BVDW
Wir sind das Netz

EU-Datenschutz-grundverordnung 2018

BVDW-Praxisleitfaden

LESEPROBE
Volle Version über **bvdw-datenschutz.de**

www.bvdw-datenschutz.de

§ RECHT
RESSORT IM BVDW

BVDW
Wir sind das Netz

EU-Datenschutz-grundverordnung 2018

BVDW-Praxisleitfaden

VORWORT

Mit der Datenschutzgrundverordnung wird ab dem 25. Mai 2018 ein neues Datenschutzrecht in ganz Europa gelten. Die von der EU-Kommission im Jahre 2012 begonnene Überarbeitung des Datenschutzrechts ist der Notwendigkeit gefolgt, das bisherige Recht den technologischen Entwicklungen und der fortschreitenden Digitalisierung anzupassen. Ein einheitlicher europäischer Rechtsrahmen ist grundsätzlich zu begrüßen, denn das neue Recht bringt für alle Unternehmen im europäischen Binnenmarkt mehr Transparenz. Leider ist es dem europäischen Gesetzgeber trotz jahrelanger Verhandlungen am Ende aber nicht gelungen, tatsächlich moderne und zukunftssichere Regeln für den Umgang mit Daten im 21. Jahrhundert zu schaffen. Vieles geht an den Realitäten und Anforderungen der Informationsgesellschaft vorbei. Vor allem im Umfeld der digitalen Geschäftsmodelle lässt die Verordnung an entscheidenden Stellen notwendige Differenzierungen und Risikoabstufungen im Bereich digitaler Verarbeitung von Daten vermissen. Zudem bringt das neue Recht ganz neue Datenschutzkonzepte und Verantwortlichkeiten mit sich, die den Umgang mit Daten in allen Unternehmen prägen werden. Der Gesetzgeber spricht von „Privacy-by-Design“ und schafft dabei mehrheitlich einwilligungsbasierte Regeln, die in ihrer Komplexität kaum zu erfassen oder rechtssicher umzusetzen sein werden.

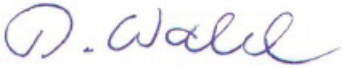
Anstatt mit praktikablen und verständlichen Regelungen mehr Rechtssicherheit zu schaffen, wird oftmals das Gegenteil bewirkt. Der Bundesverband Digitale Wirtschaft (BVDW) e.V. erwartet von der Europäischen Kommission und den zuständigen Datenschutzaufsichtsbehörden gleichermaßen deutliches Engagement bei der Konkretisierung der Verordnung mit dem Ziel, die heute etablierten Geschäftsmodelle und Möglichkeiten der Digitalen Wirtschaft zu erhalten und im globalen Wettbewerb zu fördern. Die sich stellenden Fragen der Rechtsanwendung müssen schnell und verlässlich beantwortet werden.

Datenpolitik ist bereits heute, vor allem aber zukünftig ein wesentlicher Baustein der Wettbewerbs- und Standortpolitik. Der nun geschaffene Regulierungsrahmen im Datenschutz hat entscheidenden Anteil an der Wettbewerbs- und Innovationsfähigkeit des europäischen Marktes und bestimmt in großem Maße, wo zukünftig Investitionen getätigt werden. Es gilt daher, ein pragmatisches und vor allem praktikables Verständnis des Datenschutzrechts zum Vorteil der Nutzer und der Unternehmen der Digitalen Wirtschaft zu etablieren. Anderenfalls besteht die ernst zu nehmende Gefahr, dass europäischen Unternehmen Hürden in den Weg gestellt werden, die sich als negativ auf Investitionsentscheidungen und die Innovationsfähigkeit der Digitalen Wirtschaft mit den entsprechenden Konsequenzen für Arbeitsplatzaufbau und -sicherung erweisen können.

Die Entwicklung und Gestaltung einer europäischen Datenökonomie braucht klare Leitlinien. Für die Umsetzung der ab 2018 geltenden Anforderungen haben die Unternehmen jetzt weniger als ein Jahr Zeit. Dieser Leitfaden soll einen Beitrag zur Aufklärung leisten und den Unternehmen gleichzeitig Orientierung bei der richtigen Anwendung des neuen Rechts bieten – zum Vorteil der Digitalen Wirtschaft in Deutschland und der gesamten EU.

Ich wünsche Ihnen eine erkenntnisreiche Lektüre.

Ihr



Matthias Wahl
Präsident BVDW e.V.

I. EINFÜHRUNG UND HINTERGRÜNDE

Datenschutzrichtlinie ursprünglich von 1995

Das heute noch in der Europäischen Union geltende Datenschutzrecht beruht auf der Datenschutzrichtlinie von 1995. Diese Regeln entsprachen schon aufgrund der technischen Entwicklung der letzten 20 Jahre nicht mehr den Anforderungen, die heute an ein modernes Datenschutzrecht gestellt werden. Auch aus diesem Grund hatte die EU die Novellierung des europäischen Datenschutzrechts bereits 2012 mit der Veröffentlichung eines entsprechenden Verordnungsentwurfs durch die Europäische Kommission angestoßen. Die EU-Datenschutzgrundverordnung (DSGVO) ist unter maßgeblicher Beteiligung der Öffentlichkeit und der interessierten Kreise durch das Europäische Parlament und von den Mitgliedstaaten im Rat diskutiert und entschieden worden.

Nach intensiver Diskussion einigten sich die 28 Mitgliedstaaten der EU Mitte Juni 2015 schließlich auf eine gemeinsame Textfassung der Datenschutzgrundverordnung (DSGVO). Auf diese vorläufige Einigung folgten schließlich die Verhandlungen im sogenannten Trilog, in dem ein Kompromiss mit der Fassung der DSGVO gesucht wurde, die das Europäische Parlament bereits Ende 2013 verabschiedet hatte. Am Trilog beteiligt war als dritte Partei die Europäische Kommission. Der Trilog endete am 15. Dezember 2015 mit dem Beschluss der Kompromissfassung eines Entwurfs für eine europäische Datenschutzgrundverordnung. Am 06. April 2016 wurde schließlich ein konsolidierter Entwurf der deutschen Textfassung der DSGVO veröffentlicht.

Am 14. April 2016 wurde die DSGVO durch das Plenum des EU-Parlaments angenommen und in der Folge im Amtsblatt der Europäischen Union veröffentlicht. Anders als bei einer EU-Richtlinie bedarf es keiner weiteren Umsetzung in nationales Recht. Die Verordnung wird unmittelbar anwendbares Recht.

„Grund"-Verordnung im Bereich des Datenschutzes

Der Charakter als Kompromisslösung wird bereits im Namen des Regelwerkes deutlich. Es handelt sich um eine (bislang als solche unbekannte) „Grund"-Verordnung im Bereich des Datenschutzes. Sie ist gekennzeichnet durch eine Vielzahl von Regelungsspielräumen zugunsten nationalgesetzlicher Einzelregelungen sowie der ausdrücklichen Ermächtigung des Europäischen Parlaments und des Rates, weitergehende Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten zu erlassen (delegierte Rechtsakte).

II. DIE EU-DATENSCHUTZGRUND-VERORDNUNG IM ÜBERBLICK

1. REGELUNGSZIELE

Harmonisierung und Modernisierung des Datenschutzrechts

Hauptziel der Verordnung ist die europaweite Harmonisierung und Modernisierung des Datenschutzrechts. Die rasant fortschreitende technologische Entwicklung sollte durch neue Datenschutzregeln für die On- und Offline-Welt eingefangen und abgebildet werden.

Keine Einschränkung des „free flow of data"

In ihrem Art. 1 gibt die DSGVO die Ziele der Neuregelung selbst an. So soll die Verordnung sowohl den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten als auch den freien Verkehr solcher Daten sicherstellen. Der „free flow of data" innerhalb der Europäischen Union soll durch die Regelungen des Rechts auf den Schutz personenbezogener Daten vor allem weder eingeschränkt noch verboten werden. Dieser Grundsatz ist Voraussetzung für eine funktionierende Datenökonomie in dem von der EU-Kommission angestrebten digitalen Binnenmarkt.

EU-Verordnung für alle Mitgliedstaaten unmittelbar und einheitlich verbindliches Recht

Aus den Erwägungsgründen, aber auch aus der Wahl des Regelungsmittels in Form einer Verordnung anstelle einer Richtlinie, lassen sich die weiteren Ziele der DSGVO ablesen. Im Unterschied zu einer EU-Richtlinie, welche lediglich Rechtsgrundsätze aufstellt, die in den Mitgliedstaaten in unterschiedlichster Weise in nationales Recht umgesetzt werden können, sind die Vorgaben einer EU-Verordnung für alle Mitgliedstaaten unmittelbar und einheitlich verbindliches Recht. Gerade die Umsetzungsunterschiede, die aus der alten EU-Datenschutzrichtlinie 95/46/EG resultierten, sah die EU-Kommission als ein wesentliches Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeiten an, die den Wettbewerb verzerren und die Behörden an der Erfüllung der ihnen nach dem Unionsrecht obliegenden Pflichten hindern.

Gilt für öffentlichen und privaten Sektor

Die DSGVO regelt nun erstmals europaweit einheitlich die Bedingungen für die Verarbeitung personenbezogener Daten sowohl im öffentlichen als auch im privaten Sektor. Im Mittelpunkt steht hier vor allem die Erkenntnis, dass der grenzüberschreitende Verkehr personenbezogener Daten zwischen öffentlichen und privaten Akteuren einschließlich natürlichen Personen, Vereinigungen und Unternehmen stark zugenommen hat und nun unter einheitlichen Rahmenbedingungen stehen muss.

