Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

Orientierungshilfe der Aufsichtsbehörden

für Anbieter von Telemedien

Stand:

März 2019

Inhalt

I. Einführung

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder veröffentlichte am 26. April 2018 eine Positionsbestimmung zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018. Gleichzeitig beschlossen die Datenschutzbehörden, eine Konsultation von betroffenen Wirtschaftsverbänden und Unternehmen durchzuführen.

Als Ergebnis der Auswertung der Stellungnahmen im Konsultationsverfahren und zur Erläuterung und Konkretisierung der Positionsbestimmung haben die Datenschutzbehörden die folgende Ergänzung formuliert. Das Papier soll gleichzeitig als Orientierungshilfe für die Umsetzung der datenschutzrechtlichen Anforderungen an die Verarbeitung der Daten von Nutzer*innen[1] durch Telemediendienste dienen.

Die Orientierungshilfe steht unter dem ausdrücklichen Vorbehalt eines zukünftigen - möglicherweise abweichenden – Verständnisses der maßgeblichen Vorschriften durch den Europäischen Datenschutzausschuss (EDSA) sowie einer etwaigen Rechtsänderung durch ein zukünftiges Inkrafttreten einer Überarbeitung der Richtlinie 2002/58/EG.

II. Keine Anwendbarkeit der datenschutzrechtlichen Vorschriften des TMG

Das Telemediengesetz (TMG) ist nach wie vor in all seinen Bestandteilen in Kraft. Eine Anpassung der datenschutzrechtlichen Vorschriften des TMG (4. Abschnitt; §§ 11 ff. TMG) an die Datenschutz-Grundverordnung (DSGVO) wurde nicht vorgenommen. Ein formeller Umsetzungsakt der ePrivacy-Richtlinie 2002/58/EG in der Fassung der Änderung durch die Richtlinie 2009/136/EG[2] (ePrivacy-Richtlinie) ist im 4. Abschnitt des TMG nicht erfolgt.[3] Insbesondere fehlt es an einem Umsetzungsakt für Art. 5 Abs. 3 der ePrivacy-RL im deutschen Recht insgesamt.[4] Es stellt sich daher die Frage nach der Anwendbarkeit der Vorschriften des 4. Abschnitts des TMG seit der Geltungserlangung der DSGVO.

1. Anwendungsvorrang der DSGVO und Kollisionsregel in Art. 95 DSGVO

Grundsätzlich werden mitgliedstaatliche datenschutzrechtliche Regelungen aufgrund des Anwendungsvorrangs der DSGVO durch diese verdrängt, wenn es keine spezifischen Regelungen gibt, die ein Fortbestehen bereits existierender Regelungen anordnen oder Öffnungsklauseln Spielräume zur mitgliedstaatlichen Ausgestaltung offen lassen beziehungsweise vorgeben. Die DSGVO enthält in Artikel 95 eine Kollisionsregel zum Verhältnis der DSGVO zur ePrivacy-Richtlinie. Danach werden natürlichen oder juristischen Personen in

[1] Es sollen sich stets alle Menschen angesprochen fühlen. Aus Gründen der einfacheren Lesbarkeit wird im Folgenden jedoch nur eine Form verwendet.

[2] Sofern im Folgenden eine Vorschrift der ePrivacy-Richtlinie genannt wird, ist immer die aktuelle in der Fassung der Änderung durch die Richtlinie 2009/136/EG gemeint.

[3] So auch BGH, Beschluss vom 5.10.17, Az.: I ZR 7/16, Rz. 16; in Bezug auf Art. 5 Abs. 3 der ePrivacy-Richtlinie 2002/58/EG in der Fassung der Änderung durch die Richtlinie 2009/135/EG vgl. die von der EU-Kommission veröffentlichte Studie: „ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation“ (SMART 2013/0071), Final report, 2015, Ziff. 5.2, abrufbar unter: https://ec.europa.eu/digital-single-market/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.

[4] S. dazu den Final Report, Fn. 3, a.a.O.

Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union durch die DSGVO keine zusätzlichen Pflichten auferlegt, soweit sie besonderen in der ePrivacy-Richtlinie festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

Richtlinien bedürfen gemäß Art. 288 AEUV im Unterschied zu Verordnungen der Umsetzung durch die Mitgliedstaaten. Grundsätzlich entfaltet erst das in Umsetzung der Richtlinie geschaffene mitgliedstaatliche Recht Rechtswirkung gegenüber Einzelnen; eine Richtlinie selbst kann keine Verpflichtungen für Einzelne begründen. Die Kollisionsregel in Art. 95 DSGVO umfasst daher die in Umsetzung der ePrivacy-Richtlinie erlassenen mitgliedstaatlichen Vorschriften. Dies betrifft vor allem die Regelungen des Telekommunikationsgesetzes (TKG), die als Umsetzung der ePrivacy-Richtlinie 2002/58/EG anzusehen sind. Durch die Richtlinie 2009/136/EG wurde der Anwendungsbereich der ePrivacy-Richtlinie ausgeweitet. Die Regelung des Art. 5 Abs. 3 ePrivacy-RL adressiert nicht lediglich Anbieter von öffentlichen Telekommunikationsdiensten, sondern auch Anbieter von „Diensten der Informationsgesellschaft“. Diese entsprechen den Diensten, die in Deutschland als Telemediendienste bezeichnet und durch das TMG reguliert werden. Spezielle datenschutzrechtliche Vorgaben finden sich in den §§ 11 ff. des TMG. Diese können jedoch nur dann neben der DSGVO zur Anwendung kommen, wenn es sich dabei um Umsetzungen der ePrivacy-Richtlinie handelt und sie somit der Kollisionsregel des Art. 95 DSGVO unterfallen.

2. Keine Umsetzung der ePrivacy-Richtlinie durch §§ 12, 15 Abs. 1 TMG

Aus den Antworten auf einen Fragebogen der EU-Kommission zur Umsetzung des Art. 5 Abs. 3 ePrivacy-RL geht hervor, dass die Anforderungen des Art. 5 Abs. 3 ePrivacy-RL durch die bereits vorher bestehenden Regelungen in § 12 und § 15 TMG als hinreichende Umsetzung der Richtlinie angesehen worden sind. In den Antworten auf den Fragebogen wird durch die BReg ausgeführt, dass § 12 TMG klarstelle, personenbezogene Daten dürften im Zusammenhang mit der Bereitstellung von Telemedien ohne Einwilligung nur verarbeitet werden, wenn der Gesetzgeber dies ausdrücklich erlaubt. Eine solche gesetzliche Erlaubnis enthalte § 15 TMG. Für die Speicherung und den Abruf von Informationen, wie z. B. Cookies, bedeute dies, dass solche Verfahren in Deutschland ohne Einwilligung der Nutzer nur zulässig seien, wenn dies aus technischen Gründen für die Inanspruchnahme erforderlich sei.

Im Übrigen dürften solche Verfahren ohne Einwilligung des Nutzers nicht verwendet werden.[5] Im Ergebnis bedeute dies, dass der deutsche Gesetzgeber davon ausgegangen ist, dass eine Umsetzung in Form einer gesetzlichen Anpassung nicht erforderlich ist, da sich das Einwilligungserfordernis des Art. 5 Abs. 3 ePrivacy-RL bereits aus § 12 und § 15 Abs. 1 TMG,[6] d.h. aus dem grundsätzlichen Konzept des Verbots mit Erlaubnisvorbehalt ergebe. Mangels gesetzlicher Erlaubnis in § 15 Abs. 1 TMG für die in Art. 5 Abs. 3 ePrivacy-RL geregelten Sachverhalte komme die allgemeine Regel des § 12 TMG, d. h. die Umsetzung des in Art. 7 Buchst. a DSRL geregelten Verbots mit Erlaubnisvorbehalt, zur Anwendung. [7] Auch eine Studie der EU-Kommission[8], die sich mit der Umsetzung der ePrivacy-RL in den einzelnen Mitgliedstaaten befasst, kommt

[5] S. dazu den Final Report, a.a.O.
[6] Conrad/Haussen in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 36 Rn. 12.
[7] BGH Beschluss vom 5.10.17, Az.: I ZR 7/16, Rz. 22 mit weiteren Nachweisen.
[8] EU-Kommission, „ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation“ (SMART 2013/0071), Final report, 2015.

zu dem Ergebnis, dass die Bestimmung vom deutschen Gesetzgeber nicht umgesetzt wurde. Dort heißt es, dass in Deutschland die Auffassung vertreten worden sei, dass die bestehenden Vorschriften des Telemediengesetzes über die Verarbeitung personenbezogener Daten durch (informationsgesellschaftliche) Dienstleister ausreichten, um Nutzer und Teilnehmer zu schützen.[9]

Die Konstruktion der „Umsetzung" durch das Verbot mit Erlaubnisvorbehalt in § 12 i. V. m. § 15 Abs. 1 TMG gerät allerdings bereits aufgrund der Entscheidungen des EuGH zu dynamischen IP-Adressen und des Urteils des BGH vom 16. Mai 2017 zur gebotenen richtlinienkonformen Auslegung des § 15 Abs. 1 TMG ins Straucheln. Denn die richtlinienkonforme Auslegung erfordert nach Auffassung des BGH, dass § 15 Abs. 1 TMG dahingehend auszulegen ist, dass „ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus nur erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten". Diese weitergehende Erlaubnis geht über die Möglichkeiten hinaus, die nach den engen Ausnahmeregelungen in Art. 5 Abs. 3 Satz 2 ePrivacy-RL ohne Einwilligung zulässig sind, da die Daten über den Nutzungsvorgang hinaus zur generellen Funktionsfähigkeit gespeichert bleiben können.

