Allgemeine Erklärung zur Auftragsdatenverarbeitung

der Verlag für Neue Medien Data Communicatiomns GmbH

Bötzinger Str. 48, 79111 Freiburg im Breisgau, Bundesrepublik Deutschland

Ausgabe 2018-05-20

Diese Erklärung wird durch Unterzeichnung durch den Auftraggeber und Übersendung an den Auftragnehmer zum

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

zwischen

Firma/Name
Strasse
Plz-Ort
Land / Staat
Telefon, Email, www

- nachstehend **Auftraggeber** genannt -

und der

Verlag für Neue Medien Data Communications GmbH
Bötzinger Str. 48
79111 Freiburg im Breisgau - Bundesrepublik Deutschland

- nachstehend **Auftragnehmer** genannt -

0. Präambel

Der Auftragnehmer wirkt seit 1995 aktiv am Aufbau und der Erschließung des Nutzens des Internets und dessen Möglichkeiten für Unternehmen und Privatpersonen mit. Die Kommunikation im Internet ist eine moderne, nützliche und einfache Art der zwischenmenschlichen Kommunikation. Es gehört zum guten Ton, sich beim Gespräch gegenseitig mit Namen vorzustellen. Und es wird als angenehm empfunden, wenn sich Menschen bei der nächsten Begegnung noch an einen erinnern. Und mancher freut sich sogar über einen Glückwunsch zum Geburtstag. Insofern erscheinen Regelungen der DSGVO zumindest fraglich. Ein konsequent fertiggedachtes Recht auf Vergessen zum Beispiel würde wohl so manche Gehirnoperation begründen, oder zumindest medikamentöse Behandlung von z.B. Mitarbeitern, die persönliche Daten von Kunden, Lieferanten und Kollegen auf Wunsch sofort vergessen müssen und nicht bei Gesprächen verwenden dürfen.

Der Auftraggeber unterwirft sich ausdrücklich nur mit großer Sorge und unter Vorbehalt den Vorschriften der DSGVO. Die nachfolgenden Regelungen und Zusagen beschreiben die aktuelle Realität, des Machbare und das maximal Erträgliche.

Dem Datenschutz und dem weitgehenden fairen Umgang mit persönlichen oder betrieblichen Daten von Geschäftspartnern trägt der Auftragnehmer aus Überzeugung schon seit Beginn seiner Tätigkeit auch in Bereichen außerhalb des Internets nach bestem Können, Wissen und Gewissen Rechnung.

1. Gegenstand, Grundsätzliches und Dauer des Auftrags

1.1.Gegenstand des Auftrags

Der Auftragnehmer stellt dem Auftraggeber je nach Leistungsangebot gegen Entgelt oder unentgeltlich Serverkapazitäten im Internet z.B. zum Betrieb einer Internetseite, zum Empfangen und Versenden von Emails, zum Betrieb von Kommunikations- und Werbeplattformen oder zur Teilnahme an vom Auftragnehmer bereit gestellten Kommunikations- und Werbeplattformen zur Verfügung.

Die Systeme ermöglichen dem Auftraggeber, dass er auf den bereitgestellten Systemen auch personenbezogene Daten einstellt, erfasst, ändert oder löscht. Dabei ist es Wesen der Serviceleistung, dass der Auftragnehmer personenbezogene Daten für den Auftraggeber im Sinne des Art. 4 Nr. 2 und Art. 28 DSGVO verarbeitet, was im Rahmen einer gemeinsamen Nutzung von personenbezogenen Daten auch mit anderen Auftragnehmern (z.B. beim Betrieb von Plattformen des Auftragnehmers) erfolgen kann oder auch ausschließlich für den Auftraggeber ohne eine Mitnutzung durch den Auftragnehmer (z.B. Bereitstellung von Webspace oder Online-Datenbanken zur exklusiven Nutzung durch den Auftraggeber und seiner Geschäftspartner).

Die Leistung und das entsprechende Entgelt sind in definierten Aufträgen festgelegt oder ergeben sich durch die einseitige Erklärung des Auftraggebers durch Anmeldung zu Serviceleistungen des Auftragnehmers durch Registrierung.

