Vertrag zur Auftragsverarbeitung

zwischen dem/der

X.....

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

F7 Media GmbH, Humboldtstraße 67a, 22083 Hamburg

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

Präambel

Gegenstand der Vereinbarung sind die Rechte und Pflichten der Parteien im Rahmen der Leistungserbringung gemäß Auftrag, Leistungsbeschreibung und AGB (nachfolgend Hauptvertrag), soweit eine Verarbeitung von personenbezogenen Daten durch den Auftragnehmer als Auftragsverarbeiter für den Auftraggeber gemäß Art. 28 DSGVO erfolgt.
Dies umfasst alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Auftrags erbringt und die eine Auftragsverarbeitung darstellen. Dies gilt auch, sofern der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.
Die Dauer der Verarbeitung entspricht der im Auftrag vereinbarten Laufzeit.
Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will, oder dass der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.
Sollte eine Bestimmung dieses Vertrages ab Vertragsschluss bis zum 25.05.2018 gegen das BDSG verstoßen, wird sie durch die entsprechende gesetzliche Bestimmung des BDSG ersetzt.

1. Art und Zweck der Verarbeitung

1.1. Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO zur Erfüllung des Auftrags.

1.2. Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistung im Bereich:

X

☐ Webhosting	☐ Domainservice	☐ Virtual Server Hosting
☐ Dedicated Server Hosting	☐ Internet Access	☐ Software as a Service (SaaS)
☐ IT-Support	☐ Newslettermarketing	☐ Gewinnspielentwicklung
☐ Intranet	☐ Cloud-Dienstleistungen	☐ Colocation
☐ _____		

erforderlichen Zwecke.

2. Art der personenbezogenen Daten und Kategorien von Betroffenen

2.1. Die Art der verarbeiteten Daten bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten.

2.2. Die Kategorien von Betroffenen bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten.

3. Verantwortlichkeit und Verarbeitung auf dokumentierte Weisungen
Weisungsberechtigte Personen des Auftraggebers sind:

X_____

(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragnehmer sind:

Claas Wulff, Geschäftsführer, 040 / 238 4000 30
Joachim Wulff-Nielsen, Geschäftsführer, 040 / 238 4000 30

Für Weisung zu nutzende Kommunikationskanäle:
-per Ticket (projekte.f7.de)
-per E-Mail (support@f7.de)

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

3.1. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO). Dies gilt auch im Hinblick auf die in dieser Vereinbarung geregelten Zwecke und Mittel der Verarbeitung.

3.2. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) durch einzelne Weisungen geändert werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen. Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Bei Änderungsvorschlägen teilt der Auftragnehmer dem Auftraggeber mit, welche Auswirkungen sich auf die vereinbarten Leistungen, insbesondere die Möglichkeit der Leistungserbringung, Termine und Vergütung ergeben. Ist dem Auftragnehmer die Umsetzung der Weisung nicht zumutbar, so ist der Auftragnehmer berechtigt, die Verarbeitung zu beenden. Eine Unzumutbarkeit liegt insbesondere vor, wenn die Leistungen in einer Infrastruktur erbracht werden, die von mehreren Auftraggebern / Kunden des Auftragnehmers genutzt wird (Shared Services), und eine Änderung der Verarbeitung für einzelne Auftraggeber nicht möglich oder nicht zumutbar ist.

3.3. Die vertraglich vereinbarte Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, soweit nicht etwas anderes vereinbart ist, z.B. über die Produktbeschreibung der beauftragten Leistung.

3.4. Ist Vertragsbestandteil die Registrierung von Domains bei Registrierungsstellen, die ihren Sitz in einem Drittland haben (außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums), ist auch vereinbart, dass der Auftragnehmer personenbezogene Daten – unter Beachtung der zwingend anwendbaren Vorschriften – an diese Registrierungsstellen übermittelt.

