Auftragsverarbeitungsvertrag

gemäß Art. 28 Abs. 3 S. 1 DSGVO

– nachfolgend „**AV-Vertrag**" genannt –

Zwischen dem Unternehmen / der Firma

– nachfolgend „**Auftraggeber**" genannt –

und

Peter Schober
Agnes-Bernauer-Str.69
80687 München
Deutschland

– nachfolgend „**Auftragnehmer**" genannt –

– einzeln oder gemeinsam auch als **Vertragspartei** und / oder **Vertragsparteien**

bezeichnet ein / mehrere von den Vertragsparteien abgeschlossene(r) Vertrag / Verträge.

– nachfolgend „**Hauptvertrag**" / „**Hauptverträge**" genannt –

Präambel

Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

„Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

– Verantwortlicher ist die vorstehend als Auftraggeber bezeichnete Vertragspartei –

„Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

– Auftragsverarbeiter ist die vorstehend als Auftragnehmer bezeichnete Vertragspartei –

„Unterauftragsverarbeiter" den Vertragspartner des Auftragsverarbeiters, der von diesem mit der Durchführung bestimmter Verarbeitungsaktivitäten für den Verantwortlichen beauftragt wird;

„Dritter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

„personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

„Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

„Hauptvertrag" den in Ziffer 2 näher gekennzeichneten Vertrag über die Erbringung von Internet-Dienstleistungen.

1. Gegenstand des AV-Vertrages (Art. 28 Abs. 3 DSGVO)

1.1. Der Gegenstand dieses AV-Vertrages, die im Rahmen des Auftrags durch den Auftragnehmer für den Auftraggeber verarbeiteten personenbezogenen Daten (Art. 4 Nr. 1 DSGVO; nachfolgend kurz „Daten") und die von der Verarbeitung betroffenen Personen (nachfolgend kurz „Betroffene") sowie Art, Umfang und Zwecke der Erhebung, Verarbeitung und / oder Nutzung der Daten ergeben sich aus dem zwischen den Vertragsparteien bestehenden Hauptvertrag.

1.2. In Ergänzung zu dem zwischen den Parteien bestehenden Hauptvertrag regelt dieser AV-Vertrag die gegenseitigen Rechte und Pflichten der Vertragsparteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

1.3. Die nachfolgenden Datenschutz- und Datensicherheitsbestimmungen finden Anwendung auf alle Leistungen der Auftragsverarbeitung im Sinne des Art. 28 Abs. 1 DSGVO, die der Auftragnehmer gegenüber dem Auftraggeber erbringt und auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können, wenn und soweit die in Ziffer 2.1 beschriebenen Internet-Dienstleistungen betroffen sind.

2. Gegenstand des Hauptvertrages (Art. 28 Abs. 1 DSGVO)

2.1. Gegenstand des Hauptvertrages ist das Bereitstellen und der Betrieb von virtuellen und dedizierten Webservern und das Bereitstellen von Web-Speicherplatz, die Analyse von Daten mit Tools wie Google Analytics sowie die Erbringung der damit im Zusammenhang stehenden Leistungen wie z. B. das Bereitstellen von E-Mail-Diensten und die Registrierung sowie die Betreuung / Verwaltung von Domains einschließlich diverser Service- und Sicherheitsleistungen. Im Rahmen des Hauptvertrages hat der Auftraggeber bei der Nutzung der vom Auftragnehmer zur Verfügung gestellten Dienste die Möglichkeit, Daten zu verarbeiten (zu speichern, zu verändern, zu übermitteln und zu löschen).

2.2. Gegenstand des Hauptvertrages ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer.

2.3. Im Zuge der Leistungserbringung des Auftragnehmers als zentraler IT-Dienstleister des Auftraggebers im Bereich des Hostings, der Webseiten-Betreuung und -Analyse und der Administration von Server-Systemen kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden.

3. Art der Daten und Kreis der Betroffenen sowie Art, Umfang und Zwecksetzung der Verarbeitung (Art. 28 Abs. 3, 30 Abs. 2 DSGVO)

3.1. Die Art der personenbezogenen Daten und der Kreis der betroffenen Personen sowie Art, Umfang und Zwecksetzung der Verarbeitung sind in der Anlage 1 – Einzelheiten der Datenverarbeitung zu diesem AV-

Vertrag beschrieben.

4. Weisungsberechtigte und weisungsempfangsberechtigte Personen

4.1. Die Vertragsparteien können zum Erteilen und Empfangen von Weisungen berechtigte Personen benennen. Sofern weisungsberechtigte und weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der Anlage 1 – Einzelheiten der Datenverarbeitung aufgeführt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber bzw. die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird die jeweilige Vertragspartei dies der anderen Vertragspartei unverzüglich in Textform (z. B. E-Mail, Telefax, Brief) mitteilen.

5. Rechte und Pflichten des Auftraggebers

5.1. Der Auftraggeber ist für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Der Auftraggeber ist als Verantwortlicher für die Einhaltung der datenschutzrechtlichen Vorgaben, insbesondere für die Auswahl des Auftragnehmers, die an diesen übermittelten Daten sowie erteilte Weisungen allein verantwortlich (Art. 28 Abs. 3 lit. a, 29 u. 32 Abs. 4 DSGVO). Der Auftraggeber als Verantwortlicher wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. gegebenenfalls durch Einholung von Einwilligungserklärungen) geschaffen werden, damit der Auftragsverarbeiter die vereinbarten Leistungen auch insoweit rechtsverletzungsfrei erbringen kann.

5.2. Die Rechte der durch den Datenumgang bei dem Auftragnehmer betroffenen Personen, insbesondere auf Berichtigung, Löschung und Sperrung, sind gegenüber dem Auftraggeber geltend zu machen. Er ist als Verantwortlicher für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftraggeber hat selbst jederzeit umfassenden Zugriff auf die Daten, so dass es einer Mitwirkung des Auftragnehmers in Bezug auf eine Berichtigung, Löschung und Sperrung von Daten grundsätzlich nicht bedarf.

5.3. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen in Bezug auf Art, Umfang und Verfahren der Datenverarbeitung und der Sicherheitsmaßnahmen gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen grundsätzlich in Textform (z. B. E-Mail, Telefax, Brief) erfolgen.

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

5.5. 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.

