Besondere Bedingungen zur Auftragsverarbeitung

Hostsharing eG

1. Mai 2018

Inhaltsverzeichnis

Besondere Bedingungen zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen dem Verantwortlichen,

– nachstehend Auftraggeber oder Kunde genannt —

und der

Hostsharing eG, Flughafenstraße 52a, 22335 Hamburg

— Auftragsverarbeiter, nachstehend Auftragnehmer genannt —

wird vereinbart:

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags bestimmt sich nach den der Hauptleistung zugrundeliegenden Angaben gemäß Leistungsbeschreibungen. Preisliste und AGB, auf welche hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Dauer des Auftrags

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von einer Woche zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

(3) Ferner ist diese Vereinbarung akzessorisch, also abhängig vom Hauptleistungsvertrag. Insbesondere endet sie automatisch mit der Beendigung der Leistungsvereinbarung.

2. Geltungsbereich und Konkretisierung des Auftragsinhalts

(1) Diese Besonderen Bedingungen zur Auftragsverarbeitung sind nur dann in das o.a. Vertragsverhältnis einbezogen, wenn die Vereinbarung zur Auftragsverarbeitung zwischen den o.a. Parteien von beiden Seiten geschlossen wurde.

(2) Eine Konkretisierung des Auftragsinhalts ist dort individuell vereinbart.

(3) Unabhängig vom Abschluss dieser Vereinbarung gewährleistet Hostsharing generell die Einhaltung der hier in der Anlage — technisch-organisatorische Maßnahmen aufgeführten technisch-organisatorischen Maßnahmen gemäß AGB.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

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

(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, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, 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. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

(1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

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

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

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

(5) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(6) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(7) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem

Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(8) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

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

(2) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, sofern der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab in Textform anzeigt und der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer oder in Textform gegen die geplante Auslagerung widerspricht. Dem Wechsel bzw. der Auslagerung ist eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde zu legen.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Der Auftragnehmer führt jegliche Verarbeitung in Rechenzentren innerhalb der Bundesrepublik Deutschland durch. Dies gilt auch für etwaige Unterauftragnehmer.

(5) Beim Einsatz von Unterauftragnehmern stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

(6) Eine weitere Auslagerung durch den Unterauftragnehmer ist nur in dem Umfang gestattet, wie sie mit dem Auftragnehmer vereinbart ist, dabei werden die datenschutzrechtlichen vertraglichen Regelungen auch jedem weiteren Unterauftragnehmer auferlegt, soweit sie seine Tätigkeit betreffen.

7. Kontrollrechte des Auftraggebers

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

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

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).

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

8. Mitteilung bei Verstößen des Auftragnehmers

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

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

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

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. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(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. Zusatzvereinbarungen

(1) Soweit der Auftraggeber nach Ziffer 7 Kontrollrechte ausüben wird, orientiert sich die vorab zu vereinbarende Höhe des Entgelts an einem festzulegenden Stundensatz des für die Betreuung vom Auftragnehmer abgestellten Mitarbeiters.

(2) Erteilt der Auftraggeber dem Auftragnehmer Weisungen nach Ziffer 9, so hat er durch diese Weisung entstehende Kosten zu erstatten.

(3) Soweit der Auftraggeber Unterstützung nach Ziffer 8 für die Beantwortung von Anfragen Betroffener benötigt, hat er die hierdurch entstehenden Kosten zu erstatten.

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

(5) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. Als Gerichtsstand wird das für den Auftraggeber örtlich zuständige Gericht vereinbart.

(6) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlage — technisch-organisatorische Maßnahmen

A. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

A.1. Zutrittskontrolle

Zutrittskontrolle dient dem Schutz der Datenverarbeitungsanlagen vor unberechtigtem, physischem Zutritt. Hostsharing realisiert die Zutrittskontrolle über folgende, mehrstufige Absicherung:

— Der Zutritt zu den Rechenzentren ist durch Videoüberwachung an Ein- und Ausgängen, Sicherheitsschleusen und Cages (extra abgesicherte Bereichen innerhalb des Rechenzentrumstandorts Berlin) gesichert.

— Der Zutritt zum Rechenzentrum ist ausschließlich in Begleitung autorisierten Personals zulässig. Der Zutritt zu den Rechenzentren wird kontrolliert und protokolliert.