Insgesamt sollen die Rechte betroffener Personen gestärkt und die Verpflichtungen für diejenigen, die personenbezogene Daten (pDaten) verarbeiten

oder über die Verarbeitung entscheiden, verschärft werden. Die Aufsichtsbehörden sollen gleiche Befugnisse bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung besitzen.

2. STRUKTUR

11 Kapitel und 99 Artikel

Die DSGVO gliedert sich in insgesamt 11 Kapitel und 99 Artikel, wobei sich die ersten fünf Kapitel mit den Grundsätzen und materiellen Anforderungen an Datenverarbeitungen befassen. Die Unterscheidung zwischen Verarbeitungen durch öffentliche oder durch nichtöffentliche Stellen wird in den jeweiligen Artikeln vorgenommen. Eine klare Trennung hätte bereits hier für mehr Überblick sorgen können. Die letzten Kapitel befassen sich im Wesentlichen mit formalen Themen wie der Gestaltung der Datenschutzaufsicht, Fragen der europäischen Zusammenarbeit im Datenschutz (Kohärenzverfahren) und den Sanktionen. Hervorzuheben sind die in Kapitel 9 zusammengefassten Bereiche besonderer Verarbeitungsszenarien wie Presse, Gesundheit, Forschung oder Beschäftigtendatenschutz.
Die Gliederung im Überblick (auszugsweise Übersicht):

Kapitel 1 ALLGEMEINE BESTIMMUNGEN (Art. 1–4)
- Gegenstand und Ziele
- Anwendungsbereich
- Definitionen
- Begriffsbestimmungen

Kapitel 2 GRUNDSÄTZE (Art. 5–11)
- Rechtmäßigkeit der Verarbeitung
- Bedingungen für die Einwilligung
- Einwilligung von Kindern
- Besondere Kategorien personenbezogener Daten
- Identifizierung von Personen

Kapitel 3 RECHTE DER BETROFFENEN PERSON (Art. 12–23)
- Transparenz
- Informationspflichten
- Auskunftsrechte
- Löschungsrechte (Recht auf Vergessenwerden)
- Widerspruchsrecht
- Beschränkungen

Kapitel 4 VERANTWORTLICHER UND AUFTRAGSVERARBEITER (Art. 24–43)
- Verantwortung
- Datenschutz durch Technikgestaltung
- Auftragsverarbeiter
- Verarbeitungsverzeichnis
- Sicherheit der Verarbeitung
- Datenschutz-Folgenabschätzung
- Benennung eines Datenschutzbeauftragten
- Zertifizierung

Kapitel 5 DATENÜBERMITTLUNG IN DRITTLÄNDER ODER INT. ORGANISATIONEN (Art. 44–50)

- Allgemeine Grundsätze der Datenübermittlung
- Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses
- Datenübermittlung vorbehaltlich geeigneter Garantien
- Verbindliche interne Datenschutzvorschriften
- Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung

Kapitel 6 UNABHÄNGIGE AUFSICHTSBEHÖRDEN (Art. 51–59)

- Unabhängigkeit
- Zuständigkeit, Aufgaben und Befugnisse

Kapitel 7 ZUSAMMENARBEIT UND KOHÄRENZ (Art. 60–76)

- Zusammenarbeit
- Kohärenz
- Europäischer Datenschutzausschuss

Kapitel 8 RECHTSBEHELFE, HAFTUNG UND SANKTIONEN (Art. 77–84)

- Recht auf Beschwerde bei einer Aufsichtsbehörde
- Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde
- Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter
- Vertretung von betroffenen Personen
- Aussetzung des Verfahrens
- Haftung und Recht auf Schadenersatz
- Allgemeine Bedingungen für die Verhängung von Geldbußen
- Sanktionen

Kapitel 9 VORSCHRIFTEN FÜR BESONDERE VERARBEITUNGSSITUATIONEN (Art. 85–91)

- Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit
- Verarbeitung und Zugang der Öffentlichkeit zu amtlichen Dokumenten
- Verarbeitung der nationalen Kennziffer
- Datenverarbeitung im Beschäftigungskontext
- Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken
- Geheimhaltungspflichten
- Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften

Kapitel 10 DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE (Art. 92–93)

- Ausübung der Befugnisübertragung
- Ausschussverfahren

Kapitel 11 SCHLUSSBESTIMMUNGEN (Art. 94–99)

- Aufhebung der Richtlinie 95/46/EG
- Verhältnis zur Richtlinie 2002/58/EG
- Verhältnis zu bereits geschlossenen Übereinkünften
- Berichte der Kommission
- Überprüfung anderer Rechtsakte der Union zum Datenschutz
- Inkrafttreten und Anwendung

3. RÄUMLICHE GELTUNG

Die DSGVO soll für europaweit einheitliche Anwendung stehen und damit bislang strittige Abgrenzungsfragen der Anwendbarkeit von Gesetzen in einzelnen Mitgliedstaaten lösen. In Art. 3 DSGVO ist der räumliche Anwendungsbereich näher definiert.

DSGVO gilt für alle EU-Unternehmen einheitlich

Die DSGVO gilt nunmehr einheitlich für Verarbeitungen von pDaten durch in der EU niedergelassene Unternehmen (Art. 3 Abs. 1 DSGVO). Dabei ist es nicht von Belang, ob die Verarbeitung selbst ebenfalls in der EU erfolgt. Verarbeitet ein in Deutschland niedergelassenes Unternehmen pDaten also auf Servern eines Auftragsverarbeiters in einem Nicht-EU-Staat, gilt trotzdem die DSGVO.

Marktortprinzip

Mit der DSGVO wird außerdem das sogenannte Marktortprinzip im Datenschutzrecht eingeführt. Art. 3 Abs. 2 DSGVO bestimmt, dass die DSGVO auch auf all diejenigen Verarbeitungen von pDaten durch Unternehmen anzuwenden ist, wo diese Personen betreffen, die sich in der EU befinden und das Unternehmen weder seinen Sitz noch eine Niederlassung in der EU hat. In diesem Falle ist gemäß Art. 27 DSGVO grundsätzlich ein Vertreter in der Union zu benennen. Damit soll die Zugrifftsmöglichkeit gesichert werden. Es kommt nicht darauf an, ob die angebotenen Dienste entgeltlich oder unentgeltlich zu nutzen sind. Damit werden alle – auch kostenfreie weil werbefinanzierte – Angebote erfasst.

Geltung auch für Nicht-EU-Unternehmen, soweit Aktivitäten auf den europäischen Markt gerichtet sind

Voraussetzung nach Art. 3 Abs. 2 DSGVO ist, dass die Datenverarbeitung in Zusammenhang damit steht,

a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;
b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

3.1 Anbieten von Waren oder Dienstleistungen in der EU

Ein Unternehmen muss zum einen tatsächlich beabsichtigen, Waren oder Dienstleistungen an Personen in der EU anzubieten. Zur Ermittlung können nach Erwägungsgrund 23 DSGVO Indizien wie die allgemeine Zugänglichkeit der Webseite, eine E-Mail-Kontaktadresse oder die Verwendung einer Sprache, die in dem Drittland, in dem der Verantwortliche niedergelassen ist, allgemein gebräuchlich ist, dienen. Soweit dies – wie wohl in der Mehrzahl der Fälle – nichts über die tatsächliche Absicht des Unternehmens aussagt, müssen weitere Faktoren berücksichtigt werden. Dafür sprechen dann wei-

tere Indizien wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen, oder die Erwähnung von Kunden und Nutzern, die sich in der Union befinden.

3.2 Verhaltensbeobachtung

Die DSGVO soll auch für alle Unternehmen gelten, die das Verhalten einer Person beobachten, soweit dieses in der Union erfolgt. Hierunter sind Tracking-Maßnahmen zu verstehen, die z. B. das Surfverhalten von Nutzern in der EU im Blick haben. Laut Erwägungsgrund 24 DSGVO soll zur Ermittlung dieser Frage auch entscheidend sein, ob daraufhin Verarbeitungstechniken genutzt werden, durch die von einer natürlichen Person ein Profil erstellt wird, das insbesondere die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen. Für den Bereich der digitalen Werbewirtschaft dürfte diese Geltung in vielen Fällen greifen.

3.3 Zusammenfassung

Umfassende Wirkung des Geltungsbereichs

Die Wirkung dieser Regelungen ist umfassend. Die Geltung der DSGVO ist demnach für alle national oder grenzüberschreitend tätigen EU-Unternehmen (Internetmarktplätze, Warentransporteure, digitale Dienstleister, soziale Medien) von Bedeutung, selbst wenn die Verarbeitung von pDaten gar nicht in der EU stattfindet. Bei Nicht-EU-Unternehmen entscheidet die Ausrichtung des Angebots auf den europäischen Markt.

4. INKRAFTTRETEN

Ab 25. Mai 2018 unmittelbar anwendbares Recht in der EU

Die DSGVO trat 20 Tage nach der Veröffentlichung im Europäischen Amtsblatt am 24. Mai 2016 in Kraft und wird nach einer Übergangszeit von zwei Jahren ab dem 25. Mai 2018 unmittelbar anwendbares Recht in der EU. Bis dahin muss die DSGVO auch mit dem nationalen Recht harmonisiert werden.

