Vereinbarung

zwischen dem/der

Dr. Matthias Strähler, Poststr.40, 72458 Albstadt

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

Webhost-United GmbH, Franzstr. 51, 52064 Aachen

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt, welche ab dem 25.05.2018 gilt und möglicherweise vorher abgeschlossene Auftragsdatenverarbeitungsvereinbarungen (ADV) ersetzt.

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem zwischen dem Auftraggeber und Auftragnehmer geschlossenen Vertrag (nachfolgend "Leistungsvereinbarung") in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (nachfolgend auch "Daten") des Auftraggebers verarbeiten.

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) Gegenstand

Der Auftragnehmer stellt Produkte / Leistungen aus den folgenden Bereichen zur Verfügung:

> Domains, DNS, E-Mail, Shared Webhosting, Datenbanken, managed Server, SSL Zertifikate, virtuelle Server / Private Cloud, Speicherplatz im Rechenzentrum / Storage, individuelle Lösungen wie bspw. Cluster, Hochverfügbarkeit, Private Cloud.

Der konkrete Gegenstand des Auftrags des Auftraggebers im vorliegenden Fall ergibt sich aus der zwischen den Parteien geschlossenen Leistungsvereinbarung.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

(3) Ort

Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(4) Art der Daten / Kategorien betroffener Personen

Gegenstand der Verarbeitung personenbezogener Daten sind sämtliche Datenarten/-kategorien, die der Auftraggeber zur Speicherung auf den im Rahmen der Leistungserbringung vom Auftragnehmer zur Verfügung gestellten Speichermedien überträgt. Gleiches gilt für die Kategorien der durch die Verarbeitung betroffenen Personen.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die in der Leistungsvereinbarung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art.4 Nr. 7 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragneh-

mer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz Grundverordnung (Art. 28 Abs. 3 lit. c, 32 DS-GVO sowie § 63 BDSG (neu) insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Für die Durchführung des vorliegenden Vertrages haben sich die Parteien auf den in **Anlage A** festgelegten Mindestsicherheitsstandard und die dort dokumentierten Maßnahmen geeinigt. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit wird auf die genehmigten Verhaltensregeln nach Art. 40 DS-GVO verwiesen, denen sich der Auftragnehmer unterworfen hat.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie – unter Berücksichtigung der dem Auftragnehmer zur Verfügung stehenden Informationen - bei der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten. Der Auftraggeber hat die entstehenden Aufwendungen, wie bspw. Beratungsleistungen, Technikereinsätze, etc. gemäß den üblichen Stundensätzen des Auftragnehmers an den Auftragnehmer zu vergüten.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(6) Der Auftragnehmer bestellt schriftlich einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt, soweit der Auftragnehmer hierzu gesetzlich verpflichtet ist. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt. Ist der Auftragnehmer nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet, nennt er dem Auftraggeber dennoch einen Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) 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:

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

b) 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.

c) 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.

d) 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.

e) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach diesem Vertrag.

(9) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag bereits vereinbart. Der Auftraggeber hat die entstehenden Aufwendungen, wie bspw. Beratungsleistungen, Technikereinsätze, etc. gemäß den üblichen Stundensätzen des Auftragnehmers an den Auftragnehmer zu vergüten.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe; Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Ver-

trag bereits vereinbart. Der Auftraggeber hat die entstehenden Aufwendungen, wie bspw. Beratungsleistungen, Technikereinsätze, etc. gemäß den üblichen Stundensätzen des Auftragnehmers an den Auftragnehmer zu vergüten.

(10) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Pflicht des Auftragnehmers zur Speicherung besteht. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(11) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Der Auftraggeber hat die entstehenden Aufwendungen, wie bspw. Beratungsleistungen, Technikereinsätze, etc. gemäß den üblichen Stundensätzen des Auftragnehmers an den Auftragnehmer zu vergüten.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 11 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach, stellt ihm alle hierfür erforderlichen Informationen zur Verfügung und ermöglicht und unterstützt eine Überprüfung durch den Auftraggeber oder einen von diesem beauftragten Prüfer.

