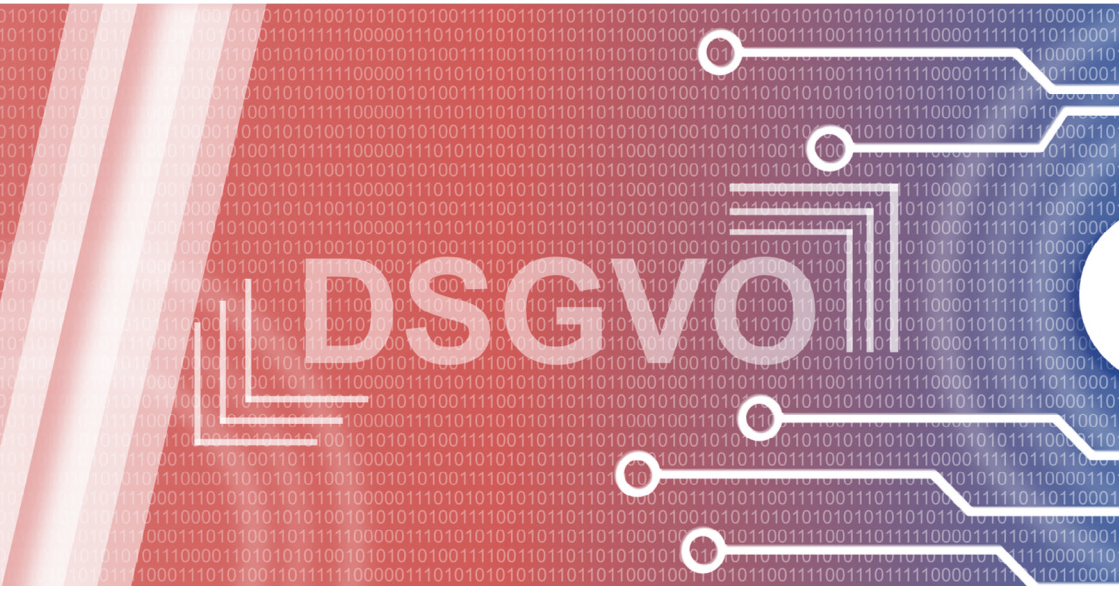
Mittelstand 4.0
Kompetenzzentrum
Chemnitz

Betrieb 4.0
machen!



EU-Datenschutzgrundverordnung und damit verbundener Anpassungsbedarf für Webseiten

Prof. Dr. Dagmar Gesmann-Nuissl & Dipl.-Jur. Univ. Gernot Kirchner

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Impressum

Herausgeber:

Mittelstand 4.0-Kompetenzzentrum Chemnitz
Geschäftsstelle
c/o Technische Universität Chemnitz
Prof. Dr.-Ing. Egon Müller
DE – 09107 Chemnitz
Tel: 0371 531 19935
Fax: 0371 531 819935

E-Mail: info@betrieb-machen.de
Web: www.betrieb-machen.de
www.kompetenzzentrum-chemnitz.digital

Redaktion & Gestaltung:

Prof. Dr. Dagmar Gesmann-Nuissl
Dipl.-Jur. Univ. Gernot Kirchner
Romy Kertzsch

Bildnachweis Titel:

Pixabay, skylarvision

Inhalt

1 Einführung

Am 25. Mai 2018 war es nun endlich soweit, die bereits im Mai 2016 in Kraft getretene DSGVO wurde wirksam, ebenso wie zahlreiche damit im Zusammenhang stehende nationale Rechtsregelungen, insbesondere im Datenschutzrecht.

Auch wenn sich sachlich nüchtern betrachtet, das Datenschutzrecht innerhalb der Bundesrepublik Deutschland hierdurch nicht um 180 Grad gewandelt hat, so ist es doch erforderlich, die Neuerungen möglichst präzise umzusetzen. Davon betroffen sind jedoch nicht nur Unternehmen, sondern auch der öffentliche Bereich und damit letztlich auch alle existierenden Mittelstand 4.0-Kompetenzzentren aus dem Förderschwerpunkt »Mittelstand-Digital«. Mittelstand 4.0-Kompetenzzentren sind beim Betreiben eines eigenen Webauftrittes nicht nur Telemediendiensteanbieter im Sinne des Telemediengesetzes (TMG), sondern verarbeiten darüber hinausgehend auch nicht ganz unerhebliche Mengen an personenbezogenen Daten (z. B. Teilnehmerdaten von Veranstaltungen, Daten von Ansprechpartnern kooperierender KMUs etc.), so dass insbesondere die eigene Datenverarbeitung im Lichte der neuen DSGVO sowie der entsprechenden nationalen Bestimmungen überprüft werden sollte. Dies vermeidet zum einen Gesetzesverstöße, wahrt daneben aber auch die vertraglich vereinbarten Förderbedingungen, die ebenfalls ausdrücklich ein datenschutzkonformes Handeln der Mittelstand 4.0-Kompetenzzentren voraussetzen.

Der nunmehr vorliegende Leitfaden zum Anpassungsbedarf für Webseiten der Mittelstand 4.0-Kompetenzzentren soll hierbei eine erste Hilfestellung geben, will und kann im Ergebnis aber eine individuelle Beratung und Prüfung nicht ersetzen.

Gerade deshalb bitten wir um Beachtung, dass der vorliegende Handlungsleitfaden lediglich dem unverbindlichen Informationszweck dient und **keine Rechtsberatung** darstellt. Die erteilten abstrakten Informationen können, sollen und dürfen eine individuelle und verbindliche Rechtsberatung nicht ersetzen. Es ist damit insbesondere nicht möglich, die in diesem Zusammenhang erteilten Informationen auf den jeweiligen konkreten Einzelfall – unproblematisch – zu übertragen. So kann insbesondere keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit der bereitgestellten Informationen übernommen werden, zumal das Recht – und vor allem auch das Datenschutzrecht – einer ständigen Dynamik unterliegt.

Prof. Dr. Dagmar Gesmann-Nuissl
Dipl.-Jur. Univ. Gernot Kirchner

2 Impressum

Die Pflicht allgemeine Informationen als Telemediendiensteanbieter zur Verfügung zu stellen (sogenannte Impressumspflicht) ergibt sich aus § 5 TMG.

2.1 Telemediendiensteanbieter

Telemediendiensteanbieter ist nach § 2 Nr. 1 TMG jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt. Bei audiovisuellen Mediendiensten auf Abruf ist Telemediendiensteanbieter jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert.