In Deutschland zusätzlich ab 25. Mai 2018 BDSG-neu

Dies ist in Deutschland bereits geschehen. Mit dem Datenschutzanpassungs- und Umsetzungsgesetz EU (DSAnpUG – E) ist in Deutschland das alte Bundesdatenschutzgesetz (BDSG) als BDSG-neu grundsätzlich umgestellt worden. Das nationale Datenschutzrecht enthält nunmehr nur noch Bestimmungen, die entweder die in der DSGVO vorgesehenen Regelungsspielräume ausnutzt oder andere, dort nicht geregelte Bereiche betrifft. Das BDSG-neu tritt zusammen mit der DSGVO ebenfalls am 25. Mai 2018 in Kraft. Einzelheiten hierzu werden in diesem Leitfaden entsprechend berücksichtigt.

III. BASICS DER DATENVERARBEITUNG

1. VERARBEITUNG PERSONENBEZOGENER DATEN

Die DSGVO ist nur dann anwendbar, wenn es um die Verarbeitung von pDaten geht. Für Daten ohne Personenbezug oder Personenbeziehbarkeit gilt die DSGVO nicht.

Automatisierte Verarbeitung und Speicherung in einem Dateisystem

Der Begriff „Verarbeitung" ist weit zu verstehen und umfasst bereits sowohl das vorgelagerte Erheben als auch das nachgelagerte Speichern von pDaten.

In Art. 2 Abs. 1 DSGVO werden die relevanten Verarbeitungsszenarien umrissen. PDaten müssen entweder ganz oder teilweise automatisiert oder – wenn es nicht automatisiert erfolgt – für die Speicherung in einem Dateisystem verarbeitet werden. Für die Digitale Wirtschaft relevant ist insbesondere die automatisierte – also computergestützte – Verarbeitung. Die Verarbeitung durch natürliche Personen zu persönlichen oder familiären Zwecken ist von der DSGVO ausgenommen. Diese sogenannte „Haushaltsausnahme" stellt klar, dass eine Verarbeitung im privaten Bereich (z. B. das Anlegen einer privaten Kontaktliste), keinen Beschränkungen unterliegt. Die Verarbeitung von Werbedaten fällt eindeutig in den Bereich der DSGVO – soweit es sich um pDaten handelt.

Weites Verständnis von personenbezogenen Daten

Das Verständnis des Begriffs der pDaten ist unter der DSGVO erheblich ausgeweitet worden. Zugleich sind ausdrücklich Online-Identifikatoren wie Cookie-IDs und mobile Geräte-Werbe-IDs unter dieses Verständnis eingeordnet worden. Es ist für die Beurteilung in Unternehmen der Digitalen Wirtschaft daher wesentlich zu verstehen, in welchen Bereichen die Definition von pDaten gilt. Dies dürfte nicht immer einfach sein.

Die Verordnung definiert in Art. 4 Nr.1 als pDaten:
„Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;"

1.1 Identifizierung einer natürlichen Person

Datum muss zur Identifizierung oder Identifizierbarkeit einer natürlichen Person führen können

Personenbezug haben Daten also immer dann, wenn sie sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Betroffene). Identifizierbar ist eine Person, wenn sie unmittelbar oder mittelbar mittels Zuordnung zu einer Kennung wie Name, Standortdaten, Online-Identifier oder physische, wirtschaftliche, kulturelle – aber auch genetische oder biometrische – Merkmale identifiziert werden kann.

In der Digitalbranche – insbesondere der Online-Werbevermarktung geht – es hauptsächlich um das Kategorisieren von Nutzungsverhalten in Segmente. Profiling anhand von Nutzungsdaten muss unter Beachtung der tatsächlich verwendeten Daten also zu einer Personenbeziehbarkeit führen, um unter den Anwendungsbereich der DSGVO zu fallen. Einen Hinweis, welche Datenverarbeitungen zur Identifizierbarkeit führen können, gibt Erwägungsgrund 26 DSGVO:
„Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern."

Es geht also darum, aus einem Nutzungsdatenprofil auf eine existierende natürliche Person schließen zu können. Als Gradmesser für eine Personenbeziehbarkeit soll der Aufwand dienen, den die verantwortliche Stelle betreiben müsste, um aus einem Datensatz eine natürliche Person zu identifizieren. Dahinein zu rechnen sind *„alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, (…) wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind."*

Identifizierung muss mit vertretbaren Mitteln erfolgen

Personenbeziehbarkeit liegt also nur vor, wenn das verantwortliche Unternehmen mit verträglichem Aufwand die erhobenen Daten eindeutig einer bestimmten, identifizierbaren natürlichen Person zuordnen kann. Dies entspricht zunächst einem relativen Verständnis der Personenbeziehbarkeit, wo ein Personenbezug dann angenommen wird, wenn die konkrete verantwortliche Stelle – und nicht irgendwer – diesen unter vertretbarem Aufwand herstellen kann.

Die DSGVO sagt nicht, wer diese Zuordnung vornehmen muss. Allerdings dürfte sich nach den Kriterien des Europäischen Gerichtshofs zur Frage der Personenbezogenheit dynamischer IP-Adressen die Debatte darum nun (fast) erledigt haben.

Beispiel dynamische IP-Adresse: Die Frage der Personenbezogenheit einer IP-Adresse ist üblicherweise relativ und kontextspezifisch zu betrachten. So kann eine dynamische IP-Adresse für einen Webseitenbetreiber allein eventuell nicht-personenbezogen sein (z. B. bei einem von vielen Nutzern frequentierten, öffentlichen „Hotspot"). Wird diese IP-Adresse jedoch mit anderen Informationen verbunden, die es erlauben würden, eine einzelne Person zu identifizieren, dann würde der Datensatz – und damit auch die IP-Adresse als dessen Bestandteil – als pDatum gelten. Der Aufwand, eine IP-Adresse einer natürlichen Person zuzuordnen, wäre – ohne weiteren Anlass – zudem nicht zu rechtfertigen.

In seinem Urteil zur Frage der Personenbezogenheit von IP-Adressen vom 19. Oktober 2016 hat der Europäische Gerichtshof (EuGH)[1] jedoch festgestellt, dass eine dynamische IP-Adresse, die von einem „Anbieter von Online-Mediendiensten" (d. h. vom Betreiber einer Website) beim Zugriff auf seine allgemein zugängliche Website gespeichert wird, für den Betreiber ein personenbezogenes Datum darstellt, wenn er über „rechtliche Mittel verfügt", die es ihm erlauben, den Nutzer anhand der Zusatzinformationen, über die dessen Internetzugangsanbieter verfügt, bestimmen zu lassen. Es geht also nicht mehr um den Aufwand, sondern nur noch um die Frage, ob entsprechende Mittel zur Verfügung stehen. Solche rechtlichen Mittel könnten Auskunftsansprüche gegenüber Behörden oder Access-Provider im Rahmen eines Strafverfahrens darstellen. Diese Möglichkeit dürfte theoretisch immer eingreifen.

Die Anforderungen an den „vernünftigen Aufwand" hat der Bundesgerichtshof (BGH) dann kürzlich noch konkretisiert.[2] Eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Internetseite, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, stellt für den Anbieter ein personenbezogenes Datum dar. Es wird davon ausgegangen, dass jedenfalls eine Bundesbehörde als Webseitenbetreiber über rechtliche Mittel verfügt, die vernünftigerweise eingesetzt werden können, um mithilfe Dritter, und zwar der zuständigen Behörde und des Internetzugangsanbieters, die betreffende Person anhand der gespeicherten IP-Adresse(n) bestimmen zu lassen.

Dynamische IP-Adressen sind pDaten

Ob man bei regulären Nutzungen und privaten Webseitenbetreibern oder gar Online-Datenverarbeitern solche absoluten Kriterien anlegen kann, dürfte nach wie vor zweifelhaft sein. Weder wäre ein solcher Aufwand hier vernünftig noch – in Anbetracht der Lebensdauer und Verwendung der Daten – relevant. Bis zu einer weiteren Entscheidung in diesem Bereich wird man allerdings nun von einem pDatum ausgehen müssen.

1 EuGH Urt. v. 19.10.2016, Az. C-582/14
2 BGH Urt. v. 16.05.2017, VI ZR 135/13

1.2 Direkte oder indirekte Identifizierbarkeit

Der in der DSGVO grundsätzlich angesprochene Gedanke, dass pDaten nur dann vorliegen, wenn eine Beziehbarkeit zu einer konkreten natürlichen Person hergestellt werden kann, erfährt durch das Kriterium der indirekten Bestimmbarkeit eine weitere erhebliche Einschränkung. Gemäß Art. 4 Abs.1 DSGVO reicht eine indirekte Identifizierbarkeit durch Zuordnung z. B. zu einer Online-Kennung oder zu Merkmalen, die Ausdruck z. B. der sozialen Identität der Person sind.

Personenbezug bei Verbindung von Personendaten und Online-Kennungen möglich, aber nicht immer zwingend

In Erwägungsgrund 30 DSGVO wird zwar erkannt, dass die Zuordnung von natürlichen Personen zu bestimmten Cookie-IDs oder IP-Adressen Spuren hinterlassen kann, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren. Die Formulierung „kann" zeigt dabei, dass dies nicht der Fall sein „muss".

Individualisierung statt Identifizierung

Das Zuordnen von Nutzungshandlungen im Internet zu einem bestimmten Nutzungsprofil unter einer eindeutigen Kennung in Form einer Werbe-ID und ohne weitere Klardatenverarbeitung (also tatsächliche Zuordnung zu einer bestimmten natürlichen Person) dürfte vordergründig in den wenigsten Fällen zur konkreten Identifizierbarkeit einer konkreten natürlichen Person führen. Nutzungsdatenverarbeitungen und -auswertungen haben allein bestimmtes Nutzungsverhalten (einer unbestimmten Person) im Blick. Es geht hier also nicht um Identifizierung einer Person, sondern vielmehr um Individualisierung eines Nutzungsverhaltens.

