Vertrag zur Auftragsdatenverarbeitung

14. November 2024

Christina Mustermann
Musterstr. 123
12345 Bremen
Kd-Nr. 123456789
– Auftraggeber –

und

TrafficPlex GmbH
Konsul-Smidt-Str. 90
28217 Bremen
– Auftragnehmer –

schließen den folgenden Vertrag:

1 Gegenstand und Dauer des Auftrags

1. Gegenstand und Dauer des Auftrags bestimmen sich vollumfänglich nach den unter der oben genannten Kundennummer im jeweiligen Vertragsverhältnis gemachten Angaben. Diese Vereinbarung ist abhängig vom Bestand eines der folgenden Hauptvertragsverhältnisse:

   - Webhosting-Dienstleistung (Shared Hosting u. Managed Hosting)
   - E-Mail-Dienstleistungen
   - Cloud-VPS

   Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne des Art. 4 Nr.2 und Art. 28 DS-GVO auf Grundlage dieses Auftrags.

2. Die Kündigung oder anderweitige Beendigung des Hauptvertragsverhältnisses beendet gleichzeitig diese Vereinbarung.

3. Das Recht zur isolierten, außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte konkret für die Vereinbarung bleiben hierdurch unberührt.

4. Dieser Vertrag bezieht sich nur auf das unter der oben genannten Kundennummer geführte Kundenkonto. Sofern der Auftraggeber beim Auftragnehmer mehrere Kundenkonten unterhält, ist dieser Vertrag für jedes Kundenkonto gesondert abzuschließen.

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

1. Der Umfang, die Art und der Zweck einer etwaigen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, die Art der Daten und der Kreis der Betroffenen werden dem Auftragnehmer durch den Auftraggeber gemäß der vom Auftraggeber ausgefüllten Anlage I und II beschrieben, soweit sich das nicht aus dem Vertragsinhalt der in Ziffer 1 beschriebenen Vertragsverhältnisse ergibt.

2. Gegenstand des Vertrags ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Bei der Administration der Serversysteme kann ein Zugriff auf sowie die Erhebung, Nutzung und Verarbeitung von personenbezogene Daten jedoch nicht ausgeschlossen werden. Dies beinhaltet unter anderem:

   - Aufzeichnen und Prüfen von Zugriffen und deren IP-Adressen zu Sicherheitszwecken (Firewall-Protokolle, fehlgeschlagene Login-Versuche, etc.)
   - Fehlerbehebung im Kundenauftrag
   - Systemüberwachung und Monitoring

3. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

4. 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.

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

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 (siehe Anlage III). Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs.3 Satz 2 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.

3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4 Berichtigung, Sperrung und Löschung von Daten

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

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

3. Soweit der Auftraggeber Unterstützung nach Ziffer 4 für die Beantwortung von Anfragen Betroffener benötigt, hat er die hierdurch entstehenden Kosten zu erstatten.

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:

- Die Bestellung eines Datenschutzbeauftragten, sobald dies gesetzlich erforderlich ist. Eine Bestellung sowie ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Ist ein Datenschutzbeauftragter bestellt, sind dessen Kontaktdaten auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

- 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.

- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechen Art. 28 Abs. 3 Satz 2 lit. c, 32 DS-GVO und Anlage III. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

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

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

- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- Dokumentation der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber laut Anlage III.

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 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. Im Rahmen der Vertragserfüllung wird der Auftragnehmer Subunternehmer beauftragen. Der Auftragnehmer wird ein Verzeichnis von Subunternehmern, die an der Auftragserfüllung beteiligt sind, veröffentlichen und aktuell halten: `https://www.lima-city.de/usercp/data_processing_contracts/contractors.pdf`

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 wahlweise erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) und/oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
4. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen und Ersatz der ihm entstehenden Kosten und Aufwände verlangen.

5. 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.

8 Mitteilung bei Verstößen des Auftragnehmers

1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.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
   - die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
   - 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
   - die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
   - 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). Eine nicht bestätigte bzw. nicht dokumentierte Weisung gilt als nicht erteilt.