2.2 Verhältnis TMG und DSGVO

Bezogen auf die Impressumspflicht wird die DSGVO wohl keine Änderungen herbeiführen. Das kann man zum einen aus Art. 95 DSGVO schließen, der ausdrücklich darauf hinweist, dass keine zusätzlichen Verpflichtungen im Bereich der öffentlich zugänglichen elektronischen Kommunikationsdienste durch die DSGVO auferlegt werden, soweit sie besonderen in der Richtlinie 2002/58/EG (ePrivacy-Richtlinie) festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen. Zum anderen aus der sich derzeit im Entwurf befindlichen ePrivacy-Verordnung (Entwurf vom 10. Januar 2017, einsehbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017PC0010), die gerade diesen Themenkomplex anbetreffen wird und damit allenfalls in der Zukunft durch die Inkraftsetzung der Verordnung Änderungen zu erwarten sind.

2.3 Allgemeine Informationspflicht nach § 5 TMG

Mithin bleibt es jetzt – und wohl vorerst – dabei, dass Diensteanbieter für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien **nachfolgend aufgelistete Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar (sogenannte Zwei-Klicks-Rechtsprechung)** zu halten haben:

- Namen und Anschrift der Niederlassung, bei juristischen Personen zusätzlich die Rechtsform, den Vertretungsberechtigten und sofern Angaben über das Kapital der Gesellschaft gemacht werden, das Stamm- oder Grundkapital sowie der Gesamtbetrag der ggf. noch ausstehenden Einlagen,

- Angaben, die schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, inkl. E-Mailadresse,
- bei genehmigungspflichtigen Diensten die zuständige Aufsichtsbehörde,
- Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister sowie die entsprechende Registernummer,
- ggf. zusätzliche Informationen bei reglementierten Berufen (u. a. Hochschuldiplom, berufliche Befähigungsnachweise): Kammer, gesetzliche Berufsbezeichnung und verleihenden Staat, berufsrechtliche Regelungen und deren Zugänglichkeit,
- Umsatzsteuer-Identifikationsnummer nach dem Umsatzsteuergesetz oder Wirtschafts-Identifikationsnummer nach der Abgabenordnung,
- bei Kapitalgesellschaften u.U. Abwicklungs-/Liquidationsangabe (AG, KGaA, GmbH).

Weitere von § 5 Abs. 1 TMG unberührte (vgl. § 5 Abs. 2 TMG) Informationspflichten können sich außerdem aus der Verordnung über Informationspflichten für Dienstleistungserbringer (Dienstleistungs-Informationspflichten-Verordnung - DL-InfoV) ergeben. Diese findet Anwendung für Personen, die Dienstleistungen erbringen, die in den Anwendungsbereich des Art. 2 Richtlinie 2006/123/EG (Europäische Dienstleistungsrichtlinie) fallen.

2.4 Beispiel-Impressum

Mittelstand 4.0-Kompetenzzentrum Musterstadt
Universität »Musterstadt« (Körperschaft des öffentlichen Rechts)
Vertretungsberechtigung: Herr/Frau Max Mustermann (Rektor)
Musterstraße 123
DE-12345 Musterstadt
+49 (0) 1234/567891 (Telefon)
+49 (0) 1234/567892 (Fax)
mustermann@muster.de (E-Mail)
www.mustermann.de (Website)

[Herausgeber i.S.d. Landespresserechts, str.]

Zuständige Aufsichtsbehörde: [...]

Umsatzsteuer-Identifikationsnummer, gem. § 27a UStG: DE 123456789

Verantwortlicher i.S.d. § 55 Abs. 2 Rundfunkstaatsvertrag (RStV):
Max Mustermann
Musterstraße 123
DE-12345 Musterstadt

Technische Umsetzung: [...]

3 Datenschutzbestimmung/-erklärung

3.1 Informationspflicht gemäß § 13 Abs. 1 TMG

Auch nach Inkrafttreten der DSGVO muss jeder Telemediendiensteanbieter gemäß § 13 Abs. 1 TMG den Nutzer **zu Beginn des Nutzungsvorgangs** über

- Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über
- die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG (Datenschutz-Richtlinie)

allgemein unterrichten. Daran wird man wohl auch festhalten müssen, wenn man die noch zu erwähnende Positionsbestimmung der unabhängigen Datenschutzbehörden zur Anwendbarkeit des TMG vom 26. April 2018 berücksichtigt, insbesondere mit Blick auf Art. 13 DSGVO.

§ 13 Abs. 1 TMG enthält eine **allgemeine Unterrichtungspflicht**, wonach der Diensteanbieter den Nutzer über **Art, Umfang, Zweck der Erhebung und Verwendung der personenbezogenen Daten zu unterrichten hat und zwar in einer Weise, dass der Nutzer jederzeit in der Lage ist, die Rechtmäßigkeit der Datenerhebung abschätzen zu können**.

Die Unterrichtungspflicht hat in **allgemein verständlicher Form** und immer dann zu erfolgen, sofern und soweit eine solche Unterrichtung nicht schon erfolgt ist. Impliziert wird damit nicht nur eine **übersichtliche, sprachlich und äußerlich ansprechende Gestaltung der Datenschutzerklärung** selbst, sondern auch, dass alle darin **enthaltenen Verlinkungen zutreffend, aktuell und anklickbar sein müssen**. Im Übrigen muss die Datenschutzerklärung auf die Bedürfnisse des jeweiligen Bereichs zugeschnitten sein, d. h. **sie muss jedenfalls alle Datenverarbeitungsvorgänge auf der Webseite abdecken**.
Als Beispiel seien hier der Newsletterversand, Kontaktformulare, Kommentar-/Bewertungsbereiche, geschützte Mitgliederbereiche etc. zu nennen, d. h. kurz zusammengefasst alle Bereiche, in denen personenbezogene Daten in irgendeiner Form verarbeitet werden.

Die **Unterrichtungspflicht gilt auch dann, wenn der Personenbezug erst im Rahmen eines automatisierten Verfahrens**, das heißt ohne individuelle Entscheidung des Nutzers, **zu einem späteren Zeitpunkt hergestellt wird (z. B. bei Cookies)**. Das heißt, sofern eine spätere Identifizierung des Nutzers möglich ist und die Erhebung oder Verwendung personenbezogener Daten diese Identifizierung vorbereitet, muss der Nutzer schon **zu Beginn des Verfahrens** über die anstehenden Abläufe unterrichtet werden.

Der Inhalt der Informationen im Rahmen der allgemeinen Unterrichtungspflicht nach § 13 Abs. 1 TMG (Datenschutzbestimmung/-erklärung) muss für den Nutzer **jederzeit abrufbar** sein.

3.2 Informationspflicht gemäß Art. 13 DSGVO

Ergänzt wird diese allgemeine Informationspflicht des Diensteanbieters nunmehr durch Art. 13 DSGVO, sofern personenbezogene Daten bei Personen erhoben werden, wenngleich die dort postulierten Informationspflichten nur dann erforderlich werden, wenn und soweit die betroffenen Personen nicht bereits über entsprechende Informationen verfügen (Art. 13 Abs. 4 DSGVO).