1.2. Erfassung, Verarbeitung, Änderung, Löschung von personenbezogenen Daten

Der Auftragnehmer gewährleistet im Rahmen der gemeinsamen Nutzung von personenbezogenen Daten durch Auftragnehmer und Auftraggeber oder im Rahmen einer ausschließlichen Nutzung und Verarbeitung durch den Auftragnehmer die Einhaltung der Regelungen der DSGVO, soweit dies mit aktuellen Programmsystemen technisch oder organisatorisch möglich ist. Bei Weiterentwicklungen von eigenen Programmsystemen und beim Einsatz von Fremdsoftware wird der Auftragnehmer darauf achten, dass diese, soweit dies mit zumutbarem organisatorischem, technischen und wirtschaftlichen Aufwand möglich ist, eingehalten werden.
Personenbezogene Daten werden in der Regel in regelmäßigen Abständen gelöscht, wenn sie von Auftraggeber oder Auftragnehmer nicht mehr auf Systemen des Auftragnehmers benötigt oder gewünscht werden. Auftraggeber sind dabei alle an den durch den Auftragnehmer betriebenen Systemen angemeldeten Nutzer – in der Regel Kunden mit Auftrag aber auch angemeldete Nutzer für Plattformen, Anfragesysteme, Newsletter, Kommunikationsfunktionen oder Gewinnspiele.

Die Erfassung, Verarbeitung, Änderung, Löschung von personenbezogenen Daten, die zur ausschließlichen Nutzung durch den Auftraggeber auf vom Auftragnehmer bereitgestellten oder betreuten Systemen verarbeitet werden, kann der Auftragnehmer in der Regel (soweit technisch oder organisatorisch möglich) selbst im Vollzugriff durchführen. Sollte hierzu die Unterstützung des Auftragnehmers notwendig sein oder gewünscht werden, sind die auf Weisung des Auftraggebers durchgeführten Maßnahmen grundsätzlich entgeltpflichtig. Dem Auftragnehmer muss im Verhältnis zum notwendigen Aufwand und unter Berücksichtigung der jeweils zur Verfügung stehenden Kapazitäten angemessen Zeit zur Durchführung der Weisung durch den Auftraggeber eingeräumt werden.

1.3. Dauer des Auftrags

Der Auftrag ist unbefristet und kann im Laufe der Zusammenarbeit nach Bedarf angepasst und erweitert werden. Eine Änderung der dem Auftraggeber bereitgestellten Leistungen kann bei unentgeltlich bereitgestellten Leistungen jederzeit einseitig durch den Auftragnehmer oder Auftraggeber auch durch einseitige Erklärung (auch online auf einer Webseite oder durch Email) erfolgen.

Abhängig von den durch den Auftragnehmer bereitgestellten Leistungen gelten Mindestvertragszeiten und Kündigungsfristen (z.B. durch Auftrag oder Allgemeine Geschäftsbedingungen festgelegt) Bei einseitiger Einschränkung des Leistungsumfangs durch den Auftragnehmer hat der Auftraggeber ein außerordentliches Kündigungsrecht. Sofern Bestimmungen der DSGVO nicht eingehalten werden bzw. eingehalten werden können, können sowohl der Auftraggeber als auch der Auftragnehmer auf Basis dieser Vereinbarung unter Berufung auf einen wichtigen Grund zusätzlich fristlos kündigen.

1.4. Kosten für gewünschte Mehraufwendungen trägt der Auftraggeber

Alle im Rahmen dieses Auftrags dem Auftragnehmer entstehenden internen Aufwendungen sind gemäß jeweils aktuellen Stundensätzen (Projektmanagement) durch den Auftraggeber zu vergüten. Externe Aufwendungen z.B. für externe Rechtsanwaltskosten bzw. die Bestellung externer Datenschutzbeauftragter sind zu den dem Auftragnehmer berechneten Entgelte zzgl. einer Verwaltungspauschale von 20% auf den Wert der eingekauften Leistung jeweils zzgl. MwSt. zu vergüten.

Für zusätzliche vom Auftraggeber erwartete oder beauftragte organisatorische Maßnehmen und Auskunftsbereitschaft im Rahmen dieser Vereinbarung wird ergänzend zu diesem Vertrag ein individueller Auftrage abgeschlossen und ein angemessenes einmaliges und laufendes Entgelt vom Auftraggeber an den Auftragnehmer entrichtet.

