**Vertrag zur Auftragsverarbeitung AV-Vertrag**

Stand: 15.11.2018

zwischen

VERLAG, ADRESSE

**- Auftraggeber = Verantwortlicher -**

und

VRS Media GmbH & Co. KG, An der Reeperbahn 6, 28217 Bremen

**- Auftragnehmer = Auftragsverarbeiter -**

**Vorbemerkung**

Zwischen den Parteien besteht oder wird zeitgleich ein (Haupt-)Vertrag über die einmalige oder regelmäßige Erbringung von Dienstleistungen geschlossen, die eine automatisierte oder nicht automatisierte Verarbeitung personenbezogener Daten konkret zum Gegenstand haben bzw. zwangsläufig mit sich bringen oder bei denen ein Zugriff auf personenbezogene Daten aus der unternehmerischen Sphäre des Auftraggebers zumindest nicht ausgeschlossen werden kann, was insbesondere bei der Prüfung und Wartung von automatisierten Verfahren oder Datenverarbeitungsanlagen der Fall ist.

Seit dem 25.05.2018 gelten in allen Mitgliedsstaaten der Europäischen Union die Regelungen der Europäischen Datenschutz-Grundverordnung (DS-GVO) unmittelbar, in deren Art. 28 die Datenverarbeitung im Auftrag geregelt wird und insbesondere das Erfordernis konkreter Festlegungen in Bezug auf den Datenschutz im Rahmen eines Vertrags oder eines anderen Rechtsinstituts des Unionrechts oder des Rechts eines einzelnen Mitgliedsstaats enthalten ist. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) ordnet die Wartung und Fernzugriffe auf Systeme als Auftragsverarbeitung ein, wenn ein Zugriff auf personenbezogene Daten notwendig oder zumindest möglich ist.

Mit dem vorliegenden schriftlichen oder elektronischen Vertrag werden die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung im Auftrag nach Maßgabe der DS-GVO im Einzelnen geregelt, die verwendeten Fachbegriffe sind in Art. 4 DS-GVO definiert. Bereits bestehende Vereinbarungen zur Regelung der Auftragsdatenverarbeitung werden durch diesen AV-Vertrag mit dessen Wirksamwerden ersetzt.

1. **Gegenstand und Dauer des Auftrags**
2. Der zugrundeliegende Auftrag hat im Wesentlichen folgende Dienstleistungen zum Gegenstand:
* Bereitstellung von Themenportalen (vrs.FamilyMarkets) und Rubrikenmärkten (vrs.AdMarkets) als White-Label-Produkt und SaaS-Lösung
* Erstellung, Bearbeitung und Veröffentlichung von Online-Anzeigen
* Bereitstellung eines Anzeigenkonfigurators (vrs.AdBooker) als SaaS-Lösung
* Ratgeberinformationen und Community-Funktionen für Besucher

Im Übrigen wird auf die Leistungsbeschreibung des Hauptvertrags verwiesen.