Gemäß Art. 13 Abs. 1 DSGVO hat der Diensteanbieter/Verantwortliche dem Betroffenen zum Zeitpunkt der Erhebung der personenbezogenen Daten Folgendes mitzuteilen:

- Namen und Kontaktdaten des Verantwortlichen sowie ggf. des Vertreters;
- ggf. Kontaktdaten des Datenschutzbeauftragten;
- Zwecke der Datenverarbeitung sowie Rechtsgrundlage;
- ggf. berechtigte Interessen i.S.d. Art. 6 Abs. 1 lit. f) DSGVO;
- ggf. Empfänger(-kategorien) der personenbezogenen Daten und
- ggf. Übermittlungsabsicht an Drittland oder internationale Organisation sowie Vorhandensein/Fehlen eines Angemessenheitsbeschlusses oder im Falle einer Übermittlung i.S.d. Art. 46, 47 oder 49 Abs. 1 UA 2 DSGVO einen Verweis auf die geeigneten/angemessenen Garantien und Kopiermöglichkeit/Verfügbarkeitshinweis.

Zusätzlich zu den vorgenannten Informationen müssen dem Betroffenen zum Zeitpunkt der Datenerhebung folgende weitere Informationen zur Verfügung gestellt werden, die notwendig sind, um eine faire, transparente Verarbeitung zu gewährleisten (Art. 13 Abs. 2 DSGVO):

- Speicherdauer bzw. Kriterien für deren Festlegung;
- Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht, Recht auf Datenübertragbarkeit;
- Widerrufsrecht für die Zukunft betreffend Einwilligung i.S.d. Art. 6 Abs. 1 lit. a) oder Art. 9 Abs. 2 lit. a) DSGVO;
- Beschwerderecht bei Aufsichtsbehörde;
- Datenbereitstellung gesetzlich/vertraglich vorgeschrieben oder für Vertragsabschluss erforderlich, Pflicht des Betroffenen zur Datenbereitstellung und mögliche Folgen bei Nichtbereitstellung sowie
- Bestehen einer automatisierten Entscheidungsfindung (inkl. Profiling, Art. 22 Abs. 1 bis 4 DSGVO) und aussagekräftige Informationen über involvierte Logik sowie Tragweite und angestrebten Auswirkungen.

3.3 Muster-Datenschutzerklärung für Webseite

Ein gutes und entsprechend der DSGVO aktualisiertes **Muster für eine Datenschutzerklärung** betreffend einen Onlineauftritt wird vom Deutschen Anwaltverein (DAV) zur Verfügung gestellt (https://anwaltverein.de/de/praxis/datenschutz?file=files/anwaltverein.de/downloads/praxis/datenschutz/dav-muster-datenschutzerklaerung.pdf). Ergänzend kann zudem auf die Musterdatenschutzerklärung für Betreiber von Webseiten von Prof. Dr. Thomas Hoeren und den Mitarbeitern der Forschungsstelle Recht des DFN-Vereins zurückgegriffen werden: https://www.uni-muenster.de/ Jura.itm/hoeren/itm/wp-content/uploads/Musterdatenschutzerk%C3%A4rung-nach-der-DSGVO.docx.

Bei jeder als Muster verfügbaren und nicht individuell angefertigten Datenschutzerklärung ist aber zu beachten, dass diese keine Rechtsberatung im konkreten Einzelfall ersetzen kann. Auch die hier verlinkten Muster können demnach **nur eine Orientierungshilfe** darstellen und müssen modifiziert und für den jeweiligen Einzelfall angepasst werden.

3.4 DSGVO-Datenschutzerklärung, Checkliste

- ☐ Namen, Kontaktdaten des Verantwortlichen sowie ggf. Vertreters
- ☐ Kontaktdaten des Datenschutzbeauftragten
- ☐ Art, Umfang und Zwecke der Datenverarbeitung
- ☐ Rechtsgrundlagen der Datenverarbeitung
- ☐ Berechtigte Interessen i.S.d. Art. 6 Abs. 1 lit. f) DSGVO (sofern relevant)
- ☐ Empfänger(-kategorien) der personenbezogenen Daten
- ☐ Übermittlung an Drittland oder internationale Organisation
  - ☐ Angemessenheitsbeschluss oder
  - ☐ geeignete/angemessene Garantien + Verfügbarkeit
- ☐ Speicherdauer, andernfalls Kriterien für die Festlegung dieser Dauer
- ☐ Auskunfts-, Berichtigungs-, Löschungsrecht, Recht auf Einschränkung der Verarbeitung, Widerspruchsrecht, Recht auf Datenübertragbarkeit
- ☐ Recht, die Einwilligung jederzeit für die Zukunft zu widerrufen
- ☐ Beschwerderecht bei Aufsichtsbehörde
- ☐ Gesetzliche/Vertragliche Pflicht zur Datenbereitstellung oder Erforderlichkeit für Vertragsabschluss bzw. Pflicht zur Bereitstellung der Daten und mögliche Verletzungsfolgen
- ☐ Automatisierte Entscheidungsfindung (inkl. Profiling): involvierte Logik sowie Tragweite und angestrebten Auswirkungen für Betroffenen

4 Erlaubnistatbestände

In Bezug auf die Verarbeitung personenbezogener Daten besteht zunächst gemäß Art. 6 Abs. 1 DSGVO ein Verbot mit Erlaubnisvorbehalt, so dass die Datenverarbeitung grundsätzlich unzulässig ist, aber diese Unzulässigkeit durch eine Erlaubnis beseitigt werden kann (»unzulässig, sofern nicht erlaubt«).

Unter Datenverarbeitung versteht man in diesem Zusammenhang gemäß Art. 4 Nr. 2 DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Bezogen auf jeden einzelnen Datenverarbeitungsfall muss – um die Unzulässigkeit zu beseitigen – geprüft werden, ob ein entsprechender Erlaubnistatbestand vorliegt.

Solche **Erlaubnistatbestände** können nach Art. 6 Abs. 1 DSGVO folgende sein:

- Einwilligung;
- Erfüllung eines (Vor-)Vertrags;
- Erfüllung rechtlicher Verpflichtung;
- Schutz lebenswichtiger Interessen einer natürlichen Person;
- Wahrnehmung Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt;
- Wahrung berechtigter Interessen des Verantwortlichen/eines Dritten unter Abwägung mit Interessen oder Grundrechte und Grundfreiheiten des Betroffenen.