2. Konkretisierung des Auftragsinhalts (Art und Zweck der Verarbeitung)

2.1. Umfang der verarbeiteten personenbezogenen und sonstigen Daten

Je nach Geschäftsbeziehung unterstützt der Auftraggeber den Auftragnehmer gegen Entgelt oder ohne Entgelt unterschiedlich bei der Erhebung, Speicherung, Verarbeitung, Nutzung, Änderung und Löschung von Daten:

Grundsätzlich gilt dieser Auftragsdatenverarbeitungsvertrag nur für Datenverarbeitung im Rahmen von Internet-Auftritten (Homepages), Bereitstellung von Email-Konten, Registrieren und Verwalten von Domainnamen, Gemeinsame Nutzung von Funktionen auf Kommunikations- und Werbeplattformen im Internet und Bereitstellung von Datenaustauschbereichen im Internet.

Für alle diese Datenverarbeitungen sind in der Regel schon seit Jahren sowohl aufgrund vertraglicher Vereinbarung als auch auf freiwilliger Basis Vorkehrungen zur Datensicherheit gegen unbefugte Benutzung durch Dritte, gegen Verlust von Daten mittels Datensicherungseinrichtungen, Zugriffs- und Veränderungsschutz durch mehrstufige Berechtigungskonzepte und passwortreglementierten Zugang zu den Systemen usw. realisiert. In der Regel sind Serviceleistungen des Auftragnehmers für Auftraggeber währen der Arbeitszeit (Mo-Fr von 8:00 bis 16:30 – außer an deutschen Feiertagen) verfügbar, wobei weder Reaktionszeiten noch Bearbeitungszeiten garantiert werden können, auch wenn erfahrungsgemäß sehr

schnelle und kundenfreundliche Bearbeitung durch den Auftragnehmer erfolgt, kann davon kein Anspruch durch Auftraggeber abgeleitet werden.

Priorisierung von Vorgängen und Aufträgen erfolgt nach eigenem Ermessen des Auftragnehmers nach Umsatz mit dem Auftragnehmer und nach Einschätzung von Dringlichkeiten, die sich aus Gefahren und möglichen zukünftigen Auswirkungen auf personenbezogene oder andere Daten ergeben. Nach eigenem Ermessen wägt der Auftragnehmer die Interessen aller Geschäftspartner (Anbieter, Nutzer, Lieferanten) nach eigenem Ermessen gegeneinander ab.

Obwohl die Grenzen fließend sind, handelt es sich bei der Auftragsdatenverarbeitung im Wesentlichen um folgende Vorgänge (ohne Anspruch auf Vollständigkeit):

2.1.1. Bloße Bereitstellung von Webspace gegebenenfalls mit Datenbanken

Der Auftragnehmer stellt hier in der Regel lediglich eine Systemplattform zur Verfügung. Die Daten und alle damit verbundenen Verarbeitungen, Abläufe und Schutzmechanismen liegen in der Verantwortung des Auftraggebers. Der Auftragnehmer unterstützt den Auftraggeber bei Bedarf in der Regel entgeltlich mit Know-how und Personalkapazität. Betreiber der Webseite und verantwortlich für den Inhalt ist der Auftraggeber. Nimmt der Auftraggeber hierbei zusätzliche Dienstleistungen des Auftragnehmers in Anspruch, erfolgen alle Eingriffe in den Funktionsbereich des Auftraggebers ausschließlich auf Weisung des Auftraggebers.

2.1.2. Bereitstellung von Werbe- und Kommunikationsplattformen

Der Auftragnehmer organisiert alle grundlegenden Darstellungen und Organisationsabläufe des Systems und stellt die wesentlichen Datenverarbeitungssysteme zur Verfügung. Betreiber der Webseite und inhaltlich verantwortlicher für das Gesamtsystem ist der Auftragnehmer, der zur Sicherstellung der Funktionsfähigkeit und bei Bedarf zur Sicherstellung der Einhaltung von Gesetzen und internen wie allgemein gültigen Regeln Daten eingeben, verändern oder löschen darf und gegebenenfalls Zugänge und Funktionen und Verarbeitungen einschränkt oder verändert. Die Auftraggeber haben je nach Funktion die Möglichkeit, Daten bereitzustellen, zu erfassen, von Dritten eingeben zu lassen und zu verarbeiten. Durch individuelle Einstellungen und die eigene Entscheidung über Art, Inhalt und Bearbeitung von Daten haben Auftraggeber umfassend Einfluss auf Darstellungen und Verarbeitungen von Daten und auf Verknüpfungen von Daten untereinander. Insofern haben die Auftraggeber eine Mitverantwortung für die Einhaltung gesetzlicher Regeln wie die Beachtung von Urheber- und Bildrechten und die Regeln der DSGVO. Insofern stellen Auftraggeber den Auftraggeber von Forderungen und Haftungen frei, die durch ihre unsachgemäße wissentlich oder unwissentlich verschuldeten von Dritten erhoben werden können. Die auf Plattformen durch Auftragnehmer eingegebenen Inhalte können in der Regel auch durch andere Auftragnehmer verwendet werden. Insofern übertragen Auftraggeber hier grundsätzlich Urheber und Nutzungsrechte an den Auftragnehmer und andere Auftraggeber und räumen bei Widerruf eine angemessene Frist zur Lösung eventueller Problemfälle während und auch nach Beendigung einer Geschäftsbeziehung ein.