Zudem ist zu berücksichtigen, dass die §§ 12 und 15 TMG keine Umsetzung des Art. 5 Abs. 3 ePrivacy-Richtlinie, sondern vielmehr eine Umsetzung von Art. 7 Datenschutzrichtlinie 95/46/EG (DSRL) darstellen. Gem. Art. 94 Abs. 1 DSGVO wurde die DSRL mit Wirkung zum 25. Mai 2018 aufgehoben. Die Regelungen zur Rechtmäßigkeit der Verarbeitung personenbezogener Daten werden nunmehr in Art. 6 DSGVO getroffen. Dort findet sich auch die Vorgabe, dass eine Datenverarbeitung nur dann rechtmäßig ist, wenn mindestens eine der in Art. 6 Abs. 1 genannten Voraussetzungen erfüllt ist. Für eine Wiederholung des Verbots mit Erlaubnisvorbehalt im nationalen Recht in Form von § 12 TMG besteht neben der DSGVO damit kein Raum.[10]

Die Kollisions-Regelung des Art. 95 DSGVO bezieht sich außerdem auf „besondere in der Richtlinie 2002/58/EG festgelegte Pflichten". Solche „besonderen" Pflichten ergeben sich aus dem allgemeinen Konzept des Verbots mit Erlaubnisvorbehalt gerade nicht.

Im Ergebnis lässt sich festhalten, dass Art. 95 DSGVO für § 12 und § 15 Abs. 1 TMG nicht zur Anwendung kommt.

3. Keine Umsetzung der ePrivacy-Richtlinie durch § 15 Abs. 3 TMG

Anders als die Bundesregierung nimmt der BGH in seinem Vorlagebeschluss vom 5. Oktober 2017 [11] im Hinblick auf die Umsetzung des Art. 5 Abs. 3 ePrivacy-RL vorrangig § 15 Abs. 3 TMG in den Blick.[12] Dies ist folgerichtig vor dem Hintergrund, dass Art. 5 Abs. 3 ePrivacy-RL auch das Speichern oder den Zugriff auf

[9] EU-Kommission, „ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regu-lation" (SMART 2013/0071), Final report, 2015, Ziff. 5.2, abrufbar unter: https://ec.europa.eu/digital-single-market/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.
[10] S. statt vieler Nettesheim, in: Grabitz/Hilf/ders. (Hrsg.), Das Recht der EU, AEUV, Art. 288, Rn. 101 f., m. w. N.
[11] BGH, Beschl. v. 5.10.17, I ZR 7/16.
[12] BGH, Beschl. v. 5.10.17, I ZR 7/16, Rz. 13, 16.

Informationen, die im Endgerät der Nutzer gespeichert sind, erfasst, wie beispielsweise die Verwendung von Cookies. § 15 Abs. 3 TMG stellt eine gesetzliche Erlaubnis für die Erstellung von Nutzungsprofilen unter Pseudonym bereit, womit auch Nutzungsprofile gemeint sein können, die etwa mit Hilfe von Cookies erstellt werden. Im Hinblick auf die Frage der Umsetzung des Art. 5 Abs. 3 ePrivacy-RL ist daher eine Auseinandersetzung mit § 15 Abs. 3 TMG und die Prüfung einer richtlinienkonformen Auslegung geboten.

Gemäß § 15 Abs. 3 TMG durfte der Diensteanbieter zu Zwecken der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile unter Verwendung eines Pseudonyms erstellen, sofern die Nutzer nicht widersprechen. Die in § 15 Abs. 3 TMG genannten Zwecke entsprechen nicht den Ausnahmetatbeständen des Art. 5 Abs. 3 Satz 2 der ePrivacy-RL. Das bedeutet, dass für die in § 15 Abs. 3 TMG genannten Zwecke nach Art. 5 Abs. 3 ePrivacy-RL grundsätzlich eine Einwilligung der Teilnehmer oder Nutzer erforderlich ist. Die Einwilligung i. S. der ePrivacy-Richtlinie ist gemäß deren Art. 2 Satz 2 lit. f) eine Einwilligung i. S. d. DSRL. Gemäß Art. 94 Abs. 2 DSGVO werden Verweise auf die DSRL zu Verweisen auf die DSGVO, so dass die Frage, welche Anforderungen an eine Einwilligung zu stellen sind, ab dem 25. Mai 2018 nach Maßgabe der DSGVO zu beantworten ist. Hieran ändert auch Art. 95 DSGVO nichts. Die Einwilligung ist in der ePrivacy-Richtlinie, wie erwähnt, nicht eigenständig geregelt, so dass insofern keine lex-specialis-Situation besteht.[13]

Hinweis:
Der maßgebliche Unterschied zwischen einer Widerspruchslösung (Opt-Out) und einer Einwilligung (Opt-In) ist, dass im Falle einer Widerspruchslösung zunächst eine Datenverarbeitung stattfindet, die lediglich durch Erklärung eines Widerspruchs für die Zukunft untersagt werden kann. Anders liegt der Fall hingegen, wenn eine Einwilligung (Opt-In) erforderlich ist. Dann darf eine Datenverarbeitung nämlich erst stattfinden, nachdem eine wirksame Einwilligung vom Nutzer tatsächlich erteilt worden ist.

Gem. Art. 4 Nr. 11 DSGVO muss die Einwilligung in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung abgegeben werden. Erwägungsgrund 32 ist zu entnehmen, dass „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person […] daher keine Einwilligung darstellen [sollten]“. Darüber hinaus ist das Widerspruchsrecht in Abgrenzung zu der Einwilligung gesondert in der DSGVO in Art. 21 geregelt. Vor diesem Hintergrund kann ausgeschlossen werden, dass das Unterbleiben eines Widerspruchs eine Einwilligung i. S. d. DSGVO darstellen kann.

Eine direkte Anwendung des § 15 Abs. 3 TMG als Umsetzung des Art. 5 Abs. 3 ePrivacy-RL in der Fassung der Änderung durch die Richtlinie 2009/136/EG scheidet damit jedenfalls seit dem 25. Mai 2018 aus.

4. Keine richtlinienkonforme Auslegung des § 15 Abs. 3 TMG

In Betracht kommt für die Beibehaltung nur eine richtlinienkonforme Auslegung des § 15 Abs. 3 TMG, um die Vorschrift über Art. 95 DSGVO weiterhin anzuwenden. Dazu stellt sich zunächst die Frage, ob § 15 Abs.

[13] Kühling/Buchner, DSGVO 2017, Art. 95 Rn. 7.

3 TMG, d. h. die Widerspruchslösung, so angewendet werden kann, dass dies nicht zu einem der Richtlinie widersprechenden Ergebnis führt. Dies ist jedenfalls seit dem 25. Mai 2018 nicht der Fall. Die Widerspruchslösung erfüllt nicht die Anforderungen an eine Einwilligung gemäß Art. 7 DSGVO.

5. Keine Öffnungsklausel für nicht-öffentliche Stellen

Die Beibehaltung der Regelungen der §§ 12, 15 Abs. 1 und 15 Abs. 3 TMG kann für nicht-öffentliche Stellen auch nicht durch eine Öffnungsklausel der DSGVO gerechtfertigt werden. Damit sind die Regelungen im nationalen Recht, die nach Ansicht des deutschen Gesetzgebers eine Umsetzung von Art. 5 Abs. 3 ePrivacy-RL darstellen oder für eine solche Umsetzung in Betracht kommen, nicht mehr anwendbar.

6. Keine unmittelbare Anwendung

Auch eine unmittelbare Anwendung der ePrivacy-Richtlinie kommt nicht in Betracht. Nach der Rechtsprechung des EuGH können sich Einzelne zwar unter bestimmten Voraussetzungen gegenüber einem umsetzungssäumigen Mitgliedstaat unmittelbar auf eine Bestimmung einer EU-Richtlinie berufen.[14] Voraussetzungen sind u.a. eine fehlende oder mangelhafte Umsetzung[15] sowie, dass die Norm der Richtlinie inhaltlich unbedingt und hinreichend genau ist.[16] Eine Richtlinie kann jedoch nicht selbst Verpflichtungen für Private begründen.[17]

7. Zwischenergebnis

Da Art. 5 Abs. 3 ePrivacy-Richtlinie in Deutschland nicht umgesetzt wurde und weder eine richtlinienkonforme Auslegung noch eine unmittelbare Wirkung des Art. 5 Abs. 3 ePrivacy-Richtlinie in Betracht kommt, entstehen hieraus für Telemediendiensteanbieter in Deutschland keine bereichsspezifischen Pflichten im Sinne des Art. 95 DSGVO, so dass dessen Voraussetzungen insoweit nicht greifen. Zudem finden sich auch keine Öffnungsklauseln in der DSGVO, die die Anwendbarkeit des § 15 TMG rechtfertigen. Es bleibt daher bei der generellen Anwendung der Regelungen der DSGVO.