5.6. Die sich aus Art. 24 DSGVO und Art. 13 sowie Art. 14 DSGVO ergebenden Informationspflichten treffen den Auftraggeber.

6. Rechte und Pflichten des Auftragnehmers

6.1. Allgemeine Pflichten

6.1.1. Der Auftragnehmer verpflichtet sich, personenbezogene Daten ausschließlich im Rahmen des Hauptvertrages und dieses AV-Vertrages sowie unter Einhaltung der vom Auftraggeber erteilten Weisungen und nur in dem hierfür notwendigen Umfang zu verarbeiten. Eine hiervon abweichende Verarbeitung von personenbezogenen Daten ist dem Auftragnehmer untersagt, es sei denn, dass entweder der Auftraggeber dieser in Textform (z. B. per E-Mail, Telefax, Brief) zugestimmt hat oder wenn der Auftragnehmer zu der Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist. 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 (Art.

28 Abs. 3 S. 2 lit. a DSGVO).

6.1.2. Soweit der Auftragnehmer Zugriff auf Daten des Auftraggebers hat, verwendet er diese ausschließlich zur Erbringung der vertraglich vereinbarten Leistung, insbesondere gibt er diese an Dritte nur weiter, soweit er hierzu entweder vertraglich berechtigt oder gesetzlich verpflichtet ist. Daten aus Adressbüchern und Verzeichnissen dürfen nur zur Kommunikation im Rahmen der Auftragserfüllung mit dem Auftraggeber verwendet werden. Eine anderweitige Nutzung und Übermittlung für eigene oder fremde Zwecke, einschließlich Marketingzwecke, ist nicht gestattet. Dem Auftragnehmer ist nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen. Hiervon ausgenommen sind verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder Erfüllung vertraglicher oder gesetzlicher Verpflichtungen erforderlich sind.

6.2. Sicherheitskonzept und diesbezügliche Pflichten

6.2.1. Der Auftragnehmer wird die innerbetriebliche Organisation in seinem Verantwortungsbereich entsprechend den gesetzlichen Anforderungen gestalten und wird insbesondere technische und organisatorische Maßnahmen (nachfolgend bezeichnet als „TOMs") zur angemessenen Sicherung, insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit von Daten des Auftraggebers, unter Beachtung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen treffen sowie deren Aufrechterhaltung sicherstellen (Art. 28 Abs. 3 und Art. 32-39 in Verbindung mit Art 5 DSGVO). Zu den TOMs gehören insbesondere die Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungskontrolle und die Sicherung der Betroffenenrechte.

6.2.2. Die diesem AV-Vertrag zugrundeliegenden TOMs ergeben sich aus der Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers. Die Vertragsparteien sind sich darüber einig, dass die TOMs entsprechend dem technischen Fortschritt weiterentwickelt und durch adäquate Schutzmaßnahmen ersetzt werden dürfen, sofern sie das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschreiten und wesentliche Änderungen dem Auftraggeber mitgeteilt werden. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

6.2.3. Der Auftragnehmer stellt sicher, dass die zur Verarbeitung der Daten des Auftraggebers befugten Personen auf Vertraulichkeit und Verschwiegenheit (Art. 28 Abs. 3 S. 2 lit. b und Art. 29, 32 Abs. 4 DSGVO) verpflichtet und in die Schutzbestimmungen der DSGVO eingewiesen worden sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

6.2.4. Die im Rahmen des AV-Vertrages überlassenen Daten sowie Datenträger und sämtliche hiervon gefertigten Kopien verbleiben im Eigentum des Auftraggebers, sind durch den Auftragnehmer sorgfältig zu verwahren, vor Zugang durch unberechtigte Dritte zu schützen und dürfen nur mit Zustimmung des Auftraggebers, und dann nur datenschutzgerecht, vernichtet werden. Kopien von Daten dürfen nur erstellt werden, wenn sie zur Erfüllung der Leistungshaupt- und Nebenpflichten des Auftragnehmers gegenüber dem Auftragnehmer erforderlich sind (z. B. Backups).

6.2.5. Sofern dies durch die DSGVO oder ergänzende, insbesondere nationale, Vorschriften vorgegeben ist, benennt der Auftragnehmer eine(n) den gesetzlichen Vorgaben entsprechende(n) Datenschutzbeauftragte(n) und informiert den Auftraggeber entsprechend (Art. 37 bis 39 DSGVO). Sofern der Auftragnehmer zur Bestellung einer / eines Datenschutzbeauftragten gesetzlich verpflichtet ist, wird diese(r) in der Anlage 1 – Einzelheiten der Datenverarbeitung benannt.

6.3. Verarbeitung in Drittländern

6.3.1. Soweit seitens des Auftragnehmers 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 (EWR).

6.3.2. Die Auftragsverarbeitung in einem Drittland, auch durch Unterauftragsverarbeiter, bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, außer wenn der Auftragnehmer zu der Verarbeitung im Drittland durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist. 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 (Art. 28 Abs. 3 S. 2 lit. a DSGVO).

6.3.3. Die Zustimmung des Auftraggebers zur Verarbeitung im Drittland gilt im Hinblick auf die in der Anlage 2 – Unterauftragnehmer genannten Verarbeitungen als erteilt.

6.4. Informationspflichten und Mitwirkungspflichten

6.4.1. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen geltendes Datenschutzrecht verstößt, wird er den Auftraggeber unverzüglich darauf hinweisen. In diesem Fall ist der Auftragnehmer berechtigt, die Ausführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. 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 zu, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen. Im Falle offensichtlich rechtswidriger Weisungen darf der Auftragnehmer die Ausführung der Weisung ablehnen.

6.4.2. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen. Der Auftragnehmer ist verpflichtet, im Rahmen seiner Tätigkeit für den Auftraggeber an ihn gerichtete Ersuchen Betroffener zur sachgerechten Bearbeitung unverzüglich an den Auftraggeber weiterzuleiten und den Auftraggeber hierbei gemäß Art. 28 Abs. 3 S. 2 lit. e. DSGVO zu unterstützen. Er ist nicht berechtigt, diese Ersuchen ohne Abstimmung mit dem Auftraggeber selbständig zu bescheiden.