2.2.3. Bereitstellung von Email-Serverkapazitäten und Email-Konten

Die Einrichtung und der Betrieb von Email-Konten und Email-Kommunikationsmöglichkeiten für Auftraggeber erfolgt in der Regel so, dass der Auftragnehmer alle Einstellungen und den Versand, den Empfang und die Weiterverteilung von Email-Nachrichten samt Anhängen selbst regelt und auch für den Virenschutz und andere Sicherheitssysteme gegen Gefahren oder unerwünschte Email-Kommunikation selbst regeln kann und selbst regelt. Nimmt der Auftraggeber hierbei zusätzliche Dienstleistungen des Auftragnehmers in Anspruch, erfolgen

alle Eingriffe in den Funktionsbereich des Auftraggebers ausschließlich auf Weisung des Auftraggebers.

2.2.4. Registrierung und Verwaltung von Domains

Die Registrierung von Domains und den entsprechenden Nameservice übernimmt der Auftragnehmer für den Auftraggeber, der immer rechtlich Verantwortlicher für die Domains ist. Der Auftragnehmer verfügt über das technische Know-how und die Erfahrung, die Domain-Administration sehr sicher und zuverlässig durchzuführen. Rechtlich verantwortlich bleibt immer der Auftraggeber, zumal der Auftragnehmer weder über die Expertise noch die Erlaubnis verfügt, in rechtlicher Hinsicht verbindliche Hinweise zu geben oder Empfehlungen auszusprechen. Eine Unterstützung ist hier deswegen nur technisch und organisatorisch möglich z.B. bei der Umsetzung von anwaltlichen oder richterlichen Vorgaben möglich. Auch wenn Fragen auf Wunsch des Auftraggebers durch Beschreibung des Erfahrungsschatzes und des Wissens um Fundstellen von Informationen im Internet beantwortet werden, erfolget dies immer rechtlich unverbindlich und ohne Gewähr von Richtigkeit und Vollständigkeit.

2.2.5. Andere Arten von Auftragsdatenverarbeitungen

Bedürfen grundsätzlich der gesonderten individuellen Regelung zwischen Auftragnehmer und Auftraggeber.

2.2. Räumliche Regelungen

Die Daten und deren Verarbeitungsmöglichkeiten stehen weltweit in der Regel auf allen am Internet angeschlossenen Endgeräten zur Verfügung.

Soweit nicht anders vereinbart, stellt der Auftragnehmer nach freiem Ermessen Datenverarbeitungssysteme an seinen eigenen Firmenstandorten und Räumlichkeiten und innerhalb der EU bzw. auch in einem darüber hinausgehenden Geltungsbereich der DSGVO zur Verfügung und nimmt dabei Leistungen von Unterauftragnehmern in Anspruch, die diese Voraussetzungen erfüllen.

Auch für Unterauftragnehmer gilt die Regel: Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.

Ausnahmen davon erfolgen nur auf Weisung des Auftraggebers, der dann alleine für die Einhaltung von diesbezüglichen Verpflichtungen verantwortlich bzw. haftbar ist.

2.3. Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind in der Regel folgende Datenarten / -kategorien:

2.3.1 Daten von Auftragnehmern und Auftraggebern

Name, Anschrift, Kommunikationsdaten wie Telefonnummer, Email-Adresse, Verträge, Historien, Ansprechpartner, Aufträge, Angebote, Rechnungen usw.

2.3.2. Webseiten und Plattformbetrieb im Internet:

Alles Daten, die laufend öffentlich oder in geschützten internen Bereichen im Internet angezeigt werden.