III. Rechtmäßigkeit der Verarbeitung

1. Einführung

Zur Vereinfachung bei der Bezugnahme auf bestimmte Vorgänge im Bereich der Nutzungsdatenverarbeitung verwendet die Positionsbestimmung u. a. den Begriff „Tracking“. Nach dem Verständnis der Aufsichtsbehörden handelt es sich bei „Tracking“ um Datenverarbeitungen zur – in der Regel website-

[14] BVerfGE 75, 223; EuGH, Slg. 2002, I-6325, (Marks & Spencer), Rn. 24.
[15] EuGH, Rs. 152/84, Slg. 1986, 723, (Marshall I), Rn. 46.
[16] EuGH, Rs. 148/78, Slg. 1979, 1629, (Ratti), Rn. 23.
[17] EuGH, Rs. 152/84, Slg. 1986, 723, (Marshall I), Rn. 48; Verb. Rs. 372 bis 374/85, Slg. 1987, 2141, (Traen), Rn. 24; Rs. 14/86, Slg. 1987, 2545, (Pretore di Salò/X), Rn. 19; Rs. 80/86, Slg. 1987, 3969, (Kolpinghuis Nijmegen), Rn. 9; Rs. C-221/88, Slg. 1990, I-495, (Busseni), Rn. 23; Rs. C-106/89, Slg. 1990, I-4135 (Marleasing) , Rn. 6; Rs. C-168/95, Slg. 1996, I-4705 (Arcaro), Rn. 36 ff.; Rs. C-97/96, Slg. 1997, I-6843 (Daihatsu Deutschland), Rn. 24; Rs. C-201/02, Slg. 2004, I-723 (Delena Wells), Rn. 56.

übergreifenden – Nachverfolgung des individuellen Verhaltens von Nutzern. Dieses Begriffsverständnis entspricht dem, welches von den europäischen Aufsichtsbehörden in Veröffentlichungen zugrunde gelegt wird.[18]

Für die Bewertung der Zulässigkeit ist aber allein entscheidend, ob eine bestimmte Verarbeitungstätigkeit rechtmäßig durchgeführt wird und der Verantwortliche allen datenschutzrechtlichen Pflichten der DSGVO nachkommt. Die Datenverarbeitung ist nur dann rechtmäßig, wenn mindestens eine der Bedingungen des Art. 6 Abs. 1 DSGVO vorliegt ist.

2. Rechtmäßigkeit der Verarbeitung

Sämtliche Erlaubnistatbestände der DSGVO sind als gleichrangig und gleichwertig zu betrachten. In Art. 6 DSGVO werden die Bedingungen für die rechtmäßige Verarbeitung personenbezogener Daten festgelegt und sechs Rechtsgrundlagen beschrieben, auf die sich Verantwortliche stützen können.[19] Für die Verarbeitung personenbezogener Daten durch nicht-öffentliche Verantwortliche bei der Erbringung von Telemediendiensten kommen insbesondere folgende Erlaubnistatbestände in Betracht:

a) Art. 6 Abs. 1 lit. a) DSGVO - Einwilligung

b) Art. 6 Abs. 1 lit. b) DSGVO - Vertrag

c) Art. 6 Abs. 1 lit. f) DSGVO - Interessenabwägung

Hinweis:
Verantwortliche müssen im Rahmen ihrer Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO nachweisen, dass die Verarbeitung personenbezogener Daten rechtmäßig erfolgt. Dies bedeutet, dass Verantwortliche vorab prüfen und dokumentieren müssen, auf welchen Erlaubnistatbestand sie die Verarbeitung stützen. Die Nutzer müssen über die Erlaubnistatbestände für sämtliche Verarbeitungen ihrer personenbezogenen Daten informiert werden (Informationspflichten nach Art. 13 f. DSGVO).

Im Folgenden werden die o. g. Erlaubnistatbestände näher erläutert.

[18] Art. 29 Datenschutzgruppe, WP 194 vom 7. Juni 2012, S. 10; EDPB, Leitlinie zur Einwilligung, WP 259, S. 4 (abrufbar unter https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Artikel-29-Gruppe/wp259-rev-0_1_DE.PDF).

[19] EDPB, Leitlinie zur Einwilligung, WP 259, S. 27 (abrufbar unter https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Artikel-29-Gruppe/wp259-rev-0_1_DE.PDF).

a) Art. 6 Abs. 1 lit. a) DSGVO – Einwilligung

Art. 4 Nr. 11 und Art. 7 DSGVO fordern eine selbstbestimmte und informierte Einwilligung der betroffenen Personen in die jeweilige Datenverarbeitung. Dies setzt voraus, dass jegliche Datenverarbeitungen transparent und nachvollziehbar sein müssen. Insbesondere wenn bei der betroffenen Person erhobene Daten von dem jeweiligen Diensteanbieter (inkl. eingebundener Dienste) website-übergreifend zusammengeführt und ausgewertet werden, ist zu berücksichtigen, dass die betroffenen Personen für eine wirksame Einwilligung vorab über jegliche Form der durchgeführten Datenverarbeitung sowie sämtliche Empfänger ausführlich informiert werden und die Möglichkeit erhalten müssen, in die einzelnen Formen der Datenverarbeitung spezifisch einzuwilligen. In Fällen, in denen sich mehrere (gemeinsame) Verantwortliche auf die ersuchte Einwilligung stützen wollen, oder in denen die Daten an andere Verantwortliche übermittelt oder von anderen Verantwortlichen verarbeitet werden sollen, müssen diese Organisationen sämtlich genannt[20] und die Verarbeitungsaktivitäten der einzelnen Organisationen hinreichend beschrieben werden. In diesen Fällen müssen alle beteiligten Akteure überprüfen, ob eine wirksame Einwilligung für ihre Aktivitäten vorliegt und ob diese von ihnen nachgewiesen werden kann (Art. 5 Abs. 2 DSGVO).[21] Eine Verarbeitung personenbezogener Daten ohne ausreichende Kenntnis der betroffenen Personen

- über die jeweiligen Datenverarbeitungsvorgänge,
- über die jeweils einbezogenen Dritten sowie
- ohne Möglichkeit der gesonderten Zustimmung

führt zur Unwirksamkeit der Einwilligung und erfolgt daher ohne Rechtsgrund. Es ist von grundlegender Bedeutung, den betroffenen Personen Informationen bereitzustellen, um von ihnen eine wirksame Einwilligung einholen zu können. Nur so ist es betroffenen Personen möglich, Entscheidungen in Kenntnis der konkreten Sachlage zu treffen und die Reichweite der Einwilligung zu verstehen.

Art. 4 Nr. 11 DSGVO setzt für eine wirksame Einwilligung weiter eine „unmissverständlich abgegebene Willensbekundung in Form einer Erklärung“ oder eine sonstige eindeutige bestätigende Handlung voraus, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten ausdrücklich einverstanden ist. Dies kann beispielweise durch Anklicken eines Kästchens beim Besuch einer Website, durch die Auswahl technischer Einstellungen oder durch eine andere Erklärung oder aktive Verhaltensweise geschehen, mit der die betroffene Person eindeutig ihr Einverständnis hinsichtlich der angekündigten und beabsichtigten Datenverarbeitung ausdrückt.

Opt-Out-Verfahren reichen dafür nicht aus. Insoweit führt Erwägungsgrund 32 DSGVO explizit aus, dass konkludente Verhaltensweisen wie „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person“ keine Einwilligungen darstellen.

[20] EDPB, Leitlinie zur Einwilligung, WP 259, S. 16.
[21] Vgl. dazu auch Aufforderungsschreiben der CNIL an Vectaury vom 9. November 2018, Informationen dazu abrufbar unter https://www.cnil.fr/en/node/24929.

Hinweis: „Cookie-Banner“ & „Consent-Tools“
Durch eine vorgeschaltete Abfrage beim ersten Aufruf einer Website oder einer Web-App kann u. a. eine wirksame Einwilligung für einwilligungsbedürftige (Fn.: Die Nutzung von Cookies ist nicht per se einwilligungsbedürftig. Entsprechende Banner sollen daher nur eingesetzt werden, wenn tatsächlich eine Einwilligung notwendig ist.) Datenverarbeitungen eingeholt werden. Dabei sind jedoch folgende Anforderungen zu beachten:

- Beim erstmaligen Öffnen einer Website erscheint das Banner beispielsweise als eigenes HTML-Element. In der Regel besteht dieses HTML-Element aus einer Übersicht aller einwilligungsbedürftigen Verarbeitungsvorgänge, die unter Nennung der beteiligten Akteure und deren Funktion ausreichend erklärt wird und über ein Auswahlmenü aktiviert werden können. Aktivieren bedeutet in diesem Zusammenhang, dass die Auswahlmöglichkeiten nicht „aktiviert“ voreingestellt sein dürfen.