3.5. Die Parteien vereinbaren außerdem, dass der Auftragnehmer berechtigt ist, personenbezogene Daten – unter Beachtung der zwingend anwendbaren Vorschriften zur Leistungserbringung in einem Drittland zu übermitteln. Dies ist insbesondere der Fall, wenn Auftragsgegenstand der Dienst eines Drittanbieters ist, der diesen Dienst ganz oder teilweise in einem Drittland erbringt.

4. Rechte des Auftraggebers, Pflichten des Auftragnehmers

4.1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor (Verpflichtung nach dem Recht der Europäischen Union oder eines Mitgliedstaates). Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

4.2. Der Auftragnehmer unterstützt angesichts der Art der Verarbeitung nach Möglichkeit den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Ansprüche der betroffenen Personen nach Kapitel III der DSGVO. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen.

4.3. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen.

4.4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Gleiches gilt für das Fernmeldegeheimnis nach § 88 TKG und – in Kenntnis der Strafbarkeit – für die Wahrung von Geheimnissen der Berufsgeheimnisträger nach § 203 StGB. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

4.5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

4.6. Der Auftragnehmer gewährleistet die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Eine Kontaktmöglichkeit wird auf der Webseite des Auftragnehmers veröffentlicht.

Beim Auftragnehmer ist als Beauftragter für den Datenschutz
Rechtsanwalt Arne Platzbecker
BKP & Partner
Palmaille 96
22767 Hamburg
(0)40 1818980 - 0
Datenschutzbeauftragter (TÜV)
Mitglied im Berufsverband der Datenschutzbeauftragten BvD e.V.
bestellt.

4.7. Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers entweder alle personenbezogenen Daten oder gibt sie dem Kunden zurück, sofern nicht nach dem Unionsrecht oder nach dem anwendbaren Recht eines Mitgliedstaates eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht oder sich aus jeweiligen vertraglichen Vereinbarungen etwas anderes ergibt. Macht der Auftraggeber von diesem Wahlrecht keinen Gebrauch, gilt die Löschung als vereinbart. Wählt der Auftraggeber die Rückgabe, kann der Auftragnehmer eine angemessene Vergütung verlangen.

4.8. Machen betroffene Person Schadensersatzansprüche nach Art. 82 DSGVO geltend, unterstützt der Auftragnehmer den

Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten. Der Auftragnehmer kann hierfür eine angemessene Vergütung verlangen.

5. Pflichten des Auftraggebers

5.1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Durchführung des Auftrags Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

5.2. Im Falle der Beendigung verpflichtet sich der Auftraggeber, diejenigen personenbezogenen Daten vor Vertragsbeendigung zu löschen, die er in den Diensten gespeichert hat.

5.3. Auf Anforderung des Auftragnehmers benennt der Auftraggeber einen Ansprechpartner in Datenschutzangelegenheiten.

6. Maßnahmen zur Sicherheit der Verarbeitung gemäß Art. 32 DSGVO

6.1. Der Auftragnehmer ergreift in seinem Verantwortungsbereich geeignete technische und organisatorische Maßnahmen, um sicher zu stellen, dass die Verarbeitung gemäß den Anforderungen der DSGVO erfolgt und den Schutz für die Rechte und Freiheiten der betroffenen Person gewährleistet. Der Auftragnehmer ergreift in seinem Verantwortungsbereich gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

6.2. Die aktuellen technischen und organisatorischen Maßnahmen sind im Anhang 1 und Anhang 2 aufgeführt.

6.3. Der Auftragnehmer betreibt ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 lit. d) DSGVO.

6.4. Der Auftragnehmer passt die getroffenen Maßnahmen im Laufe der Zeit an die Entwicklungen beim Stand der Technik und an die Risikolage an. Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, sofern das Schutzniveau nach Art 32 DSGVO nicht unterschritten wird.

