

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Zwischen

Uberspace

vertreten durch
Jonas Pasche
Kaiserstr. 15
55116 Mainz

– nachfolgend „Auftragsverarbeiter“ genannt –

und

Praxis für Physiotherapie Gröger
Hofer Straße 7
95119 Naila

– nachfolgend „Verantwortlicher“ genannt –

wird der nachfolgende Vertrag zur Datenverarbeitung im Auftrag im Sinne von Art. 28 Datenschutz-Grundverordnung (DSGVO) geschlossen.

1. Gegenstand dieses Vertrages über die Datenverarbeitung im Auftrag (Art. 28 Abs. 1 DSGVO)

1.1 Gegenstand des Vertrages ist die Bereitstellung von Webhosting-Dienstleistungen sowie der damit im Zusammenhang stehenden Leistungen wie z.B. E-Mail, Domainregistrierung, etc. durch den Auftragsverarbeiter. Im Rahmen dieses Vertrages hat der Verantwortliche unter Nutzung u.a. z.B. eines Webserver, SFTP-Servers oder SSH-Zugangs die Möglichkeit, Daten zu verarbeiten (zu speichern, zu verändern, zu übermitteln und zu löschen). Die Tätigkeit des Auftragsverarbeiters beschränkt sich dabei auf die Bereitstellung der IT-Infrastruktur, dem sog. „Uberspace“.

1.2 Gegenstand des Vertrages ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter. Im Zuge der Leistungserbringung des Auftragsverarbeiters als IT-Dienstleister im Bereich des Hostings, des Supports bzw. der Administration von Server-Systemen des Verantwortlichen, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden.

1.3 Die Einzelheiten ergeben sich aus dem Hauptvertrag, der unter dem genannten Benutzernamen geführt wird. Die Vereinbarung zur Auftragsverarbeitung findet

Anwendung auf das gesamte Dienstleistungsverhältnis, sofern die in Punkt 1.1 beschriebenen Dienstleistungen betroffen sind.

1.4 Soweit nachfolgend von Daten die Rede ist, handelt es sich ausschließlich um personenbezogene Daten im Sinne der DSGVO. Die nachfolgenden Datenschutz- und Datensicherheitsbestimmungen finden Anwendung auf alle Leistungen der Auftragsverarbeitung i.S.d. Art. 28 Abs. 1 DSGVO, die der Auftragsverarbeiter gegenüber dem Verantwortlichen erbringt und auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragsverarbeiters oder durch den Auftragsverarbeiter beauftragte Dritte mit personenbezogenen Daten des Verantwortlichen in Berührung kommen können.

1.5 In Ergänzung zu dem/den zwischen den Parteien geschlossenen Vertrag/Verträgen konkretisieren die Vertragsparteien mit vorliegendem Vertrag zur Auftragsverarbeitung die gegenseitigen Pflichten im generellen Umgang mit den Daten des Verantwortlichen.

2. Laufzeit, Beendigung, Löschung von Daten (Art. 28 Abs. 1 DSGVO)

2.1 Die Laufzeit des Vertrages richtet sich nach der Dauer der Erbringung von Hosting-Leistungen des Auftragsverarbeiters an den Verantwortlichen. Der Auftrag endet, wenn der Verantwortliche keine Hosting-Leistungen des Auftragsverarbeiters, entsprechend den Leistungsvereinbarungen/Angeboten der einzelnen Auftragsbestätigungen für Hosting-Leistungen des Auftragsverarbeiters, mehr in Anspruch nimmt.

2.2 Die Rechte der durch den Datenumgang durch den Auftragsverarbeiter betroffenen Personen, insbesondere auf Berichtigung, Löschung und Sperrung, sind gegenüber dem Verantwortlichen geltend zu machen. Er ist allein verantwortlich für die Wahrung dieser Rechte. Unterstützung leistet der Auftragsverarbeiter in dem Maße, in dem das Wesen seiner Dienstleistung eine Einflussnahme auf die Wahrung der Betroffenenrechte zulässt.