Indirekte Identifizierbarkeit

Gelingt es aber, mit einem umfangreichen Datensatz und mithilfe von speziellen Aussonderungstechniken (singling out) ein Verhalten auf eine bestimmbare Person zu beziehen (ohne diese klar zu identifizieren), sollen diese Daten ebenfalls personenbezogen sein. Es führt also nicht nur eine direkte, sondern auch jede indirekte Identifizierbarkeit zur Personenbeziehbarkeit. Die Hürden für eine Personenbeziehbarkeit sind daher weit geringer.

Online-Identifier und entsprechende Datensätze können anonyme Daten sein

Beispiel Online-Identifier: Relevant wird dies im Bereich der von der DSGVO ebenfalls erfassten Online-Identifier. Derzeit ordnen Landesdatenschutzbehörden Online-Identifier wie z. B. eine Werbe-ID den personenbezogenen Daten zu. Für die Nutzung dieser wird sogar eine Einwilligung verlangt. Zugleich spricht die DSGVO in Erwägungsgrund 30 jedoch davon, dass eine Identifizierung nicht notwendig mit der Nutzung einer Kennnummer einhergehen muss. Wo dies nicht der Fall ist, würde es sich demnach um anonyme Daten handeln, die überhaupt keiner datenschutzrechtlichen Regelung unterliegen.

Denn zumindest für Dritte ist schon nicht nachvollziehbar, welche Daten sich hinter der Kennnummer verbergen. Kann mit diesen Daten ohnehin keine Identifizierbarkeit einer natürlichen Person hergestellt werden, sollte der gesamte Datensatz eigentlich anonym sein.

Diese Ansicht ist auch nachvollziehbar. Es soll gemäß Art. 4 Nr. 1 DSGVO reichen, dass eine natürliche Person mittels Zuordnung, z. B. zu einer Online-Kennung oder Standortdaten, direkt oder indirekt identifizierbar wird. Die Identifizierbarkeit muss sich aber direkt aus der Zuordnung ergeben und nicht aus den unter einer Online-Kennung gegebenenfalls gespeicherten Nutzungsdaten. Eine Online-Kennung wie eine Werbe-ID lässt aber – anders als die in Art. 4 Nr. 1 DSGVO ebenfalls beispielsweise genannten Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind – üblicherweise keinen eigenständigen Rückschluss auf eine Person zu.

Personenbezug allein durch Zuordnung zu einer Online-Kennung

Aus diesem Grund bleiben hier Zweifel an der Anwendbarkeit der DSGVO weiterhin bestehen, weil sich nach wie vor die Frage stellt, ob die Sammlung, Aufbereitung und Verarbeitung von Nutzungsdaten (zum Beispiel im Rahmen des Programmatic Advertisings) und ihre Verknüpfung mit Online-Identifiern, also z. B. der User-ID, Cookie IDs, etc., überhaupt die Verarbeitung von personenbezogenen Daten darstellt.

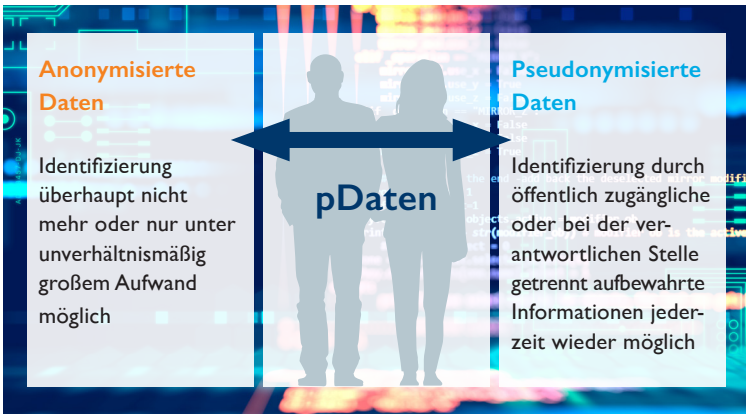
Personenbeziehbarkeit nach dem Konzept der DSGVO

Im Bereich der Werbenutzung von Daten im Rahmen von Profiling wird diese Annahme jedoch zumeist nicht tragen. Grund dafür ist, dass eine Personenbeziehbarkeit bereits durch das Zuschneiden des Profilings auf „bestimmte" Nutzungshandlungen eines konkreten Nutzers erfolgt. Es ist nicht erforderlich, dass die Person klar identifiziert wird. Allein das „Aussondern" eines Nutzers aufgrund von Nutzungsinformationen in Kombination mit einer Online-Kennung führt letztlich zu einer Personenbeziehbarkeit nach dem Konzept der DSGVO.

Entscheidend ist in diesen Fällen daher weniger die Frage des (weiten) Verständnisses des Personenbezugs, sondern vielmehr die der Möglichkeiten der Verarbeitung pseudonymer Daten.

2. ANONYME UND PSEUDONYME DATEN

In der Online-Welt besonders üblich und bekannt war bisher die Pseudonymisierung von Nutzungsdaten zum Zwecke der Werbung und Marktforschung gemäß § 15 Abs. 3 TMG. Diese Vorschrift ließ es bekanntlich zu, zum Zwecke der Werbung und Marktforschung pseudonyme Nutzerprofile zu erheben, sofern Unternehmen in ihren Datenschutzerklärungen auf diesen Umstand hinwiesen und den Nutzern zugleich die Möglichkeit gaben, ihren Widerspruch dagegen zu erklären (Opt-Out). Auch die Anonymisierung von Daten spielte bisher eine große Rolle, denn waren Daten erst einmal wirksam anonymisiert, waren sie, wie oben bereits erwähnt, dem Anwendungsbereich der Datenschutzgesetze entzogen.



2.1 Anonyme Daten

Anonymisieren ≠ Pseudonymisieren

Ein Anonymisieren von Daten lag bisher vor, wenn pDaten derart verändert werden, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Die Anonymisierung wird nicht gesetzlich in der DSGVO definiert, sie wird allerdings in Erwägungsgrund 26 angesprochen. Dort heißt es : „Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder pDaten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke."

2.2 Pseudonyme Daten

Unter einem Pseudonymisieren verstand das BDSG das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Im Anwendungsbereich der zukünftigen DSGVO werden diese Begriffe nunmehr anders definiert: „Pseudonymisierung" ist gemäß Art 4 Nr. 5 DSGVO *„die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden".*

Der Verwendung pseudonymisierter Daten wird künftig eine wesentliche Rolle zukommen. Die DSGVO privilegiert pseudonyme Daten an verschiedenen Stellen. Als geeignete technisch-organisatorische Maßnahme unter dem Stichwort „Privacy-by-Design" stellt die Pseudonymiserung gemäß Art. 25 Abs. 1 DSGVO ein Mittel zur Umsetzung der DSGVO-Datenschutzgrundsätze wie Datenminimierung (Art. 5 Abs. 1 c) DSGVO) oder Garantien zum Schutz von Betroffenenrechten bei der Weiterverarbeitung von pDaten zu anderen Zwecken dar (Art. 6 Abs. 4 DSGVO).

Die Verwendung pseudonymer Datensätze kann ebenso dort, wo eine Identifizierung von Betroffenen nicht möglich ist, dazu führen, dass die Verpflichtung zur Erfüllung von Betroffenenrechten eingeschränkt ist oder gar entfällt. Diese in Art. 11 DSGVO niedergelegte Erleichterung dürfte wesentlich im Bereich der Werbevermarktung sein. Nicht ausgenommen sind allerdings weiterhin die umfangreichen Informationspflichten aus Art. 12 ff. DSGVO.
Praktisch wichtigster Anwendungsfall dürfte jedoch die leichtere Verarbeitung aufgrund der gesetzlichen Erlaubnis aus Art. 6 Abs. 1 f) DSGVO sein. Zwar sieht die DSGVO keinen echten „Nachfolger" für § 15 Abs. 3 TMG vor. Das bedeutet jedoch nicht, dass der Regelungsgehalt damit vollständig verloren gegangen ist, wie schon zum Teil befürchtet wurde. Im Gegenteil heißt es in Erwägungsgrund 29 DSGVO gerade, dass für die Anwendung der Pseudonymisierung Anreize geschaffen werden sollen und benennt in diesem Zusammenhang ausdrücklich die Möglichkeit von Pseudonymisierungsmaßnahmen zum Zwecke einer „allgemeinen Analyse" bei „demselben Verantwortlichen". Nach Auffassung der einschlägigen Literatur spricht deshalb vieles für eine auch in Zukunft eröffnete Möglichkeit zur Erstellung von Nutzungsprofilen bei Verwendung von Pseudonymen zum Zwecke der eigenen und ebenfalls zum Zwecke der anbieterübergreifenden Werbung.