7. Nachweis und Überprüfung

7.1. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt dazu bei. Inspektionen sind grundsätzlich nur nach Terminvereinbarung möglich. Der Auftragnehmer ist berechtigt, eine Verschwiegenheitserklärung vom Auftraggeber und von dessen beauftragten Prüfer zu verlangen. Der Auftragnehmer stimmt der Benennung eines unabhängigen externen Prüfers durch den Auftraggeber zu, sofern der Auftraggeber dem Auftragnehmer eine Kopie des Auditberichts zur Verfügung stellt. Wettbewerber des Auftraggebers oder Personen, die für Wettbewerber des Auftraggebers tätig sind, kann der Auftragnehmer als Prüfer ablehnen.

7.2. Für Informationen und Unterstützungshandlungen kann der Auftragnehmer eine angemessene Vergütung verlangen. Der Aufwand für den Auftragnehmer durch eine Inspektion ist grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

7.3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige staatliche oder kirchliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gelten die vorstehenden Regeln entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

8. Subunternehmer (weitere Auftragsverarbeiter)

8.1. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO zur Vertragserfüllung einzusetzen.

8.2. Die aktuell eingesetzten weiteren Auftragsverarbeiter sind:
Artfiles New Media GmbH
Zirkusweg 1
20359 Hamburg
Telefon: +49 (0)40 3202729-0
E-Mail: info@artfiles.de
Dienstleistung: Rechenzentrum

Sendinblue SAS
47, rue de la Chaussée d'Antin,
75009 Paris, Frankreich
Dienstleistung: Direkt-Marketing / E-Mail-Versand
Der Auftraggeber erklärt sich mit deren Einsatz einverstanden.

8.3. Der Auftragnehmer informiert den Auftraggeber, wenn er eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben.

8.4. Der Einspruch gegen die beabsichtigte Änderung kann nur aus einem wichtigen datenschutzrechtlichen Grund innerhalb einer angemessenen Frist nach Zugang der Information über die Änderung gegenüber dem Auftragnehmer erhoben werden. Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder – sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer nicht zumutbar ist – die von der Änderung betroffene Leistung gegenüber dem Auftraggeber innerhalb einer angemessenen Frist nach Zugang des Einspruchs einstellen.

8.5. Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen.

8.6. Als weitere Auftragsverarbeiter im Sinne dieser Regelung sind nur solche Subunternehmer zu verstehen, die Dienstleistungen erbringen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören solche Nebenleistungen, die sich auf Telekommunikationsleistungen, Druck-/Post-/Transportdienstleistungen, Wartung und Pflege, Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der personenbezogenen Daten, Netze, Dienste, Datenverarbeitungsanlagen und sonstiger IT-Systeme, beziehen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit in Bezug auf die Daten des Auftraggebers auch bei solchen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

9. Haftung und Schadensersatz

9.1. Im Fall der Geltendmachung eines Schadensersatzanspruches durch eine betroffene Person nach Art. 82 DSGVO verpflichten sich die Parteien, sich gegenseitig zu unterstützen und zur Aufklärung des zugrundeliegenden Sachverhalts beizutragen.

9.2. Die zwischen den Parteien im Hauptvertrag zur Leistungserbringung vereinbarte Haftungsregelung gilt auch für Ansprüche aus dieser Vereinbarung zur Auftragsverarbeitung und im Innenverhältnis zwischen den Parteien für Ansprüche Dritter nach Art 82 DSGVO, außer soweit ausdrücklich etwas anderes vereinbart ist.

10. Vertragslaufzeit, Sonstiges

10.1. Die Vereinbarung beginnt mit dem Abschluss durch den Kunden. Sie endet mit Ende des letzten Vertrages unter der Kundennummer. Sollte eine Auftragsverarbeitung noch nach Beendigung dieses Vertrages stattfinden, gelten die Regelungen dieser Vereinbarungen bis zum tatsächlichen Ende der Verarbeitung.