- Während das Banner angezeigt wird, werden zunächst alle weitergehenden Skripte einer Website oder einer Web-App, die potenziell Nutzerdaten erfassen, blockiert. Der Zugriff auf Impressum und Datenschutzerklärung darf durch „Cookie-Banner“ nicht verhindert werden.

- Erst wenn der Nutzer seine Einwilligung(en) durch eine aktive Handlung, wie zum Beispiel das Setzen von Häkchen im Banner oder den Klick auf eine Schaltfläche abgegeben hat, darf die einwilligungsbedürftige Datenverarbeitung tatsächlich (durch technische Maßnahmen sichergestellt) stattfinden.

- Zur Erfüllung der Nachweispflichten des Art. 7 Abs. 1 DSGVO ist es gem. Art. 11 Abs. 1 DSGVO nicht erforderlich, dass die Nutzer dazu direkt identifiziert werden. Eine indirekte Identifizierung (vgl. Erwägungsgrund 26) ist ausreichend. Damit die Entscheidung des Nutzers für oder gegen eine Einwilligung bei einem weiteren Aufruf der Website berücksichtigt wird und das Banner nicht erneut erscheint, kann deren Ergebnis auf dem Endgerät des Nutzers ohne Verwendung einer User-ID o. ä. vom Verantwortlichen gespeichert werden. Durch ein solches Verfahren kann der Nachweis einer vorliegenden Einwilligung erbracht werden.

- Da eine Einwilligung widerruflich ist, muss eine entsprechende Möglichkeit zum Widerruf implementiert werden. Der Widerruf muss so einfach möglich sein wie die Erteilung der Einwilligung, Art. 7 Abs. 3 S. 4 DSGVO.

Verantwortliche müssen sicherstellen, dass die Einwilligung nicht nur das Setzen von einwilligungsbedürftigen Cookies umfasst, sondern alle einwilligungsbedürftigen Verarbeitungstätigkeiten, wie z.B. Verfahren zur Verfolgung der Nutzer durch Zählpixel oder div. Fingerprinting-Methoden, wenn diese nicht aufgrund einer anderen Rechtsgrundlage zulässig sind.

Auch genügt es für eine Einwilligung i. S. d. DSGVO nicht, wenn, wie bei vielen einfachen Cookie-Bannern im Web, ein Hinweis auf das Setzen von Cookies zusammen mit einem „OK“-Button erfolgt. In diesen Fällen fehlt es an der nach Art. 7 DSGVO erforderlichen Freiwilligkeit, wenn die betroffenen Personen zwar „OK“ drücken können, aber keine Möglichkeit erhalten, das Setzen von Cookies abzulehnen.

Die Einwilligung muss freiwillig sein, das heißt ohne Zwang abgegeben werden. Freiwillig ist die Einwilligung nur, wenn die betroffene Person eine echte und freie Wahl hat und somit in die Lage versetzt wird, eine Einwilligung auch verweigern zu können, ohne dadurch Nachteile zu erleiden (Erwägungsgrund 42 DSGVO). Auch eine Koppelung der Erbringung einer vertraglichen Dienstleistung an die Abgabe einer datenschutzrechtlichen Einwilligung führt gem. Art. 7 Abs. 4 DSGVO regelmäßig dazu, dass die Einwilligung nicht als freiwillig angesehen werden kann und damit unwirksam ist.[22] Der Besuch einer Website sollte auch dann noch möglich sein, wenn betroffene Personen sich gegen das Setzen von Cookies entscheiden und nicht in die personenbezogene Datenverarbeitung einwilligen. Eine Einwilligung gilt nach Erwägungsgrund 43 DSGVO auch dann nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann. Wenn bei Websites durch vorgeschaltete Abfragen eine Einwilligung eingeholt wird, müssen die einzelnen Verarbeitungsvorgänge daher gesondert anwählbar sein.

Schließlich ist Art. 25 Abs. 2 DSGVO zu beachten, der von dem datenschutzrechtlich Verantwortlichen verlangt, geeignete technische und organisatorische Maßnahmen zu treffen, um sicherzustellen, dass durch datenschutzfreundliche Voreinstellungen nur personenbezogene Daten verarbeitet werden, die für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind. Konsequenterweise sollte nicht zuletzt nach den Grundsätzen „data protection by design“ und „data protection by default“ (Erwägungsgrund 78 DSGVO) sichergestellt werden, dass die technischen Vorrichtungen ebenso datenschutzfreundlich eingestellt sind und damit die Einholung einer wirksamen Einwilligung ermöglichen. Außerdem ist durch den datenschutzrechtlich Verantwortlichen technisch sicherzustellen, dass Verfahren zur Verfolgung von Nutzeraktivitäten, die datenschutzrechtlich einer Einwilligung bedürfen, erst dann zum Einsatz kommen, wenn die betroffene Person die Information über die geplante Datenverarbeitung inhaltlich erfasst und eine Entscheidung in Form einer expliziten Willensbetätigung darüber getroffen hat.

b) Art. 6 Abs. 1 lit. b) DSGVO – Vertrag

Die Verarbeitung personenbezogener Daten des Vertragspartners auf vertraglicher Grundlage ist gemäß Art. 6 Abs. 1 lit. b) DSGVO nur möglich, wenn die Datenverarbeitung zur Erfüllung eines Vertrages oder im Rahmen vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Im Hinblick auf andauernde Diskussionen auf europäischer Ebene zur Frage der Anwendbarkeit des Art. 6 Abs. 1 lit. b) DSGVO im Zusammenhang mit der Bereitstellung von Online-Services, wird zum gegenwärtigen Zeitpunkt auf Ausführungen zu Art. 6 Abs. 1 lit. b) DSGVO verzichtet.

[22] EDPB, Leitlinien zur Einwilligung, WP 259, S. 9.

c) Art. 6 Abs. 1 lit. f) DSGVO – Interessenabwägung

Bei der Interessenabwägung gem. Art. 6 Abs. 1 lit. f) DSGVO handelt es sich um eine Vorschrift mit einem weiten und unspezifischen Anwendungsbereich. Dies hat einerseits den Vorteil, dass die Vorschrift flexibel ist und auf eine Vielzahl von Sachverhalten angewendet werden kann. Anderseits führt dies zu Rechtsunsicherheiten und Fragen bei der Anwendung im konkreten Einzelfall.

Im Folgenden werden Kriterien aufgestellt, die die Anwendung erleichtern sollen und zugleich helfen können, die Rechenschaftspflichten nach der DSGVO zu erfüllen.

Bei der Verarbeitung personenbezogener Daten auf der Grundlage des Art. 6 Abs. 1 lit. f) DSGVO ist zu berücksichtigen, dass die Vorschrift keinen Auffangtatbestand darstellt. Die Verarbeitung ist nur rechtmäßig, wenn dies zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Ob die Voraussetzungen des Art. 6 Abs. 1 lit. f) DSGVO erfüllt sind, ist anhand einer dreistufigen Prüfung zu ermitteln:

1. Stufe: Vorliegen eines berechtigten Interesses des Verantwortlichen oder eines Dritten
2. Stufe: Erforderlichkeit der Datenverarbeitung zur Wahrung dieser Interessen
3. Stufe: Abwägung mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person im konkreten Einzelfall

Hinweis:
Dieser Prüfungsaufbau soll die Überprüfung der Anforderungen des Art. 6 Abs. 1 lit. f) DSGVO erleichtern und orientiert sich sowohl an der Rechtsprechung des EuGH als auch an der Auffassung der europäischen Aufsichtsbehörden.

1. Stufe: Vorliegen eines berechtigten Interesses der Verantwortlichen oder eines Dritten

Anbieter von Telemediendiensten können eine Vielzahl von berechtigten Interessen haben.[23] Die DSGVO definiert den Begriff des „berechtigten Interesses“ nicht und nennt nur vereinzelt Beispiele für ein berechtigtes Interesse. Das berechtigte Interesse hat eine enge Verbindung zum Verarbeitungszweck und kann wirtschaftlicher, ideeller oder rechtlicher Natur sein. Der Begriff des „berechtigten Interesses“ kann als das wesentliche Motiv für die Verarbeitung verstanden werden und spiegelt den Nutzen wider, den der Verantwortliche aus der Verarbeitung ziehen möchte.

Dazu zählt beispielsweise die Erbringung des Dienstes in einer Form, die eine nutzerfreundliche Wahrnehmung des Online-Angebots möglich macht. Ausdrücklich benennt die DSGVO im Erwägungsgrund 47 zudem die Verhinderung von Betrug und die Direktwerbung als mögliche berechtigte Interessen.