1. Die Laufzeit des vorliegenden Vertrags beginnt mit der Unterzeichnung durch beide Parteien und endet zeitgleich mit dem Hauptvertrag, ohne dass es eines gesonderten Beendigungstatbestandes bedarf. Im Hauptvertrag vereinbarte Kündigungsfristen bleiben unberührt.
2. Der Auftraggeber kann (auch) den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen gesetzliche Datenschutzvorschriften oder Pflichten aus diesem 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.
3. **Konkretisierung des Auftragsinhalts**
4. Art der vom Hauptvertrag vorgesehenen Verarbeitung von personenbezogenen Daten:
* Erheben / Erfassen
* Organisation / Ordnen
* Speicherung
* Anpassung / Veränderung
* Offenlegung / Verbreitung
1. Hinsichtlich des Zwecks der Verarbeitung wird nach oben auf Ziffer 1. Abs. 1 dieses Vertrags sowie auf den Hauptvertrag verwiesen.
2. Die Datenverarbeitung findet ausschließlich in der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in einen Drittstaat bedarf der vorherigen Zustimmung des Auftraggebers. Die Verlagerung in einen Drittstaat darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.
3. Gegenstand der Verarbeitung sind folgende Arten / Kategorien personenbezogener Daten:
* Namen und Vornamen
* Adress- und Kommunikationsdaten
* Bankverbindung
* Daten besonderer Ereignisse (z.B. Geburt, Hochzeit, Jubiläen, Tod)
* Bilddaten
* Vertragsdaten
1. Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
* Mitarbeiter und Anzeigenkunden des Auftraggebers
* In geschalteten Anzeigen genannte Personen
* Besucher der Themenportale und Rubrikenmärkte
1. **Weisungsbefugnis des Auftraggebers**
2. Die Verarbeitung personenbezogener Daten erfolgt ausschließlich nach Maßgabe der dokumentierten Weisungen des Auftraggebers einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass der Auftragnehmer durch das Recht der Union oder des konkreten Mitgliedsstaats zur anderweitigen Verarbeitung verpflichtet ist. Über eine derartige Durchbrechung des Grundsatzes der Weisungsgebundenheit hat der Auftragnehmer den Auftraggeber zu informieren, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines öffentlichen Interesses verbietet.
3. Der Auftraggeber kann jederzeit ergänzende Weisungen erteilen. Mündliche Weisungen bestätigt der Auftragnehmer unverzüglich in Textform (z.B. Brief, Fax, Email).
4. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen geltende Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.
5. **Technische und-organisatorische Maßnahmen**
6. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen (TOM) vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags und diesem Vertrag als Anlage 1 beigefügt. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen und das Ergebnis in einer neuen Version der Anlage 1 zu dokumentieren.
7. Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.
8. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind in einer neuen Version der Anlage 1 zu dokumentieren.
9. **Berichtigung, Einschränkung und Löschung von Daten**
10. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
11. Soweit vom Leistungsumfang des Hauptvertrags umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.
12. **Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Die schriftliche Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Als Datenschutzbeauftragter ist beim Auftragnehmer benannt:
* Ralf Lohmann, HUBIT Datenschutz, Bergiusstr. 4, 28816 Stuhr, 0421-36490577, info@hubit.de

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

1. Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO, die über das Vertragsende hinaus gilt. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.
2. Die Umsetzung und Einhaltung aller im Rahmen des Auftrags erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (siehe Anlage 1).
3. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
4. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
5. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
6. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.
7. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrages.
8. **Unterauftragsverhältnisse**
9. 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- und 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.
10. Der Auftragnehmer darf weitere Auftragsverarbeiter als Unterauftragnehmer nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
11. Der Auftraggeber stimmt unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO der Beauftragung der in Anlage 2 aufgeführten Unterauftragnehmer zu.
12. Die generelle Auslagerung auf Unterauftragnehmer und/oder der Wechsel eines bestehenden Unterauftragnehmers sind zulässig, soweit
* der Auftragnehmer dem Auftraggeber das konkrete Vorhaben eine angemessene Zeit vorab schriftlich oder in Textform mit allen relevanten Details anzeigt und
* der Auftraggeber gegenüber dem Auftragnehmer nicht bis zum Zeitpunkt der Übergabe der Daten schriftlich oder in Textform Einspruch gegen das konkrete Vorhaben erhebt und
* der Umsetzung eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO mit dem Unterauftragnehmer zugrunde gelegt wird.
1. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
2. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, was generell nur mit vorheriger Zustimmung des Auftraggebers gemäß Ziffer 1. Abs. 3 dieses Vertrags zulässig ist, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit nach Maßgabe von Art. 44 ff. DS-GVO (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln oder genehmigte Verhaltensregeln) sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
3. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers in Textform. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.
4. **Kontrollrechte des Auftraggebers**
5. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
6. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
7. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
* die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
* die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
* aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
* eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
1. Im Falle der Unterbeauftragung erstrecken sich die Kontrollrechte übergreifend auf die gesamte Vertragskette, so dass Auftragnehmer und Unterauftragnehmer auch durch über dem jeweiligen Auftraggeber stehende Auftraggeber kontrolliert werden können.
2. **Mitwirkungspflicht des Auftragnehmers**
3. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten TOM bei der Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte sowie bei der Einhaltung der in den Artt. 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
4. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.
5. die Verpflichtung, Datenschutzvorfälle im Sinne einer Verletzung von gesetzlichen Vorschriften oder Verstößen gegen vertragliche Vereinbarungen bzw. Weisungen des Auftraggebers unverzüglich an den Auftraggeber zu melden und ihm in diesem Zusammenhang sämtliche relevanten Informationen zur Verfügung zu stellen.
6. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
7. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.
8. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.
9. Der Auftragnehmer wirkt im angemessenen Umfang an der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber mit, indem er die jeweils erforderlichen Angaben in geeigneter Weise mitteilt.
10. **Löschung und Rückgabe von personenbezogenen Daten**
11. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
12. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Hauptvertrags – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
13. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Ort, Datum Ort, Datum**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**- Auftraggeber - - Auftragnehmer –**