2.3 Nach Ende des Auftrags oder auf schriftliche Aufforderung durch den Verantwortlichen hat der Auftragsverarbeiter sämtliche Daten des Verantwortlichen vollständig datenschutzgerecht zu löschen (einschließlich der verfahrens- oder sicherheitstechnisch notwendigen Kopien) oder - im Fall physisch ausgehändigter Medien - an den Verantwortlichen zurückzugeben. Die Löschung von durch den Auftragsverarbeiter angefertigten Datensicherungen erfolgt aus technischen Gründen mit einem zeitlichen Versatz von 7 Wochen im automatisierten Verfahren. Das gleiche gilt auch für Test- und Ausschussmaterial, das bis zur Löschung oder Rückgabe unter datenschutzgerechtem Verschluss zu halten ist. Dies gilt nicht für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen oder soweit z.B. rechtliche Regelungen, gesetzliche Pflichten oder gerichtliche Verfügungen dem entgegenstehen. Entstehen durch eine Löschung vor Vertragsbeendigung zusätzliche Kosten, so trägt diese der Verantwortliche.

2.4 Der Auftragsverarbeiter ist verpflichtet, im Rahmen seiner Tätigkeit für den

Verantwortlichen an ihn gerichtete Ersuchen Betroffener zur sachgerechten Bearbeitung unverzüglich an den Verantwortlichen weiterzuleiten. Er ist nicht berechtigt, diese Ersuchen ohne Abstimmung mit dem Verantwortlichen selbständig zu bescheiden.

2.5 Der Auftragsverarbeiter hat den Verantwortlichen bei der Umsetzung der Rechte der Betroffenen nach Kapitel III der DSGVO, insbesondere im Hinblick auf Berichtigung, Sperrung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen der technischen Möglichkeiten, insbesondere hinsichtlich des Charakters der geschuldeten Dienstleistung, zu unterstützen.

2.6 Zu einem Datenträgeraustausch gemäß Art. 28 Abs. 3 lit. g DSGVO zwischen den Beteiligten dieser Auftragsdatenverarbeitung kommt es nicht. Die Rückgabe von Datenträgern bedarf insofern keiner Regelung.

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

3.1 Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten ergeben sich aus dem zwischen den Vertragsparteien bestehenden Hauptvertrag.

Der Auftragsverarbeiter ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden. Dem Auftragsverarbeiter ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikatsdateien zur leistungsgemäßen Erhebung, Verarbeitung und / oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt. Dem Auftragsverarbeiter ist nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.

Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Daten aus Adressbüchern und Verzeichnissen dürfen nur zur Kommunikation im Rahmen der Auftragserfüllung mit dem Verantwortlichen verwendet werden. Eine anderweitige Nutzung und Übermittlung für eigene oder fremde Zwecke, einschl. Marketingzwecke, ist nicht gestattet.

3.2 Soweit seitens des Auftragsverarbeiter eine Erhebung, Verarbeitung und / oder Nutzung der Daten erfolgt, geschieht dies ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Jede Verlagerung in ein anderes Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 DSGVO erfüllt sind.

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

Der Auftragsverarbeiter hat keinen Einfluss auf die Art der Daten und den Kreis der Betroffenen.

5. Pflichten des Auftragsverarbeiters

5.1 Allgemeine Pflichten, Art. 28-33 DSGVO

5.1.1 Der Auftragsverarbeiter verpflichtet sich zu einer schriftlichen Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 37, 38 DSGVO ausüben kann. Dessen Kontaktdaten werden dem Verantwortlichen auf Anforderung, zum Zweck der direkten Kontaktaufnahme, mitgeteilt.

5.1.2 Soweit seitens des Auftragsverarbeiters eine Erhebung, Verarbeitung und / oder Nutzung der Daten erfolgt, ist dies nur zulässig im Rahmen der vertraglichen Vereinbarungen zwischen Verantwortlichem und Auftragsverarbeiter. Soweit der Auftragsverarbeiter Zugriff auf Daten des Verantwortlichen hat, verwendet er diese nicht für vertragsfremde Zwecke, insbesondere gibt er diese an Dritte nur weiter, soweit hierzu eine gesetzliche Verpflichtung besteht. Kopien von Daten dürfen nur mit Zustimmung des Verantwortlichen erstellt werden. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder Erfüllung vertraglicher oder gesetzlicher Verpflichtungen erforderlich sind.