Nutzungsdaten-verarbeitung weiterhin grund-sätzlich einwilligungs-los möglich

Deshalb wird zu Recht auch die Auffassung vertreten, dass insbesondere Analyse-und Werbetechniken im Internet bei der Verwendung von Pseudonymen auch zukünftig auf der Grundlage der allgemeinen Interessenabwägungsklausel des Art. 6 Abs. If DSGVO möglich sein werden, wenn sich diese als allgemein erwartbar darstellen und die jeweilige Person transparent über deren Einsatz informiert wird. Denn das Nutzungsverhalten im Internet – und damit die entsprechenden Nutzungsdaten – sind nichts anderes als das Abbild der sozialen Realität eines Nutzers.[3] Selbst wo solche Daten personenbezogen sind, können solche Daten also nicht ausschließlich dem Betroffenen im Sinne eines absoluten Herrschaftsrechts zugeordnet werden. Eine Nutzung und Verarbeitung muss also – unter Beachtung der in der DSGVO niedergelegten Sicherungsmaßnahmen (Pseudonymisierung, Transparenz, Widerspruchsrecht, „Privacy by Design") – weiterhin einwilligungslos möglich bleiben, soll Datenschutz seinen Zweck erfüllen und die Data Economy in der EU Erfolg haben.

Nutzungsdaten sind Abbild der sozialen Realität

3. GESETZLICH ERLAUBTE DATENVERARBEITUNGEN

3.1 Vertragserfüllung und andere rechtliche Verpflichtungen

Wie im bisherigen Datenschutzrecht gilt auch bei der DSGVO, dass die Verarbeitung von pDaten dann erlaubt ist, wenn ein Unternehmen diese Daten zum Zwecke der Erfüllung von Verträgen oder wegen anderweitiger, vom Gesetz benannter, rechtlicher Verpflichtungen nutzen können muss. Neben der in Art. 6 Abs. I a) DSGVO genannten Einwilligung listen Art. 6 Abs. I b)–e) abschließende Beispiele hierfür auf.

Es ist zunächst klarstellend festzuhalten, dass die gesetzlichen Erlaubnisse neben der Einwilligung gleichwertige Rechtsgrundlagen für die Verarbeitung von pDaten darstellen. Eine Hierarchie exisitert also nicht.

Datennutzung für Vertragszwecke

Die wohl wichtigste Erlaubnis neben den berechtigten Interessen und vor allem neben der Einwilligung wird die Erlaubnis zur Datennutzung für Vertragszwecke sein. Sie ist grundsätzlich weit zu verstehen. Hierunter fallen auch Handlungen zur Vertragsanbahnung.

Welche Datenverarbeitungen – vor allem im digitalen Umfeld – notwendig für die Anbahnung, Durchführung oder Beendigung von Verträgen sind und daher unter diese gesetzliche Erlaubnis fallen, wird in Zukunft herauszuarbeiten sein. Die Rechtsgrundlage Vertrag ist insbesondere relevant vor dem Hintergrund des nur bei der Einwilligung geltenden Kopplungsverbotes.

3 vgl. BVerfG Urt. v. 15.12.1983, I BvR 209/83, I BvR 269/83, I BvR 362/83, I BvR 420/83, I BvR 440/83, I BvR 484/83

Datennutzung u.U. auch für Werbezwecke erlaubt, soweit es im Vertrag um Werbung geht

Wichtig für die Einordnung bei werbenden Maßnahmen könnte hier auch die bisherige Auffassung des Düsseldorfer Kreises werden. In ihren „Anwendungshinweisen zur Erhebung, Verarbeitung und Speicherung von personenbezogen Daten zu werblichen Zwecken" hatte die Ad-hoc-Arbeitsgruppe im Jahre 2013 klargestellt, dass pDaten unter bestimmten Umständen auch ohne Einwilligung für Werbezwecke verarbeitet werden dürfen. Danach kann die Verwendung von pDaten zu Werbezwecken im Anwendungsbereich des BDSG auch auf die Erlaubnis zur Vertragserfüllung gestützt werden (§28 Abs. 1 S.1 Nr.1-3 BDSG). Die Vorschriften bilden eine hinreichende Grundlage für die werbliche Ansprache, wenn diese Gegenstand des Schuldverhältnisses selbst ist. Das kann z. B. bei Preisausschreiben, Gewinnspielen sowie Katalog- und Prospektanforderungen der Fall sein.[4] Die Datenschutzaufsichtsbehörden werden sich unter Geltung der DSGVO künftig europaweit einheitlich positionieren müssen. Da es häufig aber auch nach 2018 um eine nationale Sichtweise gehen wird, lohnt sich eine Abklärung dieser Frage mit der zuständigen Landesdatenschutzbehörde.

In Art. 22 Abs. 2 a) DSGVO findet sich zudem eine Ausnahme für auf automatisierter Basis getroffene Entscheidungen, soweit diese für den Abschluss oder die Erfüllung eines Vertrages verantwortlich sind. Dies betrifft beispielsweise den Bereich der Überprüfung der Kreditwürdigkeit einer Person. Allerdings muss der Verantwortliche in solchen Fällen angemessene Maßnahmen treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren. Dazu gehört mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung, Art. 22 Abs. 3 DSGVO. Außerdem dürfen nicht ohne Weiteres besondere Kategorien von pDaten gemäß Art. 9 Abs. 1 DSGVO für eine solche Entscheidung genutzt werden (z. B. Gesundheitsdaten etc.).

Rechtliche Verpflichtung

In Art. 6 Abs. 1 c) DSGVO ist als Grundlage auch eine „rechtliche Verpflichtung" der verantwortlichen Stelle als Erlaubnisgrund benannt. Hier geht es um erforderliche Verarbeitungen zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt, die ihre Grundlage im Unionsrecht oder im Recht eines Mitgliedstaats haben. Wichtig ist hier, dass mehrere Verarbeitungsvorgänge auch nur auf eine einzige Gesetzesgrundlage gestützt werden können.

Eine Rechtsgrundlage kann verschiedene Verarbeitungen rechtfertigen

4 https://www.lda.bayern.de/media/ah_werbung.pdf

3.2 Berechtigte Interessen

3.2.1 Bedeutung und systematische Stellung

Eine der praktisch relevantesten gesetzlichen Erlaubnisse stellt die in Art. 6 Abs. 1 f) DSGVO getroffene Regelung zur Datenverarbeitung auf Basis berechtigter Interessen dar.[5]

> **Art. 6 Abs. 1 f)**
> (…) die Verarbeitung ist **zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich,** sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. (…)

Art. 6 Abs. 1 f) DSGVO wohl wichtigste Regelung für die Digitalwirtschaft

Art. 6 Abs. 1 f) DSGVO legitimiert Datenverarbeitungsvorgänge, auch wenn keine Einwilligung oder anderweitige gesetzliche Erlaubnis vorliegt. Obwohl der Begriff an sich nicht neu ist, ist die Einführung einer zentralen Regelung, die an berechtigte Interessen anknüpft und eine Interessenabwägung zwischen den Beteiligten vorsieht, eine maßgebliche Neuerung. Die Formulierung in Art. 6 Abs. 1 f) DSGVO ist dabei so offen gehalten, dass für die Beurteilung der rechtlichen Zulässigkeit tatsächlich in jedem Fall eine Einzelfallabwägung erforderlich ist. Dies schafft zwar Rechtsunsicherheit, da nicht absehbar ist, wie Behörden und Gerichte einzelne Sachverhalte in Zukunft beurteilen werden, ermöglicht aber auch eine flexible Anpassung der datenschutzrechtlichen Standards an technische und gesellschaftliche Entwicklungen. Anhaltspunkte zur Auslegung gibt dabei auch Erwägungsgrund 47 DSGVO.

5 vgl. BeckOK DatenSR/Albers DS-GVO Art. 6 Rn. 45 und Albrecht CR 2016, 88 (91)

Erwägungsgrund 47 DSGVO:
Die Rechtmäßigkeit der Verarbeitung kann durch die berechtigten Interessen eines Verantwortlichen, auch eines Verantwortlichen, dem die personenbezogenen Daten offengelegt werden dürfen, oder eines Dritten begründet sein, sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen; dabei sind die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen. Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht. Auf jeden Fall wäre das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Insbesondere dann, wenn pDaten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen. Da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen, sollte diese Rechtsgrundlage nicht für Verarbeitungen durch Behörden gelten, die diese in Erfüllung ihrer Aufgaben vornehmen. Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang stellt ebenfalls ein berechtigtes Interesse des jeweiligen Verantwortlichen dar. Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.

3.2.2 Tatbestandsmerkmale

Bei einer Analyse der Tatbestandsmerkmale ergibt sich Folgendes:

• „Interessen“

Der Begriff „Interessen“ dürfte sehr weit auszulegen sein und „alle nicht schon per se rechtswidrigen Vorhaben“ erfassen (z. B. Interessen im Zusammenhang mit Verträgen oder aber auch Auswertung und Sammeln von Daten für Werbezwecke)[6].

• „berechtigt“ bzw. „Berechtigung“ und „Erforderlichkeit“

Online-Werbung ist Direktwerbung

Wann ein Interesse „berechtigt“ im Sinne von Art. 6 Abs. 1 f) DSGVO ist, ist eine Wertungsfrage[7], bei der man stets den Einzelfall betrachten muss. Orientierung gibt hier Erwägungsgrund 47 DSGVO. Hier sind z. B. eine Datenverarbeitung innerhalb von Kundenbeziehungen oder der Bereich der „Direktwerbung“ (allerdings ohne weitere Definition) erwähnt. Wenn man „Direktwerbung“ als E-Mail-Marketing oder Postwerbung versteht, liegt es nahe, auch die Online-Werbung auf Websites als berechtigtes Interesse anzusehen. Schließlich ist der Eingriff für den Betroffenen hier deutlich geringer.