— Der Zutritt zu den Cages wird durch eine Schließanlage gesichert und mittels Kamera überwacht.

— Der Zutritt zum einzelnen Cage ist ausschließlich in Begleitung autorisierten Personals zulässig.

— Der Zutritt zu den Racks (den Serverschränken innerhalb der Cages), ist durch eine weitere Schließanlage gesichert und ausschließlich in Begleitung autorisierten Personals zulässig.

— Die Zutritt erfolgt nach Legitimation mit Zugangskarte und PIN. Die Schlüsselvergabe erfolgt ausschließlich an autorisierte Mitarbeiter und Kunden. Jeder Kunde erhält ausschließlich Zutritt zu seinen Racks.

A.2. Zugangskontrolle

Zugangskontrolle dient dem Schutz der Datenverarbeitungsanlagen vor unberechtigtem, logischem Zugriff. Hostsharing realisiert die Zugangskontrolle über folgende, mehrstufige Absicherung:

— Der Zugang zur Administration der Server erfolgt ausschließlich über eine geschützte Ver-

bindung.

— Der Zugang ist per Public Key-Verfahren geschützt, Zugriff erfolgt über über personenbezogenen Benutzerkonten.

— Der Zugang für administrative Zugriffe erfolgt über eine zweistufige Zugangssicherung mit Protokollierung.

A.2.1. Für alle Hauptaufträge

— Hostsharing stellt dem Kunden eine mandantenfähige Benutzerverwaltung bereit, um ihn bei der Implementation der Zugangskontrolle in seinem Verantwortungsbereich zu unterstützen.

— Der Zugang über von Hostsharing bereitgestellte Verfahren zur Administration der Server erfolgt ausschließlich über eine geschützte Verbindung.

— Der Zugang über von Hostsharing bereitgestellte Verfahren ist per Public Key-Verfahren oder Passwort geschützt.

— Der Zugang über von Hostsharing bereitgestellte Verfahren wird protokolliert.

A.2.2. Für Hauptauftrag „Managed Server“, „Managed Webspace“

— Die Verantwortung der Zugangskontrolle in Bezug auf Sicherheit und Updates der betriebsbereit vorgehaltenen Software obliegt Hostsharing.

— Die Verantwortung der Zugangskontrolle in Bezug auf Updates der vorinstallierten Software obliegt Hostsharing.

— Die Verantwortung der Zugangskontrolle in Bezug auf Sicherheit der vorinstallierten Software obliegt, soweit diese genutzt wird, dem Kunde.

— Die Verantwortung der Zugangskontrolle in Bezug auf Sicherheit und Updates bei vom Kunden selbst verantwortet installierter Software obliegt dem Kunde.

A.2.3. Für Hauptauftrag „Root Server“

— Die Verantwortung der Zugangskontrolle in Bezug auf Sicherheit und Updates bei vom Auftraggeber selbst verantwortet installierten Software obliegt dem Kunden.

A.3. Zugriffskontrolle

Zugriffskontrolle dient dem Schutz der Daten von unbefugtem Lesen, Kopieren, Verändern oder Löschen personenbezogener Daten innerhalb des Systems. Hostsharing realisiert die Zugriffskontrolle über folgende, mehrstufige Absicherung:

— Hostsharings Support-Mitarbeiter haben generell keinen Zugriff auf die Daten in den Datenbanken oder in Benutzerverzeichnissen der Kunden.

— Hostsharing hat ein verbindliches Berechtigungsvergabeverfahren für die Mitarbeiter festgelegt.

— Hostsharing soll im Falle des Bekanntwerdens von Sicherheitslücken unverzüglich Sicherheitsupdates installieren.

A.3.1. Für alle Hauptaufträge

— Hostsharing stellt sicher, dass defekte Datenträger, die nicht sicher gelöscht werden können, direkt im Rechenzentrum zerstört (geschreddert) werden.

A.3.2. Für Hauptauftrag „Managed Server“, „Managed Webspace“

— Die Verantwortung der Zugriffskontrolle in Bezug auf Sicherheit und Updates der betriebsbereit vorgehaltenen Software obliegt Hostsharing.

— Die Verantwortung der Zugriffskontrolle in Bezug auf Updates der vorinstallierten Software obliegt Hostsharing.

— Die Verantwortung der Zugriffskontrolle in Bezug auf Sicherheit der vorinstallierten Software obliegt, soweit diese genutzt wird, dem Kunden.