Die **Einwilligungserklärung** ist einer unter vielen Erlaubnistatbeständen bezogen auf die Verarbeitung personenbezogener Daten. Sie ist jedenfalls erforderlich, wenn kein anderer der genannten Erlaubnistatbestände greift. Gerade in strittigen Fallkonstellationen – z. B. bei der Berufung auf die Wahrung berechtigter Interessen – sollte jedoch eine Einwilligungserklärung vorsorglich zusätzlich eingeholt werden, um rechtssicher und nicht angreifbar zu agieren.

Die Bedingungen für die Einwilligung sind in § 7 DSGVO aufgeführt. Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, **muss diese in verständlicher und leicht zugänglicher Form, in einer klaren und einfachen Sprache erfolgen** (§ 7 Abs. 2 DSGVO). Darüber hinausgehend haben sich die **Anforderungen** im Vergleich zur Einwilligung nach dem BDSG (§§ 4a, 28 Abs. 3 BDSG a. F.) **etwas verschärft**.

Im Einzelnen:

- Zur Freiwilligkeit: Es dürfen keine sogenannten Koppelgeschäfte vorliegen (Art. 7 Abs. 4 DSGVO), d. h. die Erfüllung eines Vertrages oder die Erbringung einer Dienstleistung darf nicht von der Einwilligung abhängig gemacht werden. Die Widerrufbarkeit muss sich so einfach wie die Erteilung gestalten. Die Erbringung des Dienstes soll bei Fragen rund um die Einwilligung nicht unterbrochen werden.
- Zur Bestimmtheit: Für verschiedene Zwecke / Verarbeitungsvorgänge müssen separate Einwilligungen abgegeben werden.
- Zur Informiertheit: Der Einwilligende muss über Zweck und Umfang der Verarbeitung, über den Verantwortlichen, über das Widerrufsrecht (galt bisher im Wesentlichen nur im TMG), insbesondere auch über die Folgen der Verweigerung und des Widerrufs der Einwilligung informiert sein.
- Zur Unmissverständlichkeit: Die Einwilligung muss aus einer (regelmäßig schriftlichen) Erklärung oder einer sonstigen aktiven, eindeutig bestätigenden Handlung des Einwilligenden bestehen, z. B. durch Anklicken eines Kästchens oder Auswahl entsprechender Einstellungen (Vorsicht: Privacy by default, Art. 25 Abs. 2 DSGVO). Sie kann aber auch mündlich oder elektronisch geleistet werden (Problem: Nachweisbarkeit).
- Zur Nachweisbarkeit: Die Einwilligung muss auch noch nach Jahren nachweisbar sein (§ 7 Abs. 1 DSGVO). Insofern sollten Erklärungen z. B. eingescannt und mit dem Namen des Einwilligenden getaggt werden. Dies erleichtert die Auffindbarkeit vormals abgegebener Einwilligungserklärungen.

- Bei Minderjährigen: Bei Kindern bis 16 Jahren kann die Einwilligung in Bezug auf Dienste der Informationsgesellschaft nur mit Zustimmung des Erziehungsberechtigten erfolgen (Art. 8 DSGVO).

4.1 Newsletterversand[1]

Der **Versand eines Newsletters setzt** – wie soeben dargelegt – in der Regel **eine vorherige ausdrückliche und eindeutig bestätigende Einwilligung des informierten Nutzers voraus**. Da diese Einwilligung vom Seitenbetreiber nachgewiesen werden muss (Art. 7 Abs. 1 DSGVO), ist das sogenannte **Double-Opt-In-Verfahren** – in der Regel in Verbindung mit einer elektronischen Protokollierung i.S.d. § 13 Abs. 2 TMG – erforderlich. Ein einfaches Opt-Out-Verfahren ist dagegen nicht zulässig.

Der Nutzer hat zudem das Recht, die Einwilligung jederzeit zu widerrufen und **muss vor Abgabe der Einwilligung über sein Widerrufsrecht informiert werden** (Art. 7 Abs. 3 DSGVO). Da der Widerruf genauso einfach wie die Erteilung der Einwilligung sein muss, sollte bei jedem Versand auf die Möglichkeit einer Austragung aus dem Newsletter-Verteiler hingewiesen und ein (anklickbarer) Link zur Abmeldung vom Newsletter in den Newsletter-Mails (Opt-Out) eingebunden werden.

Ausnahmsweise ist gemäß § 7 Abs. 3 UWG elektronisch versandte Werbung **auch ohne ausdrückliche Einwilligung** zulässig, sofern alle nachfolgend genannten Voraussetzungen **kumulativ** (!) vorliegen:

- der Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse (E-Mailadresse o.a.) erhalten hat und
- der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet und
- der Kunde der Verwendung nicht widersprochen hat und
- der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

4.2 Webseiten-Formulare zur Kontaktaufnahme

Bei der **Einbindung eines Kontaktformulars auf der Webseite** ist – wie bereits oben aufgezeigt – die Datenschutzerklärung entsprechend zu ergänzen, so dass der entsprechende Datenverarbeitungsvorgang die personenbezogenen Daten über das Kontaktformular mit umfasst. Im Idealfall lässt man den Einwilligenden vor Absenden des Kontaktformulars die Datenschutzerklärung nochmals ausdrücklich bestätigen. Ungeachtet der ordnungsgemäßen Erfüllung dieser Informationspflicht berechtigt dies aber in keinem Fall dazu, sämtliche möglichen Daten zu erheben, sondern es dürfen nur die erhoben werden, die erforderlich sind, um gerade die Anfrage aus der Kontaktaufnahme zu bearbeiten (Datensparsamkeit/-minimierung, Art. 5 Abs. 1 lit. c) DSGVO).

Darüber hinausgehend ist zu gewährleisten, dass der **Datenaustausch über das Kontaktformular nur mittels verschlüsselter Verbindung** (Secure Sockets Layer – SSL bzw. dem »Nachfolger« Transport Layer Security – TLS) erfolgt. Dies wird bereits von § 13 Abs. 7 TMG vorausgesetzt und nunmehr aber nochmals durch den Grundsatz der Vertraulichkeit und Integrität personenbezogener Daten aus der DSGVO konkretisiert, Art. 5 Abs. 1 lit. f), 32 DSGVO.

Eine datenschutzrechtliche Einwilligungserklärung zur Verarbeitung der personenbezogenen Daten für die Anfragenbearbeitung ist dagegen regelmäßig nicht erforderlich, zumindest sofern die Verarbeitung auf Anfrage der betroffenen Person für die Erfüllung eines (Vor-)Vertrags erfolgt, dessen Vertragspartei die betroffene Person selbst ist (Art. 6 Abs. 1 lit. b) DSGVO), beziehungsweise die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (Art. 6 Abs. 1 lit. f) DSGVO). Gerade letzteren Erlaubnistatbestand wird man bei der bloß wunschgemäßen Bearbeitung der Kontaktanfrage – nicht jedoch für eine sich gegebenenfalls anschließende Speicherung der Daten – regelmäßig zu bejahen haben.