Hinzu kommt, dass der Begriff der „berechtigten Interessen“ nicht neu im Datenschutzrecht ist, sondern sich bereits in § 28 Abs. 1 Nr. 2 ff. BDSG findet. Er wurde über Art. 7 Abs. 1 f) der Datenschutzrichtlinie von 1995 im BDSG umgesetzt. Letzteres findet zwar bald keine Anwendung mehr, aber es spricht doch vieles für eine Kontinuität in Wertungsfragen. Hierüber wären z. B. die Verarbeitung für eigene Geschäftstätigkeiten, Teile der Werbung sowie Markt- und Meinungsforschung unter Umständen weiterhin legitimiert.

Ferner muss die Verarbeitung zur Wahrung des berechtigten Interesses erforderlich sein. Ganz unabhängig von der anschließenden Abwägung mit den Rechten der betroffenen Person, dürfte dies im Bereich datenbasierter Online-Werbung zu bejahen sein, da die Verarbeitung von Daten deren immanenter Bestandteil ist.

• Entgegenstehende „Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person“

6 vgl. Härting, Datenschutz-Grundverordnung, Das neue Datenschutzrecht in der betrieblichen Praxis, 1. Aufl. 2016, Rn. 431; für eine weite Auslegung auch Frenzel in Paal/Pauly, Datenschutz-Grundverordnung 1. Auflage 2017, Rn. 28

7 vgl. Härting – Datenschutzgrundverordnung Rn. 433

Art. 6 Abs. 1 f) erkennt neben den berechtigten Interessen des Datenverarbeiters auch entgegenstehende Interessen des Betroffenen an. Dies ist insbesondere das Recht auf informationelle Selbstbestimmung. Einen besonderen Schutz genießen ferner Kinder.

• Abwägung

Im Rahmen von Art. 6 Abs. 1 f) DSGVO muss von der verantwortlichen Stelle eine Interessenabwägung vorgenommen werden.

Vernünftige Erwartungen des Nutzers

Anhaltspunkte gibt hier erneut Erwägungsgrund 47 DSGVO. Dort wird auf den Begriff der „vernünftigen Erwartungen" abgestellt, d. h. also, ob ein Betroffener in der jeweiligen Situation damit rechnen konnte oder musste, dass bestimmte Daten erhoben werden oder nicht. Heutzutage funktionieren nahezu keine Angebote mehr ohne die Verarbeitung von Daten, sei es z. B. eine Analyse über Google Analytics oder eine Messung über die IVW. Auch OBA und Retargeting sind üblich. Es handelt sich dabei durchgehend um bekannte, transparente und auch etablierte Techniken. Sie werden in Datenschutzerklärungen oder via OBA-Button erläutert und können vom Nutzer gesteuert werden (z. B. durch Opt-out). Daher wird ein Nutzer solche Maßnahmen wohl erwarten, da niemand mehr davon ausgeht, sich vollkommen anonym im Netz zu bewegen. Nutzer dürften wissen, dass Online-Kennungen genutzt, Verbindungen zu Facebook aufgebaut, Google-Suchanfragen analysiert oder dass angesehene Produkte in anderem Zusammenhang erneut gezeigt werden.[8] Wenn ein Betreiber dies transparent darstellt – z. B. durch Hinweise zur nutzerbezogenen Werbung inkl. Opt-out-Funktionen, durch OBA-Buttons oder aber auch ergänzend durch Statusleisten zu Cookies, wird sich dies voraussichtlich auch mit den berechtigten Erwartungen decken. Die Diskussion um das Thema Online-Datenschutz ist inzwischen so allgegenwärtig, dass kaum vorstellbar ist, dass der Nutzer hiervon vollkommen „überrumpelt" wird. Das gilt nicht nur für klassische Websites, sondern auch für Apps oder aber die Nutzung von Smart-TVs. Verbindet ein Nutzer ein Smart-TV-Gerät z. B. aktiv mit dem Internet (durch Einstecken eines Kabels oder Einloggen in ein WLAN), so tut er das nach lebensnaher Auslegung, um Internetangebote zu nutzen, und dürfte davon ausgehen, dass dann auch eine Datenübertragung stattfinden wird, selbst wenn diese parallel oder überlappend mit dem TV-Signal erfolgt. Dies ist auch insofern interessengerecht, da TV-Geräte ohne Probleme auch ohne eine Verbindung mit dem Internet nutzbar sind.

Pseudonymisierung, Transparenz und Widerspruchsrecht schützen Betroffeneninteressen

Es dürften hier auch die schützenswerten Interessen des Nutzers nicht entgegenstehen, da die Daten in den allermeisten Fällen nur pseudonymisiert verarbeitet werden, was die Identifizierbarkeit des Nutzers erschwert und

8 vgl. auch Härting, Datenschutzgrundverordnung Rn. 437

seine Rechte stärkt. Pseudonymisierung hat sicher nicht mehr dieselbe Bedeutung wie nach dem BDSG und TMG, ihr Einsatz könnte aber ausreichend sein, um hier bei der Abwägung zwischen kommerziellen Interessen eines Anbieters und dem Interesse des Nutzers den Ausschlag für den Anbieter zu geben – eben weil die Nachteile für den Nutzer entsprechend gering sind.

Besonderheit bei minderjährigen Nutzern

Etwas anderes kann sich natürlich ergeben, wenn der Betroffene einer Datenverarbeitung ein Kind ist. Diese spielen nach der DSGVO eine besondere Rolle. Hinsichtlich der Einzelheiten wird auf die Ausführungen zu Art. 8 verwiesen. Ist der Betroffene ein Kind, kann dies jedoch dazu führen, dass die Abwägung eher zugunsten des Kindes als zugunsten des Verarbeiters der Daten ausgeht.

Schwierigkeiten ergeben sich aber schon dabei, zu ermitteln, ob überhaupt ein Kind Betroffener ist, insbesondere in einem Nutzungsverhältnis ohne Login. Hier ist die Wertung aus Art. 8 Abs. 2 DSGVO heranzuziehen, nach der angemessene Anstrengungen zur Ermittlung des Vorliegens von Einwilligungen unternommen werden müssen (unter der Berücksichtigung der Technik). Da die Technik in einem nicht identifizierten Nutzungsverhältnis nicht weiterhilft, können die Annahmen nur genereller Natur sein. Man wird bei Kinder-Websites annehmen, dass eine Vielzahl von Betroffenen Kinder sind. Dies ist dann in die Abwägung einzustellen. Bei Angeboten ohne eine spezifische Altersgruppe kann diese Annahme jedoch gerade nicht getroffen werden. Einem Betreiber sollte nicht zugemutet werden, stets „auf Verdacht" von Kindern als Nutzern auszugehen. In Fällen, in denen zusätzlich eine Pseudonymisierung von Daten erfolgt, wie es im OBA-Bereich der Fall ist, und Werbung auch nicht auf Kinderinteressen ausgesteuert wird, wären aber auch bei einer falschen Annahme die Rechte des betroffenen Kindes nur sehr gering beeinträchtigt. Daher sollte es für Betreiber von nicht personalisierten Angeboten keine Besonderheiten in der Abwägung geben.

3.2.3 Fazit

Es ist möglich, dass der Einsatz von bisher bekannten Techniken zur Analyse (z. B. Tracking/Analytics) und zur datengetriebenen Werbung (Targeting, Retargeting) sowie die damit zusammenhängende Verarbeitung von Daten auch nach der Datenschutzgrundverordnung auf Basis der Regelung Art. 6 Abs. 1 f) DSGVO weiterhin zulässig sein könnte. Nicht zuletzt verweist die DSGVO auch selbst in Art. 21 Abs. 1 z. B. auf ein Profiling, das auf Art. 6 Abs. 1 f) DSGVO gestützt ist.

Rechtsunsicherheiten können nur durch Gerichte beseitigt werden

Gleichwohl bringen unbestimmte Rechtsbegriffe stets Rechtsunsicherheiten mit sich, die erst in Zukunft durch die Rechtsprechung sowie behördliches Handeln ausgeräumt werden können. Es wird dauern, bis eine gefestigte Rechtsprechung zu diesen Fragen entstanden ist. Ob sich hier eine wirt-

schaftsfreundliche Ansicht durchsetzen wird oder die Gewichtung der Interessen – gerade im Bereich von Online-Werbung – entgegen der geschilderten Ausführungen doch eher zugunsten der betroffenen Person ausgehen wird, bleibt daher offen und abzuwarten. Schwierigkeiten können sich auch aus anderen Zusammenhängen ergeben, wie z.B. durch die Bereitstellung von Widerrufsmöglichkeiten über technische Verfahren „Do-Not-Track" und Browsersettings sowie etwaige verschärfte Regelungen zur Nutzererkennung und Profilbildung nach der kommenden ePrivacy-Verordnung. Zu den Einzelheiten wird auf die Ausführungen zum Tracking und zur Profilbildung verwiesen.

3.3 Zweckänderung

Zweckbestimmung muss weit sein können

Einer der markantesten Grundsätze im Datenschutzrecht betrifft die Beschränkung der Verarbeitung für den vorab definierten Zweck, zu dem pDaten erhoben werden (Grundsatz der Zweckbindung). Der Zweck der Datenverarbeitung muss bereits vorab klar definiert sein. Anderenfalls kann es mit Blick auf bestimmte Datenkategorien sein, dass eine Verarbeitung unzulässig sein kann. Die Verarbeitung von pDaten muss nicht von vornherein auf einen Zweck beschränkt sein. Soweit man sich bereits vorab klar festlegt, können auch mehr als ein Zweck mit der Datenverarbeitung abgedeckt werden. Gerade in Zeiten von Smart-Data-Anwendungen ist ein solch breites Zweckbestimmungsverständnis unabdingbar.