— Die Verantwortung der Zugriffskontrolle in Bezug auf Sicherheit und Updates bei vom Kunden selbst verantwortet installierten Software obliegt dem Kunden.

A.3.3. Für Hauptauftrag „Root Server“

— Hostsharing stellt sicher, dass zugewiesene Festplattenspeicherbereiche nach Beendigung der Zuweisung mittels definiertem Verfahren mehrfach überschrieben (gelöscht) werden.

— Die Verantwortung der Zugriffskontrolle in Bezug auf Sicherheit und Updates bei vom Kunden selbst verantwortet installierter Software obliegt dem Kunden.

A.4. Datenminimierung

Der Auftragnehmer verwendet für den Betrieb seiner Dienstleistungen persönliche Daten nur in dem für die Gewährleistung des Betriebes erforderlichen Umfang. Darüber hinaus sind die Mitglieder im Rahmen der von ihnen betriebenen Anwendungen für die Datensparsamkeit selbst verantwortlich.

A.5. Trennungskontrolle

Trennungskontrolle dient der Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden. Hostsharing realisiert die Trennungskontrolle über folgende, mehrstufige Absicherung:

— Hostsharing nutzt festgelegte Strategien und Maßnahmen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) entsprechen.

— Hostsharing verarbeitet oder speichert Daten unterschiedlicher Kunden auf den Datenverarbeitungsanlagen in getrennten Datenbanken oder Benutzerverzeichnissen.

— Hostsharing nutzt physisch oder logisch getrennte Netze für die öffentliche Anbindung der Systeme an das Internet, private Kundennetze sowie interne Funktionalität (Speicherbereitstellung, Failover, Backup) und administrative Zugriffe auf die Infrastruktur.

A.5.1. Für alle Hauptaufträge

— Hostsharing stellt dem Kunden eine mandantenfähige Benutzerverwaltung bereit, um ihn bei der Implementation der Trennungskontrolle in seinem Verantwortungsbereich zu unterstützten.

— Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) obliegt dem Kunden.

A.5.2. Für die Hauptaufträge „Managed Server“ und „Managed Webspace“

— Die Verantwortung der Trennungskontrolle in Bezug auf Sicherheit und Updates der betriebsbereit vorgehaltenen Software obliegt Hostsharing.

— Die Verantwortung der Trennungskontrolle in Bezug auf Updates der vorinstallierten Software obliegt Hostsharing.

— Die Verantwortung der Trennungskontrolle in Bezug auf Sicherheit der vorinstallierten Software obliegt, soweit diese genutzt wird, dem Kunden.

— Die Verantwortung der Trennungskontrolle in Bezug auf Sicherheit und Updates bei vom Kunden selbst verantwortet installierter Software obliegt dem Kunden.

A.5.3. Für den Hauptauftrag „Root Server“

— Die Verantwortung der Trennungskontrolle in Bezug auf Sicherheit und Updates bei vom Kunden selbst verantwortet installierten Software obliegt dem Kunden.

A.5.4. Für die Hauptaufträge „Managed Server“ und „Root Server“

— Hostsharing ermöglicht dem Kunden die Nutzung logisch getrennter, privater Kundennetze zur Kommunikation zwischen Servern desselben Kunden.

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

B.1. Weitergabekontrolle

Weitergabekontrolle dient dem Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Löschen von personenbezogenen Daten bei elektronischer Übertragung oder Transport. Hostsharing realisiert die Weitergabekontrolle über folgende, mehrstufige Absicherung:

— Hostsharing realisiert die Weitergabekontrolle durch die Beschränkung der Speicherung auf die dafür vorgesehenen Rechenzentren und Serversysteme.

— Hostsharing unterweist alle Mitarbeiter, die in Kontakt mit personenbezogenen Daten kommen, nach Art. 32 Abs. 4 DS-GVO und verpflichtet sie zur Verschwiegenheit und Sicherstellung des datenschutzkonformen Umgangs mit personenbezogenen Daten.

— Hostsharing stellt dem Kunden im Umfang der Leistungsbeschreibung des Hauptauftrages Möglichkeiten zur verschlüsselten Datenübertragung zur Verfügung.