Sämtliche mittels der Webseite erfassten Daten, insbesondere:

Freiwillig über Formularfelder eingegebene Daten wir Name, Adresse, Email, Telefon und Wunsch von Auftraggebern / Interessenten

Nutzungsdaten (z.B. IP Adresse der Besucher, Besuchte Webseiten) z.B. für Erfolgskontrolle

Intern gespeicherte und/oder im Internet verfügbar gemachte Dateien (z.B. PDF-Dateien, Textdateien, Bilder, Videos, Tabellen, Dokumente, Datenbanken)

Kommunikationsdaten (z.B. Daten aus Anfragen über die Webseite, Telefonnummern, Email-Adressen)

2.3.3. E-Mail-Kommunikation

Alle eingehenden und ausgehenden Emails mit Anhang und Kommunikatsdaten wie Zeit, Absender-IP usw.

2.3.4. Daten in Onlineshops

Kundendaten, Kundenzugangsdaten, Bestellungen, Artikeldaten, Preise, Bestellhistorie, Anfragen, Servicetickets, Bezahlinformationen, Bankdaten

2.4. Kreis der Betroffenen

Auftragnehmer
Mitarbeiter des Auftragnehmers
Kunden des Auftragnehmers
Lieferanten des Auftragnehmers
Freunde, Bekannte, Fans des Auftragnehmers

Auftraggeber (in der Regel entgeltlich)
Mitarbeiter von Auftraggebern
Kunden von Auftraggebern
Lieferanten des Auftragnehmers
Freunde, Bekannte, Fans von Auftraggebern

Spezielle einmalige oder sporadisch auftretende Auftraggeber In der Regel unentgeltlich)
Bewerber
Interessenten für Dienstleistungen
Anbieter von Leistungen
Nutzer von Anfragesystemen (z.B. Urlaubsanfragen)
Newsletter-empfänger
Gewinnspielteilnehmer
Sonstige Webseitenbesucher

3. Technisch-organisatorische Maßnahmen

3.1. Allgemeine Technische Organisatorische Maßnahmen (TOM) des Auftragnehmers

Grundsätzlich trifft der Auftragnehmer in seinem normalen Geschäftsbetrieb nur organisatorische Maßnahmen für seinen eigenen Daten-Verantwortungs-Bereich und übernimmt dafür eine Verantwortung und eine Haftung. Eine auch länger dauernde Bereitstellung von Ser-

vices für Auftraggeber begründet keinen Anspruch des Auftraggebers, dass der Auftragnehmer Services dauerhaft unentgeltlich zur Verfügung stellt.

Der Auftragnehmer kann gegen Entgelt die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung z.B. im Rahmen eines Angebots dokumentieren und dem Auftraggeber zur Prüfung übergeben. Bei Akzeptanz durch den Auftraggeber (z.B. Annahme des Angebots und Erteilung eines Auftrags) werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, kann dieser gegen Entgelt umgesetzt werden.

Insgesamt handelt es sich bei den zu treffenden Maßnahmen um vom Auftragnehmer explizit benannte Standardabläufe des Auftragnehmers (nicht auftragsspezifische Maßnahmen) hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebots, die der Auftragnehmer dem Auftraggeber entgeltlich oder unentgeltlich ohne eine Anerkennung einer dauerhaften Rechtspflicht zur unentgeltlichen Bereitstellung zur Verfügung stellt: **siehe Anlage 1** - **Allgemeine Technische Organisatorische Maßnahmen (TOM)**

3.2. Auftragsspezifische und Auftragsgeberspezifische Technische Organisatorische Maßnahmen (TOM) für den Auftraggeber

Auf Wunsch eines Auftraggebers können auftrags- oder auftragsgeberspezifische Maßnahmen, die genau auftragsspezifisch bzw. auftragsgeberspezifisch beschrieben werden müssen und in der Regel mit einem einmaligen und/oder laufenden Entgelt versehen sind, insbesondere im Hinblick auf eine Garantie für Erweiterung, die Art des Datenaustauschs / Bereitstellung von Daten, Art / Umstände der Verarbeitung / der Datenhaltung sowie Art / Umstände beim Output / Datenversand, die dann auch in einer Leistungsvereinbarung (Leistung) definiert und mit einem Entgelt (Gegenleistung) versehen sind.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer grundsätzlich auch bei auftragsspezifischen oder auftragsgeberspezifischen Maßnahmen gestattet, alternative adäquate Maßnahmen vorzuschlagen und umzusetzen. Dabei wird, soweit vom Auftragnehmer erkennbar, das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten. Eine Überschreitung des vereinbarten Sicherheitsniveaus kann mit einem zusätzlichen Entgelt belegt werden. Wesentliche Änderungen werden auf Weisung des Auftraggebers speziell dokumentiert. Der Auftragnehmer stelle dem Auftraggeber auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG in der Regel gegen ein Entgelt zur Verfügung.

4. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer wird nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, berichtigen, löschen oder sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich bzw. in einem den aktuellen zeitlichen und personellen Kapazitäten entsprend möglichen Zeitraum an den Auftraggeber weiterleiten.

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer übernimmt die in diesem Auftrag definierten und nicht gesondert vergüteten Pflichten grundsätzlich nicht und wenn, dann nur freiwillig und jederzeit einstellbar aus

Kulanzgründen. Er kann eventuelle Zusatzpflichten, die sich aus neuen gesetzlichen Regelungen ergeben aus wirtschaftlichen und zeitlichen Gründen nicht unentgeltlich und umfänglich unverzüglich übernehmen.

Alle Aufwendungen für die Übernahme von Pflichten werden vom Auftraggeber bezogen auf das Risiko angemessen und nach Aufwand zu Stundensätzen oder Pauschalen vergütet. Eine regelmäßige rechtliche Überprüfung der Einhaltung kann durch den Auftraggeber erfolgen und die eventuell notwendige Ergreifung von Maßnehmen durch den Auftraggeber gegen Entgelt beim Auftragnehmer beauftragt werden.

Der Auftragnehmer übernimmt nur nach vorherigem Auftrag oder auf Weisung und bei entsprechender, gesonderter Vergütung zusätzliche Pflichten z.B. nach Artt. 28 bis 33 DS-GVO oder wie im Folgenden beispielhaft aufgeführt:

- Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.
- Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.
- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO und Anlage.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde. 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.
- Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit vorlegen.

6. Unterauftragsverhältnisse

Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

- Die Einschaltung von Unterauftragnehmern ist grundsätzlich nur mit schriftlicher Zustimmung des Auftraggebers gestattet. Ohne schriftliche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner unter Punkt 5 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie im Einzelfall andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung oder Nutzung mitteilt.

- Der Auftragnehmer hat die vertraglichen Vereinbarungen soweit möglich und zumutbar mit dem / den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
- Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung gegen Entgelt Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen sinnvolle bzw. angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

Stand Mai 2018 werden für die Auftragsdurchführung vom Auftragnehmer auch Leistung folgender Vertragspartners in Anspruch genommen (ohne Anspruch auf Vollständigkeit):

Host Europe GmbH, Hansestr. 111, 51149 Köln, Bundesrepublik Deutschland
ALL-INKL.COM Neue Medien Münnich – Inh. René Münnich, Hauptstr. 68, 02742 Friedersdorf

Für diese Leistungen gelten zusätzlich einschränkend und nicht erweiternd die entsprechenden Regelungen des jeweiligen Partners.

7. Kontrollrechte des Auftraggebers

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. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Für die dafür notwendigen Aufwendungen des Auftragnehmers bezahlt der Auftraggeber ein Entgelt und muss dem Auftragnehmer auch unter Berücksichtigung dessen aktueller Personalkapazität und Auftragslage ausreichend Zeit einräumen.
Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zerti-

fizierung durch IT-Sicherheits- oder Datenschutzaudit erbracht werden. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Die notwendig werdende Beauftragung externer Dienstleister und die dafür notwendigen internen Kosten trägt der Auftraggeber.
Sofern durch die Wahrnehmung der Kontrollpflichten und Kontrollwünsche des Auftragnehmers Aufwendungen entstehen, die nicht im Leistungsumfang geregelt sind, für die ein Entgelt bezahlt wird, sind Zusatzleistungen grundsätzlich dem Auftragnehmer nach Preisliste zu vergüten bzw. dafür notwendige zu beauftragende Fremdleistungen mit einem zusätzlichen Aufgeld für Verwaltung und Abrechnung zu ersetzen.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten und bei der Erfüllung von Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und bei vorherigen Konsultationen.
Zusätzliche präventive Maßnahmen können vom Auftraggeber gegen Entgelt beauftragt werden.
Hierzu gehören u.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, die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden, 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 und die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung, die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.
Für Unterstützungsleistungen, die nicht ausdrücklich in bestehenden Leistungsbeschreibungen enthalten sind und nicht auf ein vorsätzliches Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen. Der Auftraggeber muss dem Auftragnehmer auch unter Berücksichtigung dessen aktueller Personalkapazität und Auftragslage ausreichend Zeit einräumen

9. Weisungsbefugnis des Auftraggebers

Mündliche Weisungen sind für den Auftragnehmer nur bindend, wenn der Auftragnehmer diese bestätigt (mind. Textform). Der Auftraggeber erteilt deswegen, will er eine Verpflichtung ableiten, nur schriftliche Weisungen. Der Auftragnehmer informiert den Auftraggeber, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist dann berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird (mind. Textform).