10.2. Die F7 Media GmbH kann die Vereinbarung nach billigem Ermessen mit angemessener Ankündigungsfrist ändern. Widerspricht der Kunde der Änderung nicht innerhalb einer von F7 Media gesetzten Frist, gilt die Änderung als genehmigt. F7 Media weist den Kunden in der Änderungs-Ankündigung darauf hin, dass die Änderung wirksam wird, wenn er nicht binnen der gesetzten Frist widerspricht.

10.3. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zur Auftragsverarbeitung den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarungen im Übrigen nicht.

10.4. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist Hamburg. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes. Dieser Vertrag unterliegt den gesetzlichen Bestimmungen der Bundesrepublik Deutschland.

10.5. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der DSGVO liegen.

Datum:

F7 Media GmbH Joachim Wulff-Nielsen – Geschäftsführung

_____ _____

Auftraggeber Auftragnehmer

Anlage 1: Technische und Organisatorische Maßnahmen F7 Media GmbH (Geschäftsräume)
Anlage 2: Technische und organisatorische Maßnahmen Rechenzentrum Artfiles New Media GmbH

Anlage 1 Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

Technische und Organisatorische Maßnahmen F7 Media GmbH (Geschäftsräume)

1. Zutrittskontrolle

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

- Alarmanlage
- Manuelles Schließsystem
- Videoüberwachung der Zugänge
- Lichtschranken / Bewegungsmelder
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Begleitung von Besuchern
- Sorgfältige Auswahl von Reinigungspersonal. Diese sind bei der F7 Media GmbH angestellt.

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Gemeint ist hiermit im Gegensatz zur Zutrittskontrolle das Eindringen in das EDV-System selbst seitens unbefugter Personen:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Nur ausgewählte Administratoren haben Zugang zum Server
- Administratoren haben individuelle Benutzerkennung
- Regelungen zum Schutz und zur regelmäßigen Änderung der Zugangspasswörter
- Erstanmeldung erfolgt über ein Initialpasswort welches nach erfolgreicher Anmeldung unregelmäßig geändert werden muss.
- Bildschirmschoner sind mit Passwortschutz versehen
- Sorgfältige Auswahl von Reinigungspersonal

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Bestehen eines Berechtigungskonzepts für die Server und für alle TYPO3-Systeme (onBoard)
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Differenzierte Zugriffsrechte entsprechend der Aufgaben der jeweiligen Mitarbeiter
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Fernzugriff auf Kundensysteme ist via verschlüsselter IP-Sec-Verbindung möglich
- Sichere Aufbewahrung von Datenträgern
- Physische Löschung von Datenträgern vor Wiederverwendung
- Mobile/Wechseldatenträger kommen nicht zum Einsatz

Folgende Überwachungstools werden eingesetzt:

- Antivirus-Software
- Firewall
- Web-Proxy / E-Mail-Proxy
- Spammarkierung
- Web-Application-Firewall
- SSL-verschlüsselte Übertragung von Daten aus Terminal-Sitzungen

4. Weitergabekontrolle

Maßnahmen, 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.

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Folgende Elemente werden protokolliert:

- Betroffener Datensatz
- Art der Aktivität (Neuanlage, Veränderung, Löschung des Datensatzes)
- Zeitpunkt der Aktivität bzw. des Ereignisses
- Ausführende Person (Benutzerkennzeichen)

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die Sie von externen Dienstleistern in Ihrem Auftrag verarbeiten lassen, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Feuerlöschgeräte in Serverräumen
- Serverräume nicht unter sanitären Anlagen
- Einhaltung von Aufbewahrungsfristen

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

Anlage 2 Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

Technische und organisatorische Maßnahmen Rechenzentrum Artfiles New Media GmbH

Die F7 Media GmbH unterhält im Rechenzentrum der Artfiles New Media GmbH, Zirkusweg 1, 20359 Hamburg externe Server. Diese Server werden ausschließlich von der F7 Media GmbH betrieben und gewartet. Folgende technischen und organisatorischen Maßnahmen zum Schutz der dort gespeicherten Daten werden von der Artfiles New Media GmbH und der F7 Media GmbH ergriffen:

1. Zutrittskontrolle

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

- Alarmanlage
- Chipkarten-/Transponder-Schließsystem
- Manuelles Schließsystem
- Biometrische Zugangssperren
- Videoüberwachung der Zugänge
- Lichtschranken / Bewegungsmelder
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Begleitung von Besuchern
- Sorgfältige Auswahl von Reinigungspersonal
- Zugangsbereiche: Chipkarte und PIN.
- Colocationfläche: Handvenenerkennung (biometrisch)

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Gemeint ist hiermit im Gegensatz zur Zutrittskontrolle das Eindringen in das EDV-System selbst seitens unbefugter Personen:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit biometrischen Verfahren
- Authentifikation mit Benutzername / Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Gehäuseverriegelungen
- Einsatz von VPN-Technologie
- Sicherheitsschlösser
- Nur ausgewählte Administratoren haben Zugang zum Server
- Administratoren haben individuelle Benutzerkennung
- Regelungen zum Schutz und zur regelmäßigen Änderung der Zugangspasswörter
- Erstanmeldung erfolgt über ein Initialpasswort welches nach erfolgreicher Anmeldung geändert werden muss. *(nicht durchgängig)*
- Bildschirmschoner sind mit Passwortschutz versehen und werden nach spätestens 3 Minuten inaktiv *(nicht durchgängig)*
- Sorgfältige Auswahl von Reinigungspersonal = *F7*
- Verschlüsselung von mobilen Datenträgern *(nicht durchgängig)*
- Verschlüsselung von Smartphone-Inhalten *(nicht durchgängig)*
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Bestehen eines Berechtigungskonzepts für die Server und für alle TYPO3-Systeme (onBoard)
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste" reduziert
- Differenzierte Zugriffsrechte entsprechend der Aufgaben der jeweiligen Mitarbeiter
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Fernzugriff auf Kundensysteme ist via verschlüsselter IP-Sec-Verbindung möglich
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- Mobile/Wechseldatenträger kommen nicht zum Einsatz.

Folgende Überwachungstools werden eingesetzt:

- Antivirus-Software
- Firewall
- Web-Proxy / E-Mail-Proxy
- Spammarkierung
- Web-Application-Firewall
- SSL-verschlüsselte Übertragung von Daten aus Terminal-Sitzungen

4. Weitergabekontrolle

Maßnahmen, 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.

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Folgende Elemente werden protokolliert:

- Betroffener Datensatz
- Art der Aktivität (Neuanlage, Veränderung, Löschung des Datensatzes)
- Zeitpunkt der Aktivität bzw. des Ereignisses
- Ausführende Person (Benutzerkennzeichen)

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die Sie von externen Dienstleistern in Ihrem Auftrag verarbeiten lassen, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

a. Maßnahmen

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

• schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG
• Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
• Auftragnehmer hat Datenschutzbeauftragten bestellt
• Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
• Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

• Unterbrechungsfreie Stromversorgung (USV)
• Klimaanlage in Serverräumen
• Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
• Schutzsteckdosenleisten in Serverräumen
• Feuer- und Rauchmeldeanlagen
• Feuerlöschgeräte in Serverräumen
• Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
• Bestehen eines Backup- & Recoverykonzepts
• Erstellen eines Notfallplans
• Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
• Serverräume nicht unter sanitären Anlagen
• Einhaltung von Aufbewahrungsfristen

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

• Logische Mandantentrennung (softwareseitig)
• Erstellung eines Berechtigungskonzepts
• Versehen der Datensätze mit Zweckattributen/Datenfeldern
• Festlegung von Datenbankrechten
• Trennung von Produktiv- und Testsystem