Im Falle von Art. 6 Abs. 1 lit. f) DSGVO ist allerdings ergänzend zu beachten, dass dem Betroffenen in diesen Konstellationen ein Widerspruchsrecht aus Art. 21 DSGVO zur Verfügung steht. Die betroffene Person muss daher spätestens zum Zeitpunkt der ersten Kommunikation mit dem Verantwortlichen ausdrücklich auf dieses Widerspruchsrecht hingewiesen werden. Der Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

Wird dagegen ungeachtet der obigen Ausführungen eine Einwilligung als Erlaubnistatbestand zur Verarbeitung der mittels Kontaktformular übermittelten personenbezogenen Daten verlangt, so sind weiter gehend u. a. die Voraussetzungen von Art. 7 DSGVO zu berücksichtigen. Die betroffene Person ist in diesem Falle vor allem vor Abgabe der Einwilligung über das insoweit bestehende Widerrufsrecht zu informieren, vgl. Art. 7 Abs. 3 DSGVO.

Abschließend ist daher festzuhalten, dass gerade der Einsatz von Kontaktformularen in der Regel eine **Einzelfallbeurteilung** erfordert, die an dieser Stelle nicht vorgenommen werden kann, so dass eine besondere Rücksicht geboten ist.

4.3 Personenbezogene Daten bei Blog-Einträgen

In Bezug auf die datenschutzkonforme Ausgestaltung von Blog-Einträgen ist **eine zwingende Einzelfallbeurteilung** erforderlich, so dass keine umfassende rechtliche Beurteilung für alle möglichen Einzelfälle erfolgen kann. Im Folgenden werden daher nur die wesentlichsten Punkte beschrieben, die regelmäßig zutreffend sind.

In jedem Fall **muss die Datenschutzerklärung im Hinblick auf die Blog-Einträge angepasst sein bzw. werden (Informationspflicht)**. Insoweit kann auf das oben Gesagte zur Datenschutzerklärung und zum Kontaktformular verwiesen werden, wobei insbesondere genauestens darauf zu achten ist, welche personenbezogenen Daten durch den Blog-Eintrag verarbeitet werden, sofern keine anonyme Nutzung eingestellt und gewünscht ist.

Bei der Kommunikation über die eigene Webseite muss zudem die **nötige Datensicherheit im Sinne von Art. 32 DSGVO und § 64 BDSG n. F. beachtet werden.** Es ist damit ebenfalls wiederum zu gewährleisten, dass der Datenaustausch nur mittels verschlüsselter Verbindung (Secure Sockets Layer – SSL bzw. dem »Nachfolger« Transport Layer Security – TLS) erfolgt, vgl. bereits § 13 Abs. 7 TMG sowie Art. 5 Abs. 1 lit. f), 32 DSGVO (Grundsatz der Vertraulichkeit und Integrität personenbezogener Daten). Dies gilt im Übrigen auch, wenn der eigene Webauftritt auf einer fremden Webseite eingebettet ist, z. B. Facebook, Xing, Twitter, YouTube etc. Der EuGH hat zudem am 5. Juni 2018 die Mitverantwortung eines Facebook-Webseiten-Betreibers für Datenschutzverstöße von Facebook bejaht (Az.: C-210/16).

In Abhängigkeit von den jeweils eingesetzten Tools sind **zudem die Anforderungen an eine Auftragsverarbeitung, die Bestimmungen zum Cookie-Einsatz sowie die Grundsätze zur Datenübertragung in ein Drittland (z. B. auch reCAPTCHA von Google) zu beachten**. Gerade weil damit Blog-Einträge ohne vorherige Einzelfallbeurteilung kaum datenschutzkonform ausgestaltet werden können, ist das Führen eines Verzeichnisses über alle Verarbeitungstätigkeiten hilfreich, Art. 30 DSGVO.

4.4 Verwendung von CRM-Systemen

CRM steht für Customer Relationship Management und damit für Systeme, die die Kundenpflege bzw. das Kundenbeziehungsmanagement betreffen. Damit sind CRM-Systeme besonders vom Datenschutz und damit auch von den Neuerungen durch die DSGVO betroffen. Wenngleich an dieser Stelle hervorgehoben werden muss, dass nicht alle denkbaren CRM-Systeme allgemein beurteilten werden können, so dass eine Begrenzung auf die Aspekte erfolgen muss, die regelmäßig anzutreffen sind.

Zunächst ist daher darauf hinzuweisen, dass es sich beispielsweise bei einer cloudbasierten CRM-Lösung regelmäßig um eine Auftragsverarbeitung i.S.d. Art. 28 f. DSGVO handeln wird, so dass die dort aufgezeigten Voraussetzungen zu beachten sind. Weitere Details werden im Anschluss gesondert vorgestellt.

Art. 5 Abs. 1 lit. a) DSGVO verlangt ferner, dass die Datenverarbeitung auf rechtmäßige Weise geschieht, wofür der Verantwortliche verantwortlich ist und die Einhaltung auch nachweisen können muss, sogenannte Rechenschaftspflicht i.S.d. Art. 5 Abs. 2 DSGVO. Für CRM-Systeme bedeutet dies, dass im System selbst die Rechtsgrundlage der Datenverarbeitung abgebildet sein muss. Das System selbst muss beispielsweise Einwilligungserklärungen für den Newsletterversand abbilden und nachweisen können, ebenso wie es Widersprüche und Widerrufe archivieren können muss, so dass eine erneute Datenverarbeitung nicht (versehentlich) erfolgen kann. Eng damit verbunden ist die Informationspflicht nach Art. 13 DSGVO, die verlangt, dass zum Zeitpunkt der Erhebung der personenbezogenen Daten die betroffene Person in der dort dargestellten Weise zu informieren ist. Regelmäßig sind es daher die CRM-Systeme selbst, bei denen die erstmalige Datenerhebung erfolgt, so dass auch das Erfüllen der Informationspflicht systemseitig sichergestellt werden muss.