[23] S. im Einzelnen beispielhaft WP 217.

Berechtigt meint, dass das Interesse im Einklang mit der Rechtsordnung steht. Das bedeutet, dass jedenfalls illegale oder diskriminierende Beweggründe in keinem Fall ein berechtigtes Interesse begründen können.

Weitere Interessen, die von Telemediendiensteanbietern für die Verarbeitung von Nutzungsdaten genannt werden, sind u. a.:

- Bereitstellung besonderer Funktionalitäten, z. B. die Warenkorb-Funktion unter Verwendung eines sog. Session-Identifiers,
- Freie Gestaltung der Website auch unter Effizienz- und Kosteneinsparungserwägungen, z. B. Einbindung von Inhalten, die auf anderen Servern gehostet werden, Nutzung von Content Delivery Networks (CDN), Web Fonts, Kartendiensten, Social-Plugins, etc.
- Integrität und Sicherheit der Website; IT-Security-Maßnahmen sind bspw. das Speichern von Log-Dateien und insbesondere IP-Adressen für einen längeren Zeitraum, um Missbrauch erkennen und abwehren zu können,
- Reichweitenmessung und statistische Analysen,
- Optimierung des jeweiligen Webangebots und Personalisierung/Individualisierung des Angebots abgestimmt auf die jeweiligen Nutzer,
- Wiedererkennung und Merkmalszuordnung der Nutzer, z. B. bei werbefinanzierten Angeboten
- Betrugsprävention, Abwehr von den Dienst überlastenden Anfragen (Denial of Service-Attacken) und Bot-Nutzung

Hinweis:
Die genannten Beispiele können auf der ersten Stufe ein berechtigtes Interesse begründen. Für die Zulässigkeit von Datenverarbeitungen zu diesen Zwecken kommt es aber auf die Erforderlichkeit und die Interessenabwägung an.

2. *Stufe: Erforderlichkeit der Datenverarbeitung zur Wahrung der berechtigten Interessen*

Allein das Vorliegen eines berechtigten Interesses reicht nicht aus, um die Datenverarbeitung zu legitimieren. Zwingend ist, dass die jeweilige Datenverarbeitung zur Wahrung dieses Interesses erforderlich ist. Erforderlichkeit meint, dass die Verarbeitung geeignet ist, das Interesse (Motiv/Nutzen der Verarbeitung) des Verantwortlichen zu erreichen, wobei kein milderes, gleich effektives Mittel zur Verfügung steht. Das bedeutet, dass der Verantwortliche die Verarbeitung auf das notwendige Maß zu beschränken hat.

Beispiel:
Der Verantwortliche betreibt eine Website und möchte wissen, wie sein Online-Angebot angenommen wird und ob gegebenenfalls Verbesserungen erforderlich sind. Dazu möchte er wissen, wie viele Nutzer die Website in einem bestimmten Zeitraum besuchen, welche Geräte die Nutzer verwenden und welche Spracheinstellungen sie haben. Der Verantwortliche benötigt diese Informationen, um sein Webangebot zu optimieren und die Darstellung an die Endgeräte anzupassen.
Die Messung der Reichweite und die sich daraus ergebenden Informationen sind geeignet, um das Webangebot anzupassen (berechtigtes Interesse). Setzt der Website-Betreiber hierfür ein Analyse-Tool ein, welches Daten über das Nutzungsverhalten betroffener Personen an Dritte weitergibt (z.B. soziale Netzwerke oder externe Analysedienste, die Nutzungsdaten über die Grenze der Website hinweg mit Daten von anderen Websites zusammenführen), ist dies nicht mehr erforderlich. Das Ziel – Reichweitenmessung – kann auch mit milderen, gleich geeigneten Mitteln erreicht werden, die deutlich weniger personenbezogene Daten erheben und diese nicht an Dritte übermitteln (z. B. ohne Einbindung Dritter über eine lokale Implementierung einer Analysesoftware).

3. *Stufe: Abwägung mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person im konkreten Einzelfall*

Dem berechtigen Interesse des Verantwortlichen stehen die Interessen sowie Grundrechte und Grundfreiheiten der Nutzer gegenüber.

Darunter fällt nicht nur das Recht auf Schutz personenbezogener Daten gem. Art. 8 Charta der Grundrechte der Europäischen Union (GRCh) oder das Recht auf Vertraulichkeit der Kommunikation gem. Art. 7 GRCh, sondern auch die Freiheit der Meinungsäußerung sowie das Interesse an einer freien Informationsgewinnung, Art. 11 GRCh. Auch andere Freiheiten und Interessen der betroffenen Personen sind zu berücksichtigen, beispielsweise das Interesse, keine wirtschaftlichen Nachteile zu erleiden (z.B. bei personalisierter Preisbildung).

Das Recht auf Vertraulichkeit der Kommunikation schützt vor der Verwendung von eindeutigen Identifiern, wie z.B. IMEI-Nummer, IMSI-Nummer, MAC-Adresse oder auch Ad-IDs (gerätespezifische Werbe-Nummern). Daneben geschützt ist auch die (Geräte-)Integrität. Werden z. B. Identifier auf dem Endgerät des Nutzers abgelegt, so ist die Integrität des Gerätes berührt.

Im Rahmen der Abwägung sind die Ausgestaltung der Verarbeitung personenbezogener Daten sowie die konkreten Auswirkungen der Verarbeitung auf die betroffenen Personen zu berücksichtigen. Bei diesem Prüfungsschritt handelt es sich um den ***Kern der Interessenabwägung.***

Die ermittelten, sich gegenüberstehenden Interessen sind zu gewichten. Hierfür kann keine allgemeingültige Regel aufgestellt werden. Verantwortliche können sich jedoch an folgenden Grundsätzen orientieren:

- Ein spezifisch, verfassungsrechtlich anerkanntes Interesse, z.B. Recht auf Schutz personenbezogener Daten gem. Art. 8 GRCh, hat ein höheres Gewicht, als ein Interesse, dass nur einfachgesetzlich in der Rechtsordnung anerkannt ist.[24]

- Ein Interesse ist gewichtiger, wenn es nicht nur dem Verantwortlichen dient, sondern gleichzeitig auch der Allgemeinheit, z.B. bei Forschungstätigkeiten, deren Erkenntnisse für medizinische Vorsorge genutzt werden sollen.

Zu beachten ist, dass im Rahmen der Abwägung ohnehin bestehende Pflichten aus der DSGVO, z.B. Informationspflichten oder die Sicherheit der Verarbeitung durch Pseudonymisierung, nicht zugunsten des Verantwortlichen berücksichtigt werden können. Die allgemeinen Pflichten der DSGVO stellen keine „best practices“ dar, sondern sind gesetzliche Anforderungen, die in jedem Fall zu erfüllen sind. Gleichwohl können durch zusätzliche Schutzmaßmaßnahmen die Beeinträchtigungen durch die Verarbeitung derart reduziert werden, dass die Interessenabwägung zugunsten des Verantwortlichen ausfallen kann.

[24] Art. 29-Datenschutzgruppe, WP 217.

Hinweis:
Im Hinblick auf die Verwendung von Pseudonymen ist generell anzumerken, dass die Tatsache, dass die Nutzer etwa über IDs oder Kennungen bestimmbar gemacht werden, keine Pseudonymisierungsmaßnahme i. S. d. DSGVO darstellt. Zudem handelt es sich nicht um geeignete Garantien zur Einhaltung der Datenschutzgrundsätze oder zur Absicherung der Rechte betroffener Personen, wenn zur (Wieder-)Erkennung der Nutzer IP-Adressen, Cookie-IDs, Werbe-IDs, Unique-User-IDs oder andere Identifikatoren zum Einsatz kommen. Denn, anders als in Fällen, in denen Daten pseudonymisiert werden, um die identifizierenden Daten zu verschleiern oder zu löschen, so dass die betroffenen Personen nicht mehr adressiert werden können, werden IDs oder Kennungen dazu genutzt, die einzelnen Individuen unterscheidbar und adressierbar zu machen. Eine Schutzwirkung stellt sich folglich nicht ein. Es handelt sich daher nicht um Pseudonymisierungen i. S. d. ErwGr 28, die die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen. Darüber hinaus ist zu berücksichtigen, dass sich Nutzer in den allermeisten Fällen früher oder später an irgendeiner Stelle im Web registrieren und in diesen Fällen auch eine Verknüpfung mit E-Mail-Adressen, Klarnamen oder Offline-Adressen möglich ist. Auf die Kenntnis des bürgerlichen Namens zur Identifikation von betroffenen Personen kommt es aber beim Personenbezug nicht an. Wenn die Nutzung des Webs, wie bei vielen Menschen, einen großen Teil der Lebenswirklichkeit widerspiegelt, dann ist es relevant, ob die Nutzer über ihre Online-Kennungen bestimmbar oder adressierbar sind. Die DSGVO geht davon aus, dass eine indirekte Identifizierung auch durch Aussondern erfolgen kann (ErwGr 26 S.3).