5.1.3 Der Auftragsverarbeiter stellt die Wahrung der Vertraulichkeit entsprechend Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO sicher. Alle Personen, die auftragsgemäß auf die unter Punkt 4.1 aufgeführten Daten der Verantwortlichen zugreifen könnten, müssen auf die Vertraulichkeit verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

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

5.1.5 Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich bei von ihm oder der bei ihm beschäftigten Personen begangenen Verstößen gegen Datenschutzvorschriften. Gleiches gilt im Falle schwerwiegender Störungen des Betriebsablaufs oder anderen Unregelmäßigkeiten im Umgang mit Daten des Verantwortlichen. Soweit den Verantwortlichen Pflichten nach Art. 32 und 33 DSGVO treffen, hat der Auftragsverarbeiter ihn hierbei zu unterstützen. Soweit den Verantwortlichen Pflichten nach Art. 32-36 DSGVO treffen, z.B. im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten durch Dritte, hat der Auftragsverarbeiter ihn hierbei im Rahmen des Charakters der durch den Auftragsverarbeiter erbrachten Dienstleistung zu unterstützen.

5.2 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

5.2.1 Der Auftragsverarbeiter gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er trifft dabei technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten vor Missbrauch und Verlust, um den Anforderungen der DSGVO zu entsprechen.

5.2.2 Die Parteien sind sich einig, dass die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der Weiterentwicklung unterliegen. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Er muss den Verantwortlichen hierüber auf Anfrage informieren und sicherstellen, dass das Sicherheitsniveau der festgelegten Maßnahme nicht unterschritten wird. Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Wesentliche Änderungen sind zu dokumentieren.

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

6.1 Der Verantwortliche ist damit einverstanden, dass der Auftragsverarbeiter zur Erfüllung seiner vertraglich vereinbarten Leistungen, insbesondere, aber nicht ausschließlich, für die Bereiche Wartung und Installation der Rechenzentrumsinfrastruktur, Telekommunikationsdienstleistungen und Benutzerservice, verbundene Unternehmen des Auftragsverarbeiters zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt.

6.2 Erteilt der Auftragsverarbeiter Aufträge an Unterauftragnehmer („weitere Auftragsverarbeiter“), so obliegt es dem Auftragsverarbeiter, seine Pflichten aus diesem Vertrag zur Auftragsverarbeitung dem Unterauftragnehmer bzw. weiteren Auftragsverarbeiter zu übertragen.

6.3 Die Auftragsverarbeiter trägt dafür Sorge, dass der Verantwortliche eine aktuelle Liste der eingesetzten Unterauftragnehmer bzw. weiteren Auftragsverarbeiter auf der Website bzw. im Dashboard stets zum Abruf zur Verfügung steht. Bei Änderung dieser Liste in Bezug auf die Hinzuziehung oder Ersetzung von weiteren Auftragsverarbeitern ergeht hierüber eine Information an den Verantwortlichen.

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

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

7.2 Der Verantwortliche hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er Verstöße des Auftragsverarbeiters gegen datenschutzrechtliche

Bestimmungen feststellt.

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

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

8.1 Der Verantwortliche hat selbst jederzeit umfassenden Zugriff auf die Daten, so dass es einer Mitwirkung des Auftragsverarbeiters insbesondere auch zu Berichtigung, Sperrung, Löschung etc. nicht bedarf. Soweit eine Mitwirkung des Auftragsverarbeiters erforderlich ist, ist der Auftragsverarbeiter hierzu gegen Erstattung der anfallenden angemessenen Kosten verpflichtet. Dem Verantwortlichen steht in diesem Fall ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung gemäß Art. 29 i.V.m. 28 DSGVO zu. Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch eine hierzu befugte Person beim Verantwortlichen bestätigt oder geändert wird.