6.4.3. Für den Fall, dass der Auftragnehmer Tatsachen feststellt, welche die Annahme begründen, dass der Schutz der für den Auftraggeber verarbeiteten Daten verletzt worden ist, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig zu informieren, unverzüglich erforderliche Schutzmaßnahmen zu ergreifen, und bei der Erfüllung der dem Auftraggeber obliegenden Pflichten gemäß Art. 33 und 34 DSGVO zu unterstützen.

6.4.4. Sollte die Sicherheit der Daten des Auftraggebers durch Maßnahmen Dritter (z. B. Gläubiger, Behörden, Gerichte etc.) gefährdet sein (z. B. durch Pfändung, Beschlagnahme, Insolvenzverfahren etc.) wird der Auftragnehmer die Dritten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei dem Auftraggeber liegen und nach Rücksprache mit dem Auftraggeber, sofern erforderlich, entsprechende Schutzmaßnahmen ergreifen (z. B. Widersprüche erheben, Anträge stellen etc.).

6.4.5. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde gegenüber dem Auftragnehmer tätig wird und deren Tätigkeit die für den Auftraggeber verarbeiteten Daten betreffen kann. Der Auftragnehmer unterstützt den Auftraggeber bei der Wahrnehmung seiner Pflichten (insbesondere zur Auskunftserteilung und Duldung von Kontrollen) gegenüber Aufsichtsbehörden (Art. 31 DSGVO).

6.4.6. Der Auftragnehmer stellt dem Auftraggeber Informationen betreffend die Verarbeitung von Daten im Rahmen dieses AV-Vertrages, die für dessen Erfüllung von gesetzlichen Pflichten (zu denen insbesondere Anfragen Betroffener oder Behörden und die Einhaltung seiner Rechenschaftspflichten gemäß Art. 5 Abs. 2 DSGVO sowie auch die Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO gehören können) notwendig sind, zur Verfügung, sofern der Auftraggeber diese Informationen nicht selbst beschaffen kann. Die Informationen müssen dem Auftragnehmer zur Verfügung stehen und müssen nicht von Dritten beschafft werden, wobei Mitarbeiter, Beauftragte und Subunternehmer des Auftraggebers nicht als Dritte gelten.

Eine diesbezügliche Anfrage hat der Auftraggeber in Textform (z. B. per E-Mail, Telefax, Brief) an den Auftragnehmer zu richten und diesem die hierdurch anfallenden Kosten zu erstatten.

6.4.7. Soweit eine Mitwirkung des Auftragnehmers erforderlich ist, wird der Auftragnehmer den Auftraggeber entsprechend unterstützen. Bei Bedarf werden sich die Vertragsparteien über Inhalt und Umfang etwaiger Unterstützungsleistungen des Auftragnehmers abstimmen.

7. Kontrollrechte des Auftraggebers

7.1. Der Auftraggeber hat das Recht, vor Beginn der Datenverarbeitung und sodann regelmäßig die Einhaltung der gesetzlichen Vorgaben und der Regelungen dieses AV-Vertrages, insbesondere der TOMs, beim Auftragnehmer im erforderlichen Umfang zu kontrollieren (Art. 28 Abs. 3 lit. h DSGVO).

7.2. Dem Auftraggeber steht hierzu auf Anfrage die durch den Auftragnehmer erstellte, regelmäßig überarbeitete und den gesetzlichen Anforderungen entsprechende Dokumentation über die vorhandenen technischen und organisatorischen Maßnahmen zur Verfügung.

7.3. Vor-Ort-Kontrollen erfolgen innerhalb üblicher Geschäftszeiten, sind vom Auftraggeber mit einer angemessenen Frist (mindestens 14 Tage, außer in Notfällen) anzumelden und durch den Auftragnehmer zu unterstützen (z. B. durch Bereitstellung von Personal). Die Kontrollen sind auf den erforderlichen Rahmen beschränkt und müssen auf Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie den Schutz von personenbezogenen Daten Dritter (z. B. anderer Kunden oder Mitarbeiter des Auftragnehmers) Rücksicht nehmen. Zur Durchführung der Kontrolle sind nur fachkundige Personen zugelassen, die sich legitimieren können und im Hinblick auf die Betriebs- und Geschäftsgeheimnisse sowie Prozesse des Auftragnehmers und personenbezogene Daten Dritter zur Verschwiegenheit verpflichtet sind.

7.4. Statt der Einsichtnahmen und der Vor-Ort-Kontrollen darf der Auftragnehmer den Auftraggeber auf eine gleichwertige Kontrolle durch unabhängige Dritte (z. B. neutrale Datenschutzauditoren), Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO) oder geeignete Datenschutz- oder IT-Sicherheitszertifizierungen gemäß Art. 42 DSGVO verweisen. Dies gilt insbesondere dann, wenn Betriebs- und Geschäftsgeheimnisse des Auftragnehmers oder personenbezogene Daten Dritter durch die Kontrollen gefährdet wären.

8. Unterauftragsverhältnisse

8.1. Nimmt der Auftragnehmer die Dienste eines Unterauftragsverarbeiters (d. h. Unterauftragnehmer oder Subunternehmer des Unterauftragnehmers) in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, dann muss er dem Unterauftragsverarbeiter im Wege eines Vertrages oder eines nach der DSGVO zulässigen anderen Rechtsinstruments insbesondere im Hinblick auf die Befolgung von Weisungen, Einhaltung der TOMs, Erteilung von Informationen und Duldung von Kontrollen dieselben Datenschutzpflichten, zu denen sich der Auftragnehmer in diesem AV-Vertrag verpflichtet hat, auferlegen. Ferner hat der Auftragnehmer den Unterauftragsverarbeiter sorgfältig auszuwählen, auf dessen Zuverlässigkeit zu prüfen und diese sowie auch dessen Einhaltung der vertraglichen und gesetzlichen Vorgaben zu überwachen (Art. 28 Abs. 2 u. 4 DSGVO).

8.2. Der Auftraggeber erklärt sich unbeschadet etwaiger im Hauptvertrag enthaltener Einschränkungen ausdrücklich damit einverstanden, dass der Auftragnehmer im Rahmen der Auftragsverarbeitung zur Erfüllung seiner vertraglich vereinbarten Leistungen, insbesondere, aber nicht ausschließlich für die Bereiche Installation und Wartung der Rechenzentrumsinfrastruktur, Telekommunikationsdienstleistungen und Benutzerservice / Kunden-Support entweder verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht und / oder dritte Unternehmen mit der Leistungserbringung unterbeauftragt.