10. Löschung von Daten und Rückgabe von Datenträgern

Kopien oder Duplikate der Daten werden ohne mit vertretbarem Aufwand des Auftraggebers zu erlangendes oder unter Berücksichtigung des allgemeinen Standards vom Auftragnehmer anzunehmendem 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 des Auftragnehmers erforderlich sind.
Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer

sämtliche in seinen Besitz gelangte 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. Nur wenn der Auftraggeber bei Beauftragung ein entsprechendes Protokolle ausdrücklich gegen Entgelt beauftragt wird der Auftragnehmer ein Protokoll der Löschung erstellen, archivieren und auf Anforderung vorlegen.
Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, können durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus gegen Entgelt aufzubewahren – der Auftragnehmer ist grundsätzlich nur für seine eigenen Aufbewahrungspflichten verantwortlich - der Auftragnehmer kann nicht alle auch individuellen Archivierungspflichten der Auftraggeber (z.B. branchenspezifisch oder aus Verträgen mit Dritten) kennen. Deshalb obliegt es dem Auftraggeber, alle Pflichten bei Beauftragung zu benennen und gegebenenfalls nachträglich gegen Entgelt zusätzlich schriftlich zu beauftragen, dass der Auftragnehmer diese übernimmt bzw. einhält.
Der Auftragnehmer kann alle Unterlagen, Daten und Dokumentationen zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Auftraggeber

Ort / Datum
Unterschrift
Name

Auftragnehmer

Ort / Datum
Unterschrift
Name

Allgemeine Technische Organisatorische Maßnahmen (TOM)

Verlag für Neue Medien Datacommunications GmbH 2018-05-20

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**: Die Server in Freiburg sind physikalisch mit verschlossener Tür geschützt, die nur mit Schlüssel geöffnet werden kann. Virtuelle oder Physische Server bei Dienstleistern (innerhalb des Gültigkeitsbereichs der DSGVO) sind bei den Dienstleistern entsprechend deren TOM geschützt.
- **Zugangskontrolle**: Die Programme, Datenbanken und Eingabebereiche interner und externer Inhalte sind weitgehend durch verschlüsselte Kennwörter geschützt und soweit möglich auch über Einschränkung der IP-Bereiche oder VPN-Netzwerk-Verbindungen.
- **Zugriffskontrolle:** Ein Lesen, Kopieren, Verändern oder Entfernen von Daten innerhalb des Systems sind durch Berechtigungen eingeschränkt. Bei Datenelementen in Datenbanken z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen, soweit diese verfügbar sind – In der Regel besteht keine umfassende Historie.
- **Trennungskontrolle:** Die Datenstrukturen haben Berechtigungen, die bestimmten Benutzern Komplettzugriff ermöglichen und anderen Benutzern nur Zugriff auf einen Teil. Um das zu gewährleisten, liegen diese Daten technisch in einer Datenbanktabelle. Die Zuordnung erfolgt logisch auf Datensatzebene. Eine komplette Mandantentrennung findet deswegen nicht statt, auch , weil dies im weitest gefassten Fall die Speicherung jedes einzelnen Datensatzes in einer separaten Datenbank erfordern würde. In der Regel können außer den Mitarbeitern des Auftragnehmers nur wenige Berechtigte (z.B. Newlsletterversender und Newsletterempfänger als Auftraggeber) Daten eingeben/erfassen, übertragen, ändern oder löschen). Mitarbeiter des Auftragnehmers verändern Daten auf Weisung von Auftraggebern oder zur Aufrechterhaltung des Betriebs oder zu Sicherungszwecken.
- **Pseudonymisierung**: (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) Der Überwiegende Teil der Daten (Kundendaten) dienen zur Anzeige von Adresse oder gesetzlich vorgeschriebenen Anzeigen auf Homepages (z.B. Name des Datenschutzbeauftragten – hier ist eine Pseudomisierung nicht möglich, weil die Daten auf Internetseiten gemäß DSGVO speziell zum Anbieter angezeigt werden müssen. Andere Daten (wie Email-Adressen von Newsletterempfängern) sind pseudomisiert sinnlos. Der Umfang der zusammen gespeicherten Daten von Personen, die diese zur Nutzung von Serviceleistung oder zum Empfang von Newslettern, zur Teilnahme von Gewinnspielen oder zur Urlaubsanfrage bereitstellen, wird durch diese Personen selbst bestimmt. Formulare enthalten in der Regel keine Pflichtfelder, sodass solche Einzelauftraggeber auch leere Datensätze eingeben können, was aber für den Eingebenden keinen Sinn macht. Zusatzdaten betreffen den Nachweis, wann welche Services von diesen Auftraggebern genutzt bzw. bereitgestellt wurden.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**: In der Regel werden die Daten per SFTP verschlüsselt übertragen. Kontaktformulare sind in der Regel per SSL verschlüsselt. Ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, ist damit weitgehend sichergestellt. Da in der Regel Fremdsoftware und meist Open-Source-Software eingesetzt wird, können prinzipiell Sicherheitslücken vom Auftragnehmer nicht ausgeschlossen werden. Das Schließen von solchen Lücken hat eine hohe Priorität beim Auftragnehmer.