Anlage 1 zum ADV-Vertrag

**Technische und organisatorische Maßnahmen (TOM)**

Stand: 15.11.2018

Folgende technische und organisatorische Maßnahmen (TOM) gemäß EU Datenschutz Grundverordnung sind grundlegend für die Datenverarbeitung im Unternehmen. Ergänzende Maßnahmen und / oder Abweichungen sind gegebenenfalls im jeweiligen Verfahren beschrieben.

Die Server werden in Rechenzentren betrieben, deren Betreiber umfangreiche technische und organisatorische Maßnahmen durchführen, damit die Systeme ständig verfügbar sind. Diese Maßnahmen sind in den TOM des entsprechenden Auftragnehmers beschrieben.

1. **Vertraulichkeit**
	1. Zutrittskontrolle
		1. Gebäude

Die Eingangstüren des Geschäftsgebäudes und des von der verantwortlichen Stelle genutzten Bürotrakts sind mit Zylinderschlössern gesichert, die zu einem Schließsystem gehören. Die Ausgabe der Schlüssel wird durch die Hausverwaltung vorgenommen und dokumentiert.

Der Haupteingang des Gebäudes ist außerhalb der Geschäftszeiten verschlossen und nur im Zeitraum von 08:00 – 19:00 Uhr frei zugänglich. Die Eingangstür zum Bürotrakt ist auch während der Geschäftszeiten geschlossen und kann von außen nur mit Schlüssel geöffnet werden. Am Ende eines jeden Arbeitstages wird der Bürotrakt durch den letzten Mitarbeiter beim Verlassen verschlossen.

* + 1. Besucher

Besucher müssen am Eingang klingeln und werden dort in Empfang genommen, um in einen Wartebereich oder den Besprechungsraum geleitet zu werden, wo betriebsfremde Personen vorrangig empfangen werden.

Nur in Ausnahmefällen wird Besuchern in Begleitung von Mitarbeitern der Zutritt zu Arbeitsbereichen mit Datenverarbeitungsanlagen gestattet, wenn sichergestellt ist, dass keine Einsicht in schützenswerte Daten genommen werden kann.

* 1. Zugangskontrolle

Der Zugang von Unbefugten zu den Datenverarbeitungsanlagen wird verhindert, indem diese mindestens durch eine Benutzeranmeldung mit Benutzername und Passwort gesichert sind; zudem kommen software-spezifische Authentifizierungen zum Einsatz.

Die erforderliche Passwortsicherheit wird durch die *Passwortrichtlinie R-0004* gewährleistet. Die Einhaltung der Passwortrichtlinie wird von einem Mitarbeiter der Entwicklungsabteilung turnusmäßig überprüft.

Die Root-Zugänge zu den Webservern sind dadurch abgesichert, dass der Zugang nur von der IP-Adresse der verantwortlichen Stelle aus möglich ist.

Der Zugang zu Front- und Backend der Themenportale und Rubrikenmärkte sowie des Anzeigenkonfigurators erfordert die Authentifizierung mit Benutzername und Passwort. Der Anzeigenkonfigurator kann auch an Fremdsysteme per Schnittstelle mit Single Sign-On angebunden werden.