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

10 Löschung und Rückgabe von personenbezogenen Daten

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

2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der

Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Der Auftragnehmer gibt dem Auftraggeber auf Anfrage hin Auskunft zur Natur und dem Zeitpunkt der Löschung.

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

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

11 Sonstige Vereinbarungen

1. Es gilt das Recht der Bundesrepublik Deutschland.

2. Die Parteien vereinbaren als Gerichtsstand den Sitz des für Bremen zuständigen Gerichts.

Bremen, 14. November 2024

.....	.....
Auftraggeber, Ort, Datum	Auftragnehmer, Ort, Datum

Anlage I
Daten-Typen

- Muster-Daten

Anlage II
Betroffene

- Muster-Betroffene

Anlage III
Technische und organisatorische Maßnahmen

Die folgenden technischen und organisatorischen Maßnahmen (kurz TOMs) werden vom Auftragnehmer umgesetzt:

1 Vertraulichkeit: Zutrittskontrolle

Telehouse Frankfurt, Main (Rechenzentrum)

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um das Gelände
- durchgehend besetzter Leitstand
- Bewachung durch zertifiziertes Werksschutzpersonal
- Videoüberwachung insbesondere der Ein- und Ausgänge
- organisatorisch getrennte Berechtigungsvergabe für den Rechenzentrums-Zutritt

Bremen (Büro)

- durchgehende Besetzung des Empfangs durch Pförtner
- Manuelle Schließanlage

2 Vertraulichkeit: Zugangskontrolle

Kundenmenü

- Das Passwort für das Kundenmenü („Verwaltung“) wird vom Auftraggeber selbst vergeben. Das Passwort muss der aktuellen Kennwortrichtlinie entsprechen.
- Die Login-Versuche zum Kundenmenü werden innerhalb eines Zeitfensters begrenzt („Rate limiting“).

Leistung „Cloud-VPS“

- Standardmäßige Deaktivierung von Server-Passwörtern für den Login, Zugang nur mit kryptografischem Schlüssel („SSH-Keys“). Für die Inbetriebnahme wird eine einmalige Berechtigungsvergabe von kryptografischen Schlüsseln des Auftraggebers durchgeführt und protokolliert.
- Der Auftraggeber kann auf Wunsch für die erstmalige Inbetriebnahme ein Server-Passwort vergeben, das verschlüsselt gespeichert wird und dem Auftragnehmer nicht bekannt ist. Der Auftraggeber wird ein eventuell gesetztes Server-Passwort bei der Inbetriebnahme ändern und die Vergabe und Dokumentation von Berechtigungen selbst verantworten.

- Für die Zugangskontrolle für auf dem Cloud-VPS installierter Software und Daten ist der Auftraggeber verantwortlich.

Leistung ,,Webhosting“

- Der Administrator-Zugang ist ausschließlich per kryptografischem Schlüssel („SSH-Keys“) durch berechtigte Mitarbeiter des Auftragsnehmers möglich.
- Der Kunden-Zugang (SSH) ist ausschließlich mit kryptografischem Schlüssel („SSH-Keys“) möglich. Berechtigungen für kryptografische Schlüssel werden vom Auftraggeber vergeben und durch den Auftragnehmer protokolliert.
- Der Kunden-Zugang zu Datenbanken ist mit einem vom Auftragnehmer erzeugten Benutzernamen und vom Auftraggeber gewählten Passwort möglich. Das Passwort muss der aktuellen Kennwortrichtlinie entsprechen.
- Der Kunden-Zugang per FTP-Protokoll ist mit einem vom Auftragnehmer erzeugten Benutzernamen und vom Auftraggeber gewählten Passwort möglich. Das Passwort muss der aktuellen Kennwortrichtlinie entsprechen.
- Die Login-Versuche für FTP-, MySQL- und SSH-Zugänge werden innerhalb eines Zeitfensters begrenzt (,,Rate limiting“).
- Für die Zugangskontrolle für auf dem Webspace installierter Software und Daten ist der Auftraggeber verantwortlich.