8.3. Die bereits zum Abschluss dieses AV-Vertrages bestehenden Unterauftragsverhältnisse werden vom Auftragnehmer in der Anlage 2 – Unterauftragnehmer angegeben und gelten vom Auftragnehmer als genehmigt.

8.4. Der Auftragnehmer trägt dafür Sorge, dass dem Auftraggeber im Kundenportal stets eine aktuelle Liste der vom Auftragnehmer eingesetzten Unterauftragnehmer zum Abruf zur Verfügung steht.

8.5. Der Auftragnehmer verpflichtet sich, den Auftraggeber über geplante Änderungen bei den Unterauftragsverarbeitern (z. B. Hinzuziehung weiterer bzw. Ersetzung bestehender Unterauftragsverarbeiter),

die für die Auftragsverarbeitung maßgeblich sind, mit einer angemessenen Vorlaufzeit zu informieren.

8.6. Der Auftraggeber verpflichtet sich, von seinem Recht auf Einspruch gegen die Hinzuziehung weiterer bzw. Ersetzung bestehender Unterauftragsverarbeiter (Art. 28 Abs. 2 DSGVO) nur unter Beachtung der Grundsätze von Treu und Glauben sowie der Angemessenheit und Billigkeit Gebrauch zu machen.

8.7. Als Unterauftragnehmer im Rahmen dieses konkreten Vertrages zur Auftragsverarbeitung gelten nur Dritte, die die vertraglich vereinbarte Hauptleistung ganz oder teilweise erbringen oder an deren Erfüllung mitwirken. Nicht als Unterauftragnehmer gelten dagegen Dritte, auf die der Auftragnehmer als reine Nebenleistung zur Unterstützung seiner geschäftlichen Tätigkeit zurückgreift (z. B. Reinigungskräfte, Bewachungsdienste, Transportdienstleister, Auskunfteien etc.) und / oder die Leistungen erbringen, die aufgrund einer gesetzlichen Vorschrift zulässig sind (z. B. Postdienste, reine Telekommunikationsleistungen von Telekommunikationsdienstleistern ohne konkreten Bezug zu den vom Auftragnehmer für den Auftraggeber zu erbringenden Leistungen etc.) und / oder die Leistungen direkt gegenüber dem Auftraggeber erbringen und daher mit dem Auftraggeber in einem direkten Vertragsverhältnis stehen (z. B. Domain-Vergabestellen, die Banken des Auftraggebers, die Zahlungen von dessen Kunden mittels Kreditkarte abrechnen etc.). Die Wartung und Pflege von IT-System oder Applikationen stellt jedoch dann ein zustimmungspflichtiges Unterauftragsverhältnis und eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme oder Applikationen betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

8.8. Der Auftragnehmer wird jedoch auch bei der Inanspruchnahme von Leistungen Dritter als reine Nebenleistung mit diesen Dritten angemessene vertragliche Regelungen treffen sowie Kontrollmaßnahmen ergreifen, um die Sicherheit der Daten und den Schutz personenbezogener Daten durch angemessene Vorkehrungen und technische und organisatorische Maßnahmen zu gewährleisten.

9. Laufzeit des AV-Vertrages, Vertragsbeendigung und Datenlöschung

9.1. Dieser AV-Vertrag beginnt mit dessen Abschluss. Er wird auf unbestimmte Zeit geschlossen und endet spätestens mit der Laufzeit des Hauptvertrages. Die Laufzeit des Vertrages richtet sich nach der Dauer der Erbringung von Hosting- oder Beratungs-Leistungen des Auftragnehmers an den Auftraggeber. Der Auftrag endet, wenn der Auftraggeber keine Hosting- oder Beratungs-Leistungen des Auftragnehmers aus dem Hauptvertrag / den Hauptverträgen, die unter der benannten Kundennummer zusammengefasst sind, mehr in Anspruch nimmt.

9.2. Der Auftraggeber kann den Vertrag jederzeit außerordentlich ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem AV-Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert. Der außerordentlichen Kündigung hat grundsätzlich eine Abmahnung der Verstöße mit angemessener Frist vorauszugehen, wobei sie nicht erforderlich ist, wenn nicht damit zu rechnen ist, dass die beanstandeten Verstöße behoben werden oder diese derart schwer wiegen, dass ein Festhalten am AV-Vertrag der kündigenden Vertragspartei nicht zuzumuten ist.

9.3. Nach Beendigung des Vertrages oder auf schriftliche Aufforderung durch den Auftraggeber hat der Auftragnehmer alle personenbezogenen Daten und deren verfahrens- oder sicherheitstechnisch notwendigen Kopien sowie sämtliche im Zusammenhang mit dem Auftragsverhältnis in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände vollständig nach Wahl des Auftraggebers entweder datenschutzgerecht zu löschen oder an den Auftraggeber zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (Art. 28 Abs. 1 S. 2 lit. g DSGVO). 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.

9.4. Die Einrede eines Zurückbehaltungsrechts, wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. Im Hinblick auf die vollständige und vertragsgemäße Löschung oder Rückgabe der Daten gelten die Auskunfts-, Nachweis und Kontrollrechte des Auftraggebers entsprechend diesem AV-Vertrag.

9.5. Im Übrigen bleiben die Verpflichtungen aus diesem AV-Vertrag im Hinblick auf die im Auftrag verarbeiteten Daten auch nach Beendigung des AV-Vertrages bestehen.

10. Vergütung

10.1. Der Auftraggeber verpflichtet sich, dem Auftragnehmer den Aufwand für dessen Informations- und Mitwirkungs- sowie Unterstützungshandlungen angemessen zu vergüten. Die Vertragsparteien werden sich in diesem Fall über eine angemessene Vergütung gesondert verständigen. Können sich die Vertragsparteien nicht einigen, so gilt die branchenübliche, in Ermangelung einer branchenüblichen die ortsübliche Vergütung als vereinbart.

11. Haftung und Freistellung

11.1. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zwischen Auftraggeber und Auftragnehmer gegenüber dem Betroffenen der Auftraggeber alleine verantwortlich.