* 1. Zugriffskontrolle
		1. Datenverarbeitungsanlagen

Durch die Einrichtung von Benutzergruppen oder –rollen sowohl auf Ebene des Betriebssystems im Firmennetzwerk als auch auf Softwareebene sowie teilweise durch die Konfigurierung von Datenfreigaben ist gewährleistet, dass nur die berechtigten Personen auf die ihrer konkreten Berechtigung unterliegenden Daten zugreifen können.

In den Themenportalen und Rubrikenmärkten sowie im Anzeigenkonfigurator sichern Benutzergruppen bzw. –rollen den Zugriff auf die unterschiedlichen Daten. Jeder Benutzer ist einer Benutzergruppe bzw. –rolle zugeordnet, die Zuordnung erfolgt durch die jeweils hierzu berechtigten Benutzer.

* + 1. WLan

Es sind zwei virtuell getrennte WLan-Netzwerke eingerichtet, die jeweils durch Netzwerkschlüssel geschützt sind. Das Gäste-WLan ermöglicht lediglich den Zugang zum Internet, nicht zum Firmennetzwerk.

* 1. Trennungsgebot

Bei Daten, die zu unterschiedlichen Zwecken erhoben wurden, ist gewährleistet, dass diese auch getrennt verarbeitet werden. Eine Trennung der Daten erfolgt durch die Nutzung unterschiedlicher Datenbanken oder die Vergabe von Keys (Schlüsseln). Ein Key ist ein Wert, der die eindeutige Zuordnung eines Datensatzes zu einem Kunden ermöglicht.

* 1. Pseudonymisierung / Anonymisierung

Sofern dies möglich oder erforderlich ist, werden Daten pseudonymisiert. Hierbei werden Daten, die einen Personenbezug ermöglichen, entfernt oder durch zufällige Werte überschrieben. Aufgrund eines Schlüssels kann wieder ein Personenbezug hergestellt werden. Der hierfür erforderliche Schlüssel ist nur einem eingeschränkten Personenkreis zugänglich. Angewendete Pseudonymisierungen werden gegebenenfalls im jeweiligen Verfahren beschrieben.

Sofern dies möglich oder erforderlich ist, werden Daten anonymisiert. Hierbei werden Daten, die einen Personenbezug ermöglichen, entfernt oder durch zufällige Werte überschrieben. Es ist nachträglich nicht mehr möglich einen Personenbezug herzustellen. Angewendete Anonymisierungen werden gegebenenfalls im jeweiligen Verfahren beschrieben.

1. **Integrität**
	1. Weitergabe- / Transportkontrolle

Der Zugriff auf die Webserver erfolgt über eine verschlüsselte Verbindung (SSH). Bei der Konfiguration von Backends werden Daten verschlüsselt übertragen (SSL), während der Import der ohnehin zu veröffentlichen Anzeigen per Webservice unverschlüsselt geschieht.

In Abhängigkeit vom konkreten Kundenauftrag werden die Webseiten der Themenportale und Rubrikenmärkte verschlüsselt übertragen. Der webbasierte Anzeigenkonfigurator wird stets verschlüsselt übertragen (SSL). Bei den Schnittstellen zu Fremdsystemen kommt ebenfalls Verschlüsselungstechnik zum Einsatz, wobei der Kunde den Grad der Verschlüsselung bestimmt.

* + 1. Virtual Private Network

Beim Zugriff auf das interne Netzwerk von außen werden grundsätzlich verschlüsselte VPN-Verbindungen genutzt.

* + 1. Datenträgervernichtung

Dokumente in Papierform werden durch einen professionellen Dienstleister digital archiviert und anschließend vernichtet. Im täglichen Büroablauf werden nicht mehr benötigte Dokumente geschreddert.

* 1. Eingabekontrolle

Die Eingabekontrolle erfolgt durch Systemprotokolle des Serverbetriebssystems und in einzelnen Programmen.

Im Entwicklungsbereich protokolliert eine Versionsverwaltungssoftware Änderungen an Dokumenten und Dateien mit Zeitstempel und Benutzerkennung und ermöglicht die Wiederherstellung von Vorgängerversionen.