— Hostsharing gewährleistet die datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

B.2. Eingabekontrolle

Eingabekontrolle dient der Nachvollziehbarkeit des Lesens, Kopierens, Veränderns oder Löschens von personenbezogenen Daten. Hostsharing realisiert die Eingabekontrolle über folgende, mehrstufige Absicherung:

— Hostsharing realisiert die Eingabekontrolle durch Aufzeichnung der durch die Hostsharing-Mitarbeiter beim administrativen Zugriff getätigten Eingaben.

— Die Verantwortung der Eingabekontrolle beim Zugriff mit dem Auftraggeber überlassenen Benutzerkonten obliegt dem Auftraggeber.

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

C.1. Verfügbarkeitskontrolle

Verfügbarkeitskontrolle dient dem Schutz personenbezogener Daten gegen zufällige oder mutwillige Zerstörung bzw. Verlust sowie der rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO). Hostsharing realisiert die Verfügbarkeitskontrolle über folgende, mehrstufige Absicherung:

— Hostsharing setzt Schutzsystemen (SPAM-Filter, Firewalls, Virenscanner, Verschlüsselung, (D)DoS-Abwehr) ein.

— Hostsharing unterstützt die Verfügbarkeit der Produktivsysteme durch den Einsatz redundanter Stromversorgung, Netzteile, Speichersysteme und Netzwerkkomponenten.

— Hostsharing unterstützt die Verfügbarkeit der Produktivsysteme durch Spiegelung aller im Produktivbetrieb befindlichen virtuellen Maschinen in Echtzeit auf Standby-Server oder alternativ redundante Auslegung auf Softwareebene.

— Hostsharing spiegelt alle Kundensysteme in Echtzeit auf Standby-Server, welche im Versagensfall des Primär-Systems die Aufgaben mit aktuellen Daten unverzüglich übernehmen können.

— Hostsharing führt täglich Datensicherungen der Konfigurations- und Serverdaten durch, welche auf separaten Servern in einem gesonderten Rechenzentrum an einem anderen Standort aufbewahrt werden.

— Hostsharing verfügt über ein partielles (einzelne Dateien) und vollständiges (virtuelle Maschinen) Datensicherungs- und Wiederherstellungskonzept.

— Hostsharing überwacht die produktiven Systeme von einem externen Standort aus.

— Hostsharing alarmiert die Mitarbeiter der technische Rufbereitschaft im Fehlerfall auf zwei unabhängigen Wegen.

— Hostsharing hat eine Eskalationskette für alle internen Systeme definiert, die vorgibt, wer im Fehlerfall zu informieren ist, um ausgefallene Systeme unverzüglich wiederherzustellen.

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

Zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Verfahren hat Hostsharing folgende Konzepte implementiert:

— Datenschutz-Management

— Incident-Response-Management

— Datenschutzfreundliche Voreinstellungen werden bei der Softwareentwicklung berücksichtigt (Art. 25 Abs. 2 DS-GVO)

D.1. Auftragskontrolle

Verfügbarkeitskontrolle dient dem Schutz personenbezogener Daten gegen nicht weisungsgemäße, unbefugte Verarbeitung.

Die verordnungsgemäße Umsetzung der Auftragsverarbeitung gemäß Art. 28 DS-GVO, wird bei Hostsharing realisiert durch eindeutige Vertragsgestaltungen, sorgfältige Auswahl des Auftragsverarbeiters, Vorabüberzeugung und Nachkontrollen, insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen.

— Hostsharing schließt Unterauftragnehmern vor Beginn der Auftragsverarbeitung Vereinbarungen über die Dienstleistungen bzw. zur Auftragsverarbeitung, so dass die Daten vertraulich behandelt bzw. nur entsprechend den Weisungen Hostsharings verarbeitet werden. Mindestens werden jedenfalls dem Sinn und Zweck der DS-GVO entsprechende technisch-organisatorische Maßnahmen vereinbart.

— Hostsharing schließt eine Nutzung oder Weitergabe der Daten durch Hostsharing-Mitarbeiter vertraglich aus.

— Hostsharing verpflichtet den Rechenzentrumsbetreiber oder weitere Auftragsverarbeiter

Weisungen nur durch autorisierte Mitarbeiter Hostsharings entgegenzunehmen. Diese Aufträge liegen in Textform vor und können nachträglich überprüft werden.

— Hostsharing verfügt über Datenschutzbeauftragte sowie einen Informationssicherheitsbeauftragten.

— Die Leistungsbeschreibungen enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.