Leistung ,,E-Mail“

- Administrator-Zugang nur per kryptografischem Schlüssel („SSH-Keys“) durch berechtigte Mitarbeiter des Auftragsnehmers
- Kunden-Zugang (E-Mail-Abruf und -Versand) durch ein vom Kunden zu vergebendes, dem Auftragnehmer nicht bekanntes, Passwort. Das Passwort muss der aktuellen Kennwortrichtlinie entsprechen.
- Mit Zustimmung des Auftraggebers wird der Auftragnehmer für bestimmte Operationen (derzeit: E-Mail-Import) ein temporäres, dem Auftragnehmer bekanntes, Passwort setzen. Nach Abschluss der Operation wird das Passwort auf den ursprünglichen kryptografischen Hash zurückgesetzt.
- Die Login-Versuche für E-Mail-Accounts werden innerhalb eines Zeitfensters begrenzt (,,Rate limiting“).

3 Vertraulichkeit: Zugriffskontrolle

Leistung ,,Cloud-VPS“ Die Zugriffskontrolle liegt in der Verantwortung des Auftraggebers.

Leistung ,,Webhosting“

- Der Auftragnehmer wird durch zeitnahes Einspielen von Sicherheitsupdates die Zugriffskontrolle sicherstellen
- Für die übertragenen Daten und installierte Software ist der Auftraggeber in Bezug auf Zutrittskontrolle und Updates verantwortlich

Leistung „E-Mail“ Der Auftragnehmer wird durch zeitnahes Einspielen von Sicherheitsupdates die Zugriffskontrolle sicherstellen

4 Vertraulichkeit: Datenträgerkontrolle

Festplatten werden bei Außerbetriebnahme einzelner Festplatten oder gesamter Serversysteme mehrfach überschrieben und damit sicher gelöscht. Defekte Festplatten, die nicht sicher gelöscht werden können, werden physikalisch unbrauchbar gemacht bzw. vernichtet.

5 Vertraulichkeit: Trennungskontrolle

- Für interne Verwaltungs- und Administrationssysteme des Auftragnehmers werden Daten physisch oder logisch getrennt von anderen Daten gespeichert. Die Datensicherung erfolgt ebenfalls physisch oder logisch getrennt.
- Test- und Produktionssysteme sind logisch getrennt.

Hauptauftrag „Cloud-VPS“ Die Trennungskontrolle ist vom Auftragnehmer zu verantworten.

Hauptauftrag „Webhosting“ und „E-Mail“

- Die Daten werden physisch oder logisch getrennt von anderen Daten gespeichert. Die Datensicherung erfolgt ebenfalls physisch oder logisch getrennt.
- Test- und Produktionssysteme sind logisch getrennt.

6 Vertraulichkeit: Pseudonymisierung

Der Auftraggeber ist für die Pseudonymisierung der Daten verantwortlich.

7 Integrität: Weitergabekontrolle

Der Auftragnehmer unterrichtet alle Mitarbeiter, die mit der Verarbeitung von personenbezogenen Daten beauftragt sind, im datenschutzkonformen Umgang mit personenbezogenen Daten und verpflichtet diese zur Einhaltung der gesetzlichen Bestimmungen.

- Der Auftragnehmer wird die Daten nach Auftragsbeendigung datenschutzgerecht löschen. Die Löschung von Daten aus Archiv- und Recovery-Systemen kann technisch bedingt mit extremem Aufwand verbunden sein. Sofern eine vorzeitige Löschung von Daten in Archiv- und Recovery-Systemen nicht zumutbar ist wird der Auftragnehmer die Daten als gelöscht markieren und für den Zugriff sperren, bis die Löschung durch den im Archiv- und Recovery-System definierten Lösch-Prozess stattfindet.
- Der Auftraggeber wird im Rahmen der technischen Möglichkeiten und der Verhältnismäßigkeit für alle Übertragungswege personenbezogener Daten eine adäquate Verschlüsselung bereitstellen. Der Auftragnehmer wird Daten ausschließlich über verschlüsselte Verbindungen übertragen, sofern diese bereitstehen.