Vor allem die Art. 12 ff. DSGVO gewähren darüber hinausgehend der betrof-

fenen Person eine Vielzahl von Rechten, die im CRM-System abbildbar sein müssen. Besonders hervorzuheben und damit zu prüfen ist beispielsweise, ob das eigene CRM-System die nachfolgenden Rechte des Betroffenen abbilden, gegebenenfalls sogar (teil-)automatisiert erfüllen und entsprechend den Nachweis hierfür (Protokollierung) erbringen kann:

- Auskunftsrecht, Art. 15 DSGVO, u. a. Verarbeitungszwecke, Kategorien personenbezogener Daten, Empfänger oder Kategorien von Empfängern, geplante Speicherdauer, Beschwerderecht bei Aufsichtsbehörde
- Berichtigungsrecht, Art. 16 DSGVO,
- Recht auf Löschung (»Recht auf Vergessenwerden«), Art. 17 DSGVO,
- Recht auf Datenübertragbarkeit, Art. 20 DSGVO,
- Widerrufs- und Widerspruchsrecht, Art. 7 Abs. 3 und Art. 21 DSGVO

5 Auftragsverarbeitung, Art. 28 f. DSGVO

Als Auftragsverarbeiter versteht man gemäß Art. 4 Nr. 8 DSGVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Anders ausgedrückt, erlaubt es die Privilegierung über die Auftragsverarbeitung Daten an Dritte zu übermitteln, ohne dass ein darüber hinausgehender gesonderter Erlaubnistatbestand hierfür vorliegen muss, da diese bei rechtskonformer Ausgestaltung zur Organisation des Verantwortlichen zu rechnen sind. Neu ist aber, dass der Auftragsverarbeiter analog zum Verantwortlichen nunmehr zum Teil mit in die Verantwortung genommen wird.

5.1 Voraussetzungen einer Auftragsverarbeitung

Ist eine solche **Auftragsverarbeitung** angedacht, so muss sichergestellt sein, dass der Auftragsverarbeiter hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung **im Einklang mit den Anforderungen der DSGVO** erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen (verbindlichen) Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten (Art. 28 Abs. 3 S. 1 DSGVO). Der Vertrag oder das andere Rechtsinstrument ist **schriftlich** abzufassen, was auch in einem **elektronischen Format** erfolgen kann. Entscheidend ist, dass dieser Vertrag den Gegenstand und die Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte der Parteien festlegt.

5.2 Auftragsverarbeitungsvertrag

Im Einzelnen sind im zugrunde liegenden Auftragsverarbeitungsvertrag insbesondere **folgende Punkte zu regeln** (Art. 28 Abs. 3 S. 2 DSGVO):

- Weisungsgemäße Datenverarbeitung (Ausnahme: gesetzliche Pflicht, aber grundsätzlich vorherige Informationspflicht)
- Vertraulichkeitsverpflichtung/angemessene gesetzlichen Verschwiegenheitspflicht
- Pflicht zu Maßnahmen nach Art. 32 DSGVO (Datensicherheit), wobei sich

an dieser Stelle anbietet, die technischen/organisatorischen Maßnahmen so konkret wie möglich zu beschreiben

- Einhaltung von Art. 28 Abs. 2, 4 DSGVO (Unteraufträge)
- Unterstützung des Verantwortlichen bzgl. Betroffenenrechte (Kap. III)
- Unterstützung des Verantwortlichen bei Pflichterfüllung nach Art. 32-36 DSGVO (Datensicherheit, Verletzungsmeldungen/-benachrichtigungen, Datenschutzfolgenabschätzung, Konsultation Aufsichtsbehörde)
- Löschung/Rückgabe nach Abschluss (Ausnahme: gesetzliche Speicherpflicht)
- Zurverfügungstellung von allen Informationen zum Nachweis der datenschutzkonformen Auftragsverarbeitung i.S.d. Art. 28 DSGVO
- Ermöglichung/Unterstützung von Überprüfungen, inkl. Inspektionen

5.3 Weisungsgebundenheit

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten (Weisungsgebundenheit, Art. 29 DSGVO), es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

In diesem Zusammenhang ist jedoch zu beachten, dass den Auftragsverarbeiter gegenüber dem Verantwortlichen selbst eine unverzügliche **Informationspflicht gemäß Art. 28 Abs. 3 a.E. DSGVO** trifft, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

5.4 Unterauftragsverarbeitung

Eine **Unterauftragsverarbeitung** i.S.d. Art. 28 Abs. 2 DSGVO ist **ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen unzulässig**. Im Fall einer allgemeinen schriftlichen Genehmigung hat der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter zu informieren. Dadurch erhält der Verantwortliche die Möglichkeit, gegen derartige Änderungen Einspruch zu erheben.

In jedem Fall müssen bei einer Unterauftragsverarbeitung jedem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen (verbindlichen) Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt werden, die in dem Vertrag oder anderen (verbindlichen) Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Art. 28 Abs. 3 DSGVO festgelegt sind (s.o.). Im Rahmen dessen müssen insbesondere hinreichende Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so **haftet der erste Auftragsverarbeiter** gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

5.5 Funktions-/Datenübertragung an Dritte

Die unter dem BDSG a. F. noch bestehende Bezeichnung der **Funktionsübertragung**, die gerade im Gegensatz zur Auftragsdatenverarbeitung nicht privilegiert ist und einen gesonderten Erlaubnistatbestand wegen der Datenübertragung an einen neuen/eigenen Verantwortlichen benötigt, **lässt sich der DSGVO dagegen so nicht mehr entnehmen**.

Art. 28 Abs. 10 DSGVO regelt insoweit aber richtungsweisend, dass unbeschadet der Art. 82, 83 und 84 DSGVO ein Auftragsverarbeiter, der unter Verstoß gegen die DSGVO die Zwecke und Mittel der Verarbeitung selbst bestimmt, in Bezug auf diese Verarbeitung eigene Verantwortung übernimmt und damit selbst als Verantwortlicher zu behandeln ist.

6 Verzeichnis aller Verarbeitungstätigkeiten

Art. 30 Abs. 1 S. 1 DSGVO verlangt, dass jeder Verantwortliche und gegebenenfalls sein Vertreter ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen, führt. Das Verzeichnis ist schriftlich oder auch in einem elektronischen Format zu führen, Art. 30 Abs. 3 DSGVO. Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters haben gemäß Art. 30 Abs. 4 DSGVO der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung zu stellen.

6.1 Ausnahmetatbestand unterhalb von 250 Mitarbeitern

Ausgenommen von der Pflicht ein Verzeichnis über alle Verarbeitungstätigkeiten zu führen sind Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, Art. 30 Abs. 5 DSGVO. Dies gilt jedoch dann nicht, wenn die von ihnen vorgenommene Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen in sich birgt, die Verarbeitung nicht nur gelegentlich oder es eine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DSGVO (besondere Kategorien personenbezogener Daten, u. a. Gesundheitsdaten) bzw. Art. 10 DSGVO (strafrechtliche Verurteilungen und Straftaten) erfolgt.