(2) Sollten im Einzelfall im Rahmen der Überprüfung nach § 6 (1) Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hin-

sichtlich im Rahmen der Prüfung ggf. berührter Betriebs- und Geschäftsgeheimnisse des Auftragnehmers abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer einen Ersatz der hierdurch entstehenden angemessenen Kosten verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

§ 7 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.

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Die Parteien sind sich darüber einig, dass Domainvergabestellen (Registries) und Zertifikatvergabestellen (CAs) keine Subunternehmer sondern Hersteller der jeweiligen Produkte sind. Der Auftragnehmer wird Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen sorgfältig auswählen und mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten, insbesondere vertraglich sicherstellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten.

Der Auftragnehmer stellt dem Auftraggeber im Kundenportal eine Liste der aktuell für den Auftragnehmer tätigen Subunternehmer zur Verfügung. Hierzu gibt er den vollständigen Namen, Anschrift und Auftragsinhalte an. Diese erhalten möglicherweise personenbezogene Daten und mit ihrer Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftraggeber stimmt zu, dass der Auftragnehmer bestehende Subunternehmer wechselt oder weitere Subunternehmer hinzuzieht. Dies ist zulässig, soweit:

- der Auftragnehmer einen solchen Wechsel bzw. eine solche Auslagerung auf Subunternehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung bzw. den Wechsel erhebt und

- zwischen dem Auftragnehmer und dem Subunternehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 EU-DSGVO zugrunde gelegt wird.

Die Weiterleitung von Daten an einen Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtung nach § 32 EU-DSGVO erfüllt hat.

Wenn der Auftraggeber Einspruch gegen die Beauftragung des Subunternehmers einlegt, dieser aber für die Durchführung des Auftrages oder des Produktes erforderlich ist, ist der Auftragnehmer berechtigt, dem Auftraggeber das Produkt nicht mehr anzubieten.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen der Leistungsvereinbarung Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

§9 Haftung und Schadensersatz

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

Oliver Dick

für den Auftraggeber zugestimmt von
Benutzer: drmat692
IP-Adresse: 77.177.185.16
Datum: Montag, 14. Mai 2018 07:18:43 UTC

für den Auftragnehmer: Oliver Dick (Geschäftsführer)

Technische und organisatorische Maßnahmen (TOMs) nach Art. 32 DS-GVO

Zugangskontrolle RZ Räume

Der Zutritt zum Rechenzentrum ist über eine Stahltüre per RFID Chipkarte und Codes geregelt, der personenbezogen freigeschaltet ist. Die Chipkarten werden vom Rechenzentrumsbetreiber ausgegeben. Der Zugang wird elektronisch durch den Rechenzentrumsbetreiber protokolliert. Dies betrifft auch fehlgeschlagene Versuche, Zugang zu erhalten. Die Protokolle werden drei Monate gespeichert. Eine Übertragung der Chipkarten und Codes ist untersagt. Ein Verlust ist durch den betroffenen Mitarbeiter unverzüglich anzuzeigen. Das Rechenzentrum besteht aus verschiedenen Räumen, die von unterschiedlichen Unternehmen gemietet werden. Der Auftragnehmer verfügt dort über einen eigenen Raum. Der Zutritt zu diesem Raum wird noch einmal separat über eine Stahltüre mit RFID Chipkarte gesichert. Nur Mitarbeiter des Rechenzentrumsbetreibers sowie des Auftragnehmers können die Türe öffnen. Der gesamte Bereich wird videoüberwacht und ein Sicherheitsdienst wird über jedes Betreten informiert. Die Bilddaten der Videoüberwachung werden drei Monate gespeichert. Das Rechenzentrum ist durch eine Einbruchmeldeanlage alarmgeschützt. Der Zutritt von Fremdpersonal ist nur in Begleitung durch einen Mitarbeiter gestattet. Die RZ-Räume des Auftragnehmers sind fensterlos und werden nur für den Betrieb der Server des Auftragnehmers verwendet. Im Raum beinhalten mehrere Schränke Ersatzteile für die vom Auftragnehmer betriebenen Server.