Wie alle anderen Informationen auch (Art. 12 DSGVO) muss dem Betroffenen der Zweck der Datenverarbeitung leicht verständlich mitgeteilt werden. Die Zwecke müssen laut Art. 5 Abs. 1 b) DSGVO vorab eindeutig festgelegt sowie legitim sein.

Eine Weiterverarbeitung, die mit dem ursprünglichen Zweck nicht in Einklang steht, ist unzulässig. Klarstellend hat der Gesetzgeber in Erwägungsgrund 50 DSGVO Zwecke benannt, die in jedem Falle zulässig sein sollen. Diese sind:

- im öffentlichen Interesse liegende Archivzwecke,
- wissenschaftliche oder historische Forschungszwecke oder
- statistische Zwecke nach Art. 89 DSGVO.

Die Beurteilung der Kompatibilität der Zwecke obliegt der verantwortlichen Stelle gemäß Art. 6 Abs. 4 DSGVO. In diese Abwägung einfließen muss dabei beispielsweise, ob es eine irgendwie geartete Verbindung zwischen dem ursprünglichen und dem neuen Zweck geben kann. Daneben wichtig ist die Art der verarbeiteten Daten, der Kontext der Datenerhebung, die Folgen der beabsichtigten Datenverarbeitung und das Vorhandensein angemessener Garantien. Das letzte Kriterium kann ein sehr entscheidendes sein. Der

Pseudonymisierung oder Verschlüsselung als angemessene Garantien

Schutz des informationellen Selbstbestimmungsrechts des Betroffenen ist in Abwägung zu solchen Schutzmaßnahmen zu stellen. Eine Verarbeitung unter Verwendung von Pseudonymisierungs- oder Verschlüsselungstechniken ist eindeutig zugunsten der verantwortlichen Stelle als angemessene Garantie zu werten. Betrachtet man dann noch die Art der Daten (z. B. reine Nutzungsdaten), sollte der „Kompatibilitätstest" positiv sein.

Bei der zweckändernden Datenverarbeitung gilt die Weiterverarbeitung der Daten als von der ursprünglichen Erlaubnis gedeckt. Hat die verantwortliche Stelle also z.B. die Erlaubnis zur Datenverarbeitung des Betroffenen, so kann die Weiterverarbeitung zu einem kompatiblen Zweck (z. B. auch unter Nutzung von Pseudonymisierungs- oder Verschlüsselungstechniken) auf diesen Rechtsgrund gestützt werden.

Konkretisierung im BDSG-neu

Im BDSG-neu ist die Frage der zweckändernden Datenverarbeitung in § 24 geregelt. Anders als noch in den Vor-Entwürfen enthält die letzte – vom Bundestag beschlossene – Version keine eigenen Ausnahmen mehr, sondern nur noch klarstellende Ausformungen des Kompatibilitätsgedankens der DSGVO. Als mit dem ursprünglichen Zweck vereinbar ist eine Weiterverarbeitung, wenn:

- sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist oder

- sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.

4. EINWILLIGUNG IN DIE VERARBEITUNG PERSONENBEZOGENER DATEN

Einwilligung als gängigstes Rechtfertigungsmittel für die Datenverarbeitung

Auch mit der Datenschutzgrundverordnung wird das Instrument der Einwilligung nicht an Bedeutung einbüßen und bleibt damit im Fokus der Digitalen Wirtschaft. Nach wie vor wird eine Einwilligung der betroffenen Person für die meisten Unternehmen die gängigste (wenn auch nicht die einzige) Möglichkeit darstellen, pDaten rechtskonform zu verarbeiten.

4.1 Inhaltliche Anforderungen an eine Einwilligung

Die DSGVO definiert die Einwilligung in Art. 4 Nr. 11 DSGVO als jede für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen

bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung ihrer personenbezogenen Daten einverstanden ist. Hiermit stellt der europäische Gesetzgeber eine Vielzahl unterschiedlicher Anforderungen an eine Einwilligung, damit diese auch wirksam erteilt wird.

4.2 Bestimmtheit

Kriterien für die Wirksamkeit der Einwilligung

Die Einwilligung muss sich auf einen bestimmten Anwendungsfall und einen bestimmten Verarbeitungszweck beziehen und diese auch konkret in der Datennutzungserklärung benennen. Es ist nicht möglich, eine abstrakte Pauschaleinwilligung einzuholen und diese im Nachhinein auf nicht konkret benannte Anwendungsfälle anzuwenden. Generell gilt: Je abstrakter die Beschreibung, desto angreifbarer ist die Einwilligung.

4.3 Freiwilligkeit

Die Person, welche die Einwilligung abgibt, muss nach Erwägungsgrund 42 DSGVO eine echte oder freie Wahl haben und somit in der Lage sein, die Einwilligung zurückzuziehen oder zu verweigern, ohne Nachteile dadurch zu erleiden. Die DSGVO verlangt hier eine Abwägungsentscheidung der betroffenen Person.

In Erwägungsgrund 43 führt der europäische Gesetzgeber auch gleich mehrere Fälle auf, in denen es an der Freiwilligkeit einer Einwilligung fehlen wird. So gilt eine Einwilligung dann nicht als freiwillig erteilt, wenn für unterschiedliche Datenverarbeitungsvorgänge nicht auch eine gesonderte Einwilligung erteilt wurde, obwohl dies die Komplexität des Einzelfalles gebietet. Auch ein klares Ungleichgewicht zwischen der betroffenen Person und dem Verantwortlichen kann dazu führen, dass es an dem Erfordernis der Freiwilligkeit fehlt.

4.4 Informiertheit

Die Abgabe der Einwilligung muss so beschaffen sein, dass die einwilligende Person vollumfänglich darüber informiert wird, dass sie eine Einwilligung abgibt und welchen Umfang die Einwilligung hat. Dazu gehört insbesondere auch ein Hinweis darauf, dass die Einwilligung widerrufen werden kann, jedoch mit Wirkung erst ab Widerruf.

4.5 Unmissverständlichkeit

Checkbox bei elektronischer Einwilligung

Die Einwilligung und alle im Rahmen des Einwilligungsprozesses kommunizierten Informationen (siehe auch Informiertheit) müssen in einer verständlichen Sprache übermittelt und leicht zugänglich sein. Alle notwendigen Informationen müssen für die einwilligende Person unmissverständlich sein. Laut der DSGVO ist dabei jede Form von Erklärung oder Handlung wirksam, aus der sich eindeutig ergibt, dass die Person mit der Verarbeitung der Daten einverstanden ist. Beispielhaft wird in Erwägungsgrund 32 DSGVO das Anklicken eines Kästchens beim Besuch einer Internetseite, die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder jede andere Erklärung oder Verhaltensweise genannt, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert.

Sicherlich legt diese Aufzählung den Schluss nahe, dass künftig nur noch ausdrücklich erteilte Einwilligungen nach dem „Opt-in-Prinzip“ möglich sind. Auch weil Erwägungsgrund 32 DSGVO ausdrücklich darauf hinweist, dass ein Stillschweigen auf ein bereits angekreuztes Kästchen oder die Untätigkeit der betroffenen Person keine Einwilligung darstellt.

XI. AUTOREN

Prof. Dr. Christoph Bauer ist Gründer und Geschäftsführer von ePrivacy GmbH, einer Firma, die im Bereich Datenschutz Beratungen und Zertifizierungen für rund 200 Unternehmen anbietet. ePrivacy bietet u.a. das Datenschutz-Siegel ePrivacyseal und die OBA-Zertifizierung an. Prof. Dr. Christoph Bauer ist akkreditierter Gutachter beim Landesdatenschutzzentrum Kiel (ULD) für Datenschutz-Siegel sowie akkreditierter Auditor für ISO 27001/ Management von Informationssicherheit und lehrt als Professor an der HSBA (Hamburg School of Business Administration).

Dr. Stefan Drewes ist ein ausgewiesener Spezialist im Datenschutzrecht in der Kanzlei Pauly & Partner. Als Fachanwalt für gewerblichen Rechtsschutz liegt sein Schwerpunkt im Zusammenspiel zwischen den datenschutz- und wettbewerbsrechtlichen Anforderungen im Bereich des Dialogmarketings/ Online-Marketings. Er ist zudem externer betrieblicher Datenschutzbeauftragter bei verschiedenen Unternehmen und Geschäftsführer der DPA Drewes Privacy Advice GmbH sowie der ADCERT Privacy Audit GmbH.

Dr. Frank Eickmeier ist Rechtsanwalt in der Hamburger IT/IP-Kanzlei Unverzagt von Have. Er ist insbesondere im Bereich des Rechts der Neuen Medien tätig und berät hier mit seinem Team namhafte Agenturen, Online- und Mobile-Vermarkter, Targeting-Anbieter, Advertiser und Publisher bei den klassischen Fragstellungen in der Socialmedia-, Online- und Mobile-Welt. Dr. Frank Eickmeier ist darüber hinaus Mitgründer der Consulting Gesellschaft ePrivacy GmbH und akkreditierter Gutachter beim ULD (Unabhängiges Landeszentrum für Datenschutz).

Dr. Stefan Hanloser ist Vice President Data Protection Law bei der ProSiebenSat.1 Media SE und verantwortet aus der Konzernzentrale heraus die gruppenweite datenschutzrechtliche Rechtsberatung und die Datenschutz-Governance der ProSiebenSat.1-Gruppe.

