Die

Name der Vertragspartners

Straße, Hausnummer

PLZ, Ort

- nachstehend **„Auftraggeber“** genannt -

und

Medien Falke UG (haftungsbeschränkt)
Gartenstraße 42
93339 Riedenburg

- nachstehend **„Auftragnehmer“** genannt -

schließen folgenden

Vertrag zur Auftragsdatenverarbeitung gemäß Art. 28 DSGVO

1. Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Angaben durch den Auftragnehmer:

Auftragnehmer stellt dem Auftraggeber einen Webhosting Account laut gültiger Preisliste zur Verfügung. Auftragnehmer verpflichtet sich im Rahmen seiner technischen Möglichkeiten, den reibungslosen Betrieb des Accounts sicherzustellen.

(2) Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von vier Wochen zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten:
Auftragnehmer bietet Internet Dienstleistungen in den Bereichen: Webhosting, Registrierung, Webspace, Domain, Subdomains an.

(2) Ort der Verarbeitung von Daten:

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt.

(3) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/ Kategorien (Aufzählung/Beschreibung der Datenkategorien):

- Personenstammdaten
- Kommunikationsdaten (Name, Vorname, Anschrift, Telefonnr., E-Mail)

(4) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Ansprechpartner
- Interessenten und Webseiten-Besucher als betroffene Personen.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt

handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. 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 DSGVO zu berücksichtigen (Einzelheiten in Anlage 1).

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

4. Berichtigung, Einschränkung und Löschung von Daten

(1) 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.

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

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

(1) Der Auftragnehmer hat als Datenschutzbeauftragte/n folgende Ansprechpartner benannt:

Projekt 29 GmbH & Co.KG

Bernhard Bock

Ostengasse 14

93047 Regensburg

(2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Einzelheiten hierzu siehe Anlage 1).

(4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(5) 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.

(6) 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.

(7) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(8) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice 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 Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
All-incl.com	Hauptstraße 68, 02742 Friedersdorf, Deutschland	Webhosting

Der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- 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).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) 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

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

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

10. Löschung und Rückgabe von personenbezogenen Daten

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

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

11. Haftung

Auf Art. 82 DSGVO wird verwiesen.

Riedenburg, den Datum Ort , den Datum

Medien-Falke UG (haftungsbeschränkt) *Unterschrift und Firmenstempel*

Anlage 1 – Technische und organisatorische Maßnahmen (TOM)

Nr.	Gebiet	Beschreibung
0	**Organisation**	
	Wie ist die Umsetzung des Datenschutzes organisiert?	Ein externer Datenschutzbeauftragter wird zur Wahrnehmung der Beratungs- und Kontrollfunktionen aus dem BGSG (neu DSGVO) eingesetzt.
	Nennen Sie uns bitte den Namen und die Kontaktdaten Ihres Datenschutzbeauftragten.	Herr Bernhard Bock Tel. 0941-298693-0 Projekt 29 GmbH & Co. KG Ostengasse 14 93047 Regensburg
	In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen?	Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit als auch eine konstante Sensibilisierung durch monatliche Datenschutznewsletter, fachbezogenen Webschulungen und persönliche Sensibilisierung durch externen Datenschutzbeauftragten.
	Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert?	Ja, die Verarbeitungen sind dokumentiert und auf Zulässigkeit im Sinne der DSGVO und des BDSG n.F. geprüft.
1	**Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)**	
1.1	**Zutrittskontrolle**	
	Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Das Gebäude ist mit einer Sicherheits-Schließanlage ausgerüstet.
	Wie werden die Räume / Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Die Räume werden ebenfalls durch das Sicherheits-Schließsystem gesichert.
	Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt?	Verarbeitungsanlagen sind durch Passwörter gesichert.
	Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft?	Durch externen Datenschutzbeauftragten.
1.2	**Zugangskontrolle**	
	Wie erfolgt die Vergabe von Benutzerzugängen?	Benutzerzugänge werden nur nach Bedarf und

Nr.	Gebiet	Beschreibung
		Genehmigung vergeben. Die Vergabe und Änderungen sind dokumentiert. Zugriff ist Passwortgeschützt.
	Wie wird die Gültigkeit von Benutzerzugängen überprüft?	Eine regelmäßige Revision wird durchgeführt und dokumentiert.
	Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert?	Benutzerzugänge werden in Server-Log dokumentiert.
	Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird?	Die Entscheidungen zur Rechtevergabe halten sich streng an die entsprechenden Vorgaben, Datenvermeidung und Datensparsamkeit.
	Ist ein Zugriff auf die Systeme / Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, Dienstleister etc.) und wie ist der Zugang gestaltet?	Der Einsatz von Heimarbeitsplätzen ist hier nicht geplant. Ein Zugang zur Fernwartung der Systeme ist nicht realisiert.
1.3	**Zugriffskontrolle**	
	Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind?	Die Passwörter werden vom jeweiligen Mitarbeiter selbst vergeben. Passwörter werden nicht gespeichert.
	Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?	Die Vorgaben Empfehlungen des BSI dienen als Vorbild für die o.g. Systemeinstellungen
	Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann / muss?	Systemeinstellung
	Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?	Schulungen und Sensibilisierung der Mitarbeiter. Einweisungen und regelmäßige Schulungen zu den verwendeten Geräten.
	Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?	Prüfung in regelmäßigen Abständen die Rechte und Benutzerstruktur. Siehe auch Punkt 1.2
	Wie erfolgt die Dokumentation von Zugriffsberechtigungen?	Regelmäßige Reports aus dem Berechtigungssystem
	Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden?	Sporadische Durchsicht der Systemprotokolle
	Wie lange werden Protokolle aufbewahrt? Wer hat Zugriff auf die Protokolle und wie oft	Keine festgelegten Fristen. Geschäftsführung