Nach dem Datenimport in die Themenportale und Rubrikenmärkte bekommt der Kunde einen Report über die eingelesenen Daten.

1. **Verfügbarkeit und Belastbarkeit**
	1. Schutzsoftware

Eine regelmäßig aktualisierte Antivirensoftware schützt Server sowie alle stationären und mobilen DVA vor Viren, Trojanern, Spyware, Malware und anderer Schadsoftware.

* 1. Datensicherung

Die regelmäßige Sicherung von Daten erfolgt nach näherer Maßgabe der *Datensicherungsrichtlinie R-0007*.

* 1. Rasche Wiederherstellung des Betriebs
		1. Datenwiederherstellung

Aus der regelmäßigen Datensicherung können einzelne Datensätze als auch alle virtuellen und physikalischen Server wiederhergestellt werden.

* 1. Internetanbindung

Die Internetanbindung verfügt in beide Richtungen (Down- und Upload) über eine hohe Übertragungsrate.

* 1. Monitoring

Ein permanentes Monitoring überwacht die Server im Rechenzentrum und deren Auslastung. Bei Überlast oder einer Funktionsstörung werden automatisch die Mitarbeiter der Entwicklungsabteilung informiert.

1. **Datenschutz-Management**
	1. Datenschutz-Konzept / Richtlinien

Es existiert ein *Datenschutz-Konzept K-0001* als Grundlage der korrekten Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten im Unternehmen. Im *Datenschutz-Konzept* sind die Datenschutzanforderungen und die zu treffenden technischen und organisatorischen Maßnahmen grundlegend beschrieben und die internen Verantwortlichkeiten geregelt.

Ergänzt wird das *Datenschutz-Konzept* durch spezielle Konzepte, Richtlinien und Merkblätter.

* 1. Datenschutzbeauftragter

Es ist ein betrieblicher Datenschutzbeauftragter bestellt. Die Kontaktdaten des Datenschutzbeauftragten sind auf der Webseite und durch Aushang im Unternehmen veröffentlicht.

Der *Datenschutzbeauftragte f*ührt regelmäßig Begehungen und Audits zur Überprüfung und Optimierung der Wirksamkeit der technischen und organisatorischen Maßnahmen durch und pflegt die Dokumentation.

Die *Beteiligung des Datenschutzbeauftragten* ist in der Richtlinie *R-0005* geregelt.

* 1. Aufsichtsbehörde

Wie mit *Anfragen der Aufsichtsbehörde* und einer möglicherweise meldepflichtigen *Datenpanne* bzw. einem solchen Verdacht umzugehen ist, regeln die Richtlinien *R-0001* und *R-0002*.

* 1. Betroffenenrechte

Im Datenschutz-Konzept sind die Rechte des Betroffenen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch, Datenübertragbarkeit sowie Beschwerde gegenüber der Datenschutzbehörde niedergelegt und deren Schutz sichergestellt.

In der Richtlinie *R-0003* ist konkret geregelt, wie mit der Anfrage eines Betroffenen umzugehen ist.

* 1. Schulung

Die Personen, die mit der Verarbeitung von personenbezogenen Daten beschäftigt sind, werden nach Maßgabe des *Schulungskonzepts K-0002* regelmäßig durch Präsenzschulungen oder Webinare geschult.

* 1. Auftragskontrolle

Die Heranziehung und der Wechsel eigener (Unter-)Auftragnehmer durch den Auftragnehmer erfolgt unter Beachtung der konkreten diesbezüglichen Vorgaben im *Vertrag zur Auftragsverarbeitung*.

Die Auftragskontrolle führt der Datenschutzbeauftragten des Auftragsnehmers nach Maßgabe der *Geschäftsführung* durch.

Anlage 2

**Unterauftragsverhältnisse**

Stand: 15.11.2018

Der Auftragnehmer bedient sich im Zuge der Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen Dritter als Subunternehmer. Es handelt sich dabei konkret um folgende(s) Unternehmen:

* Rechenzentrum:
1&1 IONOS Cloud GmbH
Greifswalder Str. 207
10405 Berlin
<https://www.ionos.de/pro/ionos-cloud>