Um Art. 6 Abs. 1 lit. f) DSGVO im Einzelfall anzuwenden, können u.a. die Erwägungsgründe der DSGVO unterstützend herangezogen werden. Aus ihnen ergeben sich insbesondere die folgenden Kriterien, die im Einzelfall im Rahmen der Interessenabwägung heranzuziehen sind:

a) Vernünftige Erwartung der betroffenen Personen und Vorhersehbarkeit / Transparenz

b) Interventionsmöglichkeiten der betroffenen Personen

c) Verkettung von Daten

d) Beteiligte Akteure

e) Dauer der Beobachtung

f) Kreis der Betroffenen (bspw. besonders schutzbedürftige Personen)

g) Datenkategorien

h) Umfang der Datenverarbeitung

a) Vernünftige Erwartung der betroffenen Personen und Vorhersehbarkeit / Transparenz

Gemäß Erwägungsgrund 47 müssen die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, berücksichtigt werden. Neben den subjektiven Erwartungen der betroffenen Person ist auch zu fragen, was objektiv vernünftigerweise erwartet werden kann. Die Erwartungen können nicht durch die nach der DSGVO vorgesehenen Pflichtinformationen (Art. 13, 14 DSGVO) erweitert werden. Kritisch ist es zu bewerten, wenn verschiedene Akteure zusammenwirken und die datenschutzrechtlichen Beziehungen der Akteure untereinander unklar oder nicht definiert sind (Verantwortlicher, Auftragsverarbeiter, gemeinsame Verantwortliche).

Im Hinblick auf die Einbindung von Diensten Dritter erwartet ein Nutzer üblicherweise nicht, dass an diese Dritten, zu denen der Nutzer regelmäßig keine Beziehungen unterhält, Informationen darüber weitergegeben werden, welche Websites er besucht oder welche Apps er nutzt. Jedenfalls dann, wenn die Dritten die Nutzerdaten zu eigenen Zwecken weiterverarbeiten, sind die Folgen und potentiellen Risiken für die Interessen, Grundfreiheiten und Grundrechte der betroffenen Personen weder einschätz- noch bewertbar. Dies betrifft insbesondere das Risiko beim Besuch anderer Dienste oder der Nutzung anderer Geräte (wieder-)erkannt zu werden und dadurch z. B. bei der Informationsgewinnung fremdgesteuert zu werden.

Diese Verarbeitungen entsprechen nicht den vernünftigen Erwartungen der Nutzer, weil sie sich im Hinblick auf die Selbstbestimmung nur nachteilig auswirken. Ebenso liegen Techniken, welche das Verhalten von Besuchern bei der Interaktion mit einem Dienst der Informationsgesellschaft exakt nachvollziehen und dokumentieren können, wie z. B. bei der Erfassung der Tastatur-, Maus- und Wischbewegungen auf Touchscreens, außerhalb der Erwartungshaltung des Nutzers.

Beispiel – Reichweitenmessung:
Der Nutzer ruft eine Website auf. Er geht davon aus, dass die Website von einem einzelnen Verantwortlichen zur Verfügung gestellt wird, nämlich von dem, mit dem zum Zeitpunkt eines Aufrufs ein direktes Nutzungsverhältnis besteht.

Dienste von Drittanbietern in Apps oder auf Websites werden von betroffenen Personen jedoch nicht bewusst wahrgenommen und regelmäßig ohne Zutun aktiviert, da der Verantwortliche sie in sein Online-Angebot eingebunden hat (z.B. Zählpixel eines Werbenetzwerks).

Im Gegensatz dazu ist es für den Nutzer vorhersehbar, dass der Verantwortliche die Reichweite seines Online-Angebots misst, etwa um das Online-Angebot bedarfsgerecht zu gestalten. Für diesen Zweck sind keine andauernde Wiedererkennung und stetig umfangreichere Profilbildung sowie keine Weitergabe von Daten an Dritte nötig. Statistische Angaben geben hinreichend Aufschluss über das allgemeine Nutzungsverhalten, sodass die Vorhaltung von individuellen Nutzungsprofilen für den Zweck Reichweitenmessung nicht erforderlich ist. Die Beeinträchtigung des Nutzers ist dann als gering zu bewerten mit der Folge, dass die Interessenabwägung zugunsten des Verantwortlichen ausfällt.

b) Interventionsmöglichkeiten der betroffenen Personen

Im Rahmen der Interessenabwägung kann – ggf. auch als Kompensationsmaßnahme – Berücksichtigung finden, in welcher Form die betroffenen Personen Möglichkeiten haben und darüber informiert werden, die personenbezogene Datenverarbeitung rechtlich wie technisch zu unterbinden, einzuschränken oder unter andere Bedingungen zu setzen.

Dabei kann z. B. die Form des Identifiers, mit welchem Geräte oder Nutzer ausgesondert und wiedererkannt werden, eine Rolle spielen. Abhängig vom Identifier kann es für die betroffenen Personen unterschiedliche Möglichkeiten geben, eine Wiedererkennung oder Nachverfolgung des Nutzungsverhaltens einzuschränken. Nutzer können etwa in den Browser-Einstellungen bestimmte Cookies löschen. Beim Device-Fingerprinting hingegen ist es praktisch unmöglich, eine (Wieder-)Erkennung nutzerseitig zu verhindern.

Darüber hinaus können den betroffenen Personen über Art. 21 DSGVO hinausgehende – überobligatorische – Widerspruchsrechte eingeräumt werden. Zwar sieht Art. 21 DSGVO vor, dass die betroffene Person das Recht hat, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die gem. Art. 6 Abs. 1 lit. f) erfolgt, Widerspruch einzulegen. Das allgemeine Widerspruchsrecht des Art. 21 DSGVO gilt somit nicht bedingungslos. Räumt der Verantwortliche dem Nutzer hingegen von vornherein ein anlassloses/bedingungsloses Widerspruchsrecht ein, so kann dies erheblich dazu beitragen, dass die Interessenabwägung zugunsten des Verantwortlichen ausfällt.

Beispiel – Reichweitenmessung:
Der Website-Betreiber bindet ein Tool zur Reichweitenmessung ein. Der Nutzer findet in den Datenschutzbestimmungen Hinweise zu einem Opt-Out-Verfahren, das er jederzeit ausführen kann. Hierzu klickt er einen Link an, der zu einem Opt-Out-Verfahren des Anbieters führt. Das Opt-Out-Verfahren wurde vom Website-Betreiber vorab geprüft. Verantwortlich für die Umsetzung des Widerspruchs bleibt der Website-Betreiber, auch wenn der Anbieter des Tools zur Reichweitenmessung ein Opt-Out-Verfahren zur Verfügung stellt. Nach Anklicken des Links wird der Widerspruch unmittelbar umgesetzt. Eine weitere Verarbeitung der Nutzungsdaten für statistische Analysen (Reichweitenmessung) findet nicht mehr statt.

Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, besteht allerdings ohnehin ein Widerspruchsrecht ohne Bedingungen, auch für ein Profiling in Verbindung mit Direktwerbung (Art. 21 Abs. 2 DSGVO). In diesen Fällen wirkt sich das Einräumen des Widerspruchsrechts nicht auf die Interessensabwägung aus. Aus Art. 25 Abs. 2 DSGVO und dem Erwägungsgrund 78 ergibt sich zudem, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen muss, die u. a. sicherstellen, dass durch die Nutzer vorgenommene technische Voreinstellungen an ihren Endgeräten zum Schutz ihrer personenbezogenen Daten (z. B. „Do Not Track“) auch eingehalten werden. Eine technische Umgehung der gewünschten Voreinstellungen, beispielsweise die Verwendung von Frist-Party-Cookies aufgrund blockierter Third-Party-Cookies, ist nicht zulässig.

c) Verkettung von Daten

Zu berücksichtigen ist, welche Möglichkeiten der Verknüpfung, Vervielfältigung von Datensätzen (z. B. durch eine höhere Anzahl an datenverarbeitenden Akteuren) und Anreicherungen von Datensätzen, insbesondere zweckunabhängig, existieren und welche Risiken für die betroffenen Personen hieraus entstehen.

Auch im Zusammenhang mit der Verkettung von Daten kann es eine Rolle spielen, welche Art von Identifikatoren genutzt werden. Zudem können Verknüpfungen von Nutzungsdaten und Inhaltsdaten (z. B. aus Kundenkonten) ebenso wie die geräteübergreifende Verkettung von Daten risikoerhöhend wirken. Darüber hinaus muss es in die Bewertung einfließen, wenn über Analysetools Dritte als Dienstleister eingebunden werden, die eine Verknüpfung mit eigenen Daten vornehmen oder Daten von verschiedenen Kunden, Websites und Geräten zusammenführen.

Zudem sind diese Verfahren technisch-organisatorisch so zu gestalten, dass ein Personenbezug frühestmöglich beseitigt wird und Nutzungsprofile – wenn überhaupt – unter Pseudonymen erstellt werden. Dies ergibt sich allerdings in der Regel bereits aus den Anforderungen des Art. 5 DSGVO und dessen technisch-organisatorischer Implementierung nach Art. 25 DSGVO, insbesondere Art. 25 Abs. 2 DSGVO (privacy by default).