- **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Es ist durch Serverprotokolle weitgehend nachvollziehbar, es erfolgt aber keine umfangrei-

che Historie pro Datensatz (z.B. wer hat den Satz von welcher IP wann historisch verändert).

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie. Die Daten werden auf den Serversystemen regelmäßig wiederherstellungsfähig gesichert. Darüber hinaus erfolgt in der Regel werktäglich eine Differenz-Sicherung auf ein spezielles Backupsystem, von dem Aus Daten und Anwendungen wieder hergestellt werden können, wenngleich eine unentgeltliche Widerherstellung nicht zugesagt wird.
- **Rasche Wiederherstellbarkeit:** (Art. 32 Abs. 1 lit. c DS-GVO). Eine Wiederherstellung ist werktags von 8:00 -16:30 technisch meist in einer angemessenen Zeit möglich. Voraussetzung ist eine Weisung und ein entgeltpflichtiger Auftrag des Auftraggebers. Über ein Online-Meldeformular https://www.vfnm.de/stoerung kann auch ein Service außerhalb der Arbeitszeiten beauftragt werden. Es gibt keine zugesagten Firsten für Reaktion oder Behebung von Störungen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Ein **Datenschutz-Management** erfolgt seit Auftragsbeginn beim Auftragnehmer jeweils durch den sinnvollen Einsatz der verfügbaren und der Anwendung angemessenen technischen und organisatorischen Mitteln. Neuverordnete Dokumentationsregularien werden vom Auftragnehmer für die Daten umgesetzt, bei denen er selbst Auftraggeber ist. Incident-Response-Management erfolgt seit Auftragsbeginn beim Auftragnehmer und führte in über 20 Jahren zu sehr hohen Verfpügbarkeiten der Services. Neuverordnete Dokumentationsregularien werden aktuell von Auftragnehmer umgesetzt, sofern sie für personenbezogene Daten gelten, für deren Verarbeitung der Auftragnehmer auch Auftraggeber ist. Wenngleich andere Auftragnehmer davon in der Regel automatisch profitieren, sind diese Serviceleistungen in der Regel entgeltpflichtig.
- **Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DS-GVO) sind soweit sinnvoll umgesetzt. Es gibt z.B. in der Regel keine Pflichtfelder oder positiv vorbelegte Entscheidungsfelder bei Formularen.
- **Auftragskontrolle**: Für die Zusammenarbeit gilt beim Auftragnehmer als Grundlage immer das gesprochene Wort oder ein Wunsch eines Auftraggebers. In der Regel werden freiwillig nur Auftragsdatenverarbeitungen durchgeführt, die von Auftraggebern gewünscht sind. Es kann deshalb ausdrücklich nicht für alle Auftraggeber zugesagt werden, dass keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen. Eine individuelle Vereinbarung ist gegen Entgelt möglich, wobei vorsorglich darauf hingewiesen wird, dass dann lange Reaktionszeiten entstehen, weil Weisungen dann z.B. nur an genau eine genau benannte weisungsempfangsberechtigte Person erfolgen müssen, weil der Auftragnehmer nur so die Forderungen organisatorisch einhalten kann.