8.2 Soweit ein Betroffener sich unmittelbar an den Auftragsverarbeiter zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragsverarbeiter dieses Ersuchen an den Verantwortlichen weiterleiten. Ist der Verantwortliche aufgrund geltender Datenschutzgesetze verpflichtet, Auskünfte zur Erhebung, Verarbeitung und / oder Nutzung von Daten zu erteilen, wird der Auftragsverarbeiter den Verantwortlichen dabei soweit notwendig bei der Bereitstellung dieser Informationen unterstützen. Eine diesbezügliche Anfrage hat der Verantwortliche schriftlich an den Auftragsverarbeiter zu richten und diesem die hierdurch entstandenen Kosten zu erstatten.

9. Kontrollrechte des Verantwortlichen

9.1 Der Verantwortliche hat das Recht, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

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

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

Auftragsverarbeiter in seinem Geschäftsbetrieb zu überzeugen. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Kosten, die dem Auftragsverarbeiter durch seine Unterstützungshandlung entstehen, sind ihm im angemessenen Umfang zu erstatten (Auditkosten).

9.4 Im Hinblick auf die Kontrollverpflichtungen des Verantwortlichen nach Art. 28 Abs. 1 DSGVO vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragsverarbeiter sicher, dass der Verantwortliche sich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann.

9.5 Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die zur Wahrung ihrer bei der Verarbeitung der oben genannten Daten bestehende Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und Nachweise zu führen. Dies gilt auch, soweit der Auftragsverarbeiter die Kontrolle seiner Unterauftragnehmer bzw. weiteren Auftragsverarbeiter für den Verantwortlichen durchführt.

10. Salvatorische Klausel, Gerichtsstand

10.1 Sollte eine Bestimmung dieses Vertrages ungültig oder undurchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieses Vertrages hiervon unberührt. Die Parteien vereinbaren, die ungültige oder undurchsetzbare Bestimmung durch eine gültige und durchsetzbare Bestimmung zu ersetzen, welche wirtschaftlich der Zielsetzung der Parteien am nächsten kommt. Das Gleiche gilt im Falle einer Regelungslücke.

10.2 Als Gerichtsstand wird Mainz vereinbart.

*Dieser Vertrag wurde am **30.07.2018** durch **Jutta Gröger** als Vertreter des Verantwortlichen online abgeschlossen.*

Anhang: Technische und organisatorische Maßnahmen

Die folgende Aufstellung umfasst die technischen und organisatorischen Maßnahmen zum Zeitpunkt des Vertragsschlusses des obigen Vertrags. Sie können gemäß § 5.2.2 des obigen AV-Vertrags jederzeit im Sinne des technischen Fortschritts erweitert und verbessert werden. Die jeweils aktuelle Fassung kann jederzeit auf der Website von Uberspace im Bereich Datenschutz abgerufen werden.

Anlage technische und organisatorische Maßnahmen (TOM)

Maßnahmen gemäß DSGVO (Sicherheit der Verarbeitung)

Stand 24.05.2018

Pseudonymisierung und Verschlüsselung

Die Pseudonymisierung und Verschlüsselung personenbezogener Daten (§ 32a DSGVO).

Pseudonymisierung

- Die Maßnahmen der Pseudonymisierung obliegt dem Verantwortlichen.

Verschlüsselung

Maßnahmen beim Produkt Uberspace:

- Verschlüsselung von Datenübertragungen beim Erstellen externer Backups.
- Verschlüsselung von Datenübertragungen zwischen Uberspace Dashboard und Uberspace Account.
- Bereitstellung verschlüsselter Übertragungswege wie sftp, ssh oder https.

Maßnahmen bei Produkten Plesk, Dedicated Hosting und Housing

- Die Maßnahmen der Verschlüsselung obliegt dem Verantwortlichen.
- Verschlüsselung von Datenübertragungen beim Erstellen externer Backups.

Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

Die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen (§ 32b DSGVO).