Zugangskontrolle Büro

Die Räume des Auftragnehmers befinden sich in der Franzstr. 51 in Aachen. Der Zutritt zu den Räumen des Auftragnehmers ist über elektromechanische RFID Schlüssel geregelt, die personenbezogen ausgegeben werden. Die Vergabe der Schlüssel und deren Protokollierung obliegt der Geschäftsführung des Auftragnehmers. Nur mit diesen Schlüsseln ist der Zutritt zum Gebäude oder der Büroräume möglich. Ein Sicherheitsdienst des Vermieters kontrolliert regelmäßig das Gebäude. Besucher des Auftragnehmers werden am Eingang abgeholt und in das Besprechungszimmer begleitet. Besucher werden nicht alleine gelassen, ein Mitarbeiter bleibt beim Besucher, bis der entsprechende Ansprechpartner den Besucher empfängt.

Datenträgerkontrolle

Datenträger werden nur innerhalb der Räume des Auftragnehmers unverschlüsselt eingesetzt. Mobile Datenträger bspw. in Laptops oder USB Sticks werden grundsätzlich verschlüsselt. Geräte und Datenträger werden nur vom Unternehmen ausgegeben, private Geräte und Datenträger sind nicht erlaubt. Alte Datenträger werden physisch durch Mitarbeiter vernichtet. Bei Veranstaltungen innerhalb der Büroräume werden alle Räumlichkeiten abgesperrt, in denen Datenträger eingesetzt werden. Für Papier-Unterlagen stehen Aktenvernichter zur Verfügung, alle Mitarbeiter sind angewiesen, diese zu nutzen.

Speicherkontrolle

Eine Übermittlung von personenbezogenen Daten durch Kunden des Auftragnehmers ist nur mittels dem jeweiligen Kunden individuell mitgeteilter Zugangsdaten oder bei der

Erstkontaktaufnahme über die Webseite oder per E-Mail möglich. Eine Kenntnisnahme, Veränderung oder Löschung ist nur von Mitarbeitern des Auftragnehmers möglich. Personenbezogene Daten werden nur für die Dauer der vertraglichen und gesetzlichen Fristen gespeichert. Die Löschung findet automatisiert statt, sobald ein Datensatz nicht mehr benötigt wird.

Benutzerkontrolle

Der Auftragnehmer setzt Benutzerkontrollen ein, damit nur Befugte mit einer Zugriffsberechtigung bei der Verarbeitung, Nutzung und nach der Speicherung auf die Daten zugreifen können.
Die Zugriffsberechtigung ist mitarbeiterbezogen und Keyfile / Kennwort gesichert. Jeder Mitarbeiter wird regelmäßig auf den verantwortungsvollen Umgang sensibilisiert. Die Zugriffe auf Systeme werden nach dem Minimalprinzip eingerichtet. Bestehende Berechtigungen werden regelmäßig überprüft.

Zugriffskontrolle

Zugriff auf Serversysteme ist nur per Key möglich, die Zugriffsberechtigungen werden zentral verwaltet. Alle Mitarbeiter sind angewiesen, eventuelle Passwörter nach einer Passwort-Richtlinie zu generieren. Es existiert ein definierter Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern. Eine Protokollierung darüber wird elektronisch gepflegt.

Übertragungskontrolle

Daten werden nur an berechtigte Empfänger (z.B. Banken im Rahmen des Zahlungsverkehrs oder einer Domainregistrierung) elektronisch übertragen. Es werden ausschließlich verschlüsselte Verbindungen eingesetzt. Beim Versand von E-Mails kann eine Übertragung unverschlüsselt vorkommen, wenn der Empfänger keine Verschlüsselung unterstützt. Die notwendigen Zertifikate und Schlüssel werden von Administratoren des Auftragnehmers verwaltet.

Eingabekontrolle

Es wird protokolliert, welcher Benutzer auf welche Daten zu welchem Zeitpunkt eingegeben oder verändert hat. Die Geschäftsleitung hat Zugriff auf diese Daten.