8 Integrität: Eingabekontrolle

Kundenmenü

- Personenbezogene Daten werden im Rahmen des Kundenmenüs vom Kunden selbst eingegeben.
- Übermittelt der Kunde auf anderem Wege Daten (u.a. mündlich, schriftlich) hat er die Korrektheit der Daten selbstständig zu prüfen und notwendige Änderungen unverzüglich mitzuteilen.

Leistung „Cloud-VPS“, ,,Webhosting“, ,,E-Mail“ Die Eingabekontrolle obliegt dem Auftraggeber.

9 Verfügbarkeit und Belastbarkeit: Verfügbarkeitskontrolle

Kundenmenü

- Backup- und Recovery-Konzept mit mindestens täglicher Sicherung aller relevanten Daten
- Sachkundiger Einsatz von Sicherheitsmaßnahmen
- Einsatz von Festplattenspiegelung bei allen relevanten Servern
- Monitoring aller relevanten Systeme
- Einsatz unterbrechungsfreier Stromversorgung
- On-Demand-DDoS-Protection

Leistung ,,Cloud-VPS“

- Die Datensicherung obliegt dem Auftraggeber
- Einsatz von Festplattenspiegelung
- Einsatz unterbrechungsfreier Stromversorgung
- Der Auftragnehmer stellt dem Auftraggeber, sofern vereinbart, eine Möglichkeit für eine physikalisch getrennte und verschlüsselte Sicherung („Snapshots“) zur Verfügung. Der Auftraggeber bleibt auch bei Nutzung dieser Möglichkeit weiterhin für die Datensicherung verantwortlich. Sofern vereinbart besorgt der Auftragnehmer für den Auftraggeber die tägliche Durchführung von „Snapshots“.
- Ein Layer 3/4-DDoS-Schutz wird nach Vereinbarung bereitgestellt, der Layer-7-DDoS-Schutz obliegt dem Auftraggeber

Leistung „Webhosting“

- Backup- und Recovery-Konzept mit täglicher Sicherung der Daten, Aufbewahrungszeitraum je nach Produktbeschreibung
- Einsatz von Festplattenspiegelung
- Einsatz von Netzersatzanlagen und unterbrechungsfreier Stromversorgung
- Einsatz von Softwarefirewalls und Portbeschränkungen
- Dauerhaft aktiver Layer 3/4-DDoS-Schutz
- Dauerhaft aktiver Layer 7-DDoS-Schutz

Leistung „E-Mail“

- Backup- und Recovery-Konzept mit täglicher Sicherung der Daten
- Einsatz von Festplattenspiegelung
- Einsatz unterbrechungsfreier Stromversorgung
- Einsatz von Softwarefirewalls und Portbeschränkungen

10 Verfügbarkeit und Belastbarkeit: Rasche Wiederherstellbarkeit

Kundenmenü Der Auftragnehmer hält interne Prozesse und/oder Systeme vor, welche die rasche Wiederherstellbarkeit ermöglichen.

Leistung „Cloud-VPS“ Die Verantwortung für die rasche Wiederherstellbarkeit obliegt dem Auftraggeber. Sofern der Auftragnehmer dem Kunden die Möglichkeit „Snapshots“ zu erstellen einräumt wird zusätzlich die Möglichkeit bereitgestellt, Snapshots über das Kundenmenü selbst wiederherzustellen.

Leistung „Webhosting“ Der Auftragnehmer stellt dem Auftraggeber im Kundenmenü die Möglichkeit zur Verfügung, Sicherungen von Datenbanken und Dateien selbst wiederherzustellen.

Leistung „E-Mail“ Der Auftragnehmer hält interne Prozesse und/oder Systeme vor, welche die rasche Wiederherstellbarkeit ermöglichen.

11 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Die Mitarbeiter werden regelmäßig im Datenschutz geschult, insbesondere im Hinblick auf die Verarbeitung von personenbezogenen Daten im Auftrag.
- Datenschutzfreundliche Voreinstellungen werden bei der Softwareentwicklung berücksichtigt. Bestehende Systeme werden laufend auf ihre Datenschutzfreundlichkeit evaluiert.