Vereinbarung

über die

Auftragsverarbeitung nach Art 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

zwischen

Firma	
Name & Funktion	
Adresse	
PLZ, Ort	
Datum	

- Auftraggeber, der Verantwortliche, der Kunde -

und

Firma	viennatec webservices & veranstaltungstechnik gmbh
Name & Funktion	Rainer Madritsch, geschäftsführender Gesellschafter
Adresse	Nothartgasse 12
PLZ, Ort	1130 Wien
Datum	07.05.2018

- **Auftragnehmer, der Auftragsverarbeiter -**

gültig ab 25.05.2018.

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertrag vom

Datum:

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 mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1) Gegenstand des Auftrags ist die Bereitstellung von Hosting-Lösungen bzw. eines (oder mehrerer) dedizierten/dedizierter Webserver sowie der damit im Zusammenhang stehenden Leistungen wie z.B. E-Mail, Domainregistrierung, etc. . Im Rahmen dieses Vertrages hat der Auftraggeber – je nach Tarif und vereinbartem Leistungsumfang – unter Nutzung u.A. z.B. eines Webservers, FTP-Servers, MySQL-Servers, E-Mail Server oder SSH (insoweit verfügbar) die Möglichkeit, Daten zu verarbeiten (zu speichern, zu verändern, zu übermitteln und zu löschen).
2) Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben. Der Auftrag endet, wenn der Auftraggeber keine Hosting-Leistungen des Auftragnehmers, entsprechend den Leistungsvereinbarungen/Angeboten der einzelnen Auftragsbestätigungen für Hosting-Leistungen des Auftragnehmers, mehr in Anspruch nimmt.

§ 2 Anwendungsbereich und Verantwortlichkeit

1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung 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 DSGVO).

2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

3) 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 Auftragnehmer 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 Rechte und Pflichten des Auftraggebers

1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 6 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen. Wendet sich eine betroffene Person mit Forderungen zur Auskunft, Berichtigung, Sperrung oder Löschung 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. Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen.

4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der Anlage 1 benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

§ 4 Allgemeine Pflichten des Auftragnehmers

1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen im Sinne des Artikel 28 Abs. 3 a) DSGVO, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.
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. 32 DSGVO) 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. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt (vgl. Anlage 2). Er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.
3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.
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) Die direkte Verarbeitung der personenbezogenen Daten durch den Auftragnehmer 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 schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 DSGVO erfüllt sind. Falls ein Unterauftragnehmer beauftragt werden soll, gelten diese Anforderungen ebenfalls für diese.

6) 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.

7) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der Anlage 1 benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

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

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 oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

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

10) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. 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 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

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

§ 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.
2) Sollten im Einzelfall 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 hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Der Auftraggeber stimmt der Benennung eines unabhängigen externen Prüfers durch den Auftragnehmer zu, sofern der Auftragnehmer eine Kopie des Auditberichts zur Verfügung stellt.
3) Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.
4) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

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) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen, insbesondere, aber nicht ausschließlich, für die Bereiche Wartung und Installation der Rechenzentrumsinfrastruktur, Telekommunikations-Dienstleistungen und Benutzerservice, verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt.

3) Der Auftragnehmer trägt dafür Sorge, dass der Auftraggeber eine aktuelle Liste der eingesetzten UnterAuftragnehmer im Kundenportal stets zum Abruf zur Verfügung steht. Bei Änderung dieser Liste in Bezug auf die Hinzuziehung oder Ersetzung von weiteren Auftragnehmern ergeht hierüber eine Information an den Auftraggeber.

4) Erteilt der Auftragnehmer Aufträge an Unter-Auftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Auftragsverarbeitungsvertrag dem UnterAuftragnehmer zu übertragen.

§ 8 Geheimhaltungspflichten

1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 9 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 des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so

berührt dies die Wirksamkeit der Anlage im übrigen nicht.

4) Es gilt österreichisches Recht.

§ 10 Haftung und Schadensersatz

1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.
2) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verbreiteten Daten und der zugehörigen Datenträger ausgeschlossen.

§ 11 Ort der Durchführung der Datenverarbeitung

Datenverarbeitungstätigkeiten werden zumindest zum Teil auch außerhalb der EU bzw des EWR durchgeführt, und zwar in Staaten in denen einzelne Leistungen des Auftraggebers bezogen werden. Z.B. .com Domain-Registrierung.

Das angemessene Datenschutzniveau ergibt sich aus

1) Einer Ausnahme für den bestimmten Fall nach Art 49 Abs 1 DSGVO.
2) Einer Ausnahme für den Einzelfall nach Art 49 Abs 1 Unterabsatz 2 DSGVO.