Diese Anforderungen sind ebenso wie die Erfüllung der Transparenzanforderungen nach Art. 12 ff. DSGVO verpflichtend umzusetzen, so dass diese im Rahmen der Interessenabwägung nicht zugunsten des Verantwortlichen berücksichtigungsfähig sind. Darüber hinaus sind zwingend die Anforderungen aus Art. 24 und 32 DSGVO zu beachten und entsprechende technisch-organisatorische Maßnahmen zu ergreifen.

d) Beteiligte Akteure

Je mehr Verantwortliche, Auftragsverarbeiter und sonstige Empfänger in die Verarbeitungstätigkeit einbezogen sind, desto größer ist die Beeinträchtigung für den Betroffenen. Dies ergibt sich daraus, dass einerseits durch die steigende Anzahl an Akteuren das Risiko einer Datenschutzverletzung steigt. Anderseits sind regelmäßig die Eingriffsmöglichen des Verantwortlichen erschwert, weil die Akteure räumlich entfernt sind und unterschiedlichen Jurisdiktionen unterliegen (z.B. Akteure mit Niederlassungen in unterschiedlichen Staaten). Dem kann der Verantwortliche entgegensteuern, indem er zusätzliche technische und organisatorische Schutzmaßnahmen ergreift, die über die Mindestanforderungen der Art. 5 Abs. 1 lit. f), Art. 25 und Art. 32 DSGVO hinausgehen.

e) Dauer der Beobachtung

Im Rahmen der Wertungen ist relevant, wie lange die Möglichkeit besteht, die Nutzer wiederzuerkennen und Informationen zum Nutzungsverhalten zu sammeln und zuordnen zu können. Relevant ist in diesem Zusammenhang z. B., welche Lebensdauer Cookies haben. Eine sehr kurze Wiedererkennungsphase könnte z. B. auch zur Kompensation in anderen Bereichen führen. Z. B. fällt der Umfang der über den Nutzer erfassten Informationen bei der Interessenabwägung weniger ins Gewicht, je kürzer die Nutzer ausgesondert und wiedererkannt werden können.

f) Datenkategorien

Bei der Bewertung ist zu berücksichtigen, welche Datenkategorien erhoben und in welchem Detaillierungsgrad Informationen erfasst werden (z. B. Protokollierung, auf welche Dateien zugegriffen wurde, Tippverlaufsaufzeichnung, Aufzeichnung des Scrollings, Erhebung von Texten aus angefangenen Formularen, auch wenn diese nicht abgeschickt werden, Suchanfragen etc.). Die Verarbeitung von pseudonymen Daten ist grundsätzlich weniger belastend, da die Identität der betroffenen Person verschleiert wird und somit die Wahrscheinlichkeit geringer ist, dass die betroffene Person durch Dritte identifiziert wird. Daher ist im Rahmen der Interessenabwägung auch zu berücksichtigen, ob die betroffene Person direkt oder indirekt identifizierbar ist.

Zudem spielt es eine Rolle, ob und in welcher Form Nutzungsprofile erstellt werden, insbesondere welche Anzahl von Nutzungsdaten zusammengefügt und ob anschließend ergänzend Interessen und Merkmale zugeordnet werden, um den Nutzer in einer bestimmten Zielgruppe zu verorten und ihn schließlich zielgruppenspezifisch anzusprechen (Profiling z. B. zu Zwecken der Werbung oder personalisierten Information). Diese Form der Profilbildung erfolgt größtenteils dienst- und geräteübergreifend und kann dadurch zu einem umfassenden, tiefgreifenden und langanhaltenden Eingriff in die Privatsphäre des Nutzers führen. Bei einer umfangreichen Verarbeitung entstehen Risiken für die Rechte und Freiheiten der Nutzer, die zu

einem physischen, materiellen oder immateriellen Schaden führen könnten. Beispielsweise können die erstellten Nutzungsprofile zu einer Diskriminierung, einem Identitätsdiebstahl, einem finanziellen Verlust, einer Rufschädigung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen. Dieses Risiko ist höher zu bewerten, wenn bei der Profilbildung persönlichkeitsbeschreibende Aspekte, wie z.B. Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder das Verhalten analysiert oder prognostiziert werden. Auch die Erstellung von Bewegungsprofilen und -prognosen ist regelmäßig als hohes Risiko einzustufen.

g) Umfang der Datenverarbeitung

Außerdem ist der Umfang der Datenverarbeitung zu berücksichtigen. Dies ergibt sich aus den Art. 24, 25, 32 und 35 DSGVO. Je größer die Menge an verarbeiteten Daten, desto höher ist das Risiko für die Rechte und Freiheiten der betroffenen Person. Je mehr Daten verarbeitet werden, desto größer ist die Gefahr, dass durch Anhäufung großer Datenmengen weitere Informationen zum Vorschein kommen, die diskriminierend oder diffamierend sein können oder z.B. Rückschlüsse auf besondere Kategorien von Daten gem. Art. 9 Abs. 1 DSGVO zulassen. Der Umfang der Datenverarbeitung ist darüber hinaus eng mit der Speicherdauer verbunden. Werden über einen langen Zeitraum permanent Daten hinzugespeichert, vergrößert dies den Umfang der Datenverarbeitung.

Ebenso spielt die Anzahl der betroffenen Personen eine entscheidende Rolle bei der Interessenabwägung. Je größer die Anzahl der betroffenen Personen, desto eher und feingranularer können Vergleichsgruppen gebildet werden. Daraus kann sich ein erhöhtes Diskriminierungspotenzial ergeben und die Gefahr, dass Merkmale ermittelt werden, die ohne Betrachtung der Vergleichsgruppe nicht erkennbar gewesen wären.

Werden personenbezogene Daten verarbeitet, die Rückschlüsse auf besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO zulassen, bedarf es in jedem Fall einer Einwilligung. Hierzu zählen beispielsweise Dating-Portale, Websites von politischen Parteien, religiösen Vereinigungen, Online-Gesundheitsportale oder Webangebote für Erkrankungen. Daher ist in diesen Fällen eine besondere Sorgfalt bei der Einholung der informierten Einwilligung nötig, die alle Aspekte der Datensammlung erläutert, einschließlich des Umstand, dass Informationen über die sexuelle Orientierung oder das Interesse an den jeweiligen politischen Parteien an Dritte weitergegeben werden.

h) Kreis der betroffenen Personen (Kinder und andere schutzbedürftige Personen)

Im Rahmen der Interessenabwägung ist zu berücksichtigen, welche Personen von Verarbeitungsmaßnahmen betroffen sind. Sofern eine erhöhte Schutzbedürftigkeit von Personen gegeben ist, führt das dazu, dass die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen höher gewichtet werden. Dies gilt insbesondere für Kinder, die ausdrücklich in Art. 6 Abs. 1 lit. f) DSGVO benannt werden. Darüber hinaus können solche Überlegungen auch eine Rolle spielen, wenn z. B. die Erhebung von Nutzungsdaten und das Profiling von Nutzern gerade auch dazu dient, besondere Anfälligkeiten oder Situationen der Wehrlosigkeit zu erkennen und nutzbar zu machen.

Es ist weiterhin das Verhältnis des Verantwortlichen zur betroffenen Person zu berücksichtigen. So kann es Situationen geben, in denen zwischen dem Verantwortlichen und der betroffenen Person ein Machtungleichgewicht besteht. Dies ist beispielsweise im Beschäftigtenverhältnis der Fall oder wenn der Verantwortliche eine Monopolstellung hat. Besteht das Machtungleichgewicht zugunsten des Verantwortlichen, so führt dies ebenfalls dazu, dass die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen höher zu gewichten sind.

Beispiel:
Der Website-Betreiber bietet eine Beratungsplattform für Suchterkrankte an. Nutzer können auf der Website neben Hinweisen zu Kontaktmöglichkeiten von Beratungsstellen vor Ort auch Informationen zur Erkrankung und Erste Hilfe finden. Der Website-Betreiber bindet eine Vielzahl an Tools von Werbenetzwerken ein, die die Nutzungsdaten der Website-Besucher für eigene Zwecke weiterverarbeiten. Hier besteht ein besonderes Verhältnis zwischen Website-Besucher und -Betreiber. Aufgrund des Informationsangebots können Rückschlüsse auf besondere Kategorien von personenbezogenen Daten gem. Art. 9 Abs. 1 DSGVO gezogen werden. Außerdem ist zu vermuten, dass die Nutzer das Informationsangebot aufgrund eigener Betroffenheit in Anspruch nehmen und daher aufgrund ihres besonderen Interesses an Vertraulichkeit bzw. an einer weitestgehend anonymen Nutzung besonders schützenswert sind.