Transportkontrolle

Daten auf mobilen Datenträgern sind per Weisung zu verschlüsseln. Defekte Datenträger werden vernichtet. Ein Austausch oder eine sonstige Rückgabe defekter Geräte (z.B. Garantie) wird nicht vorgenommen.

Wiederherstellung

Alle Daten werden zusätzlich auf Backupsystemen gesichert. Eine Wiederherstellung von Teilsystemen ist dadurch für die Administratoren zeitnah möglich. Für jedes Teilsystem existieren dafür unterschiedliche Notfall- und Backupkonzepte. Alle Daten werden per Echtzeitspiegelung auf verschiedenen Datenträgern gespeichert. Des Weiteren findet mindestens einmal täglich ein Backup auf andere Server im gleichen Raum statt. Die Speicherung der Backups ist unverschlüsselt, auf die Server haben nur Administratoren des Auftragnehmers Zugriff. Es existieren Notfallkonzepte für die Wiederherstellung aller Teilsysteme, die nicht dokumentiert sind, aber jedem Administrator des Auftragnehmers bekannt sind.

Zuverlässigkeit

Alle Teilsysteme und Dienste werden vollständig mittels einer Monitoringsoftware überwacht. Eine Meldung über ein Problem erfolgt per E-Mail an entsprechende Mitarbeiter. Wesentliche Komponenten sind redundant ausgelegt, so dass ein Ausfall einer Komponente keine Auswirkung hat.

Datenintegrität

Es erfolgen die notwendigen Updates des Betriebssystems und der sonstigen Programme. Die Administratoren sind in den nötigen Mailinglisten verschiedener Hersteller der von des Auftragnehmers eingesetzten Softwares eingetragen und sind in der Lage, jederzeit die notwendigen Maßnahmen zu treffen. Es gibt einen ausreichenden Schutz gegen Intrusion und Viren. Die Installation von Schutzprogrammen auf Windows ist Pflicht. Unter Linux arbeiten alle Mitarbeiter mit Benutzer- und nicht mit Administratorrechten. Es existiert ein Prozess zum Einspielen von Updates, der nicht dokumentiert ist, aber jedem Administrator des Auftragnehmers bekannt ist.

Auftragskontrolle

Alle Mitarbeiter des Auftragnehmers erhalten eine genaue Einweisung in die angebotenen Produkte und führen Aufträge des Kunden nach einem definierten Schema durch. Mit allen Lieferanten hat der Auftragnehmer eine entsprechende AV(ADV) vereinbart. Lieferanten aus Nicht-EU Ländern erhalten keine personenbezogenen Daten, sofern es für die Durchführung des Auftrages nicht unmittelbar erforderlich ist und vorher durch geeignete Maßnahmen ein angemessenes Sicherheitsniveau hergestellt wurde.

Verfügbarkeitskontrolle

Alle Systemkomponenten werden regelmäßig überprüft und Bauteile proaktiv ausgetauscht. Wichtige Systeme wie Router, Switche und Mailserver sind redundant ausgelegt. Die Wände des Rechenzentrums sowie die Wände des Raums des Auftragnehmers bestehen aus Massivsteinen. Der Raum im Rechenzentrum verfügt über ein Brandfrüherkennungssystem sowie eine automatische Argongaslöschanlage. Bei Auslösung eines Alarms wird automatisch der Rechenzentrumsbetreiber sowie ein Sicherheitsdienst informiert. Alle Türen im Rechenzentrum sind feuerfest. Es existiert eine Klimaanlage, die dreifach redundant ausgelegt ist.

Alle Server sind über eine USV Anlage gesichert. Alle Rackserver sind außerdem mit einer doppelten Stromzuführung/doppelten Netzteilen versehen, so dass diese bei Ausfall der USV mit Stadtnetzstrom weiter betrieben werden können. Das Rechenzentrum verfügt über redundante Dieselgeneratoren. Wartungen der genannten Komponenten finden regelmäßig durch den Rechenzentrumsbetreiber statt.

Trennbarkeit

Personenbezogene Daten werden ausschließlich nach dem Zweck der Datenerhebung verwendet. Dies wird durch unterschiedliche Datenbanken sowie deren Tabellen sichergestellt.