Nr.	Gebiet	Beschreibung
	werden sie ausgewertet?	
1.4	**Trennungskontrolle**	
	Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden?	nicht relevant.
1.5	**Pseudonymisierung**	
	Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?	Alle mit der Verarbeitung von personenbezogenen Daten betrauten Personen wurden entsprechend verpflichtet. Ein Datenschutzkonzept wird in Unternehmen eingesetzt und ist allen Mitarbeitern bekannt. Das Schulungskonzept beinhaltet eine Datenschutzunterweisung bei Beginn der Tätigkeit und eine konstante Sensibilisierung durch monatliche Datenschutznewsletter, fachbezogenen Webschulungen und persönliche Sensibilisierung durch den externen Datenschutzbeauftragten.
	Wie werden personenbezogene Daten verarbeitet /aufbewahrt, sodass diese nicht den betroffenen Personen zugeordnet werden können?	Kein direkter Kontakt bzw. Umgang mit Personenbezogenen Daten.
2	**Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**	
2.1	**Weitergabekontrolle**	
	Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?	Es werden keine personenbezogenen Daten der Auftraggeber weitergegeben
	Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt und wenn ja, welche?	Nicht relevant
	Wie wird die Weitergabe personenbezogener Daten dokumentiert?	Nicht relevant
	Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?	Eine strikte Rechtvergabe sichert die Daten vor unberechtigtem Zugriff.
	Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?	Dies wird im Rahmen der Kontrollen unter Punkt 1 mit geprüft.
2.2.	**Eingabekontrolle**	
	Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie	nicht relevant

Nr.	Gebiet	Beschreibung
	lange auf Applikationen zugegriffen hat?	
	Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?	Rollen-/Rechtekonzepte und diverse Lizenzmodelle mit unterschiedlichen Berechtigungskonzepten.
	Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß den Weisungen des Auftraggebers erfolgen kann?	Zugriffskontrolle anhand des Rollen-/Rechtekonzepts zur ordnungsgemäßen Datenbearbeitung und Speicherung.
	Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers durchführt?	Sämtliche Unterauftragnehmer unterliegen den gleichen Vorgaben wie der Auftragnehmer. Entsprechende Verträge sind geschlossen. Die Pflichten zur Überprüfung der Unterauftragnehmer übernimmt der Datenschutzbeauftragte des Auftragnehmers. Er ist auch bei der Auswahl der beauftragten Firmen maßgeblich beteiligt.
	Wie wird die Löschung / Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt?	Festlegung durch Vertragsbindung, bei Wegfall des Zweckes ist ebenfalls eine Löschung der Daten indiziert.
3	**Verfügbarkeit und Belastbarkeit**	
3.1.	**Verfügbarkeitskontrolle**	
	Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind?	Die Datenträger sind bei Unterauftragnehmer „All-incl.com“ – Subunternehmer gesichert. Entsprechender Vertrag wurde abgeschlossen.
	Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?	Ständig aktuelle Virenscanner und Spamfilter finden Einsatz. Die Systeme werden regelmäßig upgedatet.
	Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?	Physische Löschung bei funktionsfähigen Datenträgern und mechanische Zerstörung defekter Datenträger vor Entsorgung
3.2.	**Wiederherstellbarkeit**	
	Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten? (rasche Wiederherstellbarkeit nach Art. 32 Abs.1 lit.c DS-GVO)	Die eingesetzten Systeme sind technisch redundant vorhanden. Der Datenbestand unterliegt einer regelmäßigen Sicherung.
4.	**Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO, Art. 25 Abs. 1 DS-GVO)**	

Nr.	Gebiet	Beschreibung
	Welche Verfahren gibt es zur regelmäßigen Bewertung/Überprüfung, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management)?	Der externe Datenschutzbeauftragte überprüft regelmäßige und teilweise auch unangekündigt, die Einhaltung der technisch-organisatorischen Maßnahmen.
	Wie wird auf Anfragen bzw. Probleme reagiert (Incident-Response-Management)?	Ticketsystem „Mantis“, zusätzlich Telefonhotline.
	Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DS-GVO)?	Keine Vorbelegung durch Hacken; bei Anmeldung im System erfolgen keine Vorbelegungen; Benutzer muss die Anmeldeinformationen jeweils eintragen.
4.1	**Auftragskontrolle**	
	Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsdatenverarbeitung (Datenschutz-Management)?	Das Vertragswerk wurde entsprechend den neuen Richtlinien zur Auftragsdatenverarbeitung gestaltet. Der externe Datenschutzbeauftragte nimmt entsprechende Beratung- und Kontrollpflichten wahr.