Thomas Köbrich ist Rechtsanwalt und Legal Counsel der artegic AG und berät in seiner täglichen Arbeit vornehmlich auf dem Gebiet des Urheber- und Datenschutzrechts. Er ist Mitglied in der Deutschen Gesellschaft für Recht und Informatik e.V. und im Arbeitskreis EDV und Recht e.V. und Lehrbeauftragter an der Hochschule Fresenius.

Dr. Stefan Krüger ist Rechtsanwalt und Partner mit den Schwerpunkten Digital Law, IP/IT und Datenschutz bei EY Law in Eschborn/Frankfurt a. M. (bei Redaktionsschluss Partner bei King & Wood Mallesons).

Andreas Kühner ist Head of Technical Application & Media Management, United Internet Media GmbH. Nach erfolgreichem Abschluss zum Diplom-Wirtschaftsingenieur an der Universität Karlsruhe (TH) im Jahre 2006 stieg Andreas Kühner in das Online-Werbegeschäft ein. Bei der United Internet Media GmbH verantwortet er das technische Digitalmarketing. Darüber hinaus leitet der Mediatechnologie- und Admanagementexperte die Unit Adtechnology des OVKs und engagiert sich im BVDW unter anderem im Ressort Data Economy.

Svenja Maucher ist Rechtsanwältin und Partnerin bei TaylorWessing in Frankfurt und Mitglied der Practice Area Technology, Media & Telecoms. Ihr Beratungsfokus liegt im Bereich der Games-Industrie sowie der digitalen Medien und sie blickt auf eine jahrelange, erfolgreiche Zusammenarbeit mit den wichtigsten Playern der Entertainment- und Medienbranche zurück. Sie berät zu IT-rechtlichen Fragestellungen und sämtlichen Fragen des Datenschutzes. Aktuell begleitet Svenja Maucher zahlreiche Unternehmen (globale Marktführer genauso wie Start-up-Unternehmen) bei der Implementierung der DSGVO.

Michael Neuber ist Rechtsanwalt und berät als Justiziar/Leiter Recht und Regulierung den Bundesverband Digitale Wirtschaft (BVDW) e.V. und dessen Mitglieder in Rechtsfragen vor allem in den Bereichen IT-, Datenschutz-, Urheber- und Medienrecht. Neben dem Ressort Recht unterstützt er außerdem maßgeblich die Arbeit des Ressorts Digitalpolitik. Seit 2009 ist er Lehrbeauftragter an der Hochschule für Wirtschaft und Recht (HWR) sowie an der German open Business School (GoBS) Hochschule für Wirtschaft und Verwaltung.

Stefan Peintinger, LL.M. (Georgetown), ist Rechtsanwalt und Associate in der Fachgruppe IT-Recht & Digital Business bei SKW Schwarz in München (bei Redaktionsschluss Associate bei King & Wood Mallesons).

Christian Pfeiffer, ist Datenschutz-Beauftragter einer Berliner Firma für Targeting-Technologie, die mehrfach mit Datenschutz-Gütesiegeln ausgezeichnet wurde.

Timo Wilken war fünfeinhalb Jahre betrieblicher Datenschutzbeauftragter für KANTAR (vormals: TNS Infratest) in Deutschland und ist derzeit als Data Protection & Security Consultant bei Telefónica NEXT tätig.

Christoph Zippel ist Rechtsanwalt (Syndikusrechtsanwalt) und Ressortleiter Business & Legal Affairs bei der Mediengruppe RTL Deutschland. Seit 2004 ist er in der Rechtsabteilung bei RTL tätig. Seine Spezialisierung bezieht sich auf Datenschutz, digitale Vermarktung und IT-Recht.

XII. STICHWORTVERZEICHNIS

XIII. AUSGEWÄHLTE URTEILE

Gericht	Entscheidung/Datum/Aktenzeichen	Thema
OVG Münster	Beschluss v. 22.06.2017, Az.: 13 B 238/17	**Vorratsdatenspeicherung**
BGH	Urteil v. 16.05.2017, Az.: VI ZR 135/13	**Personenbezug von IP-Adressen**
VG Hamburg	Beschluss v. 24.04.2017, Az.: 13 E 5912/16	**Verwendung von WhatsApp-Daten**
BGH	Urteil v. 14.03.2017, Az.: VI ZR 721/15	**Wirksamkeit der Einwilligung**
LG Düsseldorf	Beschluss v. 19.01.2017, Az.: I-20 U 40/16	(Vorlage an EuGH)	**Verantwortliche Stelle bei Plug-ins**
EuGH	Urteil v. 19.10.2016, Az.: C-582/14	**Personenbezug von IP-Adressen**
EuGH	Urteil v. 28.07.2016, Az.: C-191/15	**Anwendbares Datenschutzrecht/ Rechtswahl**
LG Frankfurt	Urteil v. 10.06.2016, Az.: 2-03 O 364/15	**AGB bei Smart-TV**
LG Düsseldorf	Urteil v. 09.03.2016, Az.: 12 O 151/15	**Like-Button**
BVwG (Vorlage an EuGH)	Beschluss v. 25.02.2016, Az.: 1 C 28/14	**Verantwortlichkeit und Auftragsdatenverarbeitung**
LG Berlin	Urteil v. 04.02.2016, Az.: 52 O 394/15	**Datenschutzerklärung beim Online-Kontaktformular**
EuGH	Urteil v. 06.10.2015, Az.: C-362/14	**Safe Harbor**
EuGH	Urteil v. 01.10.2015, Az.: C-230/14	**Weltimmo/Anwendung des nationalen Datenschutzrechts**
EuGH	Urteil v. 13.05.2014, Az.: C-131/12	**Google Spain/Recht auf Vergessenwerden**
BVerfG	Urteil v. 27.02.2008, Az.: 1 BvR 370/07, 595/07	**Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**
BVerfG	Urteil v. 15.12.1983, Az.: 1 BvR 209/83, 484/83, 420/83, 362/83, 269/83, 440/83	**Volkszählung, informationelle Selbstbestimmung**

BUNDESVERBAND DIGITALE WIRTSCHAFT (BVDW) E.V.

Der Bundesverband Digitale Wirtschaft (BVDW) e.V. ist die zentrale Interessenvertretung für Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Mit Mitgliedsunternehmen aus unterschiedlichsten Segmenten der Internetindustrie ist der BVDW interdisziplinär verankert und hat damit einen ganzheitlichen Blick auf die Themen der Digitalen Wirtschaft.

Der BVDW hat es sich zur Aufgabe gemacht, Effizienz und Nutzen digitaler Angebote – Inhalte, Dienste und Technologien – transparent zu machen und so deren Einsatz in der Gesamtwirtschaft, Gesellschaft und Administration zu fördern. Außerdem ist der Verband kompetenter Ansprechpartner zu aktuellen Themen und Entwicklungen der Digitalbranche in Deutschland und liefert mit Zahlen, Daten und Fakten wichtige Orientierung zu einem der zentralen Zukunftsfelder der deutschen Wirtschaft.

Im ständigen Dialog mit Politik, Öffentlichkeit und anderen, nationalen und internationalen Interessengruppen unterstützt der BVDW ergebnisorientiert, praxisnah und effektiv die dynamische Entwicklung der Branche. Fußend auf den Säulen Marktentwicklung, Marktaufklärung und Marktregulierung bündelt der BVDW führendes Digital-Know-how, um eine positive Entwicklung der führenden Wachstumsbranche der deutschen Wirtschaft nachhaltig mitzugestalten.

Gleichzeitig sorgt der BVDW als Zentralorgan der Digitalen Wirtschaft mit Standards und verbindlichen Richtlinien bei Branchenakteuren für Markttransparenz und Angebotsgüte sowohl für die Nutzerseite wie für die Öffentlichkeit.

Wir sind das Netz.

www.bvdw.org

RESSORT RECHT IM BVDW

Aufgabe des themenübergreifenden Ressorts Recht ist es, die einzelnen Gremien des BVDW sowie die Mitgliedsunternehmen in Projekten im Zusammenhang mit der Arbeit im BVDW rechtlich zu beraten und bei der Anwendung des geltenden Rechts zu unterstützen.

Ziel ist es, als Expertengremium für Mitglieder sowie für die Branche zu fungieren. Dabei können die Mitglieder des Ressorts – Rechtsanwälte, die unter anderem im Recht der Neuen Medien tätig sind – auf langjährige Erfahrung und eine fundierte berufliche Praxis zurückgreifen.

http://www.bvdw.org/themen/recht.

EU-Datenschutzgrundverordnung 2018

Erscheinungsort und -datum
Düsseldorf, September 2017

Herausgeber
Bundesverband Digitale Wirtschaft (BVDW) e.V.
Berliner Allee 57
40212 Düsseldorf
Telefon 0211 600456-0
Telefax 0211 600456-33
E-Mail info@bvdw.org
Internet www.bvdw.org

Geschäftsführer
Marco Junk

Präsident
Matthias Wahl

Vizepräsidenten
Thomas Duhr
Thorben Fasching
Achim Himmelreich
Stephan Noller
Frederike Probert
Marco Zingler

Kontakt
Michael Neuber
Rechtsanwalt
Justiziar/ Leiter Recht und Regulierung
neuber@bvdw.org

Vereinsregisternummer
Vereinsregister Düsseldorf VR 8358

1. Auflage

Titelmotiv
iStock/artJazz

Herausgeber

BVDW
Wir sind das Netz

§ RECHT
RESSORT IM BVDW

Bundesverband Digitale Wirtschaft
(BVDW) e.V.
Berliner Allee 57
40212 Düsseldorf
Telefon 0211 600456-0
Telefax 0211 600456-33
E-Mail info@bvdw.org
Internet www.bvdw.org