11.2. Es gelten ferner die Haftungsbeschränkungen aus dem Hauptvertrag.

11.3. Der Auftraggeber verpflichtet sich, den Auftragnehmer von sämtlichen Ansprüchen freizustellen, die Dritte wegen der Verletzung ihrer Rechte gegen den Auftragnehmer aufgrund der vom Auftraggeber beauftragten Verarbeitung personenbezogener Daten geltend machen, wenn der Auftragnehmer nachweist, dass er für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, in keinerlei Hinsicht verantwortlich ist.

12. Schlussbestimmungen, Änderungen, Rangfolge, Kommunikationsform, Rechtswahl, Gerichtsstand

12.1. Dieser AV-Vertrag und seine Anhänge enthalten alle getroffenen Vereinbarungen. Mündliche Abreden außerhalb dieses AV-Vertrages und seiner Anhänge sind nicht getroffen worden. Änderungen, Nebenabreden und Ergänzungen dieses AV-Vertrages und seiner Anhänge bedürfen einer schriftlichen (auch in elektronischer Form zulässigen) Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses AV-Vertrages handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

12.2. Dieser AV-Vertrag verpflichtet den Auftragnehmer nur insoweit, als dies zur Erfüllung der gesetzlichen Pflichten, insbesondere nach Art. 28 ff. DSGVO erforderlich ist. Darüber hinaus erlegt er dem Auftragnehmer keine weiteren Pflichten auf. Bei Widersprüchen zwischen den Bestimmungen dieses AV-Vertrages und des Hauptvertrages, sind die Bestimmungen dieses AV-Vertrages maßgebend. Im Übrigen bleiben die Bestimmungen des Hauptvertrages unberührt und gelten für diesen AV-Vertrag entsprechend.

12.3. Vorbehaltlich einer Verpflichtung zur Schriftform in diesem AV-Vertrag und im Hauptvertrag erfolgt die Kommunikation zwischen dem Auftragnehmer und Auftraggeber im Rahmen dieses AV-Vertrages (insbesondere im Hinblick auf die Erteilung von Informationen und Weisungen) zumindest in Textform (z. B. per E-Mail, Telefax, Brief). Die Erteilung von Informationen und Weisungen in einer geringeren Form (z. B. [fern]mündlich) als der Textform kann den konkreten Umständen nach (z. B. in Notfallsituationen) im Einzelfall zulässig sein. In diesem Falle müssten die erteilten Informationen und / oder Weisungen jedoch unverzüglich zumindest in Textform (z. B. per E-Mail, Telefax, Brief) bestätigt werden. Sofern die Schriftform verlangt wird, ist die Schriftform im Sinne der DSGVO gemeint.

12.4. Es gilt das Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AV-Vertrag ist – sofern der Aufraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist oder der Aufraggeber in der Bundesrepublik Deutschland keinen Gerichtsstand hat – der Sitz des Auftragnehmers in München. Der Auftragnehmer behält sich vor, seine Ansprüche an dem gesetzlichen Gerichtsstand geltend zu machen.

12.5. Sollte eine Bestimmung dieses AV-Vertrages und / oder seiner Anhänge aus tatsächlichen oder rechtlichen Gründen ganz oder teilweise unwirksam sein oder werden, so lässt dies die Wirksamkeit der übrigen Bestimmungen unberührt; diese gelten unverändert weiter. Anstelle der unwirksamen Bestimmung gelten die einschlägigen gesetzlichen Vorschriften. Entsprechendes gilt, wenn bei der Durchführung dieses Vertrages eine ergänzungsbedürftige Lücke dieses Vertrages offenbar wird.

Anlagen:
Anlage 1 – Einzelheiten der Datenverarbeitung
Anlage 2 – Unterauftragnehmer
Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers

Für den Auftraggeber:

Ort und Datum

vollständiger Name in Druckbuchstaben

Funktion

Unterschrift

Für den Auftragnehmer:

Ort und Datum München, 30.5.78

vollständiger Name in Druckbuchstaben PETER SCHOBER

Funktion Inhaber

Unterschrift

Anlage 1 – Einzelheiten der Datenverarbeitung

1. Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung der Daten des Auftraggebers gemäß Ziffer 3 des

AV-Vertrages sind folgende Datenarten:

Personenstammdaten

z. B. Vorname, Nachname, Adresse, Geburtsdatum, Geburtsort, Nationalität, Beruf, Familienstand etc.

Kommunikationsdaten

z. B. E-Mail, Telefon-, Mobilfunk, Telefaxnummer, Kontaktdaten Sozialer Netzwerke etc.

Vertragsstammdaten

z. B. Vertragsgegenstand, Vertragsnummer, Laufzeit etc.

Vertragsabrechnung- und Zahlungsdaten

z. B. Bankverbindung, Kreditkartennummern, Zahlungshistorie etc.

Kundenhistorie

Auskunftsangaben

von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen etc.

Inhaltsdaten

z. B. Texteingaben, Fotografien, Videos etc.

Nutzungsdaten

z. B. Interessen, besuchte Webseiten, Kaufverhalten, Warenkorb, Zugriffszeiten, Steuerungsdaten, Protokolldaten etc.

Meta- / Kommunikationsdaten

z. B. IP-Adressen, Anschlusskennung, Geräte-IDs, Standortdaten etc.

Beschäftigtenstammdaten

z. B. Namen, Adressen, Lohngruppe, Steuermerkmale etc.

Bewerberdaten

z. B. Namen, Kontaktdaten, Qualifikationen, Bewerbungsunterlagen etc.

2. Verarbeitung besonderer Kategorien von Daten (Art. 9 Abs. 1 DSGVO)

Hierzu gehören Daten betreffend die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung.

Es werden grundsätzlich keine besonderen Kategorien von Daten verarbeitet, außer diese werden durch den Auftraggeber / seine Kunden, Nutzer oder Mitarbeiter etc. der Verarbeitung zugeführt. Es werden folgende besondere Kategorien von Daten verarbeitet:

3. Kreis der Betroffenen

Mitarbeiter, Beschäftigte, Bewerber und Nutzer.