Vertraulichkeit

Zutrittskontrolle (Räume)

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

- Werkschutz, Pförtner
- Verwaltung von personengebundenen Zutrittsberechtigungen
- Festlegung Zutrittsberechtigter Personen

- Protokollierung des Zutritts
- Festlegung von Sicherheitsbereichen
- Videoüberwachung der Zugänge
- Sicherheitstüren (Chipkarten-/Transponder-Schließsystem)
- Sicherheitsschlösser Serverschränke
- Tragepflicht von Mitarbeiter- / Gästerausweisen

Zugangskontrolle (Oberflächen)

Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahmen bei internen Verwaltungssystemen des Auftragsverarbeiters:

- Authentifikation mit Benutzer + Passwort
- Passwortvergabe / Passwortregeln
- Zwei-Faktor-Authentifikation wenn möglich
- Individuelle Schlüssel pro Mitarbeiter und Arbeitsgerät
- Sorgfältige Auswahl von Reinigungspersonal

Maßnahmen bei Produkten Uberspace, Plesk, Dedicated Hosting und Housing

- Die Maßnahmen der Zugangskontrollen obliegen dem Verantwortlichen.

Zugriffskontrolle (Dateien)

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.

Maßnahmen bei internen Verwaltungssystemen des Auftraggebers:

- Zertifizierte Aktenvernichtung durch Dienstleister

Maßnahmen bei Produkten Uberspace, Plesk, Dedicated Hosting und Housing

- Die Maßnahmen der Zugriffskontrolle obliegt dem Verantwortlichen.
- Bei den Produkten Uberspace, Plesk oder durch vertraglicher Vereinbarung werden regelmäßige Sicherheitsupdates eingespielt, die unberechtigte Zugriffe auf Grund von Sicherheitslücken unterbinden sollen.

Datenträgerkontrolle

Maßnahmen beim Produkt Housing:

- Beim Produkt Housing erfolgt Übergabe dekommissionierter Hardware zurück an Kunden. Die Maßnahmen der Datenträgerkontrolle obliegt dann dem Verantwortlichen.

Maßnahmen bei Produkten Uberspace, Plesk und Dedicated Hosting

- Physikalische Zerstörung von dekommissionierten Datenträgern.

Trennungsgebot

Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen beim Produkt Uberspace:

- Trennung Produkt, Support-Ticketsystem, Bankdaten und Kundendatenbank.

Maßnahmen bei Produkten Plesk, Dedicated Hosting und Housing

- Die Maßnahmen des Trennungsgebotes obliegen dem Verantwortlichen.

Auftragskontrolle

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

- Auswahl weiterer Auftragsverarbeiter unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit).
- Abschluss von Auftragsverarbeitungsverträgen.
- Beauftragte Verarbeitung durch Auftragnehmer nur nach genauer Anweisung.

Integrität

Weitergabekontrolle (Transport)

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.

- Sorgfältige Auswahl von Transportpersonal und -fahrzeugen.
- Maschinen-Authentifikation bei netzbasierten automatisierten Übertragungsvorgängen.

Verfügbarkeit

Verfügbarkeitskontrolle

Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Automatische Brandlöschung
- Feuer- und Rauchmeldeanlagen

- Unterbrechungsfreie Stromversorgung
- Überwachte Stromverteilungssysteme
- Klimaanlage in Serverräumen
- Testen der Datenwiederherstellung
- Einsatz aktueller Technologien zur Reduzierung von Ausfällen je nach Produkt (Beispiel: Clusterbetrieb)
- Erstellen von Backup- und Recoverykonzepten

Belastbarkeit

Belastbarkeitskontrolle

- Zutrittskontrolle Rechenzentrum
- Zugangskontrollen Mitarbeiter
- 24/7 Monitoring aller relevanten Systeme
- Netzwerk-Firewalls
- Rate-Limits der Netzwerkdienste

Wiederherstellbarkeit

Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (§ 32c DSGVO).

Wiederherstellbarkeit

Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind?

- 24/7 Monitoring aller relevanten Systeme
- 24/7 Bereitschaftsdienst
- Regelmäßige Datensicherung (Backup- und Restorekonzept)

Überprüfung

Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (§ 32d DSGVO).

Verfahren zur regelmäßigen Überprüfung

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

- Automatische Überprüfung und Alarmierung auf Aktualität der Datensicherungen

Verarbeitung personenbezogener Daten nur nach Anweisung

Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des

Verantwortlichen verarbeitet werden?

- Benennung des Datenschutzbeauftragten
- Verpflichtung der Mitarbeiter auf Vertraulichkeit