Dienste notwendigen Informationen.
- **Drittanbieterlizenzen:** Sollten zur Bereitstellung von bestimmten Diensten anderweitige Drittanbieterlizenzen notwendig sein, die im Rahmen der bluechip Cloud Services bezogen werden, dann können entsprechende Lizenzinformationen zwecks Abrechnung an den Lizenzgeber und/oder deren Distributoren bzw. Vertriebspartner übertragen werden, falls dies von dem jeweiligen Lizenzgeber gefordert ist.