4. *Zweck der Verarbeitung*

Betrieb und Betrieb von E-Mail-Servern mit Antispam Lösungen und Archiv
Server-Administration / Server-Wartung
Bereitstellen von Speicherplatz (Webhosting)

Erbringung von Telekommunikationsdienstleistungen (Bereitstellen von E-Mail-Diensten mit Antispam Lösungen und Archiv)
Website-Erstellung und -Pflege
Suchmaschinen-Optimierung (SEO)
Archivierung von Daten zum Zwecke der Wiederherstellung im Schadensfall
Abwehr von Angriffen und Filterung von Datenpaketen
Datenanalyse/ Beratungsleistungen
Werbung / Marketing
Erbringung von Software as a Service-Leistungen (Bereitstellen von Rechenkapazitäten, Datenbanken, Software)
Betrieb und Betrieb von E-Mail-Servern mit Antispam Lösungen und Archiv
Registrierung sowie Betreuung / Verwaltung von Domains
Erbringung von Sicherheitsleistungen (Bereitstellen von SSL-Zertifikaten)

5. Verarbeitungsort

Die Verarbeitung der Daten findet an folgenden Standorten statt:

Geschäftsräume: Peter Schober, Agnes-Bernauer-Str.69, 80687 München
Geschäftsräume: Variomedia AG, August-Bebel-Straße 68 in 14482 Potsdam
Rechenzentren: ScaleUp Technologies GmbH & Co. KG, zwei Standorte in Berlin

Innerhalb des IP Netzwerkes des Auftragnehmers

6. Weisungsberechtigte Personen des Auftraggebers

Vor- und Nachname

Funktion

Telefon

E-Mail

7. Weisungsempfangsberechtigte Personen des Auftragnehmers

Vor- und Nachname	Peter Schober
Funktion	Inhaber
Telefon	0171 3569554
E-Mail	Peter.schober@kirschgrafik.de

Anlage 2 – Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer").

Sofern nicht anders angegeben, werden Daten ausschließlich in Deutschland verarbeitet. Es handelt sich um nachfolgende Unternehmen:

Unterauftragnehmer	Kurzbeschreibung der Leistung
ScaleUp Technologies GmbH & Co. KG Süderstr. 198 in 20537 Hamburg	Erbringung von Rechenzentrums-Leistungen, Lieferung von Strom, Routing von IP-Datentransfer Vertragsgrundlage: AV-Vertrag mit Variomedia AG Garantie im Fall von Drittländern (z. B. Privacy-Shield-Zertifizierung): entbehrlich
Cyren GmbH Hardenbergplatz 2 in 10623 Berlin	E-Mail-Analyse zur Bekämpfung von Spam. Personenbezogene Daten werden nur erfasst, wenn wir E-Mails zur Behebung einer Fehlklassifizierung an Cyren weiterleiten. Vertragsgrundlage: AV-Vertrag mit Variomedia AG Garantie im Fall von Drittländern (z. B. Privacy-Shield-Zertifizierung): entbehrlich
Key-Systems GmbH Im Oberen Werk 1 in 66386 St. Ingbert	Registrar-Dienstleistungen für Domainregistrierungen, bei denen wir nicht über einen eigenen Registrarvertrag verfügen Vertragsgrundlage: AV-Vertrag mit Variomedia AG Garantie im Fall von Drittländern (z. B. Privacy-Shield-Zertifizierung): entbehrlich
INWX GmbH & Co. KG Prinzessinnenstr. 30 in 10969 Berlin	Registrar-Dienstleistungen für Domainregistrierungen, bei denen wir nicht über einen eigenen Registrarvertrag verfügen Vertragsgrundlage: AV-Vertrag mit Variomedia AG Garantie im Fall von Drittländern (z. B. Privacy-Shield-Zertifizierung): entbehrlich
Computop Wirtschaftsinformatik GmbH Schwarzenbergstr. 4 in 96050 Bamberg	Bereitstellung und Betrieb einer Bezahlplattform zur sicheren Abwicklung von Zahlungstransaktionen (Kreditkarten) Vertragsgrundlage: AV-Vertrag mit Variomedia AG Garantie im Fall von Drittländern (z. B. Privacy-Shield-Zertifizierung): entbehrlich
Tesch mediafinanz GmbH Weiße Breite 5 in 49084 Osnabrück	Bereitstellung von Bonitätsauskünften, Abwicklung von Inkassoverfahren Vertragsgrundlage: AV-Vertrag mit Variomedia AG Garantie im Fall von Drittländern (z. B. Privacy-Shield-Zertifizierung): entbehrlich

Unterauftragnehmer	Kurzbeschreibung der Leistung
vio:networks GmbH Weigandufer 45 in 12059 Berlin	Betrieb und Wartung unserer cloudbasierten Telefonanlage Vertragsgrundlage: AV-Vertrag mit Variomedia AG Garantie im Fall von Drittländern (z. B. Privacy-Shield-Zertifizierung): entbehrlich
Variomedia AG August-Bebel-Str. 86 14482 Potsdam	Dienstleister für Hosting, E-Mail Service, Domain Buchung und Webspace. Vertragsgrundlage: AV-Vertrag Garantie im Fall von Drittländern (z. B. Privacy-Shield-Zertifizierung): entbehrlich
TeamViewer GmbH Jahnstr. 30 in 73037 Göppingen	Fernwartung von Computersystemen, Service, Kommunikation Vertragsgrundlage: AV-Vertrag mit Variomedia AG Garantie im Fall von Drittländern (z. B. Privacy-Shield-Zertifizierung): entbehrlich

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers

Diese Anlage konkretisiert die im AV-Vertrag getroffenen technischen und organisatorischen Maßnahmen. Dabei werden in diesem Zusammenhang insbesondere der aktuelle Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Datenverarbeitung berücksichtigt. Des Weiteren werden die unterschiedlichen Eintrittswahrscheinlichkeiten und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen beachtet, um ein dem Risiko entsprechendes, angemessenes Schutzniveau für den Schutz personenbezogener Daten zu erreichen.

Der Auftragnehmer trifft die im Folgenden beschriebenen technischen und organisatorischen Maßnahmen zur Datensicherheit im Sinne des Art. 32 DSGVO. Diese beziehen sich, soweit nicht anders angegeben, auf die von Auftragnehmer genutzten Rechenzentren. Maßnahmen, die sich auf die Büroräume des Auftragnehmers beziehen, sind entsprechend gekennzeichnet.