IV. Fazit

Verantwortliche sollten sich bewusst machen, dass die Interessenabwägung im Rahmen des Art. 6 Abs. 1 lit. f) DSGVO eine substantielle Auseinandersetzung mit den Interessen, Grundrechten und Grundfreiheiten der Beteiligten verlangt und auf den konkreten Einzelfall bezogen sein muss. Unzureichende oder pauschale Feststellungen, dass eine Datenverarbeitung gem. Art. 6 Abs. 1 lit. f) DSGVO zulässig sei, erfüllen nicht die gesetzlichen Anforderungen.
Sollte der Verantwortliche zum Ergebnis kommen, dass die Interessenabwägung zugunsten der betroffenen Person ausfällt und keine andere Rechtsgrundlage in Betracht kommt, ist die Datenverarbeitung – falls überhaupt – nur nach voriger informierter Einwilligung (Art. 6 Abs. 1 lit. a) DSGVO) rechtmäßig („jedenfalls dann…“).

Anhang I – Beispiel für eine Interessenabwägung

Beispiel Tracking-Pixel:
Ein Unternehmen (Online-Shop für Medikamente und Kosmetikartikel), im Folgenden: „Unternehmen“, schaltet auf einem sozialen Netzwerk Werbeanzeigen. Um Werbung im sozialen Netzwerk steuern und auswerten zu können, bindet das Unternehmen ein Tracking-Pixel, sog. Zähl-Pixel, des sozialen Netzwerks auf seiner Website des Unternehmens ein. Mithilfe des Pixels werden vom sozialen Netzwerk unmittelbar Daten der Website-Besucher erfasst. Anhand dieser Nutzerdaten erhält das Unternehmen Informationen zur Website. Dazu gehören beispielsweise Angaben darüber, wie der Nutzer auf die Website gelangt, wie er die Website nutzt, wie viele Nutzer sich für Newsletter anmelden und Produkte in den Warenkorb legen.
Diese Informationen nutzt das Unternehmen, um die Werbekampagnen auf dem sozialen Netzwerk zu gestalten und Streuverluste zu vermeiden. Um eine Auswertung des Nutzungsverhaltens zu ermöglichen sowie zielgerichtete Werbung zu schalten, verwendet das soziale Netzwerk die Daten des Online-Shops auch für eigene Zwecke und greift auf Daten aus eigenen Quellen zurück.

Das Unternehmen möchte zunächst keine Einwilligung der Nutzer einholen und fragt sich, ob die Datenverarbeitung gem. Art. 6 Abs. 1 lit. f) DSGVO gestützt werden kann.

Bewertung: Rechtmäßigkeit der Verarbeitung

Gemäß Art. 6 Abs. 1 lit. f) DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn diese 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. Danach ist eine Abwägung zwischen den Interessen des Unternehmens und den Interessen der betroffenen Personen, d.h. der Kunden des Unternehmens vorzunehmen.

1. **Stufe – Berechtigte Interesse des Verantwortlichen ermitteln**

Das Interesse des Unternehmens an Werbung in einem sozialen Netzwerk kann als wirtschaftliches Interesse als berechtigt angesehen werden.

2. **Stufe – Erforderlichkeit**

Die Erforderlichkeit für die Verarbeitung der personenbezogenen Daten wäre gegeben, wenn das beschriebene Verfahren geeignet ist, um die Werbung für das Unternehmen zu optimieren und alternative, gleich effektive Mittel nicht zur Verfügung ständen.

3. **Stufe - Interessen, Grundrecht und Grundfreiheiten der betroffenen Person und Abwägung im Einzelfall**

Dem gegenüber stehen die Grundrechte der Nutzer der Unternehmenswebsite auf Achtung ihres Privat- und Familienlebens sowie Schutz personenbezogener Daten gem. Art. 7 und Art. 8 GRCh.

Im Rahmen der Abwägung sind Auswirkungen der gegebenen Verarbeitung nicht nur abstrakt oder hypothetisch zu berücksichtigen, sondern es ist auf die konkreten Auswirkungen auf die einzelne betroffene Person abzustellen. Maßgeblich sind dabei u.a. die o. g. Kriterien:

a) Vernünftige Erwartung der betroffenen Personen und Vorhersehbarkeit / Transparenz

b) Interventionsmöglichkeiten der betroffenen Personen

c) Verkettung von Daten

d) Beteiligte Akteure

e) Dauer der Beobachtung

f) Kreis der Betroffenen (bspw. besonders schutzbedürftige Personen)

g) Datenkategorien

h) Umfang der Datenverarbeitung

Indem das Pixel auf der Website des Unternehmens eingebunden wird, veranlasst das Unternehmen die Erhebung von Informationen durch das soziale Netzwerk, welche konkreten Nutzer wann die einzelnen Seiten der Website aufrufen. Dadurch erhält das soziale Netzwerk weiteres Zusatzwissen über Websitebesucher, das es ohne Tracking-Pixel nicht erlangen würde. Dieses Zusatzwissen nutzt das soziale Netzwerk wiederum für eigene Werbezwecke, um die Zielgruppen für Werbemaßnahmen zu bestimmen. Dabei wird eine Vielzahl an Nutzungsdaten erhoben, die eine umfangreiche Profilbildung des Nutzers ermöglichen. Diese Informationen werden vom sozialen Netzwerk für die eigene Profilerstellung über die Nutzer verwendet. Der Website-Besucher kann eingebundene Tracking-Pixel weder ohne weiteres erkennen, noch erwartet er, dass sein Nutzungsverhalten website-übergreifend erfasst und zur Profilbildung durch das soziale Netzwerk verwendet wird.

Nutzer von sozialen Netzwerken erwarten zwar, dass personenbezogenen Daten durch Betreiber sozialer Netzwerke verarbeitet werden, die sie im Rahmen einer aktiven Nutzung direkt auf dem sozialen Netzwerk hinterlassen. Dazu gehören beispielweise gepostete Fotos und Nachrichten oder das „Liken“ von Beiträgen anderer Nutzer. Sie sind sich ggf. auch in allgemeiner Form über die Profilbildung durch Betreiber sozialer Netzwerke im Klaren. Der durchschnittliche Nutzer sozialer Netzwerke erwartet jedoch nicht, dass Websites „unsichtbare“ Pixel einbinden, um eine Datenverarbeitung durch Dritte zu veranlassen (Vernünftige Erwartung der betroffenen Personen) und sozialen Netzwerken damit Daten zugeliefert werden, die diese wiederum zur Profilbildung nutzen. In jedem Fall steht dies außerhalb dessen, was Nutzer objektiv vernünf-

tigerweise erwarten müssen, denn solche Datenerfassungen durch Dritte wirken sich nur nachteilig auf die Möglichkeit der Nutzer aus, die Verwendung eigener Daten zu kontrollieren und darüber zu bestimmen.

Darüber hinaus hat der Nutzer keine Möglichkeit, der Datenverarbeitung zu widersprechen oder durch sonstige Weise zum Ausdruck zu bringen, dass er die Profilbildung durch einen Dritten nicht wünscht (Keine Interventionsmöglichkeiten). Auch wenn ein Widerspruchsrecht zur Verfügung stünde, würde die Intervention erst nach der Datenverarbeitung möglich werden und käme damit zu spät, um im Hinblick auf die Eingriffsintensität die erforderliche Schutzwirkung zu entfalten.

Bei der Profilbildung werden nicht nur die Nutzungsdaten über einen längeren Zeitraum gespeichert. Anhand der Nutzungsdaten ermittelt das soziale Netzwerk Merkmale und Interessen des Nutzers, um ihn anschließend Zielgruppen zuzuordnen. Dies erfolgt nicht nur auf der Website des o.g. Unternehmens. Da eine Vielzahl von Websites das Pixel einbinden, können die Daten der Nutzer website- und sogar geräteübergreifend erfasst werden. Der Nutzer kann das Ausmaß der Datenverarbeitung nicht mehr erfassen und ist auch nicht in der Lage zu bestimmen, wer und in welchem Umfang seine Daten verarbeitet (Verkettung von Daten, Beteiligte Akteure, Transparenz).

Da das Unternehmen einen Online-Shop für Medikamente betreibt, ist nicht auszuschließen, dass die Nutzer Produkte in den Warenkorb legen oder sich für Artikel interessieren, die Rückschlüsse auf den Gesundheitszustand zulassen. Hier ist bereits fraglich, ob die Rechtsgrundlagen des Art. 6 Abs. 1 DSGVO überhaupt in Betracht kommen können. Fließen diese schützenswerten Informationen in das Nutzungsprofil ein, steigt das Risiko für die betroffenen Personen (Datenkategorien, Kreis der betroffenen Personen) in jedem Fall.

Eine Abwägung der o.g. Interessen im konkreten Einzelfall ergibt, dass die Interessen der betroffenen Personen die Interessen des Unternehmens überwiegen und folglich die Einbindung des Pixels nicht gem. Art. 6 Abs. 1 lit. f) DSGVO zulässig ist. Als Rechtsgrundlage käme dann – wenn überhaupt – nur die Einwilligung in Betracht.