Unabhängig von den in Art. 30 Abs. 5 DSGVO manifestierten Ausnahmen ist aber darauf hinzuweisen, dass der Verantwortliche für die Einhaltung der in Art. 5 Abs. 1 DSGVO enthaltenen Datenschutzgrundsätze verantwortlich ist und deshalb auch deren Einhaltung nachweisen können muss (sogenannte Rechenschaftspflicht). Indirekt angesprochen wird damit folglich ein **Datenschutzmanagementsystem**, da zudem Art. 24 Abs. 1 DSGVO ergänzend von dem Verantwortlichen verlangt, dass dieser unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umsetzt, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt. Auch in den eigentlich ausgenommenen Fällen des Art. 30 Abs. 5 DSGVO kann es daher sinnvoll sein, ein Verzeichnis über alle Verarbeitungstätigkeiten vorzuhalten, um der Rechenschaftspflicht gerecht werden zu können.

6.2 Mindestinhalt – Verantwortlicher

Ist ein Verzeichnis über alle Verarbeitungstätigkeiten zu führen, so hat es gemäß Art. 30 Abs. 1 S. 2 DSGVO alle folgenden Angaben zu enthalten:

- Namen/Kontaktdaten des (gemeinsamen) Verantwortlichen und gegebenenfalls des Vertreters des Verantwortlichen sowie des Datenschutzbeauftragten;
- Verarbeitungszwecke;
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- Übermittlungen von personenbezogenen Daten an (welches) Drittland oder an (welche) internationale Organisation sowie Dokumentierung geeigneter Garantien im Fall des Art. 49 Abs. 1 UA 2 DSGVO;
- Löschungsfristen für Kategorien (sofern möglich);
- Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DSGVO (sofern möglich).

§ 70 Abs. 1 BDSG n. F. ergänzt darüber hinausgehend insbesondere die folgenden Mindestangaben für das Verzeichnis über alle Verarbeitungstätigkeiten:

- gegebenenfalls die Verwendung von Profiling;
- gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an Stellen in Drittstaat oder an internationale Organisation;
- Angaben über Rechtsgrundlage der Verarbeitung;
- die vorgesehenen Löschungsfristen oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten.

6.3 Mindestinhalt - Auftragsverarbeiter

Hat der Auftragsverarbeiter und gegebenenfalls sein Vertreter nach oben Genanntem ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Datenverarbeitung zu führen, so muss dieses gemäß Art. 30 Abs. 2 DSGVO folgende Mindestangaben enthalten:

- Namen/Kontaktdaten des/der Auftragsverarbeiter/s und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und des Datenschutzbeauftragten;
- Kategorien von Verarbeitungen, die im Auftrag durchgeführt werden;
- Übermittlungen von personenbezogenen Daten an (welches) Drittland oder an (welche) internationale Organisation sowie Dokumentierung geeigneter Garantien im Fall des Art. 49 Abs. 1 UA 2 DSGVO;
- Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DSGVO (sofern möglich).

7 Einsatz von Webtracking-Tools[2]

Bei dem Einsatz von Webtracking-Tools wie zum Beispiel Piwik/Matomo, Google Analytics, WP Statistics, Clicky handelt es sich um eine automatisierte Verarbeitung personenbezogener Daten, um u. a. bestimmte persönliche Vorlieben oder Interessen zu identifizieren, zu bewerten oder vorherzusagen (sogenanntes Profiling, Art. 4 Nr. 4 DSGVO).

Erforderlich ist hierfür der Einsatz von **Cookies**. Darunter versteht man Informationen, die auf dem Computer des Nutzers in einer kleinen Textdatei hinterlegt und bei einem erneuten Besuch einer bestimmten Internetseite von deren Betreiber ausgelesen werden. Damit beinhalten Cookies aber zugleich regelmäßig personenbezogene Daten und sind datenschutzrechtlich relevant. Dies gilt selbst dann, wenn die Informationen nicht ohne Weiteres einer spezifischen Person zugeordnet werden können, da sie im Rahmen der abgespeicherten Cookies gerade pseudonymisiert i.S.d. Art. 4 Nr. 5 DSGVO worden sind.

Zum Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien können Nutzungsprofile anhand von pseudonymisierten Daten erstellt werden, wenn der Nutzer dem nicht widerspricht (Privilegierungstatbestand des § 15 Abs. 3 TMG). Der Diensteanbieter hat den Nutzer jedoch auf sein Widerspruchsrecht im Rahmen seiner allgemeinen Unterrichtungspflicht hinzuweisen. Die DSGVO selbst regelt den Einsatz von Cookies nicht, da diese in den Anwendungsbereich der geplanten ePrivacy-Verordnung der Europäischen Union fallen. Diesbezüglich haben die unabhängigen Datenschutzbehörden des Bundes und der Länder am 26. April 2018 eine Positionsbestimmung zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018 beschlossen, welches insbesondere für den Einsatz von Web-Tracking relevant ist.

Darin heißt es, dass Art. 95 DSGVO für die §§ 11-15a TMG keine weitere Fortgeltung vorsehe und deshalb die Privilegierung aus § 15 Abs. 3 TMG für den Einsatz von Cookies auf Webseiten ab dem 25. Mai 2018 nicht mehr herangezogen werden könne. Es müsse deshalb für das Web-Tracking nach einem anderen Erlaubnistatbestand gesucht werden, wobei insbesondere Art. 6 Abs. 1 lit. a), b), f) DSGVO in Betracht kommen, d. h. die vorherige Einwilligung des Betroffenen, die Erfüllung eines (Vor-)Vertrages oder überwiegende berechtigte Interessen des Verantwortlichen, was eine Interessenabwägung im Einzelfall erfordere.

Konkret in Bezug auf den Einsatz von Web-Tracking heißt es abschließend allerdings sehr eindeutig formuliert: »Es bedarf jedenfalls einer vorherigen Einwilli-

gung beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und bei der Erstellung von Nutzerprofilen. Das bedeutet, dass eine informierte Einwilligung i. S. d. DSGVO, in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung vor der Datenverarbeitung eingeholt werden muss, d. h. z. B. bevor Cookies platziert werden bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.«[3]

Im Übrigen benötigt jede Web-Tracking-Software – selbst wenn sie über das Content-Management-System (CMS) WordPress eingepflegt worden ist – eine eigene Datenschutzkonformitätsprüfung, die vor allem dann sorgfältig durchgeführt werden sollte, wenn Aufträge zur Datenverarbeitung an Dienstleister außerhalb der Europäischen Union erteilt werden.

7.1 Einsatz von JavaScript-Plugins

Die **Nutzung von externen Webservices**, wie z. B. des Facebook-Like-Buttons und anderer aktiver JavaScript-Plugins, **ist datenschutzrechtlich nicht unproblematisch.** Sind solche Plugins auf der Webseite eingebunden, stellt der Browser direkt mit dem Besuchen der Webseite eine Verbindung mit dem fremden Server her, so dass entsprechende Nutzerdaten erhoben und der Nutzer selbst dadurch identifiziert sowie sein Nutzerverhalten analysiert wird. Mit anderen Worten werden personenbezogene Daten – z. B. die dynamische IP-Adresse des Nutzers – regelmäßig unbemerkt an einen Dritten weitergeleitet.