1. Vertraulichkeit der Daten

Die Sicherstellung der Vertraulichkeit der Datenverarbeitungssysteme gehört zu den Schlüsselelementen moderner Sicherheitsmechanismen und ist Bestandteil der wesentlichen Schutzziele der DSGVO. Maßnahmen zur Umsetzung des Gebots der Vertraulichkeit sind unter anderem auch solche, die zur Zutritts-, Zugriffs- oder Zugangskontrolle gehören. Die in diesem Zusammenhang getroffenen technischen und organisatorischen Maßnahmen sollen eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Maßnahmen zur Sicherstellung der Vertraulichkeit auf Dauer:

- Vertraulichkeitsvereinbarungen mit internen und externen Mitarbeitern
- Vertraulichkeitsvereinbarungen mit externen Dienstleistern
- Einsatz eines umfassenden Datenschutzkonzepts
- Spezifizierte, für die Datenverarbeitungstätigkeit entsprechend dem Datenschutzkonzept ausgestattete Server-Räume
- Zugriffskontrollen (siehe Ziffer 9)
- Zutrittskontrollen (siehe Ziffer 10)
- Zugangskontrollen (siehe Ziffer 11)

2. Integrität auf Dauer

Die Sicherstellung der Integrität der Datenverarbeitungssysteme gehört ebenso wie die Sicherstellung der Vertraulichkeit der Datenverarbeitungssysteme zu den wichtigsten Schutzzielen der DSGVO. Hierzu zählen Maßnahmen zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Zerstörung oder unbeabsichtigter Schädigung.

Maßnahmen zur Sicherstellung der Integrität auf Dauer:

- Tests der von Auftragnehmer bereitgestellten Standardsoftware
- Regelmäßige Updates der von Auftragnehmer bereitgestellten Standardsoftware
- Dateisysteme mit End-To-End Prüfsummen
- Prozesse zur Aufrechterhaltung der Aktualität von Daten

3. Pseudonymisierung

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Maßnahmen in Zusammenhang mit der Pseudonymisierung personenbezogener Daten:

- Pseudonymisierung von IP-Adressen in den bereitgestellten Webserver-Logdateien

4. Verschlüsselung

Die Verschlüsselung personenbezogener Daten ist eine gängige Möglichkeit diese gegen die Kenntnisnahme durch Unbefugte zu schützen. Insbesondere eignet sich die Verschlüsselung dafür, Daten von äußeren Einflüssen wie z. B. Hackangriffe und Spionage zu bewahren. Unter Verschlüsselung ist ein Verfahren zu verstehen, durch das eine klar lesbare Information in eine nicht lesbare bzw. interpretierbare Zeichenabfolge umgewandelt wird.

Maßnahmen in Zusammenhang mit der Verschlüsselung personenbezogener Daten:

- Bereitstellung von gängigen Verschlüsselungswerkzeugen- und Softwarebibliotheken (GPG, OpenSSL)

5. Verfügbarkeit der Daten

Damit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Diese Maßnahmen müssen so ausgelegt sein, dass sie die Verfügbarkeit auf Dauer gewährleisten.

Maßnahmen zur Sicherstellung der Verfügbarkeit auf Dauer:

- Einsatz von geprüfter Standardsoftware aus vertrauenswürdigen Quellen
- Tägliche Durchführung von Datensicherungen
- Einsatz von Datenspiegelungsverfahren (RAID)
- Nutzung von SSDs mit Pufferkondensatoren (Power Loss Protection)
- Einsatz von Virenschutz-Software und Firewalls
- Brandschutztüren, Feuermeldesystem und automatische Gaslöschanlage in den Server-Räumen
- Betreuung der IT durch qualifizierte und ständig weitergebildete Mitarbeiter
- Unterbrechungsfreie Stromversorgung (USV, nur im Rechenzentrum)

6. Gewährleistung der Belastbarkeit der Systeme auf Dauer

Hierzu gehören beispielsweise Maßnahmen, die schon in der Phase vor Durchführung der Datenverarbeitung durch den Auftragsverarbeiter zu ergreifen sind. Darüber hinaus ist auch eine kontinuierliche Überwachung der Systeme erforderlich.

Maßnahmen zur Sicherstellung der Belastbarkeit der Systeme und Dienste auf Dauer:

- Monitoring-Systeme zur Überwachung von Servern und Diensten
- Unterbrechungsfreie CPU- und Speicherzuweisung im laufenden Betrieb
- Regelmäßige Penetrations- und Belastungstests der Datenverarbeitungssysteme

7. Sicherstellung und Wiederherstellung der Verfügbarkeit

Zur Sicherstellung der Verfügbarkeit sind einerseits ausreichende Sicherungen erforderlich, wie aber auch Maßnahmenpläne, die beim Eintreten von Katastrophenfallszenarien den laufenden Betrieb wiederherstellen können.

Maßnahmen zur Sicherstellung und Wiederherstellung der Verfügbarkeit bei einem physischen oder technischen Zwischenfall:

- Einsatz von Datenspiegelungsverfahren
- Regelmäßige Backups der Datenbestände

- Getrennte Aufbewahrung von Backups
- Regelmäßiges Testen der Datenwiederherstellungswerkzeuge
- Durchgängig parallel-redundante Strom- und Notstromversorgung (unterbrechungsfreie Stromversorgung und Netzersatzanlage mit Kraftstoffreserven für mindestens 24 Stunden)
- Redundante Klimatisierungssysteme
- Redundante Internet-Uplinks zu unterschiedlichen Tier-1-Providern und Internet-Knoten
- Vorhalten von Reserve-Servern

8. Überprüfung und Bewertung der Datensicherheit

Maßnahmen um insbesondere die schon getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit laufend aktuell zu halten und kritisch zu begutachten. Diese Pflicht erstreckt sich auf alle technischen und organisatorischen Maßnahmen (Ziffern 1 bis 15).

Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen:

- Regelmäßige Überprüfung der vom Auftragnehmer bereitgestellten Standardsoftware auf Sicherheitsprobleme
- Regelmäßige Überprüfung der Firewall-Regeln auf Wirksamkeit gegen aktuelle Angriffe
- Regelmäßige Überprüfung von Datenverarbeitungssystemen und Verarbeitungstätigkeiten auf Sicherheitslücken, die aufgrund neuer technischer Entwicklungen oder veränderter Verarbeitungspraxis entstehen können

9. Zugriffskontrolle

Damit sind Maßnahmen gemeint, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können. Der Auftragsverarbeiter muss deswegen Maßnahmen ergreifen, die dafür Sorge tragen, dass Personen im Rahmen der Datenverarbeitung nur auf die Daten zugreifen können, für die sie über eine entsprechende Berechtigung verfügen und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen zur Verwehrung des Zugriffs auf personenbezogene Daten für Unbefugte:

- Verwendung von benutzerbezogenen und individualisierten Anmeldeinformationen (Kundenmenü, SSH, FTP, MySQL)
- Datenschutzkonforme Vernichtung von Datenträgern
- Verbot des Einsatzes privater Datenträger
- Vorgabe zur Festlegung von Passwörtern (u. a. Sonderzeichen, Mindestlänge)

10. Zutrittskontrolle

Damit sind Maßnahmen gemeint, die Unbefugten den Zutritt zu den Gebäuden und Rechenzentren verwehren, in denen personenbezogene Daten verarbeitet werden. Der Auftragsverarbeiter ergreift in diesem Zusammenhang Maßnahmen, die dafür Sorge tragen, dass nur die Personen Zutritt zu den Gebäuden und Rechenzentren haben, die über eine entsprechende Berechtigung verfügen.

Maßnahmen zur Verwehrung des Zutritts zu Datenverarbeitungsanlagen für Unbefugte:

- Festlegung zutrittsberechtigter Personen
- Mehrstufige Zutrittskontrolleinrichtungen unter Einsatz personalisierter elektronischer Ausweiskarten mit Lichtbild sowie PIN bzw. biometrischer Merkmale
- Einrichtung verschiedener Sicherheitszonen mit verschiedenen Zutrittsberechtigungen
- Dokumentation der Vergabe und des Entzugs von Zutrittsberechtigungen
- Einbruchsmeldeanlage mit Alarmübertragung zur ununterbrochen besetzten Sicherheitsleitstelle

- Besucheraufenthalte nur in Begleitung von Beschäftigten des Auftragsverarbeiters
- Ausweistragepflicht
- Videoüberwachung der Zugänge
- Videoaufzeichnung in den Serverräumen
- Zutrittskontrolle mittels Schlüssel und personalisierter elektronischer Ausweiskarte in den Büroräumen

11. Zugangskontrolle zu Datenverarbeitungssystemen

Damit sind Maßnahmen gemeint, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen. Der Auftragsverarbeiter muss in diesem Zusammenhang Maßnahmen ergreifen, die dafür Sorge tragen, dass nur Personen auf Anlagen zur Datenverarbeitung zugreifen können, die über eine entsprechende Berechtigung verfügen. Hierzu gehören beispielsweise geeignete Passwortregeln und Firewallkonfigurationen.

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Nutzung von kryptographischen Zertifikaten bzw. Kennwortverfahren zur Benutzerauthentifizierung (FTP, SSH)
- Schutz vor Brute-Force-Login-Angriffen (FTP, SSH, MySQL)
- Nutzung von Firewalls zum Schutz vor Angriffen
- Automatische Sperrung der Arbeitsplatzrechner nach Inaktivität (Büroräume)

12. Weitergabekontrolle

Damit sind Maßnahmen gemeint, die 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.

Maßnahmen zur Verwehrung der unbefugten Kenntnisnahme, der Nachvollziehbarkeit und Wahrung der Integrität bei der Datenübertragung:

- Bereitstellung von verschlüsselten Netzwerkprotokollen für Fernzugriff und Dateiübertragung (SSH, SFTP)
- Installation von SSL-Zertifikaten für den HTTPS-gesicherten Aufruf von Webseiten auf Wunsch des Auftraggebers
- Nutzung von SSL-Zertifikaten für alle durch den Auftragnehmer bereitgestellte Web-Dienste (Webmail, Kundenmenü etc.)
- Datenschutzkonforme Vernichtung von Datenträgern
- Transport von unverschlüsselten Datenträgern ausschließlich durch firmeneigene Mitarbeiter
- Nutzung von verschlüsselten Netzwerkprotokollen (Büroräume)

13. Eingabekontrolle

Damit sind Maßnahmen gemeint, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungs-Systemen bzw. -Anwendungen eingegeben, verändert oder entfernt worden sind.

Maßnahmen zur nachträglichen Überprüfung und Nachvollziehbarkeit bei Eingaben, Änderungen und Löschungen:

- Aufzeichnung und bedarfsgerechtes Vorhalten von an Systemen durchgeführten Aktionen (Logdateien)
- Gesetzeskonforme Vertragsgestaltung von Verträgen über die Datenverarbeitung personenbezogener

Daten mit Subunternehmern mit entsprechender Regelung von Kontrollmechanismen

14. Auftragskontrolle (bei Einsatz von Subunternehmen)

Damit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten, die im Auftrag bei einem Subunternehmer des Auftragsverarbeiters verarbeitet werden, nur entsprechend den Weisungen und Anforderungen an die Datenverarbeitung des Auftraggebers verarbeitet werden können.

Maßnahmen zur Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur nach Weisung des Auftraggebers verarbeitet werden:

- Kriterien zur Auswahl der Auftragnehmer festgelegt (Referenzen, Zertifizierungen, Gütesiegel)
- Detaillierte schriftliche Regelungen (Vertrag / Vereinbarung) der Auftragsverhältnisse und Formalisierung des gesamten Auftragsablaufes, auch zum Einsatz von Subunternehmern, eindeutige Regelungen der Zuständigkeiten und Verantwortlichkeiten
- Sicherstellung, dass die Auftragsdurchführung kontrolliert und dokumentiert wird
- Vertragliche Vereinbarung mit Subunternehmern, eigene und externe Mitarbeiter auf das Datengeheimnis zu verpflichten

15. Trennungskontrolle

Damit sind Maßnahmen gemeint, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können, und Unbefugte keinen Zugriff auf fremde Daten erlangen können.

Maßnahmen zur Trennnungskontrolle:

- Logische bzw. technische Trennung von Daten durch separate Server bzw. Virtualisierung
- Benutzerprofile mit Trennung der Nutzerkonten und abgestuften Zugriffsberechtigungen