Auftraggeber

Name & Funktion	
Ort, Datum	
Unterschrift	

Weisungsberechtigte Person des Auftraggebers

Name & Funktion	
Ort, Datum	
Unterschrift	

Auftragnehmer

Name & Funktion	Rainer Madritsch, geschäftsführender Gesellschafter
Ort, Datum	Wien,
Unterschrift	

Anlagen:

1) Gegenstand des Auftrags
2) Technische und organisatorische Maßnahmen

Anlage 1

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst die Bereitstellung von Hosting-Lösungen bzw. eines (oder mehrerer) dedizierten/dedizierter Webserver sowie der damit im Zusammenhang stehenden Leistungen wie z.B. E-Mail, Domainregistrierung, etc. im Rahmen der vom Auftragnehmer auf dessen Webseiten angebotenen und in den jeweiligen Leistungsbeschreibungen konkretisierten Produkte.

2. Art(en) der personenbezogenen Daten*

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- ☐ Adressdaten
- ☐ Abrechnungsdaten
- ☐ Angebotsdaten
- ☐ Finanzdaten
- ☐ Bankverbindungsdaten
- ☐ Bestelldaten
- ☐ E-Mail-Nachrichten
- ☐ Mitarbeiterdaten
- ☐ Vertragsdaten
- ☐ Stammdaten
- ☐ Nutzungsdaten
- ☐ Videos / Bilder
- ☐

* Zutreffendes vom Auftraggeber anzukreuzen

3. Kategorien betroffener Person*

Kreis der von der Datenverarbeitung betroffenen Personen:

- ☐ Kunden
- ☐ Mitarbeiter
- ☐ Angehörige
- ☐ Nutzer
- ☐ Auszubildende
- ☐ Unterhaltsberechtigte
- ☐ Interessenten
- ☐ Bewerber
- ☐ Ruheständler
- ☐ Kontaktpersonen
- ☐ Praktikanten
- ☐ Pressevertreter
- ☐ Lieferanten / Dienstleister
- ☐ frühere Mitarbeiter
- ☐ Geschädigte
- ☐ Geschäftspartner
- ☐ Berater
- ☐ Zeugen
- ☐ Gesellschafter
- ☐ Mitglieder
- ☐ Makler / Vermittler
- ☐ Mieter
- ☐

* Zutreffendes vom Auftraggeber anzukreuzen

Anlage 2

Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit

Zutrittskontrolle

1) Zutrittssystem zur Rechenzentrums-Fläche nach Anmeldung und vorheriger Avisierung und Dokumentation (Lichtbildausweis).
2) Zutritt zu Server-Racks mittels KEY Card und Fingerabdruck
3) Videoüberwachung der Außenbereiche und Räume mit Aufzeichnung
4) Detektierte Zaunanlage zur Abgrenzung des Gebäudes
5) 24 Stunden / 7 Tage besetzter Leitstand auf dem Gelände
6) 24 Stunden / 7 Tage Sicherheitspersonal vor Ort
7) Zertifizierung des Betreibers (InterXion Österreich GmbH, Wien):
   BSI ISO 22301, BSI ISO 27001

Zugangskontrolle

1) Der Auftragnehmer vermietet die Datenverarbeitungsanlage an den Kunden.
2) Dies beinhaltet die Vermietung von Hard- und Software, sowie die Bereitstellung von Anbindungen an das Internet sowie weitere Dienste entsprechend der jeweiligen Vereinbarung.
3) Der Kunde entscheidet allein und ausschließlich darüber, welche personenbezogenen Daten in welcher Weise verarbeitet werden („Herr der Daten“).
4) Die hierfür erforderlichen Programme zur Datenverarbeitung werden durch den Kunden erstellt und eingesetzt.
5) Der Auftragnehmer sorgt für die technische Einsatzbereitschaft des Systems entsprechend den vertraglichen Vereinbarungen und führt Aufzeichnungen darüber, welche Anlagen durch den Kunden in welchem Umfang genutzt werden
6) Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.
7) Besonderheiten für Webhosting-Kunden und Managed-Server-Kunden: Der Auftragnehmer nutzt autorisierte Benutzerkennungen (Benutzernamen, User, Keys) und individuelle, sichere Passwörter für den Zugang zu Datenverarbeitungssystemen. Die konkreten Verarbeitungsvorgänge beim Kunden sind dem Auftragnehmer nicht bekannt. Insofern obliegt es dem Kunden durch softwaretechnische Gestaltungen dafür Sorge zu tragen, dass die Datenverarbeitungssysteme von Unbefugten nicht genutzt werden können.

8) Besonderheiten für Root-Server-Kunden: Bei Root-Servern haben Mitarbeiter vom Auftragnehmer keinerlei Zugang. Dementsprechend obliegt es dem Kunden, das System zu sichern.

Zugriffskontrolle

1) Der Auftragnehmer hat keinen Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme, so dass der Zugriff auf Daten ausschließlich durch den Kunden erfolgen kann
2) Mitarbeiter des Auftragnehmers sind zur Einhaltung der datenschutzrechtlichen Gesetze und Regelungen verpflichtet und entsprechend geschult.
3) Adäquate Protokollierung der Tätigkeiten vom Auftragnehmer.
4) Webhosting & Managed-Server-Kunden: Monitoring und Wartung der Systeme durch den Auftragnehmer mit adäquater Protokollierung der Administrationszugriffe.
5) Bei Root-Servern haben unsere Mitarbeiter keinerlei Zugang. Ein Zugriff auf Daten erfolgt nur, insoweit der Kunde dem Auftragnehmer explizit mit einer Administrationsaufgabe beauftragt und einen Zugang einrichtet.

Trennungskontrolle

1) Bitte beachten Sie hierzu unsere Ausführungen unter „Zugangskontrolle“ und „Zugriffskontrolle“.
2) Es liegt eine physikalische oder logische Trennung einzelner Kundensysteme vor.
3) Jedes System verfügt über ein Berechtigungskonzept.

Pseudonymisierung & Verschlüsselung

1) Für die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten ist der Kunde verantwortlich, soweit dies nach dem Verwendungszweck möglich ist und keine im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

2. Integrität

Eingabekontrolle

1) Mitarbeiter vom Auftragnehmer dürfen grundsätzlich nicht auf Daten des Kunden zugreifen bzw. Daten eingeben, verändern oder löschen.
2) Der Auftragnehmer hat keinen Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme, so dass der Zugriff auf Daten ausschließlich durch den Kunden erfolgen kann.
3) Bei einer Beauftragung vom Auftragnehmer durch den Kunden erfolgt eine Aufzeichnung von Mitarbeiterzugriffen auf Daten des Kunden in Logfiles gemäß gesetzlicher Bestimmungen.
4) Sperrungen erfolgen aus rechtlichen oder technischen Gründen sowie im Falle des Zahlungsverzuges. Die Vornahme von Sperrungen wird protokolliert.
5) Die Löschung erfolgt nach dem Vertragsende automatisiert und wird protokolliert.

Weitergabekontrolle

1) Verschlüsselte Datenkommunikation für administrative Aufgaben seitens des Auftragnehmers, z.B. per TLS/SSL-Verschlüsselung
2) Verschlüsselter Transport von E-Mails (TLS/SSL)
3) Dem Kunden obliegt es durch eine Verschlüsselung, z.B. Einsatz eines SSL-Zertifkats, dafür zu sorgen, dass auch vom Kunden gespeicherte, übertragene Daten nicht lesbar sind.
4) Zugriffsrechte der einzelnen Mitarbeiter des Auftragnehmers orientieren sich an der Erforderlichkeit für die Aufgabenerfüllung (z.B. Administratoren im Rahmen der Verwaltung der Netzwerkhardware oder zur Wartung der Systeme)

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeit

1) Maßnahmen zum Brandschutz und bei Stromausfällen
    - N+1 redundant ausgelegte Klimatisierungssysteme
    - Konstante Raumtemperatur von 24° (+2/-4°)
    - Temperaturüberwachung mittels Sensoren
    - Optische/thermische Brandmelder auf zwei Ebenen (Rohdecke und Doppelboden)
    - Aktive Brandlöschung durch Inergen-Löschanlage, Doppelboden- oder Raumlöschung
    - Zwei unabhängige Stromversorgungen (A+B-Feed)
    - N+1 redundante, USV-gesicherte 3 Tage Stromversorgung mit Batterie-Backup
    - Redundante Netzwerkanbindung

Für darüber hinausgehende Schutzmaßnahmen, insbesondere auf der Ebene des Betriebssystems bei Root-Server und bei Programmierung auf Speicherebene, ist der Kunde verantwortlich. Der Auftragnehmer bietet Optionen zur Sicherstellung durch den Abschluss von individuellen Service-Level-Agreements und Backup-Tarifen.

Belastbarkeit

Alle Systeme, welche für die Infrastruktur der Dienstleistung vom Auftragnehmer relevant sind, werden redundant vorgehalten und überwacht. Für die Belastbarkeit der Systeme des Kunden ist der Kunden selbst verantwortlich. Es können Schutzmaßnahmen aktiviert werden, um DOS- und DDOS-Angriffe auf die Systeme des Kunden abzuwehren.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1) Datenschutz-Management-System
   - Eine Datenschutzleitlinie der Unternehmensleitung
   - Richtlinien zum Umgang mit personenbezogenen Daten und der zugehörigen IT für alle Mitarbeiter
   - Verfahren, die den konkreten Umgang mit personenbezogenen Daten regeln
   - Bestellung eines Datenschutzbeauftragten (insoweit erforderlich)
2) Incident Response Management
   - Richtlinien für Mitarbeiter, wie mit möglichen Sicherheitsvorfällen umzugehen ist
   - Verfahren, wie die verantwortliche Stelle mit festgestellten oder gemeldeten Sicherheitsvorfällen umzugehen hat, insbesondere, wann ein Datenschutzbeauftragter und die Datenschutzbehörde zu involvieren ist.
3) Auftragskontrolle
   - Sorgfältige Auswahl von Auftragsverarbeitern gemäß DSGVO
   - Insofern der Auftragnehmer Subunternehmer bestellt, gelten für diese die gleichen Regelungen und Bestimmungen wie für den Auftragnehmer selbst.
   - Anweisung an Mitarbeiter des Auftragnehmers über Umfang und Inhalt der vom Kunden erteilten Weisungen
   - Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis gemäß § 6 DSG