Bisher empfohlen wurde zum datenschutzkonformen Umgang mit solchen Plugins regelmäßig die sogenannte **Zwei-Klick Lösung**. Unter Anwendung dieser Lösung wird nicht der eigentliche Plugin in die Webseite integriert, sondern eine Verlinkung zwischengeschaltet, die zunächst angeklickt/aktiviert werden muss, um im Anschluss – und nach erfolgter ausdrücklicher datenschutzrechtlicher Einwilligung durch ein erneutes Klicken – die Verbindung mit dem fremden Server tatsächlich aufzubauen. **Im Hinblick auf die DSGVO kann ein solches Vorgehen aber grundsätzlich nicht mehr empfohlen werden**, da Voraussetzung für eine wirksame Einwilligungserklärung unter anderem ist, dass die betroffene Person in informierter Weise eingewilligt hat. Es müsste damit über die Datenverarbeitungsvorgänge bei den Social Media Anbietern selbst umfassend aufgeklärt werden, bevor wirksam eine Einwilligungserklärung eingeholt werden kann. Da dies in der Praxis regelmäßig zu Schwierigkeiten führen wird, kann die Zwei-Klick Lösung derzeit nicht mehr empfohlen werden.

Am Ende bleibt damit lediglich die sogenannte **Shariff Lösung**. Diese arbeitet mit direkt in die Webseite eingebetteten und mit CSS individuell designbaren HTML-Buttons (Shariff Buttons), die eine unmittelbare Kommunikation mit dem fremden Server erlauben. Dem Datenschutzrecht nach der DSGVO wird an dieser Stelle insoweit besser Rechnung getragen, als dass ein Skript auf dem Server des Diensteanbieters zwischengeschaltet wird, welches zunächst ausschließlich mit dem Server des Social Media Anbieters kommuniziert und damit keinerlei personenbezogene Daten des Nutzers an den Diensteanbieter übertragen werden. Durch Klicken auf den Shariff Button nimmt der Nutzer damit selbst aktiv die Kommunikation beispielsweise zu Facebook auf und überträgt damit auch erst eigenständig personenbezogene Daten an das Social Media Netzwerk.

7.2 Einsatz von Google Analytics

Gerade der **Einsatz von Google Analytics ist datenschutzrechtlich kritisch zu sehen**. Dies ist nicht nur durch die regelmäßig versäumte oder nur unzureichende Anonymisierung der gespeicherten IP-Adressen bedingt, sondern im Übrigen auch durch die umfassenden Informationsverpflichtungen in Bezug auf den Einsatz von Google Analytics, die nur allzu leicht nicht bzw. nur unzureichend erfüllt werden und damit im Ergebnis bedeutungs- und wirkungslos sind. Viel gravierender verhält es sich jedoch, wenn man sich das zugrunde liegende Auftragsverarbeitungsverhältnis zwischen dem Webseitenbetreiber und Google selbst vor Augen hält. Die wenigsten Webseitenbetreiber haben entsprechend der Anforderungen des Art. 28 DSGVO einen schriftlich – bzw. ab dem 25. Mai 2018 auch elektronisch – abgefassten Auftragsverarbeitungsvertrag mit Google, welcher die Mindestvertragsinhalte gemäß Art. 28 Abs. 3 DSGVO regelt. Zumal in diesem Zusammenhang auch die Datenübertragung in ein Drittland (vgl. Art. 44 ff. DSGVO) relevant werden kann, so dass vor allem sichergestellt sein müsste, dass hinreichende Garantien dafür existieren, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, damit die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Insbesondere mit Blick auf die Resolution des Europäischen Parlamentes vom 6. April 2017 hat in diesem Zusammenhang auch das »neue« EU-US Privacy Shield an Sicherheit verloren und dürfte damit nicht mehr die unumstößlichen Garantien bieten, die aber gerade auch von Art. 28 DSGVO gefordert werden. Die Auftragsverarbeitung kann damit als Erlaubnistatbestand für die Datenübermittlung nicht herangezogen werden, so dass ein anderer Erlaubnistatbe-

stand vorliegen müsste, der sich je nach Einzelfallbeurteilung aber nur schwer bis gar nicht finden lassen dürfte.

Anmerkungen

[1] Gesmann-Nuissl/Kirchner, IT-Recht, Datenschutz, Existenzgründungsportal des BMWi, http://www.existenzgruender.de/DE/Unternehmen-fuehren/Erfolgsfaktoren/E-Business-Digitalisierung-4-0/IT-Recht/IT-Recht.html?nn=181732&cms_notFirst=true&cms_docId=181786.

[2] Gesmann-Nuissl/Kirchner, IT-Recht, Datenschutz, Existenzgründungsportal des BMWi, http://www.existenzgruender.de/DE/Unternehmen-fuehren/Erfolgsfaktoren/E-Business-Digitalisierung-4-0/IT-Recht/IT-Recht.html?nn=181732&cms_notFirst=true&cms_docId=181786.

[3] https://www.datenschutz-berlin.de/pdf/publikationen/DSK/2018/2018-DSK Positionsbestimmung_TMG.pdf.

Haben Sie noch Fragen? – Gerne!

Prof. Dr. Dagmar Gesmann-Nuissl Sie ist Leiterin der Professur für Privatrecht und Recht des geistigen Eigentums der Technischen Universität Chemnitz mit einem Forschungsschwerpunkt auf dem Innovations- und Technikrecht. Als Konsortialpartnerin des Mittelstand 4.0-Kompetenzzentrum Chemnitz leitet sie außerdem die »Arbeitsgemeinschaft Recht 4.0« aller Mittelstand 4.0-Kompetenzzentren in Deutschland.

(+49) 0371/531-39233
dagmar.gesmann-nuissl@betrieb-machen.de

Dipl.-Jur. Univ. Gernot Kirchner ist wissenschaftlicher Mitarbeiter an der Professur für Privatrecht und Recht des geistigen Eigentums. Im Mittelstand 4.0-Kompetenzzentrum Chemnitz verantwortet er alle rechtlichen Themen in Bezug auf Digitalisierung und ist Experte für die EU-Datenschutzgrundverordnung.

(+49) 0371/531-30171
gernot.kirchner@betrieb-machen.de

Weitere Informationen

Das Mittelstand 4.0-Kompetenzzentrum Chemnitz gehört zu Mittelstand-Digital. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

Was ist Mittelstand-Digital?
Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenlose Nutzung aller Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter www.mittelstand-digital.de

Ihr schnellster Weg zu uns: