Heckmann

juris PraxisKommentar

Internetrecht

Telemediengesetz
E-Commerce
E-Government

LESEPROBE
6. Auflage 2019 – Auszug aus Kapitel 9 Datenschutz

Online-Kommentar inklusive E-Book

juris PraxisKommentar Internetrecht

Vorwort zur 6. Auflage des juris PraxisKommentars Internetrecht

Als dieser Kommentar vor zwölf Jahren auf den Markt kam, war Internetrecht in weiten Kreisen der Rechtswissenschaft und Rechtspraxis noch erläuterungs- und in einem gewissen Sinn auch rechtfertigungsbedürftig.

Zuweilen wurde auch bestritten, dass einem Internetrecht überhaupt eine eigene Bedeutung zukommt. 2019 ist dies anders: Digitalisierung ist auch aus juristischem Blickwinkel ein alltägliches Phänomen, Ausgangspunkt politischer und ethischer Diskussionen und zunehmend auch Gegenstand der Juristenausbildung. Hier werden hochaktuelle und zum Teil auch brisante Themen aufgegriffen, die Eingang in die parlamentarische Arbeit finden und umgekehrt ihren Ausgangspunkt nehmen in technologischen Innovationen, der Rechts- und Vertragspraxis und natürlich der Rechtsprechung. Eine überragende Rolle spielen dabei auch die Entwicklungen auf europäischer Ebene, Initiativen der Europäischen Kommission, Normgebung des Europäischen Parlaments und die Entscheidungen des Europäischen Gerichtshofs.

All dies fließt natürlich auch in die Neuauflage dieses Kommentars und die anschließenden regelmäßigen Updates ein. Die nunmehr vorliegende 6. Auflage berücksichtigt Literatur, Rechtsprechung und Gesetzgebung bis Anfang 2019 und setzt in vielen Kapiteln auch neue Akzente.

Ein so umfassendes und vielfältiges Werk kann nur als Team bewältigt werden. Ein Team, dem ich von Herzen danken möchte für großartiges Engagement und leidenschaftliche Auseinandersetzung mit den vielen rechtlichen, technischen, gesellschaftlichen und wirtschaftlichen Fragestellungen. Zum bewährten Team der Vorauflage sind neu hinzugekommen als Autoren Dr. Anne Paschke, Christina-Maria Leeb und Martin Scheurer. Nachdem Frau Dr. Paschke schon bei den Vorauflagen hervorragend mitgearbeitet hat, freue ich mich sehr, dass sie ihre Spezialbereiche E-Commerce und Urheberrecht als (Co-)Autorin übernommen hat. Zusätzlich hat sie auch bei dieser Auflage wiederum in sehr bewährter Weise die Gesamtkoordination übernommen; dafür danke ich sehr. Frau Leeb ist neue Co-Autorin im Kapitel E-Justice, was mich auch deshalb freut, weil sie sich in ihrer Dissertation zu Legal Tech als Spezialistin in diesem Bereich erwiesen hat. Ebenso bin ich dankbar, dass ich das so bedeutsame Kapitel zum Datenschutzrecht, das in seinen Auswirkungen im Prozess der Digitalen Transformation nicht hoch genug eingestuft werden kann, nunmehr mit Herrn Scheurer teilen darf, der sich über seine Dissertation im Datenschutzrecht eine hervorragende Expertise verschafft hat. Darüber hinaus mitgewirkt haben die wissenschaftlichen Mitarbeiterinnen und Mitarbeiter Christoph Halder, Marie Nawrocki, Tobias Schmidt, Thomas Schneck, Amrei Walker sowie Jannik Zerbst. Engagiert haben sich auch die studentischen Hilfskräfte Florian Jurina, Simon Raab, Tobias Springer und Phillip Starke. Ihnen allen herzlichen Dank!

Wie bei allen Vorauflagen hat sich meine liebe Ehefrau Elke Heckmann um die redaktionelle Betreuung der regelmäßigen Online-Updates gekümmert. Dafür sei auch ihr sehr herzlich gedankt.

Ich wünsche Ihnen viel Freude mit der 6. Neuauflage des juris PraxisKommentars Internetrecht.

Passau, im März 2019

Prof. Dr. Dirk Heckmann

juris PraxisKommentar Internetrecht

Bearbeiter

Prof. Dr. Wilfried Bernhardt ..... Kapitel 6
Staatssekretär a. D., Rechtsanwalt, Honorarprofessor Universität Leipzig

Prof. Dr. Frank Braun ..... Kapitel 7
Professor für Staats- und Verwaltungsrecht an der Fachhochschule für Öffentliche Verwaltung des Landes Nordrhein-Westfalen (FHöV NRW), Hagen; Lehrbeauftragter für IT-Recht an der Hochschule für angewandte Wissenschaften Landshut

Prof. Dr. Dirk Heckmann (Hrsg.) ..... Kapitel 1 bis 3, 5, 8 und 9
Mitglied des Bayerischen Verfassungsgerichtshofes; Inhaber des Lehrstuhls für Öffentliches Recht, Sicherheitsrecht und Internetrecht und Leiter der Forschungsstelle für ITRecht und Netzpolitik For..Net an der Universität Passau

Christina-Maria Leeb ..... Kapitel 6
Wissenschaftliche Mitarbeiterin Praxisgruppe IT, IP und Medienrecht, Heussen Rechtsanwaltsgesellschaft, München

Dr. Anne Paschke ..... Kapitel 3, 4
Akademische Rätin a. Z., Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht Prof. Dr. Dirk Heckmann, Universität Passau

Prof. Dr. Jan Dirk Roggenkamp ..... Kapitel 10
Professor für Öffentliches Recht an der Hochschule für Wirtschaft und Recht Berlin

Martin Scheurer ..... Kapitel 9
Wissenschaftlicher Mitarbeiter, Lehrstuhl für Öffentliches Recht, Sicherheitsrecht undInternetrecht Prof. Dr. Dirk Heckmann und Wissenschaftlicher Mitarbeiter, DFG-Graduiertenkolleg 1681/2 „Privatheit und Digitalisierung", Universität Passau

Thomas Stadler ..... Kapitel 10
Rechtsanwalt, Fachanwalt für IT-Recht und Fachanwalt für gewerblichen Rechtsschutz

Bearbeiter der Vorauflage:

Prof. Dr. Louisa Specht ..... Kapitel 3

© 2019 juris GmbH | www.juris.de

Kapitel 9 [Auszug]
Datenschutz

Gliederung

© 2019 juris GmbH | www.juris.de

[...]

© 2019 juris GmbH | www.juris.de

5. Vorgaben zum Einsatz von Cookies

654 Eine **eklatante Verschärfung** gegenüber dem ursprünglichen Entwurf erfuhr Art. 10 ePVO durch das EU-Parlament. Dieser enthält Vorgaben in Bezug auf Offline-Tracking, Messenger und E-Mail-Werbung und vor allem zum Einsatz von Cookies.

655 Cookies, die bereits zur technischen Funktion einer Website, beispielsweise der Warenkorbfunktion, **notwendig** sind, unterfallen aller Voraussicht nach dem Erlaubnistatbestand des Art. 8 Abs. 1 lit. a/c ePVO und sind ohne weitere Einwilligung zulässig (vgl. allgemein zum Einsatz von Cookies auch Rn. 139 ff.).

656 Für **andere Arten** von Cookies sind insbesondere die in Art. 10 Abs. 1 ePVO niedergelegten Regelungen relevant. So muss bereits die Software, welche die elektronische Kommunikation ermöglicht (meistens Webbrowser oder App), Voreinstellung bezüglich der Privatsphäre enthalten, die die Nutzung von Cookies nicht ermöglicht („Privacy by Default" – vgl. dazu Rn. 426 ff.), den Nutzer nach der Installation über diese Einstellungen informieren und ihm die Möglichkeit geben, diese zu ändern[1208] sowie seine Einwilligung[1209] zu der Verwendung von Cookies abzugeben.

657 Darüber hinaus legt Art. 10 ePVO gewisse **technische Standards** fest, die in der Software umgesetzt werden müssen (beispielsweise leichte Zugänglichkeit der Einstellungen, Art. 10 Abs. 1 UAbs. 1 Satz 2 ePVO; Hinweis Art. 10 Abs. 1a UAbs. 1 ePVO; Einwilligungspflicht für einen bestimmten Dienst, Art. 10 Abs. 1b Satz 1 ePVO).

658 Ausdrücklich durch den Parlamentsentwurf in Art. 8 Abs. 1a ePVO aufgenommen wurde ein **striktes Koppelungsverbot**[1210]. Mithin darf die Nutzung des Dienstes grundsätzlich nicht von der Abgabe einer Einwilligung in nicht erforderliche Verarbeitungsprozesse abhängig gemacht werden (vgl. allgemein zum Koppelungsverbot nach den Vorgaben der DSGVO unter Rn. 259 ff.).

B. Ausgewählte Problemkreise des Datenschutzrechts

I. Datenschutz und Cloud-Computing unter besonderer Einbeziehung der Art. 44 ff. DSGVO

1. Allgemeines

659 Cloud-Computing gehört zu den wichtigsten Technologien unserer Zeit. Mittlerweile verwenden 66 Prozent der Unternehmen mit mehr als 20 Arbeitnehmern Cloud-Computing.[1211] Bei Unternehmen mit mehr als 2.000 Beschäftigten greifen bereits 83 Prozent auf Cloud-Computing-Technologien zurück.[1212] Diese Technologie verwirklicht nichts Geringeres als den Traum von allgegenwärtiger Informationstechnologie, die derart einfach zur Verfügung steht wie der elektrische Strom aus der Steckdose.[1213]

[1208] Für eine zudem konsequente Umsetzung des Grundsatzes „Privacy by Design" sprechen sich *Maier/Schaller* aus. *Maier/Schalle* ZD 2017, 373, 375 f.

[1209] *Schleipfer* vertritt die Meinung, dass die von der ePVO geforderten Einwilligungen nicht allein durch die Browsereinstellung erteilt werden können. Vgl. *Schleipfer*, ZD 2017, 460, 465.

[1210] Kritische Sicht auf den Mechanismus des Koppelungsverbots: *Krohm/Müller-Peltzer*, ZD 2017, 511.

[1211] Bitkom, Zwei von drei Unternehmen nutzen Cloud-Computing, 2018. Abrufbar unter: www.bitkom.org/Presse/Presseinformation/Zwei-von-drei-Unternehmen-nutzen-Cloud-Computing.html (zuletzt abgerufen am 28.02.2019).

[1212] Bitkom, Zwei von drei Unternehmen nutzen Cloud-Computing, 2018. Abrufbar unter: www.bitkom.org/Presse/Presseinformation/Zwei-von-drei-Unternehmen-nutzen-Cloud-Computing.html (zuletzt abgerufen am 28.02.2019).

[1213] *Heckmann* in: Hill/Schliesky, Innovationen im und durch Recht, 2010, S. 97.

© 2019 juris GmbH | www.juris.de

660 In der Rechtswissenschaft wird der Themenbereich Cloud-Computing dem IT-Outsourcing zugerechnet. Neben vertrags- und haftungsrechtlichen Fragen stehen datenschutzrechtliche Konfliktlagen, insbesondere die Art. 28, Art. 44 ff. DSGVO, im Vordergrund.

2. Technische Grundlagen des Cloud-Computings

a. Virtualisierungstechnologie

aa. Evolution des Cloud-Computings

661 Seit der Erfindung des Computers hat die elektronische Datenverarbeitung verschiedene Etappen durchlaufen.[1214] Von der Miniaturisierung über die Verbreitung von Personalcomputern in Privathaushalten bildete die Kommerzialisierung des Internet Service Providings einen bedeutsamen Meilenstein.[1215] Ergänzende Dienstleistungen wie E-Mail-Postfächer, Webhosting und Applications as a Service (ASP) gelten daher als Wegbereiter des Geschäftsmodells Cloud-Computing.[1216]

662 Die Entstehung des Cloud-Computings wird bereits heute als gleichermaßen bedeutsam eingeschätzt wie die Erfindung des elektrischen Stroms während der industriellen Revolution.[1217] Nach dieser These wird Cloud-Computing die Abhängigkeit physisch vorgehaltener Informationstechnologie am Standort des Nutzers endgültig aufheben und so einfach beziehbar machen wie bereits heute die Elektrizität aus der Steckdose.[1218]

bb. Virtualisierung

663 Cloud-Computing basiert auf sog. Virtualisierungstechnologien. Physische Hardwareressourcen werden dabei mittels einer Software (sog. Hypervisor oder Virtual Machine Monitor) abstrahiert, in Pools zusammengefasst und zur gemeinsamen Nutzung simuliert bzw. virtualisiert zur Verfügung gestellt.[1219] IT-Ressourcen können somit gleichzeitig von Nutzern verteilt und on demand genutzt werden.

664 Mit der Auflösung der direkten Anbindung von Betriebssystemen und Applikationen an ihre Hardware ermöglicht Virtualisierung daher die einfache, bedarfsorientierte Verteilung von Leistung. Viele Betriebssysteme und folglich zahllose Applikationen können auf diese Weise auf einem einzigen Server anstatt einer Vielzahl von Servern betrieben werden.[1220] Diese Ersparnis von physikalischen Servern senkt Betriebs-, Wartungs- und Anschaffungskosten und ermöglicht flexible Geschäftsmodelle ohne Abhängigkeit von bestimmter Hardware (sog. Vendor Lock-in[1221]).[1222]

[1214] Vgl. hierzu *Maisch*, Informationelle Selbstbestimmung in Netzwerken, S. 101 ff.

[1215] *Maisch*, Informationelle Selbstbestimmung in Netzwerken, 2015, S. 101 ff.

[1216] *Maisch*, Informationelle Selbstbestimmung in Netzwerken, 2015, S. 101 ff.; *Mather/Kumaraswamy/Latif*, Cloud Security and Privacy, 2009, S. 2.

[1217] *Carr*, The Big Switch, 2009, S. 5.

[1218] *Carr*, The Big Switch, 2009, S. 5.

[1219] *Heidrich/Wegener*, MMR 2010, 803 ff.; *Maisch/Seidl*, VBlBW 2012, 7; *Hennrich/Maisch*, AnwZert ITR 15/2011 Anm. 2; *Schuster/Reichl*, CR 2010, 38; *Lehmann/Giedke*, CR 2013, 608, 611.

[1220] *Warren/Davis/Brown*, ICT Futures, 2008, S. 72; *Lehmann/Giedke*, CR 2013, 608, 612.

[1221] Vgl. *Conrad* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 39 Rn. 79; *Metzger/Hoppen*, CR 2017, 625, 626.

[1222] *Warren/Davis/Brown*, ICT Futures, 2008, S. 72; *Kremer/Völkel*, CR 2015, 501.

© 2019 juris GmbH | www.juris.de

b. Definitionsansätze des Cloud-Computings

665 Der Begriff Cloud-Computing bedeutet „Datenverarbeitung in der Wolke".[1223] Die „Wolke" steht metaphorisch für das Internet als weltweites, komplexes Datennetz.[1224] Nach überwiegender Literaturauffassung beschreibt Cloud-Computing keine neue Technologie – obwohl der Medienhype gerade diesen Schluss vermuten ließe[1225] –, sondern steht für eine Kombination von vorhandenen Technologien, Outsourcing-Konzepten sowie Geschäfts- und Abrechnungsmodellen[1226].

666 Im Rahmen des Cloud-Computings werden verschiedene Daten und Programme über eine IT-Infrastruktur von Servern und Software virtuell und verteilt gespeichert.[1227] Darüber hinaus kann über dieses Netzwerk ein Programm ausgeführt werden, so dass eigene Rechnerkapazität gespart wird.[1228] Somit können über Cloud-Computing-Dienste fremde Infrastrukturen virtuell genutzt werden. Die Nutzungsdauer und/oder Intensität bestimmt vielfach über die diesbezügliche Abrechnung.[1229] Allerdings gibt es auch vermeintlich kostenfreie Produkte, bei denen dem Nutzer Werbung angezeigt wird und worüber sich dieses Geschäftsmodell amortisiert.

667 Eine einheitliche, allgemeingültige beziehungsweise gesetzliche **Definition** des Begriffs Cloud-Computing existiert bislang nicht.[1230] Auf Grundlage unterschiedlicher Ansätze hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) allerdings die folgende Begriffsdefinition festgelegt: „Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud-Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z.B. Rechenleistung, Speicherplatz), Plattformen und Software."[1231]

668 Differenziert wird ferner zwischen echtem und unechtem Cloud-Computing.[1232] Die Besonderheit von echtem Cloud-Computing besteht darin, dass die Leistungen nicht von einem Server oder einer „Server-Farm", sondern von einem weltweit verteilten Server-Netz erbracht werden.[1233] Beim unechten Cloud-Computing sind physische IT-Ressourcen auf bestimmte Server oder Rechenzentren eingrenzbar.[1234]

1223 *Weichert*, DuD 2010, 679, 679.

1224 Vgl. *Mather/Kumaraswamy/Latif*, Cloud Security and Privacy, 2009, S. 22.

1225 Vgl. *Heckmann* in: Hill/Schließky, Innovationen im und durch Recht, 2010, S. 97 ff; *Schulz* in: Taeger/Wiebe, Inside the Cloud, 2009, S. 403, 404 f.

1226 *Mather/Kumaraswamy/Latif*, Cloud Security and Privacy, 2009, S. 23; vgl. *Maisch/Seidl*, VBlBW 2012, 7.

1227 *Wiebe* in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, Rn. 60.

1228 *Wiebe* in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, Rn. 60.

1229 *Wiebe* in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, Rn. 60.

1230 BSI, Eckpunktepapier – Sicherheitsempfehlungen für Cloud Computing Anbieter, 2012, S. 14. Abrufbar unter: www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf;jsessionid=377C17C93C9BABD25DB871E815F95864.1_cid351?__blob=publicationFile&v=6 (abgerufen am 28.02.2019).

1231 BSI, Eckpunktepapier – Sicherheitsempfehlungen für Cloud Computing Anbieter, 2012, S. 15.

1232 *Heckmann* in: Hill/Schließky, Innovationen im und durch Recht, 2010, S. 97, 98.

1233 *Heckmann* in: Hill/Schließky, Innovationen im und durch Recht, 2010, S. 97, 98.

1234 *Heckmann* in: Hill/Schließky, Innovationen im und durch Recht, 2010, S. 97, 98.

© 2019 juris GmbH | www.juris.de

c. Service-Ebenen

669 Es gibt nicht „das" Cloud-Computing.[1235] Cloud-Services lassen sich vielmehr in teilweise bekannte Dienstleistungsmodelle untergliedern. Anerkannt ist dabei eine Einteilung in „X-as-a-Service"-Dienste in ein **Drei-Ebenen-Modell** („Cloud Services Delivery Model"[1236]).[1237]

670 Einen ausführlichen Überblick zu den Schutzzielen, Risiken sowie technischen und organisatorischen Maßnahmen der spezifischen Cloud-Modelle gibt der Arbeitskreis Technik und Medien des Düsseldorfer Kreises in seiner Orientierungshilfe Cloud-Computing 2.0.[1238] *Eckhardt* bezeichnet die **Orientierungshilfe Cloud-Computing 2.0** deshalb als „Pflichtlektüre zum Thema Cloud-Computing".[1239] Er weist aber auch zu Recht darauf hin, dass diese Orientierungshilfe keine Gesetzeskraft hat und daher für die Gerichte keine bindende Wirkung entfalten kann.[1240]

aa. Infrastructure-as-a-Service

671 Auf der untersten Ebene („Infrastructure-as-a-Service", „IaaS") der **IT-Ressourcen on-demand** stehen Rechenleistung und Speicherplatz auf virtuellen Servern, standardisierte Netzwerkinfrastruktur-Funktionalitäten und „intelligentes" Systemmanagement-as-a-Service zur Verfügung.[1241] Bekannte Beispiele für „IaaS" sind Amazon EC2[1242] und die Microsoft Windows Azure Platform. „IaaS" richtet sich v.a. an IT-Dienstleister und Cloud-Provider.[1243]

bb. Platform-as-a-Service

672 Auf der mittleren Ebene sind **IT-Dienstleistungen für Entwickler-Plattformen** angesiedelt („Platform-as-a-Service", „PaaS"), mit denen sich Anwendungskomponenten entwickeln und integrieren lassen. Bekannte technische Frameworks sind Force.com, Google Apps Engine und Microsoft Azure Services[1244].[1245]

cc. Software-as-a-Service

673 Auf der obersten Ebene des Cloud-Computings werden Anwendungen bzw. Software bereitgestellt („Software-as-a-Service", „SaaS").[1246] Diese Dienste richten sich an Cloud-Nutzer als Business-, Privat- oder Public Sector-Kunden und werden als **standardisierte Geschäftsanwendungen**

1235 *Hennrich*, CR 2011, 546.

1236 *Mather/Kumaraswamy/Latif*, Cloud Security and Privacy, 2009, S. 17.

1237 Vgl. *Mather/Kumaraswamy/Latif*, Cloud Security and Privacy, 2009, S. 18 f.; Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM), Cloud Computing Leitfaden, 2010, S. 22; *Schneidereit*, Haftung für Datenverlust im Cloud Computing, 2017, S. 50 ff.; vgl. auch *Nägele/Jacobs*, ZUM 2010, 281, 282; *Weichert*, DuD 2010, 679, 679; teilweise wird auch Business Process as a Service (BPaaS) als weitere Ebene hinzugezählt, vgl. *Niemann/Paul*, K&R 2009, 444, 445; ein Fünf-Ebenen-Modell, das zusätzlich zu „IaaS" hardwarebasierte Ebenen (Hardware/Firmware und Software Kernel/Middleware) differenziert, wird von *Schuster/Reichl*, CR 2010, 38, 39 f. skizziert.

1238 Abrufbar unter: www.datenschutz-bayern.de/print/technik/orient/oh_cloud.pdf (zuletzt abgerufen am 28.02.2019).

1239 *Eckhardt*, DuD 2015, 176, 182. Einen guten Überblick zur Orientierungshilfe Cloud Computing 2.0 bietet auch *Bierekoven*, ITRB 2015, 169 ff.

1240 *Eckhardt*, DuD 2015, 176, 182.

1241 Vgl. BITKOM e.V., Cloud Computing Leitfaden, 2010, S. 22; *Nägele/Jacobs*, ZUM 2010, 281, 282; *Schuster/Reichl*, CR 2010, 38, 39.

1242 Vgl. auch *Mather/Kumaraswamy/Latif*, Cloud Security and Privacy, 2009, S. 203 f.

1243 Vgl. BITKOM e.V., Cloud Computing Leitfaden, 2010, S. 24 ff. Abrufbar unter: www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2009/Leitfaden/Leitfaden-Cloud-Computing/090921-BITKOM-Leitfaden-CloudComputing-Web.pdf (abgerufen am 28.02.2019).

1244 Vgl. auch *Mather/Kumaraswamy/Latif*, Cloud Security and Privacy, 2009, S. 206 f.

1245 BITKOM e.V., Cloud Computing Leitfaden, 2010, S. 25 ff.; *Schuster/Reichl*, CR 2010, 38, 39.

1246 Zur vertragsrechtlichen Einordnung und Service Level Agreements, vgl. *Hellwig/Koglin* in: Taeger/Wiebe, Inside the Cloud, 2009, S. 175; *Schuster/Reichl*, CR 2010, 38, 39.

© 2019 juris GmbH | www.juris.de

von einem Cloud-Dienstleister zur Verfügung gestellt.[1247] IT-Ressourcen und Applikationen[1248] werden gebündelt und bedarfsgerecht zur Nutzung bereitgestellt. Nutzer kennen „SaaS“ bspw. in Form von Unified Communications-Diensten[1249], die über das Internet bezogen werden (Voice over IP, Instant Messaging, E-Mail-Services, auch sog. „Communication-as-a-Service“).[1250]

674 Cloud-Dienste ermöglichen den **gemeinsamen Zugriff** auf Dokumente, Kalender, Adressverwaltung, Telefonie, Web- und Videokonferenzsysteme sowie Blogs/Wikis und Foren.[1251] Googles G Suite, Microsoft Online Services, Salesforce und Microsoft Live Services für Privatkunden sind bekannte Beispiele[1252] für „SaaS“ neben bereits allgegenwärtigen Webmail- und Storage-Services.

d. Bereitstellungsmodelle

675 Beim Cloud-Computing werden interne (sog. Private Clouds) und externe (sog. Public Clouds) Verwendungsmodelle („Cloud Deployment Models“) unterschieden.[1253] Die Unterscheidung richtet sich nach der Beziehung der Cloud zu einem Cloud-Kunden.[1254]

aa. Private Cloud

676 Der Begriff Private Clouds beschreibt in sich **geschlossene,** häufig auch unternehmens-, körperschafts- oder einfach standortgebundene Cloud-Computing-Infrastrukturen („On-premise“).[1255] Den Marketingstrategien vieler Cloud-Anbieter zufolge sollen Private Clouds die Vorteile des Cloud-Computings nutzbar machen, ohne dabei datenschutz-, datensicherheits- und IT-sicherheitsrechtliche Fallstricke zu enthalten. Im Grunde handelt es sich hier jedoch um Produkte auf der Basis von Virtualisierungstechnologien, wie sie bereits im Rahmen des „normalen“ IT-Outsourcings fest etabliert sind.[1256]

bb. Public Cloud

677 Public Clouds sind **allgemein zugreifbare Ressourcen,** die von Dritten i.S.v. Art. 4 Nr. 10 DSGVO, dabei insbesondere von großen Cloud-Anbietern wie Microsoft („Windows Azure“[1257]), Amazon, Google (bspw. „Google Docs“) oder Salesforce betrieben werden.[1258]

678 Im Unterschied zur Private Cloud richtet sich das Angebot an eine **Vielzahl von Kunden,** denen jedoch wenig bis kein Gestaltungsspielraum für Kontrollen oder Weisungen verbleibt. Ferner ist den Kunden Transparenz bei datenschutz- oder IT-sicherheitsrelevanten Informationen, bspw. eine Übersicht über die Orte der tatsächlichen Datenverarbeitung, über die Anzahl und Namen

---

1247 BITKOM e.V., Cloud Computing Leitfaden, 2010, S. 23; 27f.

1248 Zur Abgrenzung von ASP vgl. *Söbbing*, MMR Heft 5 2008, XII.

1249 Zum Begriff „Unified Communications“ und rechtlichen Fallstricken vertiefend vgl. *Brisch/Laue*, MMR 2009, 813.

1250 Vgl. BITKOM e.V., Cloud Computing Leitfaden, 2010, S. 28.

1251 Vgl. BITKOM e.V., Cloud Computing Leitfaden, 2010, S. 28.

1252 Vgl. BITKOM e.V., Cloud Computing Leitfaden, 2010, S. 23.

1253 *Mather/Kumaraswamy/Latif*, Cloud Security and Privacy, 2009, S. 22; zu Hybrid Clouds und weiteren Mischformen vgl. *Weichert*, DuD 2010, 679, 680.

1254 *Mather/Kumaraswamy/Latif*, Cloud Security and Privacy, 2009, S. 22.

1255 Vgl. *Rogge*, BB 2015, 1823, 1824; *Münch/Doubrava/Essoh*, DuD 2011, 322.

1256 Näheres zur Möglichkeit von Visualisierung physischer Cloud-Infrastruktur in Form von Virtual Private Clouds, vgl. *Bedner*, Cloud Computing: Technik, Sicherheit und rechtliche Gestaltung, 2012, S. 35.

1257 Vgl. https://azure.microsoft.com/de-de/ (zuletzt abgerufen am 28.02.2018).

1258 *Niemann/Hennrich*, CR 2010, 686, 687; vgl. *Weichert*, DuD 2010, 679, 680.

© 2019 juris GmbH | www.juris.de

der Unterauftragnehmer oder die Gewährleistung von IT-Sicherheitsvorgaben, verwehrt.[1259] Diese Informationspolitik wird mit dem Schutz der Sicherheits- und Geheimhaltungsinteressen gerechtfertigt.[1260]

cc. Community Cloud

679 Als weiteres Bereitstellungsmodell kommt nach der Orientierungshilfe Cloud-Computing 2.0 des Düsseldorfer Kreises zudem die Form der „Community Cloud" in Betracht: Dabei **schließen sich zwei oder mehrere Cloud-Anbieter aus privaten Clouds zusammen,** „um für einen definierten Kundenkreis IT-Dienstleistungen für Cloud-Services zu erbringen".[1261]

dd. Hybrid Cloud

680 Als weitere Modifikation der Bereitstellungsmodelle kommen schließlich noch sog. „Hybrid Clouds" in Betracht. Diese bezeichnen die **Verknüpfung** von Public, Private oder Community Clouds zur Erhöhung der Verfügbarkeit oder zur effizienten Lastverteilung. Dabei bewahren die einzelnen Clouds jedoch ihre Selbstständigkeit.[1262]

e. Cloud-Service-Provider

681 Amazon Inc. gilt als Pionier des Cloud-Computings. Zu einem frühen Zeitpunkt erkannte das US-amerikanische Unternehmen, dass sich über das Internet nicht nur Bücher, sondern auch die IT-Ressourcen der unternehmenseigenen E-Commerce Plattform vertreiben lassen.[1263] Amazon entwickelte einen Applikationsdienst, Amazon Web Services (AWS), der nach dem **Baukastenprinzip** die **Nutzung verschiedener Dienste** enthält.[1264] IT-Infrastruktur im Sinne von Rechenkapazitäten bündelte Amazon in dem Dienst Elastic Compute Cloud (EC2), auf den wohl der Begriff des Cloud-Computings zurückgeht.[1265] Die Abrechnung richtet sich nach gewählter sog. Instanz und Zeitablauf.[1266]

682 Zunehmend treten nicht nur „Global Player" als Cloud-Service-Provider bzw. Cloud-Anbieter auf. Auch kleine- und mittelständische Dienstleister bieten Public- oder Private-Cloud-Dienstleistungen an.

f. Cloud-Nutzer

aa. Öffentlicher Sektor

683 Im öffentlichen Sektor wird Cloud-Computing das Potential zugeschrieben, einen bedeutenden **Paradigmenwechsel** in der IT-Struktur der öffentlichen Verwaltung herbeiführen zu können.[1267] Die IT-Infrastruktur, die zu den wesentlichen Säulen für die Leistungserbringung der öffentlichen Verwaltung zählt, stellt sich – in „Eigenregie" betrieben (Inhouse-IT) – häufig als großer „Kostentreiber" heraus.[1268]

1259 Vgl. *Mather/Kumaraswamy/Latif*, Cloud Security and Privacy, 2009, S. 23.

1260 *Niemann/Hennrich*, CR 2010, 686, 690.

1261 Orientierungshilfe Cloud Computing 2.0, S. 7.

1262 *Strittmatter* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 22 Rn. 7.

1263 *Herrmann*, Computerwoche v. 12.12.2008, www.computerwoche.de/knowledge_center/software_infrastruktur/1881599/ (zuletzt abgerufen am 28.02.2019).

1264 *Maisch*, AnwZert ITR 15/2009 Anm. 4.

1265 T-Systems, White Paper, 2010, Cloud Computing, S. 4.

1266 Amazon EC2, Preisliste, abrufbar unter http://aws.amazon.com/de/ec2/pricing/ (abgerufen am 28.02.2019).

1267 *Maisch/Seidl*, VBlBW 2012, 7.

1268 *Maisch/Seidl*, VBlBW 2012, 7.

© 2019 juris GmbH | www.juris.de

684 Unflexible Rechenstrukturen bringen zu Spitzen- wie zu Nebenzeiten stets dieselbe Leistung. Eine bedarfsgerechte Anpassung von Hard- und Software gelingt nur selten. Ohne IT-Outsourcing lässt sich eine **effiziente Verwaltung** im (kommunalen) E-Government nicht mehr verwirklichen.[1269] Das Schlagwort Cloud-Computing verspricht als neuer Lösungsansatz im IT-Outsourcing nichts Geringeres als die Senkung der Anschaffungs-, Betriebs-, Wartungs- und Personalkosten gegenüber einer Inhouse-IT.[1270]

685 Die erfolgreiche Inbetriebnahme von Cloud-Computing in der öffentlichen Verwaltung setzt aber u.a. voraus, dass die **Auslagerung** von IT-Ressourcen **verfassungs-, organisations-**[1271] **und datenschutzrechtlich zulässig** ist.[1272]

686 **Verfassungsrechtlich** ist zu berücksichtigen, dass öffentliche Aufgaben nicht grenzenlos an privatwirtschaftliche (IT-)Dienstleister ausgelagert werden dürfen.[1273] Gemäß **Art. 33 Abs. 4 GG** ist die Ausübung hoheitsrechtlicher Befugnisse als ständige Aufgabe in der Regel Angehörigen des öffentlichen Dienstes zu übertragen, die in einem öffentlich-rechtlichen Dienst- und Treueverhältnis stehen. Ein nach Art. 33 Abs. 4 GG den Beamten vorbehaltener Aufgabenbereich darf aus dem staatlichen Organisationszusammenhang nicht ausgegliedert werden.[1274] Die Wahrnehmung bloßer technischer Hilfsfunktionen, wie bspw. Auftragsverarbeitung in der Cloud i.S.v. Art. 28 DSGVO, ist jedoch davon ausgenommen und von einer hoheitsrechtlichen eigenverantwortlichen Aufgabenwahrnehmung abzugrenzen.

687 Mit der Auslagerung von IT-Ressourcen und Inhalten wird die IT-Herrschaft der Verwaltung zugunsten der Vorteile des Cloud-Computings aufgegeben.[1275] Dies zieht nicht nur Fragen zur Vereinbarung von Standards und Grundlagen der Zusammenarbeit von Bund und Ländern im Kontext von informationstechnischen Systemen gem. Art. 91c Abs. 1, 2 GG nach sich.[1276] Vielmehr ist zu prüfen, ob mit der IT-Herrschaft auch die Verfahrensherrschaft reduziert wird.[1277] Die **Ökonomisierung** der öffentlichen Verwaltung ist dabei **nicht grenzenlos möglich:** Wird eine organisatorische Ausgestaltung gewählt, die gezielt mit einer gewissen Wahrscheinlichkeit zu einer Missachtung gesetzlicher Vorgaben führt, nur um finanzielle Vorteile zu ermöglichen, so ist die Lösung – bspw. auch beim Cloud-Computing – verfassungswidrig.[1278] Auch die Datenhoheit, die jenseits des Internets mit behördlichen Aktenschränken gewahrt wird, könnte mit Cloud-Computing-Lösungen nichtöffentlicher Stellen aus dem Gleichgewicht geraten.[1279]

1269 *Heckmann* in: Bräutigam, IT-Outsourcing und Cloud-Computing, 3. Aufl. 2013, S. 718 ff.; *Roggenkamp*, Web 2.0 im kommunalen E-Government, 2009, S. 80 ff.

1270 *Pohle/Ammann*, CR 2009, 273 ff.; *Schulz*, MMR 2010, 75.

1271 Grundlegend *Schulz*, MMR 2010, 75, 77.

1272 Vertiefend für die öffentliche Verwaltung, *Maisch/Seidl*, VBlBW 2012, 7; *Schulz*, MMR 2010, 75.

1273 Vgl. *Heckmann* in: Bräutigam, IT-Outsourcing und Cloud-Computing, 3. Aufl. 2013, Teil 10 Rn. 27 ff.

1274 *Heckmann* in: Hill/Schließky, Innovationen im und durch Recht, 2010, S. 97, 102.

1275 *Heckmann* in: Hill/Schließky, Innovationen im und durch Recht, 2010, S. 97, 101.

1276 Dazu vertiefend *Braun/Albrecht*, jurisPR-ITR 1/2010 Anm. 2.

1277 *Heckmann* in: Hill/Schließky, Innovationen im und durch Recht, 2010, S. 97, 101.

1278 *Heckmann* in: Hill/Schließky, Innovationen im und durch Recht, 2010, S. 97, 103.

1279 *Heckmann* in: Hill/Schließky, Innovationen im und durch Recht, 2010, S. 97, 101.

© 2019 juris GmbH | www.juris.de

688 In **strafrechtlicher Hinsicht** kann sich bei der Nutzung von Cloud-Computing eine Strafbarkeit nach **§ 203 Abs. 2 StGB** wegen Geheimnisverrats ergeben (vgl. dazu bereits Rn. 88 ff.). Insbesondere Berufsgeheimnisträger wie etwa Ärzte oder Rechtsanwälte,[1280] aber auch der öffentliche Sektor, müssen bei der Auslagerung etwaiger Verarbeitungsprozesse an Externe auf die gesonderten Vorgaben des § 203 StGB achten.[1281]

689 Nach der Reform von § 203 StGB ist eine Datenweitergabe durch einen Verantwortlichen der Datenverarbeitung an den Cloud-Dienstleister **grundsätzlich möglich,** da eine Weitergabe von fremden Geheimnissen durch den Geheimnisträger gegenüber Personen, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist, nicht als Offenbaren angesehen wird, § 203 Abs. 3 Satz 2 StGB. Das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der Geheimnisträger mitwirken. Somit ist auch eine Unterbeauftragung durch den Auftragsverarbeiter möglich.

690 Allerdings muss der Geheimnisträger dafür sorgen, dass der Cloud-Dienstleister zur **Geheimhaltung verpflichtet** wurde, sonst macht Ersterer sich nach § 203 Abs. 4 StGB strafbar. Gleiches gilt für Cloud-Dienstleister, die sich eines Dritten bedienen. Öffentlich-rechtliche Geheimnisträger können zudem eine förmliche Verpflichtung privater Anbieter auf Grundlage des Verpflichtungsgesetzes (§ 1 Abs. 1 Nr. 1 Var. 3 VerpflG) vornehmen.[1282] Aufgrund der rechtlich novellierten Vorgaben des § 203 StGB ist eine dergestalt förmliche Verpflichtung aber nicht zwingend geboten, vielmehr ist die Verpflichtung grundsätzlich formfrei möglich.[1283] Aus Gründen der Nachweisbarkeit sollte bei der Verpflichtung jedoch zumindest auf die Textform zurückgegriffen werden.[1284]

bb. Privatwirtschaft

691 Die Inanspruchnahme von Cloud-Leistungen kann für Unternehmen zahlreiche Vorteile haben. **Kostenstrukturen** können **langfristig verbessert** werden, da mittel- und langfristige Investitionen in Inhouse-IT entfallen.[1285] Auch kostenintensive Wartung, technische oder bauliche Maßnahmen, bedarfsgerechte Anpassungen von Hard- und Softwarelösungen in Reaktion auf Markt- oder Betriebsveränderungen fallen nicht mehr an.[1286] Microsoft bietet bspw. seit Juni 2011 im Rahmen seiner „Online Services" Büroprogramme als Software-as-a-Service an.[1287] „MS-Office 365" richtet sich u.a. an Selbstständige und kleine Unternehmen (max. 300 Nutzer).[1288] MS-Word, Excel, PowerPoint und OneNote stehen dabei in den Webversionen als Pay-as-you-go-Abonnement zur Verfügung.

cc. Privater Endkunde

692 Im Internet stehen **zahlreiche entgeltliche und unentgeltliche Cloud-Anwendungen** für private Endkunden bzw. Verbraucher zur Verfügung. Von User-Generated-Content-Plattformen, sozialen Netzwerken und anderen Telemedien, die cloudbasiert betrieben werden, abgesehen, stellen v.a.

1280 Vgl. dazu etwa *Cornelius*, NJW 2017, 3751 ff.; *Grosskopf/Momsen*, CCZ 2018, 98 ff.

1281 *Redeker*, ITRB 2018, 215, 217.

1282 Vgl. *Redeker*, ITRB 2014, 232, 233 f. m.w.N.

1283 *Redeker*, ITRB 2018, 215, 217.

1284 *Redeker*, ITRB 2018, 215, 217.

1285 *Maisch*, AnwZert ITR 15/2009 Anm. 4.

1286 Vgl. auch *Spies*, MMR 2009, Heft 5, XI. Gleichsam bestehen Einsparungsmöglichkeiten durch neue Arbeitsplatzmodelle, vgl. *Giedke*, Cloud Computing: Eine wissenschaftliche Analyse mit besonderer Berücksichtigung des Urheberrechts, 2013, S. 8 f.

1287 https://products.office.com/de-de/business/office (abgerufen am 28.02.2019).

1288 https://products.office.com/de-de/compare-all-microsoft-office-products?tab=2 (abgerufen am 28.02.2019).

© 2019 juris GmbH | www.juris.de

Google und Microsoft Lösungen bereit. Google betreibt bspw. mit „Google Docs“ ein Textverarbeitungsprogramm zur kostenlosen Nutzung on-demand.[1289] Online-Fotoalben können mit „Google Fotos“ oder „Flickr“ geführt werden. Bereits heute spricht vieles dafür, dass nicht nur Software-as-a-Service und Storage-as-a-Service[1290] für Verbraucher bereitgestellt werden können, sondern bald auch Betriebssysteme on-demand und mobil genutzt werden[1291]. Der PC als lokale IT-Ressource in der heute bekannten Form wird zum Auslaufmodell.

3. Datenschutzrecht und Cloud-Computing

a. Internationale Dimension

693 Werden personenbezogene Daten an Destinationen außerhalb der EU in ein Drittland übermittelt, ist dies zulässig, sofern in dem jeweiligen Empfängerstaat ein **angemessenes Schutzniveau** besteht, vgl. Art. 44 ff. DSGVO.[1292] Danach ist eine Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses möglich, vgl. Art. 45 DSGVO. Von der EU-Kommission wurde ein Angemessenheitsbeschluss i.S.d. Art. 45 Abs. 3 DSGVO unter anderem für die Schweiz, Argentinien und Kanada erlassen. Ferner ist durch das **EU-US Privacy Shield**[1293] eine Datenübermittlung an U.S. Unternehmen möglich. Die vorhergehende Safe Harbor-Vereinbarung wurde mit Urteil des EuGH für ungültig erklärt.[1294] Ist ein angemessenes Schutzniveau nicht gewährleistet, hat eine Datenübermittlung grundsätzlich zu unterbleiben.

694 Ein **Gerichtsurteil bzw. eine behördliche Entscheidung aus einem Drittland,** aufgrund dessen der Verantwortliche oder ein Auftragsverarbeiter personenbezogene Daten offenbaren soll, dürfen unbeschadet anderer Gründe für die Datenübermittlung in ein Drittland nur anerkannt oder vollstreckt werden, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedsstaat gestützt sind, Art. 48 DSGVO.

695 Ob darunter beispielsweise auch ein Executive Agreement nach den Vorgaben des US-amerikanischen **CLOUD Acts** fällt (vgl. dazu bereits Rn. 216), ist noch nicht absehbar.[1295] Überwiegend wird allerdings zwischenzeitlich vertreten, dass ein solches Executive Agreement zwischen einem europäischen Mitgliedstaat und den USA nicht den Anforderungen des Art. 48 DSGVO genügt.[1296] Es ist daher davon auszugehen, dass betroffene Unternehmen, welche personenbezogene Daten auf Grundlage des CLOUD Acts an US-amerikanische Behörden übermitteln, gegen Art. 48 DSGVO verstoßen und sich der Gefahr eines Bußgeldes gem. Art. 83 Abs. 5 lit. d DSGVO aussetzen.[1297] Einen möglichen „Rettungsanker“ könnte in diesem Fall allerdings Art. 49 Abs. 1 lit. e

---

1289 www.google.de/intl/de/docs/about/ (aufgerufen 28.02.2019); *Fickert* in: Taeger/Wiebe, Inside the Cloud, 2009, S. 419, 423.

1290 Bspw. Dropbox, www.dropbox.com/ (abgerufen am 28.02.2019).

1291 Bereits heute stehen Cloud-Betriebssysteme zur Verfügung, bspw. eyeOS, https://eyeos.de.softonic.com/ (abgerufen am 28.02.2019).

1292 Die EU-Kommission hat ein angemessenes Datenschutzniveau für die Übermittlung personenbezogener Daten aus der EU festgestellt für Andorra, Argentinien, Kanada, Färöer, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Schweiz, Uruguay und nach Maßgabe des Privacy Shields auch für die USA. Aktuell finden Verhandlungen mit Japan und Südkorea statt. Hierzu https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en (abgerufen am 28.02.2019).

1293 www.privacyshield.gov/welcome (abgerufen am 28.02.2019).

1294 EuGH v. 06.10.2015 - C-362/14 - ECLI:EU:C:2015:650.

1295 *Determann/Nebel*, CR 2018, 408, 412.

1296 Vgl. dazu m.w.N. *Lejeune*, ITRB 2018, 118, 121; *Spies*, ZD-Aktuell 2018, 04291; *Rath/Spies*, CCZ 2018, 229, 230; *Gausling*, MMR 2018, 578, 581.

1297 *Rath/Spies*, CCZ 2018, 229, 230; *Gausling*, MMR 2018, 578, 581.

© 2019 juris GmbH | www.juris.de

DSGVO darstellen, der eine Übermittlung personenbezogener Daten an ein Drittland für zulässig erachtet, wenn diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.[1298]

aa. EU-Standardvertragsklauseln und Binding Corporate Rules

696 Wenn ein Angemessenheitsbeschluss nicht vorliegt, besteht ferner die Möglichkeit der Datenübermittlung an ein Drittland oder eine internationale Organisation vorzunehmen, wenn **geeignete Garantien nach Art. 46 DSGVO** bestehen und dem Betroffenen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Hierzu gehören neben verbindlichen internen Datenschutzvorschriften i.S.d. Art. 47 DSGVO auch Standardvertragsklauseln, die von der Kommission gemäß dem Prüfverfahren nach Art. 93 Abs. 2 DSGVO erlassen bzw. genehmigt wurden Art. 46 Abs. 2 lit. c, lit d DSGVO.

697 EU-Standardvertragsklauseln[1299] sind **Vertragsklauseln** bei deren Verwendung durch ein Unternehmen ein angemessenes Schutzniveau als garantiert gilt.[1300] Eine Überprüfung des angemessenen Schutzniveaus durch die Aufsichtsbehörden ist bei Verwendung der Klauseln nicht mehr erforderlich – die Vorlage des Vertragswerks kann jedoch verlangt werden, um die tatsächliche Verwendung der Klauseln zu überprüfen.[1301]

698 Allerdings wird demnächst durch den EuGH darüber entschieden, ob diese bisherige Grundlage für den Datentransfer in Drittländer ein weiterhin zulässiges Mittel ist. Aufgrund der EuGH-Entscheidung zum Safe-Harbor-Abkommen bestehen zumindest dahingehende **Vermutungen,** dass der **EuGH** aufgrund der unbeschränkten Zugriffsmöglichkeiten von US-Geheimdiensten auf personenbezogene Daten von EU-Bürgern hierdurch **kein adäquates Schutzniveau gewahrt sieht.**[1302] Wenngleich die Entscheidung des EuGH noch nicht absehbar ist und jedenfalls bis zu der Entscheidung von einer Gültigkeit der Standardvertragsklauseln ausgegangen werden kann,[1303] kann der Rückgriff auf die Klauseln langfristig nur bedingt als rechtssicher empfohlen werden[1304].

699 Des Weiteren können verbindliche durch die zuständige Aufsichtsbehörde genehmigte interne Datenschutzvorschriften nach Art. 47 DSGVO eine Datenübermittlung in Drittländer ermöglichen, sog. **„binding corporate rules" (BCRs)**[1305]. BCRs sind **freiwillige Selbstverpflichtungen,** die dazu dienen, gerade in internationalen Konzernunternehmen ein einheitliches und angemessenes Datenschutzniveau sicherzustellen.[1306] BCRs können unter anderem für Unternehmen einer „Auftragsverarbeitungs-Unternehmensgruppe", welche im Rahmen ihrer Geschäfte personenbezogene Daten im Auftrag verarbeiten, oder Unternehmen einer Unternehmensgruppe, die personenbezogene Daten an gruppenangehörige Unternehmen in Drittländer transferieren wollen, in-

---

1298 *Rath/Spies*, CCZ 2018, 229, 230; in diesem Sinne auch *Determann/Nebel*, CR 2018, 408, 412.

1299 Ausführlich *Hladjk*, DuD 2017, 77 ff.; *Lensdorf*, CR 2010, 735 ff.; *Moos*, CR 2010, 281 ff.; *Geppert*, ZD 2018, 62, 65; *Determann/Weigl*, EuZW 2016, 811 ff.

1300 Vgl. dazu bereits *Spindler* in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 4c BDSG, Rn. 20; *Maisch/Seidl*, VBlBW 2012, 7; *Hennrich/Maisch*, AnwZert ITR 15/2011 Anm. 2.

1301 *Schantz* in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 46 DSGVO Rn. 31; vgl. dazu bereits *Gola/Schomerus*, BDSG, 12. Aufl. 2015, § 4 c Rn. 14.

1302 *Böse/Rockenbach*, MDR 2018, 70, 73; *Hoeren*, Fallen nach „Safe Harbor" auch die Standardverträge? Abrufbar unter:www.lto.de/recht/hintergruende/h/max-schrems-high-court-irland-standardvertraege-vorlage-eugh-datenschutz/ (abgerufen am 28.02.2019).

1303 Darauf abstellend *Wybitul/Ströbel/Ruess*, ZD 2017, 503, 506.

1304 Tendenziell gegen eine Heranziehung etwaiger Standardvertragsklauseln *Böse/Rockenbach*, MDR 2018, 70, 73.

1305 Zu Binding Corporate Rules vertiefend *Baumann*, DSRITB 2017, S. 59 ff; *Grapentin* in: Taeger/Wiebe, Inside the Cloud, 2009, S. 457-468; *Heil*, DuD 2009, 228.

1306 *Baumann*, DSRITB 2017, S. 59; dazu bereits *Simitis* in: Simitis, BDSG, 8. Aufl. 2014, § 4c Rn. 59.

 © 2019 juris GmbH | www.juris.de

teressant sein.[1307] Anders als etwa Standardvertragsklauseln können BCRs regelmäßig flexibel und unternehmensspezifisch eingesetzt und angepasst werden, wobei zu beachten ist, dass auch nach den Vorgaben der DSGVO ein zeitaufwendiges und regelmäßig komplexes Genehmigungsverfahren erforderlich ist.[1308]

700 Nach **Genehmigung durch die Aufsichtsbehörde** ermöglichen BCRs grenzüberschreitende Datentransfers innerhalb der verbundenen Unternehmen. Diese Regeln müssen nunmehr die in Art. 47 Abs. 2 DSGVO genannten Anforderungen erfüllen.

701 Ferner bestehen nach Art. 49 DSGVO weitere Ausnahmen für eine Übermittlung von personenbezogenen Daten in Drittländer.

bb. Safe Harbor und Privacy Shield

702 Bedingt dadurch, dass innerhalb der USA strukturell als auch historisch begründet ein divergierendes Datenschutzrecht vorherrscht, mangelt es an einem allgemeinen Angemessenheitsbeschluss durch die Kommission.[1309] Viele prominente Cloud-Anbieter unterhalten indes Rechenzentrumsstandorte in den USA. Aufgrund der großen wirtschaftlichen Bedeutung von Datentransfers in die USA wurde daher zunächst das sog. „Safe Harbor"-Abkommen[1310] ins Leben gerufen.[1311] Mit dem Angemessenheitsbeschluss 2000/520/EG vom 26.07.2010[1312] gemäß Art. 25 Abs. 6 RL 95/46/EG hatte die EU-Kommission anerkannt, dass ein ausreichendes Schutzniveau bei Unternehmen besteht, die auf einer Liste des US-Handelsministeriums (Federal Trade Commission) eingetragen sind und sich verpflichtet haben, die Grundsätze von Safe Harbor einzuhalten.[1313] Die Vereinbarung enthielt sieben Grundprinzipien zum Datenschutz[1314], die zudem durch eine verbindliche Liste häufig gestellter Fragen (FAQ) ergänzt wurden[1315].

703 Der EuGH hat mit Urteil vom 06.10.2015 in der **Rechtssache Schrems** den Beschluss 2000/520/EG für ungültig erklärt.[1316] Die Kommission hätte begründet feststellen müssen, dass die USA tatsächlich ein Schutzniveau für personenbezogene Daten gewährleisten, das dem in der EU der Sache nach gleichwertig ist.[1317] Eine solche Feststellung habe die Kommission aber nicht getroffen, sondern sich stattdessen darauf beschränkt, die Safe Harbor-Grundsätze und die FAQ zu prüfen (vgl. Art. 2 Entscheidung 2000/520/EG).[1318] US-Behörden seien allerdings von Safe Harbor nicht erfasst und

---

1307 Vgl. Orientierungshilfe Cloud Computing 2.0, S. 18.

1308 *Wybitul/Ströbel/Ruess*, ZD 2017, 503, 506; weiterführend dazu *Baumann*, DSRITB 2017, S. 67 ff.

1309 Vgl. dazu m.w.N. *Schantz* in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 45 DSGVO Rn. 41 ff.

1310 Safe-Harbor-Datenschutzvereinbarung zwischen der Europäischen Union und den Vereinigten Staaten von Amerika (USA) in Bezug auf die Übermittlung personenbezogener Daten; vgl. *Rath/Rothe*, K&R 2013, 623; *Ritchie*, PinG 2014, 45 ff.; *Sädtler,* Rechtskonformes Identitätsmanagement im Cloud Computing, 2016, S. 161 ff.

1311 Vgl. *Hennrich/Maisch*, AnwZert ITR 15/2011 Anm. 2; *Lederer*, www.lto.de/de/html/nachrichten/2345/den-sicheren-hafen-gibt-es-nicht-safe-harbor-abkommen-in-der-kritik/ (abgerufen am 28.02.2019).

1312 Entscheidung der Kommission vom 26.07.2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 v. 25.08.2000, S. 7.

1313 Vgl. *Hennrich/Maisch*, AnwZert ITR 15/2011 Anm. 2.

1314 Vgl. zu den sieben Prinzipien: U.S.-EU Safe Harbor Overview, http://2016.export.gov/safeharbor/eg_main_018362.asp (zuletzt abgerufen am 28.02.2018); *Erd*, K&R 2010, 624, 625; *Marnau/Schlehahn*, DuD 2011, 311, 312.

1315 Vgl. *Simitis* in: Simitis, BDSG, 8. Aufl. 2014, § 4b Rn. 70; *Marnau/Schlehahn*, DuD 2011, 311, 312.

1316 EuGH v. 06.10.2015 - C-362/14 - ECLI:EU:C:2015:650 - Schrems mit Anm. *Heckmann/Starnecker*, jM 2016, 58 ff.; *Kamps/Bonanni*, ArbRB 2015, 334; *Seiler*, jurisPR-BKR 11/2015 Anm. 2.

1317 EuGH v. 06.10.2015 - C-362/14 - juris Rn. 83 - ECLI:EU:C:2015:650 - Schrems mit Anm. *Heckmann/Starnecker*, jM 2016, 58 ff.; *Kamps/Bonanni*, ArbRB 2015, 334; *Kühling/Heberlein*, NVwZ 2016, 7 ff.; *Seiler*, jurisPR-BKR 11/2015 Anm. 2.

1318 EuGH v. 06.10.2015 - C-362/14 - juris Rn. 83 - ECLI:EU:C:2015:650 - Schrems mit Anm. *Heckmann/Starnecker*, jM 2016, 58 ff.; *Kamps/Bonanni*, ArbRB 2015, 334; *Kühling/Heberlein*, NVwZ 2016, 7 ff.; *Seiler*, jurisPR-BKR 11/2015 Anm. 2.

daher auch nicht in ihrer Überwachungstätigkeit eingeschränkt.[1319] Des Weiteren seien die zertifizierten Unternehmen verpflichtet, im Zweifel Zugriffsersuchen von US-Behörden auf personenbezogene Daten nachzukommen.[1320] Schließlich seien die Befugnisse der US-Behörden im Hinblick auf ihre Reichweite, anlassunabhängige Überwachung jeder Art von elektronischer Kommunikation und im Hinblick auf die fehlenden Rechtsschutzmöglichkeiten von EU-Bürgern nicht mit den Wertungen der EU-Grundrechtecharta zu vereinbaren.[1321] Damit ist Safe Harbor nicht mehr in der Lage, eine Datenübermittlung in die USA zu legitimieren.[1322]

704 In der Literatur wurde das **Safe Harbor-Urteil kritisch diskutiert.** Bei der materiellen Begründung weise es Schwächen auf, zumindest sofern die Ungültigkeit des Kommissionsbeschlusses, wenn auch nur implizit, auf die Zugriffe durch die NSA gestützt werde, da in solchen Fällen nationaler Sicherheit der Anwendungsbereich der Richtlinie aber schon nach Art. 3 Abs. 2 RL 95/46/EG gar nicht eröffnet sei.[1323] Auch werde der Begriff des „angemessenen Datenschutzniveaus" durch den EuGH nur unzureichend ausgelegt; es sei nicht klar geworden, wann ein Weniger an Datenschutz noch angemessen sei.[1324]

705 Zudem wurde die Frage aufgeworfen, inwiefern Daten **europäischer Nutzer überhaupt vor Zugriffen durch US-Behörden geschützt werden können** bzw. inwieweit US-Unternehmen (auch zukünftig) durch US-Gerichte verpflichtet werden können, solche Daten herauszugeben, die auf den europäischen Servern des Tochterunternehmens gespeichert sind.[1325] Zwischenzeitlich wurde in den USA der sog. „CLOUD Act" erlassen, der den Zugriff auf außerhalb der USA befindliche Daten ermöglichen soll.[1326] Hier könnten insofern sog. Datentreuhand-Modelle eine praktische Lösung darstellen, wie das von Microsoft und T-Systems vorgestellte Modell der „deutschen Cloud", wobei auch hier letztendlich fraglich ist, inwiefern dies einen Zugriff auf deutsche Datenbestände vollständig verhindern kann (vgl. dazu bereits Rn. 216 sowie Rn. 694).[1327] Zudem ist nunmehr **Art. 48 DSGVO** zu beachten, der besagt, dass ein Gerichtsurteil bzw. eine behördliche Entscheidung aus einem Drittland, die einen Verantwortlichen oder einen Auftragsverarbeiter verpflichtet, personenbezogene Daten zu offenbaren, nur anzuerkennen oder in der EU zu vollstrecken ist, wenn diese auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedsstaat gestützt ist.

1319 EuGH v. 06.10.2015 - C-362/14 - juris Rn. 88 - ECLI:EU:C:2015:650 - Schrems mit Anm. *Heckmann/Starnecker*, jM 2016, 58 ff.; *Kamps/Bonanni*, ArbRB 2015, 334; *Kühling/Heberlein*, NVwZ 2016, 7 ff.; *Seiler*, jurisPR-BKR 11/2015 Anm. 2.

1320 EuGH v. 06.10.2015 - C-362/14 - juris Rn. 83 - ECLI:EU:C:2015:650 - Schrems mit Anm. *Heckmann/Starnecker*, jM 2016, 58 ff.; *Kamps/Bonanni*, ArbRB 2015, 334; *Kühling/Heberlein*, NVwZ 2016, 7 ff.; *Seiler*, jurisPR-BKR 11/2015 Anm. 2.

1321 EuGH v. 06.10.2015 - C-362/14 - juris Rn. 94 f. - ECLI:EU:C:2015:650 - Schrems mit Anm. *Heckmann/Starnecker*, jM 2016, 58 ff.; *Kamps/Bonanni*, ArbRB 2015, 334; *Seiler*, jurisPR-BKR 11/2015 Anm. 2.

1322 *Kamps/Bonanni*, ArbRB 2015, 334; *Härting*, CR 2015, 640; *Moos/Schefzig*, CR 625, 631.

1323 *Kühling/Heberlein*, NVwZ 2016, 7, 10.

1324 *Kühling/Heberlein*, NVwZ 2016, 7, 9.

1325 Vgl. *Kühling/Heberlein*, NVwZ 2016, 7, 11; *Rath/Kuß/Maiworm*, CR 2016, 98 ff.

1326 *Spies*, ZD-Aktuell 2018, 04291; vgl. auch *Spies*, ZD-Aktuell 2017, 05829.

1327 *Rath/Kuß/Maiworm*, CR 2016, 98, 103.

© 2019 juris GmbH | www.juris.de

706 **Keinesfalls** sollte aber der Datentransfer in die USA weiter auf **Safe Harbor** gestützt werden. Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit (HmbBfDI) teilte per Pressemitteilung vom 06.06.2016 mit, dass die Behörde gegen die Unternehmen Adobe, Punica und Unilever Bußgelder wegen Nichtbeachtung des Schrems-Urteils verhängt hatte und die Bescheide bestandkräftig wurden.[1328]

707 Am 02.02.2016 hat sich die EU-Kommission mit den USA auf einen neuen Rechtsrahmen für die transatlantische Übermittlung von Daten geeinigt, das sog. **„EU-US-Privacy-Shield“**.[1329] Am 12.07.2017 verabschiedete die EU-Kommission offiziell die endgültige Fassung des Privacy Shields als Angemessenheitsbeschluss.[1330] Das Privacy Shield sieht strengere Aufklärungspflichten und Zustimmungserfordernisse bei der Datenverarbeitung vor.[1331] Auch der nachrichtendienstliche Datenzugriff soll stärker reglementiert werden. EU-Bürger sollen hier die Möglichkeit bekommen, sich mit Anfragen oder Beschwerden an eine speziell hierfür eingerichtete Ombudsstelle zu wenden. Beteiligte US-Unternehmen können sich seit dem 01.08.2016 durch eine Selbstzertifizierung in der „Privacy Shield List“ auf die Einhaltung der im Privacy Shield niedergelegten Datenschutzgrundsätze verpflichten.

708 Ob der Angemessenheitsbeschluss zum Privacy Shield **mit europäischem Datenschutzrecht vereinbar ist, wird sich noch zeigen.** Die Kritik hieran reißt jedenfalls nicht ab.[1332] Insbesondere der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des **Europäischen Parlaments** reichte am 26.06.2018 einen Entschließungsantrag ein, der die Kommission eindringlich dazu aufforderte „[…] sämtliche Maßnahmen zu ergreifen, die erforderlich sind, damit der Datenschutzschild uneingeschränkt im Einklang mit der ab dem 25. Mai 2018 geltenden Verordnung 2016/679 und der EU-Grundrechtecharta steht, sodass das Kriterium der Angemessenheit nicht zu Schlupflöchern oder Wettbewerbsvorteilen für US-Unternehmen führt […]“.[1333]

709 Auch der Erlass der **Executive Order vom 25.01.2017 zur „Verbesserung der öffentlichen Sicherheit“** durch US-Präsident Trump mehrte die Zweifel, ob der Privacy Shield (weiterhin) ein angemessenes Datenschutzniveau gewährleisten kann.[1334] Grund ist Section 14 des Dekrets, wonach grundsätzlich nur noch amerikanische Staatsbürger und Personen mit dauerhafter Aufenthaltserlaubnis unter den Schutz des Privacy Shields fallen sollen. Das könnte die EU-Kommission dazu bewegen, im Rahmen der jährlichen Überprüfung des Privacy Shields den Angemessenheitsbeschluss zurückzunehmen.

[1328] Heise Online, Hamburg: Erste Bußgelder wegen Nichtumsetzung des Safe-Harbor-Urteils, abrufbar unter: www.heise.de/newsticker/meldung/Hamburg-Erste-Bussgelder-wegen-Nichtumsetzung-des-Safe-Harbor-Urteils-3228350.html (abgerufen am 28.02.2019).

[1329] Europäische Kommission, Pressemitteilung v. 29.02.2016, abrufbar unter http://europa.eu/rapid/press-release_IP-16-433_en.htm (abgerufen am 28.02.2019).

[1330] Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12.07.2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, ABl. L 207 v. 01.08.2016, S. 1.

[1331] Ausführlich zu den Änderungen durch das Privacy Shield vgl. *Lewinski*, EUR 2016, 412 ff.

[1332] Vgl. etwa *Molnár-Gábor/Kaffenberger*, ZD 2018, 162, 163 ff.; *Pauly* in: Paal/Pauly, DS-GVO/BDSG, Art. 45 DSGVO Rn. 24c; Heise Online, „Privacy Shield“: Bürgerrechtler schießen scharf gegen geplanten Datenschutzschuld, abrufbar unter www.heise.de/newsticker/meldung/Privacy-Shield-Buergerrechtler-schiessen-scharf-gegen-geplanten-Datenschutzschild-3093494.html (abgerufen am 28.02.2019).

[1333] Europäisches Parlament, Entschließungsantrag v. 26.06.2018, S. 13, abrufbar unter: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2018-0305+0+DOC+PDF+V0//DE (abgerufen am 28.02.2019).

[1334] Vgl. etwa Datenschutzbeauftragter-INFO, Präsident Trump und die Executive Order – Das Aus für den Privacy Shield? Abrufbar unter www.datenschutzbeauftragter-info.de/praesident-trump-und-die-executive-order-das-aus-fuer-den-privacy-shield/ (abgerufen am 28.02.2019); *Spies*, ZD-Aktuell 2018, 04291.

710 Die **Kommission bestätigte** allerdings im Rahmen ihrer zweiten jährlichen Überprüfung der Funktionsweise des EU-US-Datenschutzschildes vom 19.12.2018, „[…] dass die Vereinigten Staaten nach wie vor ein angemessenes Datenschutzniveau für diejenigen personenbezogenen Daten gewährleisten, die aus der EU im Rahmen des Datenschutzschildes an teilnehmende Unternehmen in den USA übermittelt werden."[1335]

711 Vor diesem Hintergrund empfiehlt es sich bei der Übermittlung personenbezogener Daten an Drittstaaten an **alternative Übermittlungsgrundlagen** im konkreten Fall zu denken. Die am gangbarsten scheinende Lösung des „Safe-Harbor"- bzw. nunmehr „Privacy Shield"-Dilemmas dürfte in der informationellen Selbstbestimmung und damit letztendlich in der **Einwilligung** des Nutzers liegen.[1336] Hierfür muss hinreichend sachlich, nicht verharmlosend und nicht dramatisierend über die mit dem Transfer der Daten verbundenen Risiken informiert werden, wofür letztendlich innovative Einwilligungskonzepte mit einer interessengerechten und verhältnismäßigen Begrenzung der Widerruflichkeit erforderlich werden.[1337] Ähnlich sehen dies auch *Kühling/Heberlein*, die darüber hinaus betonen, dass die Einwilligung zwar keine generelle Rechtsgrundlage für die Datenübermittlung darstellen könne und eine pauschale Einwilligung für eine Vielzahl von Fällen unzulässig sei, die Dispositionsbefugnis des Einzelnen jedoch nicht gänzlich versagt werden könne.[1338]

b. Die Auftragsverarbeitung als Privilegierung der Datenverarbeitung im Rahmen des Cloud-Computings

712 Innerhalb der Vorgaben der DSGVO finden sich keine konkreten Bestimmungen zur datenschutzrechtlichen Einordnung des Cloud-Computings.[1339] Einigkeit besteht allerdings dahingehend, dass **Cloud-Computing-Dienstleistungen** regelmäßig als **Auftragsverarbeitung** im Sinne der Art. 4 Nr. 8 DSGVO beziehungsweise Art. 28 DSGVO einzuordnen sind.[1340]

713 Diese Einordnung ist für die (datenschutzrechtlich) praktische Ausgestaltung der Cloud-Computing-Dienstleistungen von erheblicher Relevanz.[1341] Insbesondere vor dem Hintergrund, dass der Verantwortliche auch die Datenverarbeitung durch einen Cloud-Dienstleister auf eine entsprechende Rechtsgrundlage stützen muss, ist der **privilegierenden Wirkung**[1342] des Auftragsverarbeitungsverhältnisses entscheidende Bedeutung beizumessen.[1343] Der Rückgriff auf spezielle „Cloud-Erlaubnistatbestände" ist, wie bereits eingangs erwähnt, nicht möglich, die Einwilligung birgt zumindest das „Risiko" der jederzeitigen freien Widerrufbarkeit.[1344]

1335 Europäische Kommission, Pressemitteilung v. 19.12.2018, abrufbar unter: http://europa.eu/rapid/press-release_IP-18-6818_de.htm (abgerufen am 28.02.2019).

1336 *Heckmann/Starnecker*, jM 2016, 58, 61.

1337 *Heckmann/Starnecker*, jM 2016, 58, 61.

1338 *Kühling/Heberlein*, NVwZ 2016, 7, 10 f.; ähnlich: *Borges*, NJW 2015, 3617, 3620.

1339 *Hofmann*, ZD-Aktuell 2017, 05488.

1340 Vgl. etwa *Böse/Rockenbach*, MDR 2018, 70, 72; *Schmid/Kahl*, ZD 2017, 54, 56; *Härting*, ITRB 2016, 137, 138; *Spoerr* in: Wolff/Brink, Beck'scher Onlinekommentar, Art. 28 DSGVO Rn. 21; *Hartung* in: Kühling/Buchner, DS-GVO/BDSG, Art. 28 DSGVO Rn. 45.

1341 Vgl. statt vieler Der Bayerische Landesbeauftragte für den Datenschutz, Auftragsverarbeitung – Orientierungshilfe, Stand: 25. Mai 2018, S. 7. Abrufbar unter: www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf (abgerufen am 28.02.2018).

1342 Insbesondere innerhalb der Literatur ist zwar umstritten, ob die Vorgaben der DSGVO tatsächlich eine Form der Privilegierung darstellen, Einigkeit besteht aber dahingehend, dass bei Einhaltung der Vorgaben der DSGVO zur Auftragsverarbeitung keine weitere Rechtsgrundlage zwischen dem Auftraggeber und Auftragnehmer erforderlich ist. Vgl. dazu m.w.N. *Bertermann* in: Ehmann/Selmayr, DS-GVO, Art. 28 DSGVO Rn. 5 ff.; *Hartung* in: Kühling/Buchner, DS-GVO/BDSG, Art. 28 DSGVO Rn. 13 ff.

1343 Der Bayerische Landesbeauftragte für den Datenschutz, Auftragsverarbeitung – Orientierungshilfe, Stand: 25. Mai 2018, S. 7.

1344 Vgl. Der Bayerische Landesbeauftragte für den Datenschutz, Auftragsverarbeitung – Orientierungshilfe, Stand: 25. Mai 2018, S. 7.

© 2019 juris GmbH | www.juris.de

714 Soweit zwischen dem Cloud-Dienstleister und dem Verantwortlichen ein Auftragsverarbeitungsvertrag geschlossen wird, der insbesondere den Anforderungen des Art. 28 Abs. 3 DSGVO entspricht, wird eine **datenschutzrechtlich ausreichende Basis** für die Übermittlung der personenbezogenen Daten im Einzelfall geschaffen.[1345] In diesem Fall ist der Cloud-Dienstleister zwar Empfänger der Daten im Sinne des Art. 4 Nr. 9 DSGVO, nicht aber Dritter nach den Vorgaben des Art. 4 Nr. 10 DSGVO.[1346] Zu den Anforderungen an die Auftragsverarbeitung nach den Vorgaben der DSGVO vgl. Rn. 220.

II. Allgemeine Vorgaben des Datenschutzes in sozialen Netzwerken

1. Allgemeines

715 Die Nutzung sozialer Netzwerke[1347] ist dadurch geprägt, dass zunehmend Informationen, die in früheren Zeiten noch in einer abgetrennten Sphäre des „Für-sich-Behaltens“ oder „Mit-Freunden-Teilens“ verblieben wären, einer so großen Menge an anderen Menschen mitgeteilt oder zur Verfügung gestellt werden, dass dies einer **Veröffentlichung** dieser Informationen **gleichkommt.**[1348] Ein Hauptmerkmal der sozialen Netzwerke ist dabei, dass sie hochattraktive und vielfach nützliche Funktionen unentgeltlich zur Verfügung stellen.[1349]

716 **Unentgeltlich** bedeutet allerdings **nicht „ohne Gegenleistung“**.[1350] Die Gegenleistung besteht in der Preisgabe von personenbezogenen Daten, welche durch die Social Media-Anbieter genutzt werden. Wenngleich es an einer gesetzlichen Bestimmung zu der Frage des **Entgeltcharakters personenbezogener Daten** bislang fehlt, besteht Einigkeit, dass deren Hergabe vom zivilrechtlichen Begriff des Entgelts umfasst ist.[1351] Für diesen Befund spricht zudem der Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte.[1352] Insbesondere sieht Art. 3 Abs. 1 des Richtlinienvorschlags vor, dass sich der Anwendungsbereich der Richtlinie auf alle Verträge erstreckt, auf deren Grundlage ein Anbieter einem Verbraucher digitale Inhalte bereitstellt oder sich hierzu verpflichtet und der Verbrauer als **Gegenleistung** einen Preis zahlt oder aktiv eine andere Gegenleistung als Geld in Form **personenbezogener oder anderer Daten** erbringt.[1353] Mithin sind Daten die Währung des Internets.[1354]

[1345] Der Bayerische Landesbeauftragte für den Datenschutz, Auftragsverarbeitung – Orientierungshilfe, Stand: 25. Mai 2018, S. 7.

[1346] Der Bayerische Landesbeauftragte für den Datenschutz, Auftragsverarbeitung – Orientierungshilfe, Stand: 25. Mai 2018, S. 7.

[1347] Definition bei *Fox*, DuD 2009, 53.

[1348] *Heckmann*, K&R 2010, 770, 771.

[1349] *Heckmann*, K&R 2010, 770, 771.

[1350] Vgl. dazu etwa m. w. N. *Bräutigam*, MMR 2012, 635, 638 ff.

[1351] Vgl. dazu m.w.N. *Zdanowiecki*, Data is Cash – Daten als Entgelt, DSRITB 2018, S. 559 ff.

[1352] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte v. 09.12.2015, COM(2015) 634 final. Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52015PC0634&from=DE (abgerufen am 28.02.2019).

[1353] Vgl. dazu weiterführend *Zdanowiecki*, Data is Cash – Daten als Entgelt, DSRITB 2018, S. 561.

[1354] So bereits *Heckmann* in: Hoffmann/Leible, Online-Recht 3.0, 2010, S. 18; vgl. *Fox*, DuD 2009, 53; vom Rohstoff des 21. Jahrhunderts sprechen insoweit *Mainusch/Burtchen*, DuD 2010, 448, 449.

© 2019 juris GmbH | www.juris.de

717 Vor diesem Hintergrund wird insbesondere vertreten, dass die Aufforderung zur Abgabe einer **datenschutzrechtlichen Einwilligungserklärung als Gegenleistung** des jeweiligen Dienstes erfasst werden könnte.[1355]

718 Die Entwicklung ist aus **datenschutzrechtlicher Sicht durchaus problematisch.** Die mehr oder weniger freiwillige Preisgabe von Informationen bezüglich des Beziehungsstatus, zur religiösen oder sexuellen Orientierung, zum Konsumverhalten oder politischen Einstellungen, zu Vermögensverhältnissen oder Vorkommnissen im privaten und beruflichen Alltag wirft die Frage auf, ob der **Staat** den Einzelnen vor seinem sorglosen Handeln **schützen muss** oder vielmehr eine solche Selbstgefährdung[1356] in Kauf zu nehmen hat[1357].[1358]

719 Weitgehend ungeklärt ist zudem die Problematik, wie damit umzugehen ist, dass von den Nutzern sozialer Netzwerke zunehmend **Informationen über Dritte** aus einem ebenso sensiblen sozialen Kontext preisgegeben werden.[1359] Aus datenschutzrechtlicher Sicht besteht insoweit das Hindernis, dass derjenige, um dessen Privatheit es geht, nicht unbedingt in die Datennutzung eingewilligt hat. Das gilt zum Beispiel für das Verbreiten privater (Party-)Fotos, wozu bestimmte Funktionen wie die des „Teilens" auf Facebook geradezu einladen.[1360] Die in der Wissenschaft bereits aufkommende Forderung, technische Anforderungen und rechtliche Voraussetzungen auch auf private Datenverarbeiter auszuweiten[1361], scheint somit zunehmend an Berechtigung zu gewinnen. Gleichermaßen erscheint der Umgang mit fremden Persönlichkeitsrechten regelungsbedürftig, weil strafrechtliche Normen wie die Ehrverletzungsdelikte (§§ 185 ff. StGB) in Fällen wie dem sog. **Cybermobbing** (vgl. hierzu Kapitel 8 Rn. 428 ff.) bestenfalls formal greifen, aber keinen wirksamen Schutz gewährleisten.[1362]

2. Gesetzliche Grundlagen

720 Soziale Netzwerke, die dem Bereich der Telemedien zuzuordnen sind, haben in datenschutzrechtlicher Hinsicht zunächst die einschlägigen Bestimmungen der **DSGVO**[1363] und zukünftig auch der **ePVO** zu beachten. Mit Blick darauf, dass es aber an umfassenden spezialgesetzlichen Regelungen, wie etwa noch innerhalb des TMG vorgesehen, mangelt, wird kritisiert, dass Rechtssicherheit in Bezug auf den telemedienrechtlichen Datenschutz erst auf Grundlage weiterführender behördlicher beziehungsweise gerichtlicher Entscheidungen gewährleistet werden kann (zur eingeschränkten Fortgeltung der TMG-Bestimmungen bereits unter Rn. 63).[1364]

1355 Vgl. dazu *Zdanowiecki*, Data is Cash – Daten als Entgelt, DSRITB 2018, S. 563 ff; *Golland*, MMR 2018, 130, 135; *Specht*, GRUR Int. 2017, 1040 ff.; *Bräutigam*, MMR 2012, 635, 637; *Duden*, in: Gsell/Krüger/Lorenz/Reymann, Beck'scher Großkommentar, § 107 BGB Rn. 121; kritisch hinsichtlich der Handelbarkeit der datenschutzrechtlichen Einwilligung *Bull*, CR 2018, 425, 430.

1356 Zum Selbstdatenschutz hingegen *Schnabel/Freund*, CR 2010, 718.

1357 *Heckmann*, K&R 2010, 770, 772.

1358 Vgl. dazu auch *Sandfuchs*, Privatheit wider Willen?, 2015.

1359 *Heckmann*, K&R 2010, 770, 772.

1360 Vgl. dazu umfassend *Lauber/Rönsberg*, NJW 2016, 744 ff.

1361 In diesem Sinne bereits EuGH v. 06.11.2003 - C-101/01 - ECLI:EU:C:2003:596; vgl. *Albrecht*, JurPC Web-Dok. 95/2011, Abs. 11 unter Bezugnahme auf *Hornung*; *Albrecht/Maisch*, www.lto.de/de/html/nachrichten/3661/datenschutz_in_sozialen_netzwerken_wenn_das_leben_der_anderen_tabu_ist/ (abgerufen am 28.02.2019).

1362 Zum Ehrschutz im Zusammenhang mit sozialen Netzwerken *Heckmann*, NJW 2012, 2631; www.arag.com/german/press/pressreleases/group/00448/ (abgerufen am 28.02.2019).

1363 Vgl. dazu jüngst EuGH v. 05.06.2018 - C-210/16 - ECLI:EU:C:2018:388 = EuZW 2018, 534, 536 Rn. 25 ff.

1364 Vgl. dazu weiterführend etwa *Schmitz* in: Spindler/Schmitz, TMG, vor §§ 11 ff. TMG Rn. 15 ff.

© 2019 juris GmbH | www.juris.de

721 Dass soziale Netzwerke wie bspw. Facebook ihr rasantes Wachstum gerade der bewussten Missachtung datenschutzrechtlicher Vorgaben, die einer unkomplizierten und inhaltsreichen Kommunikation entgegenstehen, verdanken[1365], steht der Anwendbarkeit des Rechts selbstverständlich nicht entgegen.

a. Accounteröffnung

722 Derjenige, der sich unter einem **Klarnamen** bei sozialen Netzwerken anmeldet, hinterlässt dort zwingend eine Vielzahl personenbezogener Daten, die dem Regelungsregime des Datenschutzrechts unterliegen.[1366] Daten wie den Namen, die E-Mail-Adresse, das Geburtsdatum sowie die IP-Adresse der Nutzer besitzen unproblematisch Personenbezug.

723 Grundsätzlich unterliegen die im Rahmen der Accounteröffnung hinterlassenen personenbezogenen Daten dem Vorbehalt der **Erforderlichkeit.**[1367] D.h., dass seitens der Betreiber aufgrund des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO, vgl. dazu bereits Rn. 196) nur die Informationen als Pflichtangaben verlangt werden dürfen, die zur Erfüllung der abgefragten Dienstleistung benötigt werden.[1368] Um welche Daten es sich insoweit handelt, lässt sich nur im konkreten Einzelfall unter Berücksichtigung des jeweiligen Verwendungszweckes bestimmen.[1369]

b. Profildaten

724 Schwer zu vereinbaren sind die unterschiedlichen Bedürfnisse der Nutzer, die einerseits Privatsphäre und Datenschutz wünschen, sich anderseits aber möglichst umfassend und detailliert der Netzöffentlichkeit präsentieren wollen[1370] und sich mit den Bedingungen der Diensteanbieter zu unreflektiert abfinden. Es ist aber keinesfalls so, dass sich soziale Netzwerke und Datenschutz nicht vertragen würden. Allzu oft wird außer Acht gelassen, dass **Informationstechnologien auch datenschutzfördernd wirken können.** Mittels eines technologiebasierenden Smart Privacy Managements[1371] bzw. des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO, vgl. dazu Rn. 419 ff.) kann dem Nutzer eine selbstbestimmte Datenverarbeitung ermöglicht werden, die gleichwohl innovativen Lösungen nicht entgegensteht.

725 Werden Profile der Nutzer ausschließlich aufgrund automatisierter Verarbeitung erstellt, sind die Vorgaben des Art. 22 DSGVO zu beachten. Diese Informationen werden im virtuellen Raum für personalisierte Werbung verwendet.[1372]

c. Der Like-Button

726 Der **Like-Button** ist ein Social Plug-in, das jeder Webseiten-Betreiber auf seiner eigenen Website einbinden kann[1373], um so Facebook-Nutzern zu ermöglichen, die dort aufgeführten Webinhalte auf ihrem Facebook-Profil mit einem „Gefällt mir" zu verlinken (vgl. dazu bereits umfassend unter Rn. 142 ff.).[1374] Dies ist vergleichbar mit der bekannten „tell a friend"-Funktion.[1375] Webseiten-Betreibern dient der Like-Button zugleich als Webanalysedienst, grundsätzlich vergleichbar mit

---

1365 *Mainusch/Burtchen*, DuD 2010, 448, 449.

1366 Zu den Unterrichtungspflichten der Betreiber sozialer Netzwerke *Hoeren* in: FS Heussen, 2009, S. 208 f.

1367 Vgl. *Iraschko-Luscher/Kiekenbeck*, RDV 2010, 261, 261.

1368 *Iraschko-Luscher/Kiekenbeck*, RDV 2010, 261, 261.

1369 *Iraschko-Luscher/Kiekenbeck*, RDV 2010, 261, 261.

1370 Vgl. *Mainusch/Burtchen*, DuD 2010, 448.

1371 Grundlegend *Heckmann*, K&R 2011, 1; vgl. *Heckmann*, NJW 2012, 2631.

1372 Vgl. *Gierschmann*, MMR 2018, 7 ff.

1373 *Krieg*, K&R 2011, 357; vgl. zur strafrechtlichen Relevanz *Schulte/Kanz*, ZJS 2013, 24.

1374 *Ernst*, NJOZ 2010, 1917.

1375 *Gennen/Kremer*, ITRB 2011, 59, 61; vgl. *Terhaag/Schwarz,* K&R 2012, 377.

© 2019 juris GmbH | www.juris.de

Google Analytics (zu Persönlichkeitsprofilen vgl. auch Rn. 795 ff.). Zur Nutzung des Like-Buttons auf einer Website muss ein iframe oder Javascript von Facebook installiert werden, das zur laufenden Übertragung personenbezogener Daten von Facebook-Nutzern an Facebook führt[1376], die gerade die Website besuchen.[1377] Das Betätigen des Like-Buttons ist jedoch für die Datenübertragung nicht erforderlich.[1378] Ob tatsächlich Daten, wie zum Beispiel IP-Adressen, auch von Nicht-Facebook-Mitgliedern durch das bloße Ansehen der Website an Facebook gesendet werden, ist aufgrund der fehlenden einwandfreien Datenschutzbelehrung bzw. einer eindeutigen Stellungnahme seitens Facebook unklar.[1379]

727 Für eine Verarbeitung sind die **Vorgaben der DSGVO** zu beachten, d.h. es bedarf einer Einwilligung des Betroffenen oder einer gesetzlichen Grundlage. Letztere ist allerdings auch nach Geltungserlangung durch die DSGVO nicht ersichtlich.[1380]

728 Auch eine **Einwilligung** als Verarbeitungsgrundlage scheitert nach der derzeitigen Lösung daran, dass eine vorherige Information des Nutzers über die konkrete und zweckgerichtete Verwendung seiner Daten durch bspw. einen eigenen Link oder ein Pop-Up-Fenster fehlt.[1381] Die Funktionsweise des Like-Buttons wird nicht erläutert. Der Like-Button kann somit nach hier vertretener Auffassung derzeit nicht gesetzeskonform eingesetzt werden.[1382]

729 **Unsicherheit** besteht in diesem Zusammenhang zudem hinsichtlich der Frage, wen die datenschutzrechtliche Verpflichtung eigentlich trifft, den Webseiten-Betreiber oder Facebook. Letztendlich verarbeitet primär Facebook die personenbezogenen Daten, dies wird jedoch erst durch den Webseiten-Betreiber ermöglicht.[1383] Das **KG Berlin**[1384] hat insoweit entschieden, dass neben Facebook auch den Webseiten-Betreiber durch das Einbinden des Like-Buttons eine Informationspflicht trifft.[1385]

730 Das **OLG Düsseldorf** hat in einem Vorlagebeschluss dem EuGH die Frage vorgelegt, ob ein Webseitenbetreiber durch die **Einbindung des „Like-Buttons“** datenschutzrechtlich **verantwortliche Stelle** im Sinne von Art. 2 lit. d RL 95/46/EG ist (vgl. dazu auch Rn. 147 ff.).[1386] Dabei scheint das OLG Düsseldorf ähnlich wie das BVerwG[1387] zur Ablehnung der datenschutzrechtlichen Verantwortlichkeit zu tendieren, indem es darauf hinweist, dass der Einbindende weder einen rechtlichen noch einen tatsächlichen Einfluss auf die Entscheidung hat, wie personenbezogene Daten verarbeitet werden. Zudem mache die Gegenansicht eine derartige Einbindung praktisch unmöglich,

---

1376 Der Besucher kann durch die Verknüpfung mit seinem Facebook-Account eindeutig identifiziert werden, vgl. *Maisch*, AnwZert ITR 19/2010 Anm. 2.

1377 LG Berlin v. 14.03.2011 - 91 O 25/11.

1378 *Ernst*, NJOZ 2010, 1917; *Maisch*, AnwZert ITR 19/2010 Anm. 2.

1379 *Ernst*, NJOZ 2010, 1917; *Maisch*, AnwZert ITR 19/2010 Anm. 2.

1380 Vgl. *Ernst*, NJOZ 2010, 1917, 1919; *Maisch*, AnwZert ITR 19/2010 Anm. 2; vgl. *Schwenke*, WRP 2013, 37.

1381 *Ernst*, NJOZ 2010, 1917, 1919; *Maisch*, AnwZert ITR 19/2010 Anm. 2.

1382 *Ernst*, NJOZ 2010, 1917, 1919; *Maisch*, AnwZert ITR 19/2010 Anm. 2.

1383 *Ernst*, NJOZ 2010, 1917, 1918; *Maisch*, AnwZert ITR 19/2010 Anm. 2.

1384 KG Berlin v. 29.04.2011 - 5 W 88/11.

1385 *Lauge*, DSB 6/2011, 11, 12; *Maisch*, AnwZert ITR 19/2010 Anm. 2.

1386 OLG Düsseldorf v. 19.01.2017 - I-20 U 40/16 - MMR 2017, 254. Das Verfahren ist beim EuGH anhängig unter dem Aktenzeichen C-40/17.

1387 BVerwG v. 25.02.2016 - 1 C 28/14 - ZD 2016, 393.

© 2019 juris GmbH | www.juris.de

denn der hierdurch ausgelöste Datenverarbeitungsvorgang sei für den Einbindenden nicht zu kontrollieren. Diese Auffassung ist allerdings durchaus angreifbar, weshalb bei der Einbindung von Social Plug-ins weiterhin Vorsicht geboten ist;[1388] vgl. dazu umfassend Rn. 144 ff.

731 Eine weitere Vorlagefrage des OLG Düsseldorf behandelt die Problematik, ob in zivilrechtlicher Hinsicht Art. 2 lit. d RL 95/46/EG insofern abschließend ist, als eine **zivilrechtliche Haftung** für von Dritten zu verantwortende Datenschutzverstöße ausgeschlossen ist und die Haftung auf die Verantwortlichen beschränkt ist.[1389] Ansonsten scheint das OLG Düsseldorf eine Haftung des Einbindenden für eventuelle Verstöße von Facebook als „Störer" in Betracht zu ziehen, wie sie das BVerwG bereits angedeutet hatte.[1390]

732 Schließlich ist zu erwähnen, dass der Like-Button auch Raum für cyberkriminelle Straftaten, wie bspw. das **„Clickjacking"** mit Hilfe von Schad-Webseiten, bietet.[1391] Hierbei wird der Nutzer dazu gebracht, auf als „Gefällt mir"-Button maskierte Links zu klicken und dadurch die Attacke über Newsfeeds und Statusupdates an seine gesamte Freundesliste zu schicken.[1392] So kann Schadsoftware bestmöglich verbreitet werden.[1393]

d. Profilbilder

733 Das Erstellen eines Profils in einem sozialen Netzwerk umfasst meist auch das Einstellen eines Profilbildes, das anderen Nutzern beim Aufrufen des Profils angezeigt wird und vergleichbar mit einem Passfoto ist.[1394] Ein Profilbild ist grundsätzlich nicht zwingend erforderlich, jedoch dient es vielen Benutzern der Selbstdarstellung, um vor allem das Interesse anderer an der eigenen Seite zu wecken.

734 Die Verwendung fremder Fotos als Profilbild kann ohne entsprechende Einwilligung der dargestellten Person zu einem **Verstoß gegen die §§ 22, 23 KunstUrhG** führen und Schadensersatz-, Bereicherungs-, Unterlassungs- bzw. Beseitigungsansprüche sowie Auskunfts- und Gegendarstellungsansprüche nach sich ziehen. Eine Ausnahme stellen hier nur Bildnisse der Zeitgeschichte dar, die auch ohne Einwilligung der Betroffenen verbreitet oder öffentlich zur Schau gestellt werden dürfen.[1395] Problematisch kann zudem auch das Einstellen der Abbildungen von Comic- oder Cartoonfiguren sein, denn auch diese sind urheberrechtlich geschützt.[1396] Zudem sind auch Bilder der eigenen Person, die durch Dritte angefertigt wurden, urheberechtlich geschützt, so dass eine Verwendung nach vorheriger Gestattung anzuraten ist.

1388 Vgl. die Anm. *v. Schulte*, K&R 2017, 198, 199.

1389 Vgl. *Degen*, GRUR-Prax 2017, 129.

1390 BVerwG v. 25.02.2016 - 1 C 28/14 - juris Rn. 35 - ZD 2016, 393; vgl. dazu *Martini/Fritzsche*, NVwZ 2015, 1497, 1498.

1391 *Noack*, Deutscher Präventionstag, „Soziale Netzwerke – mehr als eine Kommunikationsplattform. Gefahren bei Facebook, Twitter und Co.", Nr. 26. Abrufbar unter: www.praeventionstag.de/html/GetDokumentation.cms?XID=681 (abgerufen am 28.02.2019); vgl. *Braun/Gemein/Höfling/Maisch/Seidl*, DuD 2012, 502.

1392 *Noack*, Deutscher Präventionstag, „Soziale Netzwerke – mehr als eine Kommunikationsplattform. Gefahren bei Facebook, Twitter und Co.", Nr. 26. Abrufbar unter www.praeventionstag.de/html/GetDokumentation.cms?XID=681 (abgerufen am 28.02.2019); vgl. *Braun/Gemein/Höfling/Maisch/Seidl*, DuD 2012, 502.

1393 *Noack*, Deutscher Präventionstag, „Soziale Netzwerke – mehr als eine Kommunikationsplattform. Gefahren bei Facebook, Twitter und Co.", Nr. 26. Abrufbar unter www.praeventionstag.de/html/GetDokumentation.cms?XID=681 (abgerufen am 28.02.2019); vgl. *Braun/Gemein/Höfling/Maisch/Seidl*, DuD 2012, 502.

1394 Vgl. *Forst*, NZA 2010, 427 ff.; vgl. ferner *Höch/Kadelbach*, WRP 2012, 1060.

1395 *Fuchs/Maisch*, AnwZert ITR 15/2010 Anm. 2.

1396 *Ruttig*, Das Urheberrecht im Profil. Abrufbar unter: www.lto.de/de/html/nachrichten/1991/comicbilder-bei-facebook-das-urheberrecht-im-profil/ (abgerufen am 28.02.2019).

735 Auch das **Verfremden der Bilder** durch Bildbearbeitungsprogramme ist nicht sonderlich hilfreich, denn der Schutz des Urhebers hört erst auf, wenn das ursprüngliche Bild vollständig unerkenntlich ist, was zumeist nicht das Ziel des Nutzers ist und womöglich erst recht zur Verärgerung der tatsächlichen Rechteinhaber führt.[1397]

736 Hierbei ist zudem zu berücksichtigen, dass **Fotografien** als **personenbezogene Daten** im Sinne des Art. 4 Nr. 1 DSGVO zu verstehen sind und damit grundsätzlich sowohl dem Anwendungsbereich des KUG als auch dem der DSGVO unterfallen.[1398] Inwieweit das **KUG neben der DSGVO,** abseits journalistischer Zwecke,[1399] bestehen bleiben wird, ist noch nicht vollständig abzusehen. Voraussichtlich verbleibt dem KUG lediglich ein Anwendungsbereich im Rahmen der Spezifizierungsklausel des Art. 85 DSGVO.[1400] Aber selbst für diesen Fall bietet es sich an, die hinreichend (richterlich) gefestigten Vorgaben des KUG bei der Auslegung der entsprechenden Normen der DSGVO zu berücksichtigen.[1401]

e. Umgang mit Daten Dritter

737 Gerade die amerikanischen Netzwerke berufen sich häufig auf die Notwendigkeit des **Selbstdatenschutzes**[1402] und sehen sich aus der Verantwortung entlassen, wenn willentlich personenbezogene Daten seitens der Nutzer in ihre Datenbanken eingebracht werden[1403]. Eine derartige Betrachtung kann allerdings nicht mit den europäischen Datenschutzvorgaben in Einklang gebracht werden. Die datenschutzrechtliche Verantwortlichkeit ergibt sich eben nicht zwingend daraus, bestimmte datenschutzrechtlich relevante Vorgänge initiiert zu haben, sondern vielmehr aus der Entscheidungsbefugnis über die Zwecke und Mittel der korrespondierenden Verarbeitungsvorgänge. Dergestalt entscheidungsbefugt wird aber in aller Regel allein der Betreiber des jeweiligen Dienstes sein (allgemein zur datenschutzrechtlichen Verantwortlichkeit siehe Rn. 202 ff.).

738 Zudem können sich die Betreiber sozialer Netzwerke nur schwer ihrer Verantwortung entziehen, wenn sie durch entsprechende Funktionen die Einbringung von personenbezogenen Daten Dritter fördern (und fordern). Besonders problematisch sind in diesem Zusammenhang sog. **Friend-Finder-Funktionen,** die den Betreibern sozialer Netzwerke bspw. den Zugriff auf E-Mail-Datenbanken ihrer Nutzer gestatten und somit datenschutzrechtliche Relevanz für Nicht-Mitglieder aufweisen.[1404] Hier lässt sich bereits darüber streiten, wer als datenschutzrechtlich verantwortliche Stelle angesehen werden muss.[1405]

739 In diesem Kontext ist auf die jedenfalls vergleichbare Adressabgleichfunktion des Messenger-Dienstes **WhatsApp** hinzuweisen. Diesbezüglich kommt die Landesbeauftragte für den Datenschutz Niedersachsen (LfD Niedersachsen) zu dem Ergebnis, dass die Übermittlung von Kontaktdaten aus Adressbüchern an WhatsApp in der Regel nicht mit den Vorgaben des Datenschutzrechts

---

1397 *Ruttig*, Das Urheberrecht im Profil. Abrufbar unter: www.lto.de/de/html/nachrichten/1991/comicbilder-bei-facebook-das-urheberrecht-im-profil/ (abgerufen am 28.02.2019).

1398 *Faulhaber/Scheurer*, jM 2019, 2, 3.

1399 Vgl. dazu OLG Köln, v. 18.06.2018 - 15 W 27/18 - ZD 2018, 434, 435.

1400 Ausführlich *Lauber-Rönsberg/Hartlaub*, NJW 2017, 1057 ff.

1401 *Faulhaber/Scheurer*, jM 2019, 2, 3.

1402 *Schnabel/Freund*, CR 2010, 718.

1403 Vgl. *Mainusch/Burtchen*, DuD 2010, 448, 449; zur datenschutzkonformen Gestaltung des Friend-Finding-Verfahrens von Facebook, MMR-Aktuell 2011, 313916.

1404 *Gennen/Kremer*, ITRB 2011, 59, 61 f.; vgl. *Gennen/Kremer*, ITRB 2011, 59.

1405 *Albrecht/Maisch*, Wenn das Leben der Anderen tabu ist. Abrufbar unter: www.lto.de/de/html/nachrichten/3661/datenschutz_in_sozialen_netzwerken_wenn_das_leben_der_anderen_tabu_ist/ (abgerufen am 28.02.2019).

© 2019 juris GmbH | www.juris.de

vereinbar ist.[1406] Wenngleich als Rechtsgrundlage für die Übermittlung der Adressdaten Art. 6 Abs. 1 Satz 1 lit. f DSGVO in Betracht kommt, wird die erforderliche Interessenabwägung jedenfalls dann zu Lasten des App-Nutzers ausfallen, wenn auch Daten solcher Kontakte übermittelt werden, welche den Messenger nicht nutzen.[1407] Die Übermittlung der Adressdaten könnte damit regelmäßig nur auf Grundlage einer Einwilligung der betroffenen Kontakte erfolgen, eine solche wird aber in aller Regel nicht vorab vorliegen.[1408] Erschwerend tritt hinzu, dass bereits die Einwilligungsverweigerung eines einzelnen Kontaktes dazu zwingt, von der Übermittlung des Kontaktadressendatensatzes abzusehen.[1409]

740 Insbesondere für den Fall, dass der Messenger WhatsApp im **betrieblichen Kontext** genutzt werden soll, ist der Zugriff der App auf gespeicherte Kontaktdaten zu unterbinden.[1410] Selbst für diesen, deutlich eingeschränkten, Nutzungsfall kann die Datenschutzkonformität des Messengers aber nicht gewährleistet werden, sodass derzeit letztlich von einer Nutzung zu betrieblichen Zwecken **abgeraten** werden muss.[1411] Es bietet sich der Rückgriff auf anonym nutzbare Messenger, wie etwa Threema an.[1412]

741 Eine vergleichbare datenschutzrechtliche Brisanz weisen aber auch sog. **Tagging-Funktionen** auf. Hier werden Profile verlinkt oder Fotos und Videos mit Markierungen versehen, was den Netzwerkcharakter eines sozialen Netzwerks noch verstärkt.[1413] Solche Anwendungen vertragen sich häufig aber nicht mit einer selbstbestimmten Informationspolitik der betroffenen Dritten, die häufig erst nachträglich erfahren, welche Informationen zu ihrer Person „getaggt" wurden.[1414]

f. Die datenschutzrechtliche Verantwortlichkeit der Diensteanbieter sowie Dritter bei der Nutzung sozialer Netzwerke

742 Grundsätzlich sind gem. Art. 4 Nr. 7 DSGVO die **Betreiber** der sozialen Netzwerke als Verantwortliche Adressaten des Datenschutzrechts und den hieraus folgenden Verpflichtungen (vgl. umfassend zum Verantwortlichen nach den Vorgaben der DSGVO Rn. 202 ff.).[1415] Eine Zuweisung der datenschutzrechtlichen Verantwortung an die **Nutzer** wird unter Berücksichtigung auf den in Art. 2 Abs. 2 lit. c DSGVO geregelten Ausschluss des sachlichen Anwendungsbereichs der DSGVO bei Nutzung der Daten für persönliche oder familiäre Belange **grundsätzlich abgelehnt** (vgl. dazu auch Rn. 169).[1416]

[1406] Die Landesbeauftragte für den Datenschutz Niedersachsen, Merkblatt für die Nutzung von „WhatsApp" in Unternehmen, S. 2. Abrufbar unter: www.lfd.niedersachsen.de/startseite/themen/wirtschaft/nutzung_von_whatsapp_im_unternehmen/merkblatt-fuer-die-nutzung-von-whatsapp-in-unternehmen-166297.html (abgerufen am 28.02.2019).

[1407] Die Landesbeauftragte für den Datenschutz Niedersachsen, Merkblatt für die Nutzung von „WhatsApp" in Unternehmen, S. 2.

[1408] Die Landesbeauftragte für den Datenschutz Niedersachsen, Merkblatt für die Nutzung von „WhatsApp" in Unternehmen, S. 2.

[1409] Die Landesbeauftragte für den Datenschutz Niedersachsen, Merkblatt für die Nutzung von „WhatsApp" in Unternehmen, S. 2.

[1410] Die Landesbeauftragte für den Datenschutz Niedersachsen, Merkblatt für die Nutzung von „WhatsApp" in Unternehmen, S. 3.

[1411] So im Ergebnis auch die Landesbeauftragte für den Datenschutz Niedersachsen, Merkblatt für die Nutzung von „WhatsApp" in Unternehmen, S. 2 ff; so auch *Faas*, ArbRAktuell 2018, 594, 596.

[1412] *Faas*, ArbRAktuell 2018, 594, 596.

[1413] Telemedicus, Datenschutz und Datensicherheit in sozialen Netzwerken. Abrufbar unter: www.telemedicus.info/article/1806-Datenschutz-und-Datensicherheit-in-sozialen-Netzwerken.html (abgerufen am 28.02.2019).

[1414] Mit der Forderung, auch private Personen zur datenschutzrechtlich verantwortlichen Stelle zu erklären, www.telemedicus.info/article/1806-Datenschutz-und-Datensicherheit-in-sozialen-Netzwerken.html (abgerufen am 28.02.2019).

[1415] Vgl. dazu jüngst EuGH v. 05.06.2018 - C-210/16 - ECLI:EU:C:2018:388 = EuZW 2018, 534, 536 Rn. 30.

[1416] *Kühling/Raab* in: Kühling/Buchner, DS-GVO/BDSG, Art. 2 DSGVO Rn. 24.

743 Erwägungsgrund 18 der DSGVO postuliert hierfür den **vollständig fehlenden Bezug**[1417] zu einer **beruflichen oder wirtschaftlichen Tätigkeit** und nennt einige Beispiele, etwa das Führen des Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten. Eine Beschränkung auf private Kontakte ist dabei nicht vorzunehmen.[1418] Wirtschaftliche und berufliche Tätigkeiten sind nicht abhängig davon, ob eine Gewinnerzielung(sabsicht) oder Selbstständigkeit vorliegt.[1419] Auch die Verarbeitung im Rahmen eines Ehrenamts (z.B. Verein/Kommunen) ist nicht von der Ausnahme umfasst.[1420]

744 **Verantwortliche oder Auftragsverarbeiter,** die die Instrumente für die Verarbeitung zur Verfügung stellen, werden indes von der Ausnahmeregelung nicht umfasst.[1421]

745 Wie auch nach den Vorgaben des BDSG a.F. beziehungsweise des TMG bereitet die **familiäre Datennutzung mit Öffentlichkeitsbezug Abgrenzungsprobleme.**[1422] Ob die in Erwägungsgrund 18 genannte Nutzung sozialer Netze vollumfänglich dem Ausschluss unterfällt, ist fraglich und abzulehnen.[1423] Der EuGH hat insoweit auf das Kriterium des **unbestimmten Personenkreises** abgestellt, an welchen die Informationen gerichtet sind.[1424] Eine Änderung der diesbezüglichen Rechtslage war mit der DSGVO nicht bezweckt.[1425]

746 Eine **vergleichbare Problematik** weist beispielsweise die **Videoüberwachung** auf, wenn diese dergestalt erfolgt, dass auch öffentliche Räume erfasst werden (allgemein zur Videoüberwachung unter Rn. 841 ff.).[1426] Werden ausschließlich nichtöffentliche Bereiche erfasst und erfolgt die Verarbeitung zu privaten Zwecken wie dem Schutz der Wohnung, liegt es nahe, den Tatbestand des Art. 2 Abs. 2 lit. c DSGVO hierauf zu erstrecken.[1427] Selbiges gilt für die in den letzten Jahren aufkommende Problematik der Dashcams im Straßenverkehr[1428], die jedoch bereits aufgrund ihres Verwendungszwecks nicht unter den Ausnahmetatbestand fallen.[1429]

g. Die Datenschutzerklärung

747 Hinsichtlich der für die Nutzung sozialer Netzwerke verwendeten Datenschutzerklärungen wird häufig deren **mangelnde Transparenz** moniert.[1430] So sieht sich bspw. bezüglich der Datenschutzrichtlinien von Facebook *Erd* veranlasst, diesen „schon allein wegen des äußeren Erscheinungsbilds die Rechtswidrigkeit zu bescheinigen".[1431] Vor dem Hintergrund der Anforderungen der DSGVO

1417 Zur Kritik an dieser Einschränkung *Kühling/Raab* in: Kühling/Buchner, DS-GVO/BDSG, Art. 2 DSGVO Rn. 28.

1418 *Kühling/Raab* in: Kühling/Buchner, DS-GVO/BDSG, Art. 2 DSGVO Rn. 24.

1419 *Kühling/Raab* in: Kühling/Buchner, DS-GVO/BDSG, Art. 2 DSGVO Rn. 26.

1420 EuGH v. 06.11.2003 - C-101/01 - juris Rn. 45 - ECLI:EU:C:2003:596; *Kühling/Raab* in: Kühling/Buchner, DS-GVO/BDSG, Art. 2 DSGVO Rn. 26; *Schantz* in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 314; *Gola/Lepperhoff*, ZD 2016, 9, 10.

1421 *Kühling/Raab* in: Kühling/Buchner, DS-GVO/BDSG, Art. 2 DSGVO Rn. 25.

1422 Vgl. EuGH v. 06.11.2003 - C-101/01 - juris Rn. 47 - ECLI:EU:C:2003:596; *Kühling/Raab* in: Kühling/Buchner, DS-GVO/BDSG, Art. 2 DSGVO Rn. 25.

1423 *Schantz*, NJW 2016, 1841, 1843; *Kühling/Raab* in: Kühling/Buchner, DS-GVO/BDSG, Art. 2 DSGVO Rn. 25.

1424 EuGH v 06.11.2003 - C-101/01 - juris Rn. 47 - ECLI:EU:C:2003:596; *Kühling/Raab* in: Kühling/Buchner, DS-GVO/BDSG, Art. 2 DSGVO Rn. 25.

1425 *Kühling/Raab* in: Kühling/Buchner, DS-GVO/BDSG, Art. 2 DSGVO Rn. 25.

1426 EuGH v. 11.12.2014 - C-212/13 - juris Rn. 33 - ECLI:EU:C:2014:2428; *Kühling/Raab* in: Kühling/Buchner, DS-GVO/BDSG, Art. 2 DSGVO Rn. 27.

1427 Vgl. *Kühling/Raab* in: Kühling/Buchner, DS-GVO/BDSG, Art. 2 DSGVO Rn. 27.

1428 *Kühling/Raab* in: Kühling/Buchner, DS-GVO/BDSG, Art. 2 DSGVO Rn. 27.

1429 Weiterführend dazu *Starnecker* in: Gola/Heckmann, BDSG, § 4 Rn. 18.

1430 Vgl. *Erd* in: Taeger, Digitale Evolution – Herausforderungen für das Informations- und Medienrecht, 2010, S. 259; zu den Nutzungsbedingungen *Härting/Schätzle*, ITRB 2011, 40.

1431 *Erd* in: Taeger, Digitale Evolution – Herausforderungen für das Informations- und Medienrecht, 2010, S. 259.

© 2019 juris GmbH | www.juris.de

in Sachen Einfachheit, Transparenz, Verständlichkeit und Zugänglichkeit (vgl. dazu Rn. 352 ff.) ist davon auszugehen, dass die derzeitigen Datenschutzbestimmungen sozialer Netzwerke nicht mit den Vorgaben des Datenschutzrechts übereinstimmen.

748 Darüber hinaus verbleibt die Problematik, dass entsprechende Datenschutzerklärungen seitens der **Nutzer oftmals (bewusst) nicht zur Kenntnis** genommen werden.[1432] In diesem Zusammenhang stellt sich die Frage, ob über das Bereitstellen der erforderlichen Informationen eine **Pflicht zur entsprechend (didaktischen) Aufbereitung** besteht. Mithin spricht auf Grundlage der novellierten datenschutzrechtlichen Transparenzvorgaben vieles dafür, dass es nicht nur auf das „ob" der Informationserteilung, sondern insbesondere auch auf das „wie" der Informationsaufbereitung ankommt, um dem letztlich intendierten Versprechen grundrechtlicher Selbstbestimmung zu genügen.

749 Unabhängig von Struktur und Erscheinungsbild dienen die seitens der Betreiber sozialer Netzwerke verwendeten Datenschutzerklärungen meist dazu, die **Einwilligung** der Mitglieder[1433] in umfangreiche Datenverarbeitungsprozesse zu dokumentieren[1434]. Die Wirksamkeit der Einwilligung setzt gem. Art. 4 Nr. 11 DSGVO eine freiwillige in informierter Weise abgegebene Willensbekundung des Betroffenen voraus. Eine Einwilligungserklärung muss demnach auch hinsichtlich ihrer **Strukturierung nachvollziehbar aufgebaut werden.** Als vorteilhaft wird bspw. eine Untergliederung der Datenschutzerklärung nach den technischen Gegebenheiten empfohlen.[1435] In inhaltlicher Hinsicht bedeutet dies, „dass dem Nutzer klar werden muss, welche Daten z.B. bei bloßem ‚Surfen' und welche Daten nach z.B. einer möglichen Registrierung (in einem Web-Shop, Forum etc.) erhoben und verarbeitet werden" (umfassend zu den Anforderungen an den Einwilligungsprozess unter Rn. 259 ff.).[1436]

h. Google Analytics

750 Bei Google Analytics handelt es sich um ein unentgeltliches Programm des Konzerns Google, das Webseitenbetreibern dient, das Verhalten der Webseitennutzer mittels statistischer Auswertungsergebnisse zu analysieren.[1437] Hintergrund dieses Angebots ist, dass Werbetreibende präzisere Berichte erhalten, wie Besucher auf ihre Werbung auf bestimmten Webseiten reagieren.[1438] Mithin lässt sich auf Grundlage einer solchen Webanalyse letztlich der Erfolg einer bestimmten Webseite messen.[1439]

751 **Problematisch** ist dabei vor allem, dass Google die erlangten Nutzungsdaten unter anderem auch für weitere eigene Auswertungen nutzen könnte. Der Einsatz von Google Analytics kann u.a. zur Folge haben, dass die Anonymität des Nutzers sozialer Netzwerke (soweit eine solche gegeben ist) zusätzlichen Bedrohungen ausgesetzt ist.[1440] Auch im Hinblick auf die mangelhafte

---

1432 Vgl. dazu *Buchner/Rothmann*, DuD 2018, 342, 344.

1433 Allgemein zur datenschutzrechtlichen Einwilligung *Buchner*, DuD 2010, 39; *Menzel*, DuD 2008, 400; *Iraschko-Luscher*, DuD 2006, 706.

1434 Vgl. *Wintermeier*, ZD 2013, 21, 22; *Conrad/Hausen* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 36 Rn. 128.

1435 *Wintermeier*, ZD 2013, 21, 22.

1436 *Wintermeier*, ZD 2013, 21, 22.

1437 Vgl. *Lepperhoff/Petersdorf*, DuD 2008, 266, 267; vgl. *Lepperhoff/Petersdorf/Thursch*, DuD 2013, 301; vgl. auch *Schleipfer*, ZD 2017, 460 ff.

1438 Vgl. *Lepperhoff/Petersdorf*, DuD 2008, 266, 267; vgl. *Lepperhoff/Petersdorf/Thursch*, DuD 2013, 301; *Schleipfer*, ZD 2017, 460, 461.

1439 Vgl. dazu *Schleipfer*, ZD 2017, 460, 461.

1440 *Hoeren*, ZRP 2010, 251.

© 2019 juris GmbH | www.juris.de

Umsetzung des Widerspruchsrechts und der fehlenden Beachtung der Vorgaben zur Auftragsverarbeitung scheint der Einsatz von Google Analytics – ungeachtet der weiten Verbreitung – aus datenschutzrechtlicher Sicht äußerst problematisch.[1441]

752 Der Einsatz von Google Analytics sollte daher wohlüberlegt sein. Mit Blick auf die Vorgaben der DSGVO hat die DSK festgehalten, dass der datenschutzkonforme Einsatz von **Tracking-Mechanismen,** die das Verhalten der Betroffenen im Internet nachvollziehbar machen, grundsätzlich von der **Einwilligung** der betroffenen Person abhängig ist.[1442] Unabhängig davon, ob das Tracking beispielsweise pseudonymisiert erfolgt, geht die Konferenz der unabhängigen Datenschutzbehörden also davon aus, dass der Einsatz etwaiger Tracking-Mechanismen, also auch der Einsatz von Google Analytics, nur auf Grundlage einer Einwilligung rechtmäßig ist.[1443]

i. Geolokalisation

753 Mit Hilfe einiger Dienste wie beispielsweise „Foursquare" kann der **Standort** einer Person leicht und schnell ausfindig gemacht werden. Die Ortung erfolgt dabei z.B. über die IP-Adresse oder über ein eingebautes GPS-Modul, durch das der Standort bis auf wenige Meter genau angegeben werden kann.[1444] So können der betreffenden Person **Informationen über ihre Umgebung** zugeschickt werden.

754 Auch in sozialen Netzwerken tritt das Phänomen der Geolokalisation immer häufiger auf.[1445] Bereits im Jahre 2010 hat Facebook ein Patent für die Geolokalisation erhalten, das jetzt unter dem Namen „Facebook Places" bekannt ist. Standortbasierte Statusmeldungen, sog. „Check-Ins", können auf diese Weise empfangen, versendet und auch gespeichert werden.[1446] Facebook-Nutzer schreiben ihren Freunden ihren Aufenthaltsort und sie erfahren, wer sich gerade noch an diesem Ort befindet. Dadurch können Bewegungsprofile der einzelnen Personen erstellt werden. Die Standortdaten können jedoch auch Unternehmen vermittelt werden. Diese nutzen die Geolokalisation zur Kundenbindung, versprechen kleine Auszeichnungen und Gewinne oder verschicken gezielt Werbung.[1447]

755 **Problematisch** ist hier, dass in der Vergangenheit die Standardeinstellungen der Privatsphäre bei Facebook nur geringen Schutz bieten und die Nutzer die Risiken oft nicht erkannten. So kann aufgrund falscher Privatsphäre-Einstellungen der Standort z.B. auch der Allgemeinheit zugänglich gemacht werden, wodurch die Gefahr von Einbrüchen oder Überfällen erhöht wird. Es bleibt abzuwarten, inwieweit Art. 25 DSGVO und die Vorgaben der ePVO Facebook zu datenschutzfreundlicheren Voreinstellungen bewegen wird.

1441 *Huth*, AnwZert ITR 12/2011 Anm. 2.

1442 Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder v. 26.04.2018, Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, S. 3. Abrufbar unter: www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf (abgerufen am 28.02.2019).

1443 Vgl. dazu auch GDD, Stellungnahme zur Position der Datenschutzkonferenz. Abrufbar unter: www.gdd.de/aktuelles/startseite/zulaessigkeit-des-tracking-nach-der-ds-gvo (abgerufen am 28.02.2019).

1444 Ausführlich zu der Technik *Hoeren*, ZfWG 2008, 229 ff.

1445 Vgl. *Koch*, ITRB 2011, 158.

1446 McCarthy/Kaden, Facebook erhält Patent auf Geolokalisierung. Abrufbar unter: www.zdnet.de/news/41538851/facebook-erhaelt-patent-auf-geolokalisierung.htm (abgerufen am 28.02.2019).

1447 *Strack*, Geolokalisierung: Kundenbindung in sozialen Netzwerken. Abrufbar unter: www.experto.de/b2b/existenzgruendung/startup/geolokalisierung-kundenbindung-in-sozialen-netzwerken.html (abgerufen am 28.02.2019).

© 2019 juris GmbH | www.juris.de

756 Inwieweit diese Informationen über den Aufenthaltsort dem **Datenschutz** unterfallen, ist fraglich.[1448] Diskutiert wird bereits, ob es sich stets um personenbezogene Daten handelt, da die Ortung mit Hilfe der IP-Adresse oder des GPS-Systems nicht zweifelsfrei einer bestimmten Person zugeordnet werden kann (allgemein zur Frage der Identifizierbarkeit einer Person Rn. 112 ff.). Es besteht nämlich die Möglichkeit, dass z.B. auch Dritte entsprechende Endgeräte nutzen. Werden die Daten dagegen bei einem persönlichen Login-Vorgang erhoben, bei dem der Nutzer mit seiner Kennung und seinem Passwort auftritt, so lässt sich die Person mit ausreichender Wahrscheinlichkeit identifizieren. Es handelt sich somit regelmäßig um personenbezogene Daten, zu deren Verwendung die **Einwilligung** des Betroffenen erforderlich ist.[1449]

j. Gesichtserkennung

757 Mitte 2011 führte Facebook als erstes soziales Netzwerk europaweit eine automatische Gesichtserkennung für Fotos ein[1450] und zog so den Argwohn der Datenschützer auf sich[1451]. Die neue Anwendung prüfte bereits vorhandene andere Fotos auf Übereinstimmungen mit von Mitgliedern neu in das Netzwerk hochgeladenen Fotos und schlug dann „passende" Namen aus dem Facebook-Freundeskreis zur Verknüpfung vor. Die Funktion **war standardmäßig aktiviert**[1452] und konnte auch unter den Privatsphäre-Einstellungen von Facebook nicht abgeschaltet werden.[1453] Wenngleich die Gesichtserkennungstechnologien bei großen Datenmengen noch störungsanfällig sind, muss in absehbarer Zeit mit einer erheblichen Effizienzsteigerung gerechnet werden.[1454]

758 Obgleich Facebook zunächst ungeachtet der datenschutzrechtlichen Bedenken am Einsatz der Gesichtserkennungssoftware festhielt und sich insoweit auf die (ausschließliche) Geltung des irischen Rechts berief[1455], blieben deutsche Datenschutzbehörden nicht untätig. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Caspar[1456] erließ am 21.09.2012 gegenüber Facebook eine **Verwaltungsanordnung,** welche das Unternehmen dazu verpflichtete, die Gesichtserkennung auch rückwirkend datenschutzkonform zu gestalten und sicherzustellen, dass nur mit der aktiven Zustimmung der bereits registrierten Nutzer biometrische Profile erzeugt und dauerhaft gespeichert werden.[1457] Daraufhin hat sich Facebook entschieden, die Gesichtserkennung

---

[1448] Vgl. *Backu*, ITRB 2009, 88 ff.

[1449] Vgl. dazu etwa *Oettinger*, Geolokalisierung und Datenschutz. Sind die Daten personenbezogen oder nicht? Abrufbar unter www.computerwoche.de/management/compliance-recht/2359764/ (abgerufen am 28.02.2019).

[1450] Zur Bedrohung der informationellen Selbstbestimmung durch im staatlichen Einsatz befindliche „Smart Cameras" *Hornung/Desoi*, K&R 2011, 153; vgl. hierzu ferner *Karg*, HumFoR 2012, 120.

[1451] *Heuer*, Datenschützer warnen vor flächendeckender Gesichtserkennung. Abrufbar unter: www.heise.de/newsticker/meldung/Datenschuetzer-warnen-vor-flaechendeckender-Gesichtserkennung-1269926.html (abgerufen am 28.02.2019).

[1452] *Bohnensteffen/Fuest*, Gesichtserkennung ist nicht nur auf Facebook üblich. Abrufbar unter: www.welt.de/wirtschaft/webwelt/article13426306/Gesichtserkennung-ist-nicht-nur-auf-Facebook-ueblich.html (abgerufen am 28.02.2019).

[1453] Stiftung Warentest, Soziale Netzwerke: Facebook lernt Gesichtserkennung. Abrufbar unter: www.test.de/themen/computer-telefon/meldung/Soziale-Netzwerke-Facebook-lernt-Gesichtserkennung-4247075-4247077/ (abgerufen am 28.02.2019).

[1454] *Hornung/Desoi*, K&R 2011, 153, 154.

[1455] Stiftung Warentest, Soziale Netzwerke: Facebook lernt Gesichtserkennung. Abrufbar unter www.test.de/themen/computer-telefon/meldung/Soziale-Netzwerke-Facebook-lernt-Gesichtserkennung-4247075-4247077/ (abgerufen am 28.02.2019).

[1456] www.datenschutz-hamburg.de/wir-ueber-uns-kontakt/prof-dr-johannes-caspar.html (abgerufen am 28.02.2019).

[1457] https://ebibliothek.beck.de/Print/CurrentDoc?vpath=bibdata/reddok/becklink/1022602.htm&printdialogmode=CurrentDoc&hlword= (abgerufen am 28.02.2019); Gleiches gilt nunmehr auch für die automatisierte Gesichtserkennung durch die Hamburger Polizei; https://datenschutz-hamburg.de/pressemitteilungen/2018/08/2018-09-31-polhh-g20-videmo360 (zuletzt abgerufen am 28.02.2019).

© 2019 juris GmbH | www.juris.de

für alle europäischen Mitglieder zu deaktivieren.[1458] Alle zuvor erhobenen biometrischen Daten wurden zwischenzeitig gelöscht.[1459] Die gegenüber Facebook erlassene Verwaltungsanordnung wurde anschließend aufgehoben.[1460]

759 Im Rahmen der Umstellung auf die Neuerungen der DSGVO (und während des „Datenskandals“[1461]) hat Facebook schließlich im **April 2018** die **Gesichtserkennung** auch in Europa **(wieder) aktiviert.**[1462] Facebook begründet die Aktivierung insbesondere damit, dass die Gesichtserkennung ein Mehr an Kontrolle und Verwendung der entsprechenden Bilder bieten kann.[1463] Auch soll so dem Identitätsdiebstahl vorgebeugt werden können, indem Fake-Profile, die Bilder eines anderen gebrauchen, entlarvt werden können.[1464] Zumindest setzt Facebook im Rahmen der Wiedereinführung auf die Einwilligung der Nutzer.[1465] Zudem beginnen auch die Sicherheitsbehörden damit, die Gesichtserkennung zur Gefahrenabwehr heranzuziehen (vgl. dazu Rn. 872).

760 Die DSGVO untersagt die Verarbeitung von biometrischen Daten als besonders schutzwürdige Kategorien von personenbezogenen Daten grundsätzlich und gestattet sie nur in den in Art. 9 Abs. 2 DSGVO besonders normierten Ausnahmefällen (allgemein zu besonderen personenbezogenen Daten vgl. Rn. 115 ff.). So kann eine ausdrückliche freiwillige und informierte Einwilligung des Nutzers eine entsprechende Verarbeitung gestatten, vgl. Art. 9 Abs. 2 lit. a DSGVO. Zudem ist eine Verarbeitung zulässig, wenn die betroffene Person diese Daten offensichtlich öffentlich gemacht hat, Art. 9 Abs. 2 lit. e DSGVO. Da entsprechende Social Media-Profile nach Art. 25 DSGVO über datenschutzfreundliche Voreinstellungen verfügen müssen, kann nur eine entsprechende ausdrückliche Einstellungsänderung durch den Nutzer zu einer offensichtlichen öffentlichen Zugänglichmachung führen.

k. Datenübermittlung an Dritte

761 Auch die Übermittlung von personenbezogenen Daten aus sozialen Netzwerken bedarf einer gesetzlichen Rechtsgrundlage bzw. der (einzelfallbezogenen) Einwilligung der Betroffenen. Aus datenschutzrechtlicher Sicht sind insbesondere die in der Vergangenheit durch die Netzwerke genutzten pauschal gehaltenen Vereinbarungen zur Weitergabe von personenbezogenen Daten an Dritte als unwirksam anzusehen (zu den Anforderungen der datenschutzrechtlichen Einwilligung

---

1458 Zeit Online, Facebook hat alle Daten aus Gesichtserkennung gelöscht. Abrufbar unter: www.zeit.de/digital/datenschutz/2013-02/facebook-gesichtserkennung-verfahren-caspar (abgerufen am 28.02.2019).

1459 Zeit Online, Facebook hat alle Daten aus Gesichtserkennung gelöscht.

1460 Zeit Online, Facebook hat alle Daten aus Gesichtserkennung gelöscht.

1461 Vgl. dazu *Brühl/Hauck/Hurtz*, Was ist eigentlich bei Facebook los? Abrufbar unter: www.sueddeutsche.de/digital/datenmissbrauch-was-ist-eigentlich-gerade-bei-facebook-los-1.3932349 (abgerufen am 28.02.2019).

1462 Vgl. *Drösser*, Diese Facebook-Einstellung müssen Sie beachten. Abrufbar unter: www.zeit.de/digital/datenschutz/2018-04/datenschutz-facebook-dsgvo-aenderungen-datenmissbrauch (abgerufen am 28.02.2019); *Dachwitz*, Facebook nutzt Anpassung an Datenschutzgrundverordnung, um Gesichtserkennung auch in Europa zu starten. Abrufbar unter: www.netzpolitik.org/2018/facebook-nutzt-anpassung-an-datenschutzgrundverordnung-um-gesichtserkennung-auch-in-europa-zu-starten/ (abgerufen am 28.02.2019).

1463 *Lido*, Facebook: Gesichtserkennung rollt nun auch in Deutschland aus. Abrufbar unter: www.curved.de/news/facebook-gesichtserkennung-rollt-nun-auch-in-deutschland-aus-600562 (abgerufen am 28.02.2019).

1464 *Drösser*, Diese Facebook-Einstellung müssen Sie beachten. Abrufbar unter: www.zeit.de/digital/datenschutz/2018-04/datenschutz-facebook-dsgvo-aenderungen-datenmissbrauch (abgerufen am 28.02.2019).

1465 *Dachwitz*, Facebook nutzt Anpassung an Datenschutzgrundverordnung, um Gesichtserkennung auch in Europa zu starten. Abrufbar unter: www.netzpolitik.org/2018/facebook-nutzt-anpassung-an-datenschutzgrundverordnung-um-gesichtserkennung-auch-in-europa-zu-starten/ (abgerufen am 28.02.2019).

© 2019 juris GmbH | www.juris.de

vgl. Rn. 259 ff.).[1466] Die bisher beispielsweise von Facebook verwendeten Einwilligungen werden daher als intransparent und unbestimmt gewertet,[1467] insbesondere da eine granulare Einwilligung bisher nicht vorgesehen ist.

762 Mögliche Ermächtigungsnormen hängen von der jeweiligen Datenverarbeitung im Rahmen des sozialen Netzwerkes ab. Werden beispielsweise Produkte über ein soziales Netzwerk erworben und in diesem Kontext personenbezogene Daten zur Vertragsabwicklung an das involvierte Finanzinstitut oder den Verkäufer übermittelt, ergibt sich die gesetzliche Gestattung hierfür über **Art. 6 Abs. 1 Satz 1 lit. b DSGVO.**

763 Hinsichtlich der weiteren Datenübermittlung in Europa kann teilweise auf **Art. 6 Abs. 1 Satz 1 lit. f DSGVO** zurückgegriffen werden, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Erhalten beispielsweise spezielle IT-Sicherheitsunternehmen einen Zugriff auf die Daten, um die Datensicherheit im Unternehmen zu erhöhen, sind die Grundrechte der betroffenen Person nur marginal berührt, da IT- und Datensicherheit auch für sie von Bedeutung sind und ein Missbrauch der Daten durch Dritte auf diese Weise verhindert wird.

764 Auch die Übermittlung der Daten eines europäischen sozialen Netzwerks an (Mutter-)Unternehmen in **Drittländern** bedarf der datenschutzrechtlichen Rechtfertigung, da es kein wirkliches Konzernprivileg im europäischen Datenschutzrecht gibt. Facebook beruft sich hierbei inzwischen insbesondere auf **Standardvertragsklauseln** und „[verlässt] sich […] für Datenübermittlungen aus dem EWR in die USA und andere Länder ggf. auf die von der Europäischen Kommission erlassenen **Angemessenheitsbeschlüsse** bezüglich bestimmter Länder."[1468] Dies scheint auf den ersten Blick wenig transparent. Zudem stehen die Standardvertragsklauseln in der Kritik und werden derzeit genau wie das Privacy Shield vor dem EuGH geprüft.[1469]

765 Datenschutzrechtliche Vorgaben werden in diesem Kontext seitens der Betreiber sozialer Netzwerke oft wirtschaftlichen Interessen untergeordnet. Insbesondere bei Facebook herrschte in der Vergangenheit ein Verständnis vor, das die datenschutzrechtliche Verantwortung schwerpunktmäßig seinen Nutzern auferlegt und sich somit mit den europäischen datenschutzrechtlichen Bestimmungen nur schwer in Einklang bringen lässt.[1470] Es bleibt abzuwarten, inwieweit sich diese Einstellung auch nach Geltungserlangung der DSGVO fortsetzt.

I. Fanseiten

aa. Allgemeines

766 Soziale Netzwerke bieten Unternehmen, gemeinnützigen Einrichtungen, Künstlern und Prominenten **spezielle Benutzeraccounts** (sog. Fanseiten) an, die im Interesse der Öffentlichkeitsarbeit eingerichtet werden können. Davon machen auch – wenngleich mit rechtlichen Einschränkungen – Behörden Gebrauch.[1471]

[1466] Vgl. *Fox*, DuD 2009, 53; zur Problematik der Übermittlung von Nutzerdaten an andere Nutzer sozialer Netzwerke *Hoeren* in: FS Heussen, 2009, S. 212.

[1467] Vgl. *Buchner/Rothmann*, DuD 2018, 342, 344; *Graf von Westphalen*, VuR 2017, 323, 323 ff.; LG Berlin v. 28.10.2014 - 16 O 60/13 - ZD 2015, 133.

[1468] Facebook, Datenschutzrichtlinie – Wie verarbeiten und übermitteln wir Daten im Rahmen unserer globalen Dienste? Abrufbar unter: https://de-de.facebook.com/policy.php (abgerufen am 28.02.2019).

[1469] *Dachwitz*, Schrems gegen Facebook: EuGH wird auch Privacy Shield prüfen. Abrufbar unter: https://netzpolitik.org/2018/schrems-gegen-facebook-eugh-wird-auch-privacy-shield-pruefen/ (abgerufen am 28.02.2019).

[1470] *Erd* in: Taeger, Digitale Evolution – Herausforderungen für das Informations- und Medienrecht, 2010, S. 264 f.

[1471] Zu Behörden-Fanseiten in sozialen Medien vgl. *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 ff.; *Zilkens/Cavin*, ZD 2013, 603 ff.

© 2019 juris GmbH | www.juris.de

bb. Die Problematik der datenschutzrechtlichen Verantwortlichkeit bei dem Betrieb einer Facebook-Fanpage

767 **(1) Grundlagen und Problemaufriss:** Bei Facebook muss sich derjenige, der eine Fanseite einrichten möchte, zunächst registrieren. Hiernach kann er die **von Facebook unterhaltene Plattform** dazu nutzen, **sich (nicht nur) den Nutzern dieser Plattform zu präsentieren** und Äußerungen aller Art in den Medien- und Meinungsmarkt einzubringen.[1472] Nutzer der Plattform können eigene Beiträge auf der Plattform posten. Die technischen Abläufe beim Aufruf einer Fanpage bei Facebook durch einen Nutzer (sog. Facebook-Mitglieder) sind danach zu differenzieren, ob der Nutzer ein Nicht-Facebook-Mitglied ist oder als Facebook-Mitglied beim Besuch der Fanpage gerade als solches eingeloggt ist oder nicht.[1473] In jedem Fall werden hierbei IP-Adressen übertragen und Cookies bei den Nutzern gesetzt.[1474]

768 Das **unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD)** hat sich in einigen vor dem VG Schleswig geführten Musterverfahren[1475] u.a. darauf berufen, dass beim Aufruf der Fanseiten Angaben über die Nutzung der Fanseite durch Facebook-Mitglieder und -Nichtmitglieder in rechtswidriger Weise in die USA an Facebook übermittelt würden. Aufgrund dieses Umstandes wurde von dort die Deaktivierung der Fanseiten angeordnet. Die Betreiber der Fanseiten wandten sich gegen die Deaktivierungsverfügung und verwiesen u.a. darauf, dass sie insoweit nicht als verantwortliche Stellen i.S.d. § 3 Abs. 7 BDSG a.F. herangezogen werden könnten.

769 Das **VG Schleswig** hat entschieden, dass eine datenschutzrechtliche (Mit-)**Verantwortlichkeit** der **Fanseitenbetreiber** für die mit der Eröffnung einer Fanpage ausgelösten Vorgänge der Erhebung, Verwendung und Verarbeitung personenbezogener Daten von Nutzern der Fanpage durch Facebook **zu verneinen ist.**[1476] Der Betreiber einer Fanseite dürfte zwar als Diensteanbieter i.S.d. § 2 Satz 1 Nr. 1 TMG, wonach Diensteanbieter jede natürliche oder juristische Person ist, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt, anzusehen sein, jedoch fehle den Betreibern einer Fanseite die datenschutzrechtliche (Mit-)Verantwortlichkeit für die durch den Besuch einer solchen Seite ausgelöste Erhebung, Verwendung und Verarbeitung personenbezogener Daten durch Facebook.[1477] Die Betreiber einer Fanseite seien folglich nicht verantwortliche Stelle i.S.d. § 3 Abs. 7 BDSG a.F. Zudem sei eine Verantwortlichkeit der Betreiber einer Fanseite im Rahmen einer Auftragsdatenverarbeitung ausgeschlossen.[1478] Im Übrigen sei auch eine Störer- oder zivilrechtliche Haftung abzulehnen.[1479]

770 Das **OVG Schleswig** hat sich als Berufungsgericht dem VG Schleswig hinsichtlich des § 3 Abs. 7 BDSG a.F. **angeschlossen**[1480] und ergänzend angeführt, die ULD habe das gestufte Verfahren nach § 38 Abs. 5 BDSG a.F. nicht eingehalten[1481]. Die unvermittelte Anordnung der Deaktivierung

---

1472 VG Schleswig v. 09.10.2013 - 8 A 218/11 - juris Rn. 3 mit Anm. *Albrecht*, jurisPR-ITR 24/2013 Anm. 6; vgl. *Rosenbaum/Tölle,* MMR 2013, 209.

1473 Eine Darstellung der technischen Abläufe findet sich bei VG Schleswig v. 09.10.2013 - 8 A 218/11 - juris Rn. 4 ff. mit Anm. *Albrecht*, jurisPR-ITR 24/2013 Anm. 6.

1474 Ausführlich hierzu *Luch*, www.landtag.ltsh.de/infothek/wahl17/umdrucke/2900/umdruck-17-2988.pdf (abgerufen am 28.02.2019).

1475 VG Schleswig v. 09.10.2013 - 8 A 218/11 - juris Rn. 11 mit Anm. *Albrecht*, jurisPR-ITR 24/2013 Anm. 6; VG Schleswig v. 09.10.2013 - 8 A 14/12; VG Schleswig v. 09.10.2013 - 8 A 37/12.

1476 VG Schleswig v. 09.10.2013 - 8 A 218/11 - juris Rn. 59 mit Anm. *Albrecht*, jurisPR-ITR 24/2013 Anm. 6.

1477 VG Schleswig v. 09.10.2013 - 8 A 218/11 - juris Rn. 62 mit Anm. *Albrecht*, jurisPR-ITR 24/2013 Anm. 6.

1478 VG Schleswig v. 09.10.2013 - 8 A 218/11 - juris Rn. 63 mit Anm. *Albrecht*, jurisPR-ITR 24/2013 Anm. 6.

1479 VG Schleswig v. 09.10.2013 - 8 A 218/11 - juris Rn. 91 f. mit Anm. *Albrecht*, jurisPR-ITR 24/2013 Anm. 6.

1480 OVG Schleswig v. 04.09.2014 - 4 LB 20/13 - juris Rn. 70, 74 mit Anm. *Starnecker/Tausch*, jurisPR-ITR 24/2014 Anm. 3.

1481 OVG Schleswig v. 04.09.2014 - 4 LB 20/13 - juris Rn. 72 mit Anm. *Starnecker/Tausch*, jurisPR-ITR 24/2014 Anm. 3.

© 2019 juris GmbH | www.juris.de

der Fanseite sei auch deswegen rechtswidrig gewesen, weil die ULD nach § 38 Abs. 5 BDSG a.F. selbst bei schwerwiegenden Mängeln als ersten Schritt nur die Mängelbeseitigung hätte verlangen können.[1482]

771 Das **BVerwG** hat sich im darauffolgenden Revisionsverfahren sinngemäß dahingehend erklärt, dass die zwei Argumentationsstränge des OVG Schleswig einander widersprächen.[1483] Da der Anbieter der Fanseite keinen Einfluss auf die rechtswidrige Datenverarbeitung durch die irische Facebook Ltd. hätte, könne man von ihm auch nicht mit der Mängelbeseitigung etwas Unmögliches verlangen.[1484] Dass die Anbieterin der Facebook-Seite keine verantwortliche Stelle i.S.d. § 3 Abs. 7 BDSG a.F. ist, sieht das BVerwG im Ergebnis genauso wie die vorinstanzlichen Gerichte.[1485] Allerdings überlegt das BVerwG dann jedoch weiter in Richtung **Haftung des Zweckveranlassers**/mittelbaren Störers, ohne diese Rechtsfigur konkret beim Namen zu nennen.[1486] Der fehlende Einfluss des Fanseiten-Anbieters schlösse jedenfalls bei unterstellter datenschutzrechtlicher Pflichtenstellung eine Anwendung des „adressatenoffenen" § 38 Abs. 5 BDSG a.F. nicht aus.[1487] Allerdings sieht das BVerwG noch Klärungsbedarf, ob die – inzwischen außer Kraft getretene – Datenschutzrichtlinie eine Verantwortlichkeit auch außerhalb seines Art. 2 lit. d zulässt, und hat insoweit den EuGH um Vorabentscheidung ersucht.[1488] Das Urteil des EuGH[1489] wird nicht allein für Anbieter von Fanseiten auf Facebook, sondern generell hinsichtlich **mehrstufiger Informationsanbieterverhältnisse** Rechtssicherheit bringen.[1490] Hierunter fällt auch der Anwendungsbereich des Behavioral Targeting. So wird sich die Entscheidung des EuGH in Sachen Facebook-Fanpages auch auf die Einbindung von Social Plug-ins wie z.B. Like-Buttons auswirken (vgl. dazu auch Rn. 143 sowie Rn. 715 ff.), welche dem EuGH[1491] durch eine Vorlage des OLG Düsseldorf[1492] derzeit ebenso zur Vorabentscheidung vorliegt (vgl. dazu auch Rn. 148 ff.).

772 **(2) Aktuelle Rechtslage unter Einbeziehung des Urteils des EuGH vom 05.06.2018:** Am 27.06.2017 fand vor dem EuGH die mündliche Verhandlung statt; am 24.10.2017 hat der **Generalanwalt** dem Gericht seine **Schlussanträge**[1493] vorgelegt. Er gelangt darin zu dem Ergebnis, dass Art. 2 lit. d Datenschutzrichtlinie dahin auszulegen sei, dass der **Fanpage-Betreiber (mit-)verantwortliche Stelle** ist. Diesem stehe ein bestimmender Einfluss auf die Datenverarbeitung insoweit zu, als dass er diese durch Schließen der Facebook-Seite jederzeit eigenständig beenden könne. Auch der Umstand, dass der Fanpage-Betreiber keinen Zugang zu der Datenverarbeitung und den Daten von Facebook habe, stünde dem nicht entgegen, da er zu Beginn den Vertragsbedingungen des Dienstes freiwillig zugestimmt habe. Dies hätte zur Konsequenz, dass Fanpage-

---

1482 OVG Schleswig v. 04.09.2014 - 4 LB 20/13 - juris Rn. 70 mit Anm. *Starnecker/Tausch*, jurisPR-ITR 24/2014 Anm. 3.

1483 BVerwG v. 25.02.2016 - 1 C 28.14 - juris Rn. 26 mit Anm. *Berlit*, jurisPR-BVerwG 13/2016 Anm. 3; *Petri*, ZD 2016, 398 f.; *Kartheuser*, ITRB 2016, 151 f.

1484 BVerwG v. 25.02.2016 - 1 C 28.14 - juris Rn. 8 mit Anm. *Berlit*, jurisPR-BVerwG 13/2016 Anm. 3; *Petri*, ZD 2016, 398 f.; *Kartheuser*, ITRB 2016, 151 f.

1485 BVerwG v. 25.02.2016 - 1 C 28.14 - juris Rn. 27 mit Anm. *Berlit*, jurisPR-BVerwG 13/2016 Anm. 3; *Petri*, ZD 2016, 398 f.

1486 *Kartheuser*, ITRB 2016, 151, 152.

1487 BVerwG v. 25.02.2016 - 1 C 28.14 - juris Rn. 22 mit Anm. *Berlit*, jurisPR-BVerwG 13/2016 Anm. 3; *Petri*, ZD 2016, 398 f.; *Kartheuser*, ITRB 2016, 151 f.

1488 BVerwG v. 25.02.2016 - 1 C 28.14 - juris Rn. 16 mit Anm. *Berlit*, jurisPR-BVerwG 13/2016 Anm. 3; *Petri*, ZD 2016, 398 f.; *Kartheuser*, ITRB 2016, 151 f.

1489 Das Verfahren wird unter dem Aktenzeichen C-210/16 geführt.

1490 *Petri*, ZD 2016, 398, 399.

1491 Das Verfahren wird unter dem Aktenzeichen C-40/17 geführt.

1492 OLG Düsseldorf v. 19.01.2017 - 20 U 40/16 mit Anm. *Piltz,* ZD 2017, 336 ff.; *Schulte*, K&R 2017, 198 f.; *Meyer*, MMR 2017, 256 ff.

1493 Celex-Nr. 62016CC0210.

Betreiber die Nutzer einerseits – neben der eigenen Verarbeitung – auch über die Datenverarbeitung durch Facebook informieren müssten (vgl. insbesondere Art. 13 DSGVO), andererseits wären sie als Gesamtschuldner auch vollumfänglich für entsprechende Datenschutzverstöße der Plattform haftbar, sei es mit Blick auf etwaige aufsichtsrechtliche Maßnahmen wie z.B. Geldbußen oder auch für Schadensersatzansprüche der Nutzer. Ohne Änderung der zugrundeliegenden Verträge von Facebook würde dies aller Voraussicht nach dazu führen, dass letztlich keine Fanpages mehr betrieben werden.[1494]

773 Die vorgenannte Argumentationslinie des Generalanwalts hat bislang in der **Literatur** sowohl aus datenschutz- als auch rein europarechtlicher Sicht in der Literatur nur **wenig Zustimmung** erfahren. Argumentiert wird damit, dass bei einer Mitverantwortlichkeit von Fanpage-Betreibern das wesentliche Harmonisierungsziel der Erleichterung des Datenverkehrs im europäischen Binnenmarkt der DSGVO negiert wird, welchem die Verordnung jedoch gerade Rechnung tragen sollte.[1495] Aus datenschutzrechtlicher Sicht wird vielfach das Vorhandensein eines gewissen Grades an Einflussnahme auf die Datenverarbeitung angezweifelt.[1496] Es bleibt daher mit abzuwarten, ob sich der **EuGH** – wie in der weit überwiegenden Anzahl an Verfahren – auch in dieser Sache den Schlussanträgen des Generalanwalts anschließt. Das Gericht ist hieran jedenfalls **nicht gebunden** und kann ohne weiteres – wie in letzter Zeit auch auffallend häufig – eine abweichende Bewertung vornehmen.

774 **(3)** Mit Urteil vom 05.06.2018 hat sich der EuGH letztlich der Ansicht des Generalanwalts angeschlossen und entschieden, dass Art. 2 lit. d der Datenschutz-Richtlinie „[…] dahin auszulegen ist, dass der Begriff des ‚für die Verarbeitung Verantwortlichen' im Sinne dieser Bestimmung den Betreiber einer bei einem sozialen Netzwerk unterhaltenen Fanpage umfasst."[1497] Dabei kommt das Gericht zwar zu der Überzeugung, dass die **bloße Nutzung** eines sozialen Netzwerks **nicht ausreicht,** um eine gemeinsame Verantwortlichkeit zu begründen.[1498] Die **Einrichtung** einer entsprechenden **Fanpage** samt „Parametrierung u. a. entsprechend seinem Zielpublikum" trägt aber nach Überzeugung des Gerichts maßgeblich zu der Entscheidung über die Zwecke und Mittel der Verarbeitung durch Facebook bei und **begründet** damit die **gemeinsame Verantwortlichkeit** im Sinne des Art. 2 lit. d der Datenschutz-Richtlinie.[1499]

775 Zugleich betont das Gericht allerdings, dass das Vorliegen einer gemeinsamen Verantwortlichkeit **nicht zwangsläufig zu einer gleichwertigen Verantwortlichkeit** der Beteiligten führt.[1500] Es bedarf einer Einzelfallbeurteilung, nach der die unterschiedlichen Beteiligten in unterschiedlichen Phasen des Verarbeitungsvorgangs unterschiedliche Verantwortungsanteile tragen können.[1501]

1494 Wie *Ritzer/Schläfer*, Newsdienst Compliance 2017, 22025 anmerken, würde alleine eine vollumfängliche Haftungsfreistellung der Fanpage-Betreiber durch Facebook im Innenverhältnis zu einer anderen Entwicklung führen.

1495 Hierzu ausführlich *v. Lewinski/Herrmann*, ZD 2016, 467 ff.; in dieselbe Richtung auch *Schantz* in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 363.

1496 So etwa *Martini* in: Paal/Pauly, DS-GVO/BDSG, Art. 26 DSGVO Rn. 19; *Schaffland/Holthaus* in: Schaffland/Wiltfang, DSGVO, Loseblatt, Art. 4 Rn. 182. Zu demselben Ergebnis noch in Bezug auf § 3 Abs. 7 BDSG a.F. gelangt auch *Heberlein,* Datenschutz im Social Web, 2017, S. 103 m.w.N.

1497 EuGH v. 05.06.2018 - C-210/16 - ECLI:EU:C:2018:388 = EuZW 2018, 534, 537 Rn. 44; vgl. dazu *Wagner*, jurisPR-ITR 15/2018 Anm. 2.

1498 EuGH v. 05.06.2018 - C-210/16 - ECLI:EU:C:2018:388 = EuZW 2018, 534, 537 Rn. 35.

1499 EuGH v. 05.06.2018 - C-210/16 - ECLI:EU:C:2018:388 = EuZW 2018, 534, 537 Rn. 39.

1500 EuGH v. 05.06.2018 - C-210/16 - ECLI:EU:C:2018:388 = EuZW 2018, 534, 537 Rn. 43.

1501 EuGH v. 05.06.2018 - C-210/16 - ECLI:EU:C:2018:388 = EuZW 2018, 534, 537 Rn. 43.

© 2019 juris GmbH | www.juris.de

776 Zwar hatte die Entscheidung noch die Vorgaben der Datenschutz-Richtlinie zum Gegenstand, die Entscheidungsgründe lassen sich jedoch auf die Bestimmungen der **DSGVO übertragen,** da die Definition des Verantwortlichen unverändert übernommen wurde.[1502]

777 Mit Beschluss vom 05.09.2018 fordert die DSK, „[…] dass nun die Anforderungen des Datenschutzrechts beim Betrieb von Fanpages erfüllt werden."[1503] In der Folge sollen die gemeinsamen Verantwortlichen insbesondere Klarheit über die konkrete Sachlage schaffen und den Betroffenen die **erforderlichen Informationen** bereitstellen.[1504] Darüber hinaus haben die Verantwortlichen die Rechtmäßigkeit der Verarbeitung zu gewährleisten, wobei die DSK klarstellt, dass sich die Betroffenen gem. Art. 26 Abs. 3 DSGVO zur Geltendmachung ihrer Betroffenenrechte an alle beteiligten Verantwortlichen richten können.[1505] Anhand eines Fragenkatalogs, der sowohl von Facebook als auch von dem Betreiber der Fanpage beantwortet werden muss, soll die Rechtmäßigkeit der Verarbeitung im konkreten Fall überprüft werden können.[1506]

778 Vor diesem Hintergrund ist die **pauschale Abschaltung** aller Fanpages allerdings **nicht geboten.**[1507] Insbesondere hat der EuGH eben nicht über die allgemeine Datenschutzwidrigkeit der Unterhaltung einer Fanpage, sondern lediglich über die diesbezügliche datenschutzrechtliche Verantwortungsteilung entschieden.[1508] Die Frage der Datenschutzkonformität wird sich gegebenenfalls innerhalb spezifischer Entscheidungen der damit befassten Verwaltungsgerichte stellen.[1509] Allerdings sind die Fanpage-Betreiber nunmehr insbesondere in der Pflicht, die auch seitens der DSK ausdrücklich geforderten **Informationen** auf ihrer Fanpage bereitzuhalten.[1510] Zu diesem Zweck sind zunächst Angaben im Sinne des Art. 13 DSGVO bereitzuhalten (eine entsprechende Musterformulierung findet sich unter Rn. 394 ff.).[1511] Darüber hinaus sollte auch auf Spezifika der Verarbeitung seitens Facebook (Cookies, statistische Auswertung etc.) verwiesen werden, wobei sich eine Einbeziehung der diesbezüglichen Facebook-Datenschutzerklärung anbietet.[1512]

1502 *Wagner*, jurisPR-ITR 15/2018 Anm. 2; *Niethammer*, BB 2018, 1480, 1485.

1503 Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder v. 05.09.2018, Beschluss der DSK zu Facebook Fanpages, S. 2. Abrufbar unter: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Beschluss%20der%20DSK%20zu%20Facebook%20Fanpages_1.pdf (abgerufen am 28.02.2019).

1504 Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder v. 05.09.2018, Beschluss der DSK zu Facebook Fanpages, S. 2.

1505 Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder v. 05.09.2018, Beschluss der DSK zu Facebook Fanpages, S. 2.

1506 Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder v. 05.09.2018, Beschluss der DSK zu Facebook Fanpages, S. 3.

1507 So auch *Wagner*, jurisPR-ITR 15/2018 Anm. 2.; *Härting/Gössling*, NJW 2018, 2523, 2526; *Schätzle/Waldeck*, Die 8 Fragen des Beschlusses der DSK und Facebooks „Joint Controllership Vertrag. Abrufbar unter: www.haerting.de/neuigkeit/die-8-fragen-des-beschlusses-der-dsk-und-facebooks-joint-controllership-vertrag (abgerufen am 28.02.2019).

1508 *Härting/Gössling*, NJW 2018, 2523, 2526.

1509 *Härting/Gössling*, NJW 2018, 2523, 2526.

1510 *Niethammer*, BB 2018, 1480, 1486; *Wagner*, jurisPR-ITR 15/2018 Anm. 2.

1511 *Härting/Gössling*, NJW 2018, 2523, 2526.

1512 Dazu *Härting/Gössling*, NJW 2018, 2523, 2526. Vgl. dazu ebenfalls Facebook, Ein Update für Betreiber von Facebook-Seiten. Abrufbar unter: https://de.newsroom.fb.com/news/2018/06/ein-update-fuer-betreiber-von-facebook-seiten/ (abgerufen am 28.02.2019).

© 2019 juris GmbH | www.juris.de

3. Datenschutz bei Minderjährigen und Jugendschutz

779 Die Zahl der Minderjährigen, die soziale Netzwerke nutzen, nimmt beständig zu. Bereits 2011 verwendeten in der EU 77% der 13- bis 16-jährigen und 38% der 9- bis 12-jährigen Internetnutzer diese Medien.[1513] Dieser Trend hält ungebrochen an. So nutzten beispielsweise im Jahr 2017 **89 Prozent** der 12- bis 13-Jährigen den Messengerdienst WhatsApp, 67 Prozent die Plattform Youtube und immerhin 34 Prozent das Netzwerk Instagram.[1514] Die Nutzung sozialer Netzwerke ist somit für Minderjährige nicht nur zur **Selbstverständlichkeit und Lebenswirklichkeit** geworden, sie ist vielmehr für einen Großteil der Jugendlichen **unverzichtbar** geworden.[1515]

780 Es verwundert daher nicht, dass insbesondere Kinder und Jugendliche in den Fokus unternehmerische Interessen rücken.[1516] Da Kinder und Jugendliche aber oftmals nicht in der Lage sind, die **Risiken und Folgen** der Verarbeitungsprozesse innerhalb sozialer Medien richtig einzuschätzen, sieht die DSGVO gesonderte Schutzmechanismen bei der Verarbeitung personenbezogener Daten von Kindern vor.[1517]

781 Sofern die Datenverarbeitung auf Grundlage einer Einwilligungserklärung (vgl. allgemein zu den Anforderungen der Einwilligung Rn. 259 ff.) legitimiert werden soll, gilt es zukünftig insbesondere die Vorgaben des **Art. 8 DSGVO** zu berücksichtigen. Mithin hat der Verordnungsgeber jedenfalls im Bereich der Dienste der Informationsgesellschaft ein datenschutzrechtliches Mindestalter für die Einwilligung festgelegt. Innerhalb des Anwendungsbereichs des Art. 8 Abs. 1 DSGVO wird die **Einwilligungsfähigkeit** des Kindes **fingiert,** sobald es das **16. Lebensjahr vollendet** hat (vgl. dazu bereits Rn. 259 ff.).

782 Hat das Kind noch nicht die genannte Altersgrenze erreicht, so ist die Datenverarbeitung auf Grundlage einer Einwilligung im Rahmen sozialer Netzwerke nach Art. 8 Abs. 1 Satz 2 DSGVO **nur rechtmäßig,** sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.

783 Zwischenzeitlich zeigt sich allerdings, dass große Diensteanbieter wie etwa Facebook beziehungsweise dessen Tochterunternehmen WhatsApp keine signifikanten Hürden zur Altersverifikation integriert haben. Während Facebook eine elterliche Bestätigung via E-Mail voraussetzt, lässt sich WhatsApp das datenschutzrechtlich erforderliche Alter mittels Wischgeste bestätigen.[1518] Ob eine solche Vorgehensweise als angemessene Anstrengung im Sinne des Art. 8 Abs. 2 DSGVO zu werten ist, darf allerdings bezweifelt werden (vgl. allgemein dazu bereits Rn. 262).

784 Lediglich wenige Mitgliedstaaten, wie beispielsweise Österreich (§ 4 Abs. 4 DSG – 14 Jahre) haben von der **Spezifizierungsklausel** in Art. 8 Abs. 1 Satz 3 DSGVO, der den Mitgliedstaaten die Verringerung dieser Altersgrenze bis zum dreizehnten Lebensjahr gestattet, Gebrauch gemacht.

[1513] Europäische Kommission, Pressemitteilung v. 21.06.211 – Digitale Agenda: Nur zwei soziale Netze schützen standardmäßig die Profile Minderjähriger. Abrufbar unter: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/762&format=HTML&aged=0&language=DE&guiLanguage=en (abgerufen am 28.02.2019).

[1514] bitkom, Kinder und Jugend in der digitalen Welt, 2017, S. 8. Abrufbar unter: www.bitkom.org/sites/default/files/pdf/Presse/Anhaenge-an-PIs/2017/05-Mai/170512-Bitkom-PK-Kinder-und-Jugend-2017.pdf (abgerufen am 28.02.2019).

[1515] Vgl. dazu bitkom, Jeder Dritte kann sich ein Leben ohne Social Media nicht mehr vorstellen – Repräsentative Umfrage 2018. Abrufbar unter: www.bitkom.org/Presse/Presseinformation/Jeder-Dritte-kann-sich-ein-Leben-ohne-Social-Media-nicht-mehr-vorstellen.html (abgerufen am 28.02.2019).

[1516] Vgl. dazu *Heckmann/Paschke* in: Ehmann/Selmayr, DS-GVO, Art. 8 DSGVO Rn. 1.

[1517] Vgl. dazu auch Erwägungsgrund 38 Satz 1 DSGVO.

[1518] Vgl. dazu etwa *Müller*, Teenies verärgert über neue Datenschutzregeln, FAZ v. 28.05.2018. Abrufbar unter: www.faz.net/aktuell/wirtschaft/diginomics/teenies-veraergert-ueber-die-dsgvo-in-social-media-15611547.html (abgerufen am 28.02.2019).

© 2019 juris GmbH | www.juris.de

785 Sofern die Verarbeitung personenbezogener Daten von Kindern und Jugendlichen auf Grundlage einer **Interessenabwägung** erfolgen soll, wie dies grundsätzlich bei der Nutzung etwaiger Tracking-Mechanismen vorgeschlagen wird (vgl. dazu Rn. 139 ff.), sind die gesonderten Vorgaben des Art. 6 Abs. 1 Satz lit. f DSGVO zu berücksichtigen. Aufgrund dieser Regelung sieht die DSGVO vor, dass die Interessen, Grundrechte oder Grundfreiheiten insbesondere dann überwiegen können, wenn es sich bei der betroffenen Person um ein Kind handelt. Ob die **erhöhten Anforderungen** an die Interessenabwägung daher beispielsweise zur Legitimation von Werbe- oder Trackingzwecken bei Kindern erfüllt werden können, ist fraglich.[1519] Diesbezüglich hält Erwägungsgrund 38 Satz 2 fest, dass die (überwiegende) Schutzwürdigkeit der Kinder insbesondere in den Fällen anzunehmen ist, in denen deren personenbezogene Daten zu Werbezwecken oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen verarbeitet werden sollen.[1520]

4. Betroffenenrechte

786 Auch im Kontext sozialer Netzwerke steht den Nutzern die Geltendmachung der allgemeinen datenschutzrechtlichen Betroffenenrechte zur Verfügung (vgl. hierzu Rn. 352 ff.). Im Folgenden soll ergänzend auf einige Besonderheiten, die im Rahmen der Nutzung sozialer Netzwerke zu beachten sind, eingegangen werden.

a. Identitätsdiebstahl

787 Im Internet kann sehr schnell und mit geringem Aufwand die Identität einer anderen Person zur Anlegung eines Nutzerkontos missbraucht werden.[1521] Diese Gefahr besteht nicht nur im Kontext sozialer Netzwerke.[1522] Sofern ein solcher Identitätsdiebstahl zur Kenntnis der **Betreiber** gebracht wird, haben diese falsche Informationen zu **berichtigen und Vorkehrungen zur Verhinderung** künftiger Verstöße zu treffen.[1523]

788 Nutzt ein Dritter hingegen **fremde Kennzeichen** für ein eigenes Profil (bspw. sog. inoffizielle Fanseiten), riskiert dieser den Vorwurf der markenrechtlichen Rechtsverletzung.[1524] Natürliche Personen können sich ggf. auf das aus § 12 BGB folgende Namensrecht und § 22 KUG berufen.[1525]

b. Verlassen sozialer Netzwerke

789 Soziale Netzwerke verleiten ihre Nutzer, möglichst viele personenbezogene Daten preiszugeben.[1526] Diese Daten können nicht selten mittels sog. Personensuchmaschinen aufgefunden und mit weiteren Informationen vernetzt werden.[1527] Dies bringt die Gefahr der Bildung von Persönlichkeitsprofilen mit sich. So wurde bekannt, dass das britische Unternehmen **Cambridge Analytica** Daten

---

1519 Vgl. dazu auch *Remmertz*, MMR 2018,

1520 Vgl. Erwägungsgrund 38 Satz 2 DSGVO; in diesem Sinne auch *Gierschmann*, MMR 2018, 7, 11.

1521 Zur Bildveröffentlichung bei Twitter ohne Einwilligung des Abgebildeten, *Fuchs/Maisch*, AnwZert ITR 15/2010 Anm. 2.

1522 *Iraschko-Luscher/Kiekenbeck*, RDV 2010, 261, 264.

1523 *Iraschko-Luscher/Kiekenbeck*, RDV 2010, 261, 264 unter Bezugnahme auf BGH v. 10.04.2008 - I ZR 227/05 - Namensklau bei eBay.

1524 *Härting/Schätzle*, ITRB 2011, 11, 12.

1525 *Härting/Schätzle*, ITRB 2011, 11, 12; vgl. *Härting/Schätzle*, ITRB 2010, 39, 40.

1526 *Fox*, DuD 2009, 53.

1527 *Fox*, DuD 2009, 53.

© 2019 juris GmbH | www.juris.de

von 30 Millionen Menschen „lizensierte“, die der Anbieter über eine Facebook-App erhoben und unrechtmäßig weitergegeben hatte.[1528] Apps erhielten Zugriff auf zahlreiche Daten des Benutzers, die der App-Anbieter grundsätzlich nach seinen eigenen Zwecken verwenden konnte.[1529]

790 Grundsätzlich gilt, dass die in einem sozialen Netzwerk hinterlassenen personenbezogenen Daten nach der Kündigung der Mitgliedschaft durch den Betroffenen gem. Art. 17 Abs. 1 lit. a und b DSGVO zu **löschen** sind (vgl. dazu weiterführend Rn. 352 ff.). Diese Regelung spiegelt sich in der datenschutzrechtlichen Realität nur unzureichend wider. Einerseits wird die Möglichkeit der Profillöschung durch einige Betreiber sozialer Netzwerke vorsätzlich mittels versteckter und unübersichtlicher Löschungsfunktionen erschwert, anderseits können Daten im Kontext sozialer Netzwerke mit Profilen anderer Nutzer verknüpft und somit auch zu den Profilen von Dritten gespeichert sein.[1530]

791 Häufig behalten sich die Netzwerkbetreiber in ihren AGB aber auch die Speicherung persönlicher Daten über die Mitgliedschaft hinaus vor oder sperren lediglich, anstatt endgültig zu löschen.[1531] Im Rahmen der Entwicklung der DSGVO wurde die Diskussion unter dem Stichwort eines „Rechts auf Vergessenwerden“ geführt.[1532] Unabhängig vom Verhalten der Netzwerkbetreiber und deren AGB entwickeln einmal ins Netz gestellte Daten allerdings ein **Eigenleben** und können trotz (endgültiger) Löschung auf einer Webseite oder Plattform jederzeit wieder von Dritten veröffentlicht werden.[1533]

5. Soziale Netzwerke und Beschäftigtendatenschutz

792 Die Nutzung sozialer Netzwerke schafft im betrieblichen Kontext nicht nur Begehrlichkeiten hinsichtlich der Verwendungsbefugnis bezüglich der im Rahmen dieser Netzwerke gespeicherten Profil- und Kontaktinformationen[1534], sondern wirft vielmehr auch komplexe Fragestellungen des Beschäftigtendatenschutzes[1535] auf[1536].

793 Diese beginnen bereits bei der Bewerberauswahl, die nicht selten durch die Ergebnisse einer Recherche des potenziellen Arbeitgebers über den Stellenbewerber in den von diesem genutzten sozialen Netzwerken beeinflusst wird.[1537] Diese Form des **Background- oder Pre-Employment-Checks,** also die Verarbeitung personenbezogener Daten eines Bewerbers, die dieser nicht selbst zur Verfügung gestellt hat, sondern über Dritte, anhand von öffentlich zugänglichen Internetquellen oder aber anhand von sozialen Netzwerken erhoben wurden, ist datenschutzrechtlich **bedenk-**

1528 *Wittenhorst*, Trump-Wahlhelfer Cambridge Analytica: Streit um 50 Millionen Facebook-Profile. Abrufbar unter: www.heise.de/newsticker/meldung/Trump-Wahlhelfer-Cambridge-Analytica-Streit-um-50-Millionen-Facebook-Profile-3997820.html (abgerufen am 28.02.2019).

1529 Vgl. dazu Facebook-Plattform-Richtlinien, abrufbar unter: https://developers.facebook.com/policy/?locale=de_DE (abgerufen am 28.02.2019).

1530 *Erd* in: Taeger, Digitale Evolution – Herausforderungen für das Informations- und Medienrecht, 2010, S. 265.

1531 *Lerg*, Alle Daten löschen. Abrufbar unter: http://computer.t-online.de/persoenliche-daten-loeschen-in-sozialen-netzwerken-wie-facebook/id_19676540/index (abgerufen am 28.02.2019).

1532 Hierzu *Hornung/Hofmann*, JZ 2013, 163 ff.; *Maisch*, AnwZert ITR 7/2013 Anm. 2; *Kodde*, ZD 2013, 115 ff.; *Jandt/Kieselmann/Wacker*, DuD 2013, 235 ff. Skeptisch *Gerling/Gerling*, DuD 2013, 445 ff.

1533 Vgl. dazu etwa Ministerium für Ländlichen Raum und Verbraucherschutz Baden-Württemberg, Risiken von sozialen Netzwerken – worauf müssen Sie achten? Abrufbar unter: https://web.archive.org/web/20120805173412/http://www.internet-verbraucherrechte.de/servlet/PB/menu/2875017/index.html (abgerufen am 28.02.2019).

1534 *Braun*, AnwZert ITR 3/2011 Anm. 2; *Braun*, AnwZert ITR 16/2011 Anm. 3.

1535 Zum Beschäftigtendatenschutz vgl. *Taeger/Rose*, BB 2016, 819 ff.; *Braun/Lederer/Maisch*, AnwZert ITR 11/2012 Anm. 2 sowie Kapitel 7 ff.

1536 *Wächter*, JurPC-Web-Dok. 28/2011; *Ernst*, NJOZ 2011, 953; *Oberwetter*, NJW 2011, 417; *Erd*, NVwZ 2011, 19; *Bierekoven*, ITRB 2011, 110; *Lelley/Fuchs*, CCZ 2010, 147; *Geis*, DSB 7-8/2011, 20.

1537 Vertiefend *Forst*, NZA 2010, 427; *Wenzel*, SPA 2017, 85 ff.; *Dzida*, NZA 2017, 541, 543 f.

© 2019 juris GmbH | www.juris.de

lich.[1538] Zunächst ist auch im Rahmen eines Background-Checks darauf zu achten, dass eine entsprechende **Rechtsgrundlage** für die Verarbeitung erforderlich ist.[1539] Abseits der regelmäßig gerade nicht vorliegenden Einwilligung kommen insbesondere die Erlaubnistatbestände des § 26 BDSG in Betracht. Mithin lässt sich das Screening in den Fällen rechtfertigen, in denen dieses zur Begründung des Beschäftigungsverhältnisses erforderlich im Sinne des **§ 26 Abs. 1 Satz 1 BDSG** ist.[1540] Die Frage nach der Erforderlichkeit ist auf Grundlage einer umfassenden Interessenabwägung zu beantworten, wobei sowohl die Interessen des Arbeitgebers als auch die Interessen des Arbeitnehmers im Sinne praktischer Konkordanz gebührend zu berücksichtigen sind.[1541] In diesem Zusammenhang ist insbesondere die **Quelle** der personenbezogenen Daten **entscheidend.**[1542] Während das „Googeln" des Arbeitnehmers beziehungsweise die Heranziehung etwaiger Informationen aus beruflichen Netzwerken wie etwa Xing oder LinkedIn auf Grundlage berechtigter Interessen des Arbeitgebers gerechtfertigt werden kann, muss die Interessenabwägung bei offensichtlich privaten Informationen innerhalb „privater" Netzwerke wie Facebook regelmäßig zugunsten des Arbeitnehmers ausfallen.[1543] Für den Fall, dass dennoch rechtswidrig „private" Informationen herangezogen werden, kommt ein Schadensersatzanspruch des Bewerbers aufgrund einer Verletzung vorvertraglicher Verpflichtungen gem. § 311 Abs. 2 BGB i.V.m. § 280 Abs. 1 BGB in Betracht.[1544]

794 Der europäische Verordnungsgeber hat aufgrund der Regelung des Art. 88 DSGVO die Regulierung der **Datenverarbeitung im Beschäftigtenkontext** weitestgehend den **Mitgliedstaaten überlassen.** Dem ist der deutsche Gesetzgeber mit der Schaffung des **§ 26 BDSG** nachgekommen. Danach gelten Bewerber für ein Beschäftigtenverhältnis als Beschäftigte, vgl. § 26 Abs. 8 Satz 2 BDSG, vgl. dazu die Ausführungen unter Rn. 857 ff. (vgl. zum Beschäftigtendatenschutz auch Kapitel 7 Rn. 347 ff.).

III. Datenschutz und Persönlichkeitsprofile

1. Allgemeines

795 Soziale Netzwerke (z.B. Google+, Facebook, XING), Microblogs (z.B. Twitter), Blogs (z.B. Jurablogs.com, for-net.info/for-net-blog/), User-Generated-Content-Plattformen (z.B. Youtube), Browsergames (z.B. Farmville) oder kleine Programme für Smart Phones (sog. Apps[1545]) können zumindest in der Basisversion im Regelfall kostenlos genutzt werden. Gewinne werden überwiegend aus **Werbeeinnahmen** generiert. Diese können durch zielgruppenspezifische Werbung auf der Basis von personenbezogenen Daten des Adressaten erhöht werden.[1546]

1538 Definition nach *Kort*, RdA 2018, 24, 26.

1539 Artikel-29-Datenschutzgruppe, Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz, WP 249, S. 12. Abrufbar unter: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 (abgerufen am 01.03.2019).

1540 *Schwarz*, ZD 2018, 353, 354; in diesem Sinne auch die Artikel-29-Datenschutzgruppe, Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz, WP 249, S. 12. Abrufbar unter: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 (abgerufen am 01.03.2019).

1541 Vgl. dazu etwa *Schwarz*, ZD 2018, 353, 354.

1542 Artikel-29-Datenschutzgruppe, Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz, WP 249, S. 12.

1543 In diesem Sinne auch Artikel-29-Datenschutzgruppe, Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz, WP 249, S. 12; *Gola* in: Gola/Heckmann, BDSG, § 26 Rn. 61. Strenger *Kort*, RdA 2018, 24, 26 der selbst das „Googeln" etwaiger Bewerber nicht mit grundrechtlichen Vorgaben vereinbar hält.

1544 *Däubler* in: Däubler/Wedde/Weichert/Sommer, DSGVO/BDSG, 2018, § 26 BDSG Rn. 46 m. w. N.

1545 Vgl. hierzu *Selent*, DSB 2013,

1546 *Maisch*, ITRB 2011, 13.

796 Personenbezogene Daten bilden daher bisher noch die inoffizielle **Währung** im Web. Die Bedeutung von Persönlichkeitsprofilen z.B. im Rahmen von sozialen Netzwerken spiegelt sich auch im Börsenwert des Unternehmens Facebook wider, der im Jahr 2018 538 Mrd. US-Dollar betrug.[1547] Verschiedene technische Spuren und Hilfsmittel erlauben Werbetreibenden eine gezielte Auswertung des Nutzerverhaltens im Internet.

2. Personenbezogene Daten

797 Die Verarbeitung (personenbezogener) Daten im Internet ermöglicht regelmäßig eine Identifizierung von Nutzern. Hierbei werden personenbezogene Daten verarbeitet, die vom Nutzer **bewusst preisgegeben** werden. Es werden allerdings auch die für die informationstechnischen Prozesse notwendigen Daten durch die Unternehmen genutzt.[1548] Zu diesen Daten zählen insbesondere IP-Adressen, MAC-Adressen sowie Browser Fingerprints (ausführlich zur Frage des Personenbezugs dieser Datengruppen unter Rn. 103 ff.).[1549]

3. Zulässigkeit der Datenverarbeitung

a. Nutzungsprofile anhand von Cookies

798 Mittels Cookies können Nutzer identifiziert und ihr Nutzungsverhalten analysiert werden. Nach dem Willen des EU-Parlaments sollen Cookies nicht ohne Wissen des Nutzers auf dessen Rechner gespeichert werden können. In der Richtlinie 2009/136/EG (sog. **Cookie-Richtlinie)**[1550] ist daher vorgesehen, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet wird, wenn der betreffende Nutzer auf der Grundlage von klaren und umfassenden Informationen seine Einwilligung gegeben hat.[1551] Aus der umstrittenen[1552] Richtlinie wird allgemein geschlossen, dass der Nutzer vorher einwilligen muss, falls ein Cookie auf seinem Computer installiert werden soll **(Opt-in-Lösung)**. Die Beibehaltung von Standardeinstellungen des Internet-Browsers kann nach Auffassung der Art. 29 Datenschutzgruppe nicht ipso iure als Einwilligung gewertet werden.[1553] Vielmehr könnte die Einwilligung durch eine Pop-up-Fenster-Lösung oder ein Do-not-track-Plug-in im Browser gelöst werden.[1554]

799 Ob die Cookie-Richtlinie 2009/136/EG bereits in den bisherigen TMG-Vorschriften umgesetzt wurde, ist umstritten.[1555] Nach einem Urteil des OLG Frankfurt vom 17.12.2015 soll für den rechtskonformen Einsatz[1556] von Cookies jedenfalls eine Einwilligung, die im Rahmen des Opt-out-Verfahrens i.S.d. TMG erteilt wird, ausreichen.[1557] Danach konnten Cookies gem. § 15 Abs. 1 TMG erhoben, verarbeitet und gespeichert werden, sofern sie als Nutzungsdaten erforderlich zur

---

1547 Vgl. Kleiner Perkins Caufield & Byers, Börsenwert der größten Internetunternehmen weltweit im Mai 2018. Abrufbar unter: https://de.statista.com/statistik/daten/studie/217485/umfrage/marktwert-der-groessten-internet-firmen-weltweit/ (abgerufen am 01.03.2019).

1548 *Maisch*, ITRB 2011, 13.

1549 Vgl. hierzu *Kremer/Kramm*, jurisPR-ITR 22/2013 Anm. 5.

1550 Hierzu *Schürmann*, DSB 2013, 250; *Beine*, ZD 2013, 8 ff.

1551 *Maisch*, AnwZert ITR 23/2010 Anm. 3.

1552 *Patalong*, Wie die EU Internet-Nutzer nerven will. Abrufbar unter www.spiegel.de/netzwelt/web/0,1518,622121,00.html (abgerufen am 01.03.2019).

1553 Artikel 29 Datenschutzgruppe, Stellungnahme v. 22.06.2010, 00909/10/EN.

1554 *Maisch*, Kritik an digitalen Fährtenlesern. Abrufbar unter: www.lto.de/de/html/nachrichten/2520/datenschutz_bei_google_analytics_kritik_an_digitalen_faehrtenlesern/ (abgerufen am 01.03.2019).

1555 Der Ansicht scheint jedenfalls die EU-Kommission zu sein, vgl. dazu etwa www.telemedicus.info/article/2716-EU-Kommission-Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html (abgerufen am 01.03.2019).

1556 OLG Frankfurt v. 17.12.2015 - 6 U 30/15 mit Anm. *Starnecker/Wessels*, jurisPR-ITR 5/2016 Anm. 2.

1557 Vertiefend *Rauer/Ettig*, ZD 2015, 255 ff.

© 2019 juris GmbH | www.juris.de

Inanspruchnahme und Abrechnung von Telemedien, bspw. eCommerce-Plattformen, sind. Für Erstellung von Nutzungsprofilen gem. § 15 Abs. 3 TMG eignen sich neben Log-Files auch Cookies.[1558] Zum Zweck der Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien darf der Telemedienanbieter nach § 15 Abs. 3 TMG, sofern der Nutzer nicht widerspricht, solche Nutzungsprofile erstellen, sofern er diese unter Pseudonymen erstellt.

800 Allgemein zur Zulässigkeit des Einsatzes etwaiger Cookies bereits unter Rn. 139 ff. Darüber hinaus wird die **ePVO** den Umgang mit Cookies für die Werbewirtschaft tendenziell einschränken, vgl. dazu Rn. 623 ff.

b. Tracking durch Social Plug-ins sowie Browser Fingerprinting

801 Durch den Like-Button werden personenbezogene Daten des Betroffenen verarbeitet, da dieser anhand des Facebook-Cookies eindeutig als Facebook-Nutzer identifiziert werden kann (vgl. dazu auch Rn. 146 ff.).[1559]

802 Facebook erhebt und verarbeitet die personenbezogenen Daten beispielsweise mit Hilfe des Like-Buttons und ist daher **Verantwortlicher** i.S.v. Art. 4 Nr. 7 DSGVO.[1560] Der Diensteanbieter wird dabei insbesondere nicht als Auftragsverarbeiter tätig, da es an den Voraussetzungen der Auftragsverarbeitung fehlt. Es ist ungeklärt, ob der Diensteanbieter, der mit der Einbettung des Like-Buttons die Datenverarbeitung ermöglicht hat, ebenfalls zumindest als gleichsam für die Verarbeitung Verantwortlicher i.S.v. Art. 26 DSGVO zu bewerten ist. Vgl. dazu bereits die Ausführungen unter Rn. 149 ff.

c. Tracking durch Google Analytics

803 Neben den Social Plug-ins dienen andere **Webanalysedienste** der Auswertung von Informationen, bspw. über die etwaige geographische Herkunft eines Nutzers, sein Surfverhalten sowie die durchschnittliche Häufigkeit und Dauer seiner Besuche auf einer Webseite. Anhand dieser Daten können Diensteanbieter Inhalte, Services und Werbemaßnahmen zielgruppenspezifisch zuschneiden und damit insbesondere unentgeltliche Dienste durch **Werbeeinnahmen** refinanzieren.[1561] Webanalysedienste wie Google Analytics[1562] setzen technisch einen sog. Zählpixel in der Webseite voraus, mit dem der Dienst aktiviert wird. Sobald eine Webseite aufgerufen wird, fordert der Browser unter Angabe der IP-Adresse des Nutzers alle vorgesehenen Inhalte an. Dabei wird auch der nicht sichtbare Zählpixel wie eine Bilddatei von dem Server angefordert, auf dem er gespeichert ist.[1563] Umgekehrt erhält der Server Informationen über den Nutzer.

804 Unter den Webanalysediensten ist das kostenlose Skript Google Analytics sehr verbreitet. Zu dessen rechtlichen Implikationen bereits unter Rn. 750 ff.

[1558] Vgl. *Spindler/Nink* in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, 12. Teil, 4. Abschnitt, § 15 TMG Rn. 9.

[1559] *Ernst*, NJOZ 2010, 1917, 1918; *Maisch*, AnwZert ITR 19/2010 Anm. 2; vgl. zur strafrechtlichen Perspektive *Schulte/Kanz*, ZJS 2013, 24.

[1560] Vgl. zur alten Rechtslage *Duchrow*, MMR-Aktuell 2011, 320091.

[1561] *Maisch*, Kritik an digitalen Fährtenlesern. Abrufbar unter: www.lto.de/de/html/nachrichten/2520/datenschutz_bei_google_analytics_kritik_an_digitalen_faehrtenlesern/ (abgerufen am 01.03.2019).

[1562] Vertiefend zum Thema Google Analytics vgl. *Kirsch*, MMR-Aktuell 2011, 313724; *Huth*, AnwZert ITR 12/2011 Anm. 2; *Maisch*, Kritik an digitalen Fährtenlesern. Abrufbar unter: www.lto.de/de/html/nachrichten/2520/datenschutz_bei_google_analytics_kritik_an_digitalen_faehrtenlesern/ (abgerufen am 01.03.2019); *Krieg*, AnwZert ITR 24/2008 Anm. 3; *Schöttler*, AnwZert ITR 25/2008 Anm. 3.

[1563] *Maisch*, Kritik an digitalen Fährtenlesern. Abrufbar unter: www.lto.de/de/html/nachrichten/2520/datenschutz_bei_google_analytics_kritik_an_digitalen_faehrtenlesern/ (abgerufen am 01.03.2019).

© 2019 juris GmbH | www.juris.de

IV. Der Datenschutz im Spannungsverhältnis zu Wissenschafts-, Presse-, Informations- und Meinungsfreiheit

805 Nach Erwägungsgrund 4 der DSGVO sollte die Verarbeitung personenbezogener Daten im Dienste der Menschheit stehen. Das Recht auf Schutz der personenbezogenen Daten muss danach im Hinblick auf seine gesellschaftliche Funktion gesehen werden und findet seine Grenzen in der Abwägung mit anderen Grundrechten.[1564] Der Schutz personenbezogener Daten gem. Art. 8 GRCh steht dabei in einem Spannungsverhältnis mit dem Grundrecht auf Meinungsäußerung und der Informationsfreiheit gem. Art. 11 GRCh sowie mit der Kunst- und Wissenschaftsfreiheit gem. Art. 13 GRCh. Die kollidierenden Grundrechtspositionen sind daher regelmäßig in einen angemessenen Ausgleich zu bringen.[1565] Dieser Gemengelage unterschiedlicher schützenswerter Positionen begegnet die DSGVO mit einer Durchbrechung des datenschutzrechtlichen Verbots für besondere Verarbeitungssituationen.

1. Datenverarbeitung im Kontext der Meinungsäußerungs- und Informationsfreiheit

806 Eine solche Durchbrechung findet sich in Art. 85 DSGVO. Nach Art. 85 DSGVO ist es Aufgabe der Mitgliedstaaten, im grundrechtlichen Spannungsverhältnis zwischen der Freiheit der Meinungsäußerung und der Informationsfreiheit und dem Recht auf den Schutz personenbezogener Daten zu einer verhältnismäßigen Konfliktlösung zu gelangen.[1566] Als **Abwägungsgebot** formuliert Art. 85 Abs. 1 DSGVO den Auftrag an die Mitgliedstaaten, das Recht auf den Schutz personenbezogener Daten aus Art. 8 Abs. 1 GRCh in Einklang mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit aus Art. 11 Abs. 1 GRCh zu bringen.[1567] Hierzu gehört die Verarbeitung von Daten zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken.

807 Art. 85 Abs. 2 DSGVO überträgt den **Mitgliedstaaten** die Aufgabe im Hinblick auf die Datenverarbeitungen, die zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgen, **Abweichungen** und **Ausnahmen** von den Verordnungen der Kapitel II bis VII und IX der DSGVO **vorzunehmen,** wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.

808 Insofern verpflichtet die Norm Mitgliedstaaten über den in Absatz 1 normierten allgemeinen Auftrag hinaus und verankert damit ein **Medien- und Wissenschaftsprivileg.**[1568] Nach Erwägungsgrund 153 ist der Begriff des Journalismus, ebenso wie der anderer Zwecke, die mit der Meinungsfreiheit verbunden sind, weit auszulegen.[1569]

1564 Vgl. *Stender-Vorwachs* in: Wolff/Brink, Beck'scher Onlinekommentar, Art. 85 DSGVO Rn. 1.

1565 Vgl. Erwägungsgrund 153 DSGVO, der Art. 11 GRCh explizit nennt.

1566 *Specht/Bienemann* in: Sydow, DSGVO, Art. 85 DSGVO Rn. 7.

1567 *Schiedermair* in: Ehmann/Selmayr, DS-GVO, Art. 85 DSGVO Rn. 9; vgl. Erwägungsgrund 153 DSGVO, der Art. 11 GRCh explizit nennt.

1568 *Schiedermair* in: Ehmann/Selmayr, DS-GVO, Art. 85 DSGVO Rn. 23.

1569 *Specht/Bienemann* in: Sydow, DSGVO, Art. 85 DSGVO Rn. 8; *Buchner/Tinnefeld* in: Kühling/Buchner, DS-GVO/BDSG, Art. 85 DSGVO Rn. 17.

© 2019 juris GmbH | www.juris.de

809 Eine Datenverarbeitung zu einem journalistischen Zweck wird bereits dann angenommen, wenn sie auf eine Verbreitung in der Öffentlichkeit, im Sinne eines unbestimmten Personenkreises abzielt.[1570] Insbesondere sind auch Daten im audiovisuellen Bereich sowie in Nachrichten- und Pressearchiven erfasst. Art. 85 DSGVO trägt somit der Bedeutung der Meinungs-, Informations- im Allgemeinen und der Pressefreiheit im Speziellen für den Erhalt der demokratischen Gesellschaft Rechnung.[1571]

810 Art. 85 Abs. 3 DSGVO normiert eine Meldepflicht für die Mitgliedstaaten im Hinblick auf Rechtsvorschriften, die auf der Grundlage von Absatz 2 erlassen wurden, sowie alle Änderungen dieser Vorschriften.

2. Datenverarbeitung im Kontext des Zugangs der Öffentlichkeit zu amtlichen Dokumenten

811 Nach Art. 86 DSGVO können personenbezogene Daten in amtlichen Dokumenten, die sich im Besitz einer Behörde oder einer öffentlichen Einrichtung oder einer privaten Einrichtung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe befinden, von der Behörde oder der Einrichtung gemäß dem Unionsrecht oder dem Recht des Mitgliedstaats, dem die Behörde oder Einrichtung unterliegt, offengelegt werden, um den Zugang der Öffentlichkeit zu amtlichen Dokumenten mit dem Recht auf Schutz personenbezogener Daten gemäß dieser Verordnung in Einklang zu bringen. Während der Datenschutz seinen primärrechtlichen Rückhalt in Art. 8 GRCh findet, wird das Recht auf Zugang zu (staatlichen) Dokumenten insbesondere im europäischen Kontext durch Art. 42 GRCh geschützt.[1572]

812 Durch Art. 86 DSGVO wird somit der Zugang der Öffentlichkeit zu amtlichen Dokumenten ungeachtet der Vorgaben der DSGVO geregelt, sofern Zugangsrechte durch mitgliedstaatliche oder unionsrechtliche Regelungen bestehen.[1573] Zudem gestattet Art. 86 DSGVO den Mitgliedstaaten eine entsprechende Ausgestaltung der Voraussetzungen eines solchen Anspruches.[1574] Dabei soll der Zugang der Öffentlichkeit zu amtlichen Dokumenten und die Weiterverwendung von Informationen des öffentlichen Sektors mit dem Recht auf Schutz personenbezogener Daten in Einklang gebracht werden.[1575]

3. Datenverarbeitung zu Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

813 Art. 89 DSGVO nennt die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken und schafft somit eine diesbezügliche **bereichsspezifische Privilegierung.**[1576] Art. 89 DSGVO normiert

---

1570 *Buchner/Tinnefeld* in: Kühling/Buchner, DS-GVO/BDSG, Art. 85 DSGVO Rn. 17.

1571 Vgl. *Specht/Bienemann* in: Sydow, DSGVO, Art. 85 DSGVO Rn. 1; *Pauly* in: Paal/Pauly DS-GVO/BDSG, Art. 85 DSGVO Rn. 1. Zur Frage, ob auch Bewertungsportale von den Vorgaben des Art. 85 DSGVO erfasst werden vgl. *Michel*, ZUM 2018, 836 ff.

1572 *Ehmann* in: Ehmann/Selmayr, DS-GVO, Art. 86 DSGVO Rn. 2.

1573 *Ehmann* in: Ehmann/Selmayr, DS-GVO, Art. 86 DSGVO Rn. 6.

1574 *Pauly* in: Paal/Pauly, DS-GVO/BDSG, Art. 86 DSGVO Rn. 1.

1575 Vgl. Erwägungsgrund 154 DSGVO.

1576 *Buchner/Tinnefeld* in: Kühling/Buchner, DS-GVO/BDSG, Art. 89 DSGVO Rn. 1.

© 2019 juris GmbH | www.juris.de

jedoch keinen eigenen Erlaubnistatbestand für die Verarbeitung personenbezogener Daten.[1577] Vielmehr setzt Art. 89 DSGVO einen solchen voraus, welcher sich aus Art. 6 DSGVO und Art. 9 Abs. 2 lit j. DSGVO ergibt.[1578]

814 Die Restriktionen, die die Regelung vorsieht, dienen der Kompensation der niedrigeren Verarbeitungsvoraussetzung hinsichtlich derartiger Daten.[1579] Soweit die Verarbeitung personenbezogener Daten zu diesen privilegierten Zwecken erfolgt, müssen danach **geeignete Garantien zum Schutz der betroffenen Personen getroffen werden.** Nähere Bestimmungen hierzu beinhaltet Art. 89 Abs. 1 Sätze 2-4 DSGVO, insbesondere müssen technische und organisatorische Maßnahmen ergriffen werden. Art. 89 Abs. 2-4 DSGVO regelt dahingehend wiederum die Reichweite der Privilegierung hinsichtlich der Betroffenenrechte.

815 Auf Grundlage der Spezifizierungsklauseln in Art. 9 Abs. 2 lit. j DSGVO und Art. 89 Abs. 2 und 3 DSGVO hat der deutsche Gesetzgeber **§§ 27, 28 BDSG** erlassen.[1580]

816 **§ 27 BDSG** weicht die datenschutzrechtlichen Anforderungen bei einer Datenverarbeitung zu **wissenschaftlichen oder historischen Forschungszwecken** und zu statistischen Zwecken auf. Nach Absatz 1 der Norm ist insbesondere die Einwilligung bei der diesbezüglichen Verarbeitung von besonderen Kategorien entbehrlich. Ferner werden nach § 27 Abs. 1 Satz 1 BDSG die Betroffenenrechte (Art. 15, 16, 18, 21 DSGVO) insoweit beschränkt, wie sie voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist.

817 Eine **Veröffentlichung** personenbezogener Daten ist auch im **Forschungskontext** nur zulässig, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist (§ 27 Abs. 4 BDSG).

818 Die Datenverarbeitung zu im öffentlichen Interesse liegenden **Archivzwecken** wird in Deutschland durch **§ 28 BDSG** präzisiert. Auch in diesem Kontext werden die **Betroffenenrechte eingeschränkt.** Nach § 28 Abs. 1 BDSG besitzt die betroffene Person **keinen Auskunftsanspruch** (Art. 15 DSGVO), wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen.

819 **Ebenfalls eingeschränkt** ist das **Recht auf Berichtigung** der betroffenen Person gemäß Art. 16 DSGVO, wenn die personenbezogenen Daten zu Archivzwecken im öffentlichen Interesse verarbeitet werden, § 28 Abs. 3 Satz 1 BDSG. Allerdings ist der betroffenen Person die Möglichkeit der Gegendarstellung einzuräumen und diese zu den Unterlagen zu nehmen, § 28 Abs. 3 Sätze 2 und 3 BDSG.

820 Ferner werden die Betroffenenrechte aus **Art. 18** (Recht auf Einschränkung der Verarbeitung), **20** (Recht auf Datenübertragung), **21** (Widerspruchsrecht) DSGVO **weitreichend,** entsprechend den Vorgaben aus Art. 89 Abs. 3 DSGVO, **ausgeschlossen,** § 28 Abs. 4 BDSG.

1577 *Hense* in: Sydow, DSGVO, Art. 89 DSGVO Rn. 1; *Buchner/Tinnefeld* in: Kühling/Buchner, DS-GVO/BDSG, Art. 89 DSGVO Rn. 1.

1578 *Buchner/Tinnefeld* in: Kühling/Buchner, DS-GVO/BDSG, Art. 89 DSGVO Rn. 1.

1579 *Pauly* in: Paal/Pauly, DS-GVO/BDSG, Art. 89 DSGVO Rn. 1.

1580 Vgl. *Eichler* in: Wolff/Brink, Beck'scher Onlinekommentar, Art. 89 DSGVO Rn. 3, 20, 24.

© 2019 juris GmbH | www.juris.de

V. Datenschutz und Bewertungsportale

1. Bewertungsgegenstände und Bewertungsfunktionen

821 Neben sozialen Netzwerken wie Facebook oder XING gehören Bewertungsportale zu den am meisten genutzten Angeboten im Web 2.0. Sind es bei den sozialen Netzwerken persönliche Nachrichten, Bilder oder Links, die der Einzelne mit anderen Nutzern teilt, geht es bei den Bewertungsportalen um Erfahrungen, Einschätzungen und Assoziationen, die in Bezug auf bestimmte Bewertungsgegenstände innerhalb eines Interessentenkreises ausgetauscht werden. Als **Bewertungsgegenstände** kommen (ungeachtet ihrer rechtlichen Zulässigkeit) sowohl Objekte, insbesondere Produkte[1581] als auch Subjekte, insbesondere Personen als Dienstleister[1582] und sogar Personen in ihrem privaten Verhalten[1583] in Betracht[1584].

822 Mit internetbasierten Bewertungsportalen werden drei typische Bedürfnisse befriedigt:

823 Aus Sicht der potentiellen Interessenten erfüllen Bewertungen von Subjekten oder Objekten ein spezifisches **Informationsinteresse,** das typischerweise im Zusammenhang mit Entscheidungen über die Inanspruchnahme von Leistungen Dritter steht. Das können Kauf-, Konsum- oder Auswahlentscheidungen sein. Je nach Qualität oder Intensität der Bewertung kann diese die Entscheidung maßgeblich beeinflussen.

824 Aus Sicht der Bewertenden befriedigen Bewertungen auch ein spezifisches **Affektionsinteresse**, das über das bilaterale Informationsinteresse hinausgehen kann. Das Mitteilungsbedürfnis mag auf Begeisterung, Ärger oder Rache beruhen, kann aber auch altruistisch motiviert sein.

825 Aus Sicht der Bewerteten dienen Bewertungen schließlich einem **Qualitätssicherungsinteresse.** Die in jeglichen Produkt- oder Personenbewertungen enthaltene Feedbackwirkung liefert dem Anbieter, Hersteller oder Leistungsträger wertvolle Informationen über die Haltung der beteiligten Verkehrskreise bzw. Marktteilnehmer zum Gegenstand der Bewertung. Nicht selten richten sich Angebotsstrategien nach diesem Feedback der Konsumenten.

[1581] Produktbewertungen im weiteren Sinne finden sich sowohl in eigenen Bewertungsportalen wie holidaycheck als auch integriert in Online-Shops (wie Amazon) oder Portalen (wie eBay, vgl. hierzu Kapitel 4.3 Rn. 280 ff.).

[1582] Diese zweite Hauptgruppe der Bewertungsportale umfasst viele Berufsgruppen wie Lehrer (spickmich, hierzu *Greve/Schärdel*, MMR 2008, 644 ff.), Hochschullehrer (meinprof, hierzu *Greve/Schärdel*, MMR 2008, 644 ff.), Ärzte (jameda.de, BGH v. 20.02.2018 - VI ZR 30/17, BGH v. 01.03.2016 - VI ZR 34/15 - GRUR 2016, 855, BGH v. 23.09.2014 - VI ZR 358/13 - GRUR 2014, 1228) u.v.a.m.

[1583] Durchaus fragwürdige Beispiele liefern Portale wie „dontdatehimgirl", Nachbarbewertungsportale oder. Fahrerbewertungsportale. Zu letzterem OVG NRW v. 19.10.2017 - 16 A 770/17.

[1584] Zur Kategorisierung der Bewertungsportale *Kamp*, Personenbewertungsportale, 2011, S. 3 ff.; vgl. *Ballhausen/Roggenkamp*, K&R 2008, 403.

© 2019 juris GmbH | www.juris.de

2. Rechtliche Problemkreise

826 Der Betrieb und die Nutzung von Bewertungsportalen im Internet werfen eine Vielzahl rechtlicher Fragen auf, die durch die Rechtsprechung in den letzten Jahren[1585] geklärt wurden, was aber noch keine umfassende Rechtssicherheit gebracht hat. Zu unterscheiden sind die eher formalen Fragen der Datenverarbeitung in Bewertungsportalen (Datenschutz, vgl. Rn. 826 ff.) und die materielle Frage der Zulässigkeit bestimmter Bewertungsinhalte (Persönlichkeitsschutz, vgl. Rn. 845 ff.).[1586]

3. Bewertungsportale und der Datenschutz

827 Dass im Rahmen von Bewertungsportalen eine Vielzahl von **personenbezogenen Daten** verarbeitet wird, liegt auf der Hand.[1587] Das betrifft bereits die „Eckdaten" der Bewertungsgegenstände, etwa Namen, Adressangaben etc. von Anbietern (bei Produktbewertungen) oder Betroffenen (bei Personenbewertungen). Bewertungsportale liefern ihren Nutzern regelmäßig den „Service", dass die Bewertungsgegenstände „vorausgefüllt" zur Verfügung gestellt werden. Ganz im Sinne des „Plug-and-Play"-Gedankens[1588] liefern Portalbetreiber diese „Rohdaten", damit der Nutzer über eine einfache Navigation möglichst schnell seine Bewertung abgeben kann. Aber auch die Bewertungen, denen neben einem Tatsachenkern schwerpunktmäßig eine Meinungsäußerung zugrunde liegt, werden als personenbezogenes Datum eingeordnet.[1589] Damit ist der Anwendungsbereich des Datenschutzrechts regelmäßig eröffnet.[1590]

828 In der Vergangenheit wurde die **Verarbeitung jener (personenbezogener) Daten,** die der Portalbetreiber in Bezug auf den Bewertungsgegenstand (im Falle von spickmich etwa die Namen, schulische Funktionen etc. der Lehrkräfte) erhoben hat, um sie den Portalnutzern zu Bewertungszwecken zur Verfügung zu stellen, über **§ 29 Abs. 1 BDSG a.F.** gerechtfertigt.[1591] Der BGH sah in Bewertungsportalen einen Anwendungsfall, der der Tätigkeit von Auskunfteien oder der Markt- und Meinungsforschung jedenfalls vergleichbar ist. Die **Rechtfertigung der „Vorausfüllung" von Bewertungsportalen** erfolgte bisher über § 29 Abs. 1 Nr. 1 BDSG a.F. bzw. über § 29 Abs. 1 Nr. 2 BDSG a.F.

829 Die DSGVO enthält keine dem § 29 Abs. 1 BDSG a.F. entsprechende Verarbeitungserlaubnis. Allerdings käme vorliegend die Anwendung von **Art. 6 Abs. 1 Satz 1 lit. f DSGVO in Betracht.** Danach ist die Verarbeitung personenbezogener Daten, die zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich sind, gestattet, sofern nicht die Interessen

---

[1585] Grundlegend BGH v. 23.06.2009 - VI ZR 196/08 - spickmich - MMR 2009, 608. Das BVerfG hat durch seine Nichtannahmeentscheidung (BVerfG v. 16.08.2010 - 1 BvR 1750/09) die grundsätzliche Zulässigkeit von Bewertungsportalen (jedenfalls solchen, die in ähnlicher Weise wie spickmich konzipiert sind) bestätigt. Zumindest aus praktischer Hinsicht relevant insoweit die mündliche Erklärung des Berichterstatters in diesem Verfahren, *Johannes Masing*, auf einem wissenschaftlichen Kongress des Studienkreises Presserecht und Pressefreiheit e.V. am 10.05.2011 in Berlin, hierzu https://web.archive.org/web/20110814133510/http://www.faz.net/artikel/C31328/meinungsfreiheit-kein-privileg-von-presse-und-funk-die-verfassung-schuetzt-das-internet-30336778.html (abgerufen am 01.03.2019). Aus der weiteren Rechtsprechung bspw. LG Hannover v. 13.05.2009 - 6 O 102/08 - MMR 2009, 870; LG Regensburg v. 02.02.2009 - 1 O 1642/08 (2) - meinprof - MMR 2009, 363; LG Hamburg v. 20.09.2010 - 325 O 111/10 - MMR 2011, 488.

[1586] Zu weiteren Einzelfragen vgl. *Kamp*, Personenbewertungsportale, 2011, S. 201 ff.; vgl. *Schwartmann*, RDV 2012, 1 ff.; eingehend zu Bewertungsportalen und den Abwehrrechten Betroffener *Pötters/Traut*, RDV 2015, 117 ff.

[1587] Zu rechtlichen und technischen Lösungsansätzen *Schulz* u.a., ZD 2013, 60 ff. Vgl. auch *Schwartmann*, RDV 2012, 1 ff.

[1588] Vgl. etwa *Heckmann*, NJW 2012, 2631 ff.; *Claus*, Vom Kampf ums Private. Abrufbar unter www.welt.de/print/welt_kompakt/debatte/article13438782/Vom-Kampf-ums-Private.html (abgerufen am 01.03.2019); *Heckmann*, Herausforderungen für das Gemeinwesen 2.0, digma 2011.1, S. 11, 16; *Heckmann*, K&R 2011, 1, 4.

[1589] BGH v. 23.06.2009 - VI ZR 196/08 - MMR 2009, 608 - spickmich; hierzu *Roggenkamp*, K&R 2009, 571.

[1590] Vgl. dazu auch *Buchner/Petri* in: Kühling/Buchner, DS-GVO/BDSG, Art. 6 DSGVO Rn. 169 ff.; Die Anwendbarkeit des sog. Medienprivilegs (§ 41 BDSG a.F.) auf Bewertungsportale lehnt der BGH v. 23.06.2009 - VI ZR 196/08 - MMR 2009, 608, 610 - spickmich ab; *Roggenkamp*, K&R 2009, 571.

[1591] BGH v. 23.06.2009 - VI ZR 196/08 - MMR 2009, 608, 610 - spickmich; *Roggenkamp*, K&R 2009, 571; vgl. *Ballhausen/Roggenkamp*, K&R 2008, 403, 407 f.

© 2019 juris GmbH | www.juris.de

oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (vgl. zu den Vorgaben der Vorschrift Rn. 335 ff.). Daher wird nunmehr eine umfassende Interessenabwägung zwischen dem schutzwürdigen Interesse des Betroffenen, diese Daten nicht zu Bewertungszwecken zu verwenden, und dem Interesse des Portalbetreibers, die Bewertung unter Verwendung dieser personenbezogenen Daten zu ermöglichen, für die einzelnen Bewertungsportale erfolgen müssen.

830 Hierbei ist zu berücksichtigen, dass die personenbezogenen Daten für die Bewertungen vielfach aus **allgemein zugänglichen Quellen,** wie etwa den Homepages von Schulen[1592], Dienstleistungsbetrieben, Homepages oder Online-Shops stammen. Zudem stellt die Meinungsfreiheit, unter die entsprechende Bewertungen fallen, auch im europäischen Rechtsrahmen ein hohes Gut dar. Allerdings darf auch nach Maßgabe europäischer Grundrechte **nicht** davon ausgegangen werden, dass die entsprechenden Kommunikationsgrundrechte prinzipiellen Vorrang genießen.[1593]

831 Bei seiner **Interessenabwägung** stellte der BGH in der Vergangenheit maßgeblich auf den Bewertungsgegenstand ab. Bei Personenbewertungen (wie im Falle von spickmich[1594]) ist danach zu unterscheiden, welcher Sphäre der Bewertungsgegenstand zuzuordnen ist.[1595] So sind Bewertungen, die dezidiert der **Privat- oder Intimsphäre** zuzurechnen sind, von vorneherein unzulässig (weshalb Plattformen wie dontdatehimgirl.com nach deutschem Datenschutzrecht – aber auch Persönlichkeitsrecht – unzulässig wären). Anders ist dies bei einem Bewertungsgegenstand, welcher die **Sozialsphäre,** insbesondere die berufliche Sphäre, betrifft. Hier kann das Interesse der Verkehrskreise an einer Leistungsbewertung als Auswahlhilfe oder zur Qualitätssicherung (welches der Portalbetreiber aufgreift) überwiegen.[1596]

832 So hat der BGH auf der vormaligen deutschen Rechtsgrundlage entschieden, dass einem **Arzt** kein Anspruch auf Löschung seiner Daten aus einem Bewertungsportal zusteht.[1597] In der vom Beklagten betriebenen Bewertungsplattform können kostenfrei Informationen zu Ärzten abgerufen werden. Abrufbar sind hierbei der Name, Praxisanschrift, Fachrichtung sowie abgegebene Bewertungen. Ein in dem Portal aufgeführter Arzt wollte die Löschung seiner Daten erreichen. Der BGH gewichtet aber vorliegend das Interesse der Öffentlichkeit an (neutralen) Informationen über die ärztlichen Leistungen höher als dasjenige des Arztes an seiner Privatsphäre. Insbesondere stammen die betroffenen Daten des Arztes allesamt aus der Sozialsphäre, in welcher der Arzt mit der Beobachtung seines Verhaltens in der Öffentlichkeit rechnen müsse.

833 Allerdings hat der BGH im Jahr 2018 erstmalig die Bewertungsplattform **jameda.de** dazu verpflichtet die Daten einer Ärztin vollständig zu löschen, da er die Plattform nicht mehr als neutrale Informationsplattform einstufte.[1598] Diese Wertung des Gerichts beruhte auf dem Geschäftsmodell des Bewertungsportals, das neben dem Basisprofil für jeden zu bewertenden Arzt kostenpflichtige „Premium"-Profile bereithält. Letztere werden mit Fotos und in optisch freundlicherer Gestaltung, bei örtlichen Konkurrenzärzten, die lediglich über ein (unfreiwilliges) Basisprofil verfügen, eingeblendet. Bei Inhabern der kostenpflichtigen „Premium"-Profile wurde eine solche Werbung jedoch

---

1592 Hierzu aber auch *Heckmann*, jurisPR-ITR 1/2008 Anm. 5.

1593 *Buchner/Petri* in: Kühling/Buchner, DS-GVO/BDSG, Art. 6 DSGVO Rn. 169.

1594 Vgl. *Götting/Lauber-Rönsberg*, AL 2013, 165.

1595 BGH v. 23.06.2009 - VI ZR 196/08 - MMR 2009, 608, 611 - spickmich.

1596 BGH v. 23.06.2009 - VI ZR 196/08 - MMR 2009, 608, 611 - spickmich; *Roggenkamp*, K&R 2009, 571, 572.

1597 BGH v. 23.09.2014 - VI ZR 358/13 mit Anm. *Starnecker/Tausch*, jurisPR-ITR 1/2015 Anm. 3; *Ernst*, jurisPR-WettbR 12/2014 Anm. 4; *Meyer*, K&R 2014, 807 ff.

1598 BGH v. 20.02.2018 - VI ZR 30/17 - GRUR 2018, 636 ff.

© 2019 juris GmbH | www.juris.de

nicht eingeblendet. Hierdurch geht nach Auffassung des BGH die Neutralität der Bewertungsplattform verloren. Das grundsätzliche Geschäftsmodell, Bewertungsplattformen bereitzuhalten, stellte der BGH allerdings nicht in Frage.

834 Indem der BGH bisher die Abwägung grundsätzlich zulasten der Bewerteten löste, geht er von keinem Vorrang datenschutzrechtlicher Vorschriften vor den Kommunikationsgrundrechten aus, wie ihn aber der EuGH in Google Spain[1599] angenommen hat.[1600] Es bleibt daher abzuwarten, ob durch die **DSGVO die Praxis** der **Bewertungsportalbetreiber** sich **ändern** muss.

835 Einerseits wird die Anonymität der Bewertungen auf Online-Plattformen kritisiert.[1601] Andererseits wurde zumindest in der Vergangenheit vertreten, dass die **Anonymität der Bewertung** zu den Wesensmerkmalen eines Bewertungsportals gehört. Auch wenn dadurch der eine oder andere Missbrauch unterstützt werden mag[1602], konnte nach bisher vertretener Auffassung eine Portalgestaltung, die auf eine Authentifizierung der Bewertenden abstellen würde, nicht gefordert werden[1603]. Bewertungen von Ärzten konnten deshalb in der Vergangenheit anonym erfolgen, weil die zu bewertenden Patienten ansonsten eigene sensible Daten preisgeben müssten. Auch die Bewertung von Lehrern setzt zumindest nach außen eine Möglichkeit zur Anonymisierung voraus, weil negative Auswirkungen sonst nicht ausgeschlossen werden könnten. Schließlich sollte einer Selbstzensur entgegengewirkt werden.[1604]

836 Das Recht auf **anonyme Nutzung** von Bewertungsportalen gehörte daher zur ständigen Rechtsprechung des BGH.[1605] Der Betreiber eines Bewertungsportals war bisher nicht verpflichtet, die Anmeldedaten eines Nutzers, der eine anonyme negative Bewertung abgegeben hat, zu übermitteln. Einem Auskunftsanspruch aus § 14 Abs. 2 TMG analog stand in der Vergangenheit § 12 Abs. 2 TMG entgegen, welcher alle anderen Übermittlungsbefugnisse sperrte, soweit sich diese nicht ausdrücklich auf Telemedien beziehen.[1606]

837 Allerdings stellte der BGH in der Entscheidung Ärztebewertung III[1607] im Interesse des bewerteten Dienstleisters fest, dass Bewertungsportale im **Konfliktfall** verpflichtet sein können, den gesamten Sachverhalt nicht nur umfassend zu überprüfen, sondern auch bestimmte Daten an den Bewertenden zu übermitteln.[1608] Hält der Bewertungsportalanbieter Informationen zurück, die er ohne Verstoß gegen § 12 Abs. 1 TMG hätte übermitteln dürfen, gerät er selbst in die mittelbare Störerhaftung.[1609]

838 In diesem Kontext muss nunmehr jedoch der **Auskunftsanspruch (Art. 15 DSGVO)** für betroffene Personen, d.h. die Bewerteten, berücksichtigt werden. Nach Art. 15 Abs. 1 lit. g DSGVO steht dem Betroffenen ein Auskunftsanspruch über die Herkunft seiner personenbezogenen Daten für

---

1599 EuGH v. 13.05.2014 - C-131/12 - ECLI:EU:C:2014:317 - Google Spain mit Anm. *Caspar*, PinG 2014, 133.

1600 Vgl. *Stadler*, Das Datenschutzrecht schützt nicht vor einer Leistungsbewertung im Internet. Abrufbar unter: www.internet-law.de/2014/09/das-datenschutzrecht-schuetzt-nicht-vor-einer-leistungsbewertung-im-internet.html (abgerufen am 01.03.2019).

1601 Vgl. u.a. *Buchner/Petri* in: Kühling/Buchner, DS-GVO/BDSG, Art. 6 DSGVO Rn. 170.

1602 VGH München v. 10.03.2010 - 7 B 09.1906, mit Anm. *Jäger*, jurisPR-ITR 10/2011 Anm. 6; OVG Lüneburg v. 26.01.2010 - 2 ME 444/09, mit Anm. *Jäger*, jurisPR-ITR 9/2011 Anm. 3.

1603 Vgl. allgemein zur anonymen Nutzung sozialer Netzwerke *Albrecht*, AnwZert ITR 1/2011 Anm. 2.

1604 *Roggenkamp*, K&R 2009, 571, 572; *Ballhausen/Roggenkamp*, K&R 2008, 403, 406.

1605 BGH v. 01.07.2014 - VI ZR 345/13 - Ärztebewertung I; BGH v. 23.09.2014 - VI ZR 358/13, Ärztebewertung II; BGH v. 01.03.2016 - VI ZR 34/15 - Ärztebewertung III.

1606 BGH v. 01.07.2014 - VI ZR 345/13 - juris Rn. 9 ff. - Ärztebewertung I, ausführlich hierzu *Paschke/Halder*, MMR 2016, 723 ff.

1607 BGH v. 01.03.2016 - VI ZR 34/15 - Ärztebewertung III.

1608 BGH v. 01.03.2016 - VI ZR 34/15 - juris Rn. 43 - Ärztebewertung III.

1609 Vgl. BGH v. 01.03.2016 - VI ZR 34/15 - juris Rn. 43 - Ärztebewertung III.

© 2019 juris GmbH | www.juris.de

die Fälle zu, in denen seine Fälle nicht bei ihm erhoben wurden (vgl. dazu ebenfalls Rn. 352 ff.).[1610] Aufgrund dessen könnten zukünftig Bewertungsplattformen, die anonyme Bewertungen anzeigen, der Vergangenheit angehören. Sollte der Verantwortliche dem Auskunftsanspruch nicht nachkommen, kann deren Durchsetzung bei privatwirtschaftlichen Bewertungsplattformen vor den Zivilgerichten erwirkt werden, vgl. Art. 79 DSGVO.[1611]

839 Eine äußere Grenze bietet bei Bewertungsplattformen auch weiterhin die potentielle **Prangerwirkung**[1612], die bestimmten Bewertungsformen innewohnen kann.[1613] Ein Löschungsanspruch besteht auch bei **unwahren Tatsachenbehauptungen,** sonstigen **beleidigenden Bewertungen** oder sonst unzulässigen Bewertungen.[1614] Ein Löschungsanspruch hinsichtlich einer schlechten Benotung wurde daher vom OLG München einem bewerteten Arzt zuerkannt, soweit für die getroffene Bewertung keine tatsächlichen Anhaltspunkte bestanden.[1615]

840 Umgekehrt kann die Person des Bewerteten auch die Zulässigkeit der Datennutzung zu Bewertungszwecken begründen. *Roggenkamp* nennt hier als Orientierungshilfe: „Je herausragender und öffentlicher die Position des zu Bewertenden, desto eher ist eine öffentliche Erörterung und Bewertung dieser Person hinzunehmen."[1616]

841 Der BGH hat auf Grundlage des bisherigen nationalen Datenschutzrechts über die generelle Zuordnung zu einer bestimmten Sphäre **weitere Kriterien** entwickelt, die bei der Interessenabwägung zu berücksichtigen sind. Es bleibt abzuwarten, ob diese auch unter der **DSGVO** von Bestand sein werden. Ausgangspunkt ist das Gefährdungspotential, das von Bewertungsportalen im Internet insbesondere gegenüber dem Persönlichkeitsrecht ausgeht. Dem kann und ist auch mit einer entsprechenden (technisch-organisatorischen) Portalgestaltung zu begegnen.[1617] Hierzu zählen:

842 Der **Registrierungsmodus:** Die Notwendigkeit zur Verifizierung einer E-Mail-Adresse macht dem Bewertenden die Verbindlichkeit und Zurechenbarkeit seiner Bewertung deutlich, ohne dass damit dessen Anonymität nach außen aufgehoben werden muss.

843 Die Vermeidung einer Verknüpfung mit **Suchmaschinen:** Einzelne Bewertungen sind so nur im Kontext der konkreten Portalnutzung unter Berücksichtigung der Nutzungsbedingungen möglich und wirken einer diffusen Streuwirkung der Bewertungen entgegen.

844 Der **Löschungsmodus:** Das Bewertungsinteresse verliert mit zunehmendem Abstand zum Bewertungszeitpunkt an Schutzwürdigkeit.

845 Ein **Abuse-Button:** Die technisch einfache Möglichkeit zur Meldung eines Missbrauchs dient dem Rechtsgüterschutz und hat zugleich abschreckende Wirkung.

4. Bewertungsportale und der Persönlichkeitsschutz

846 In inhaltlicher Hinsicht unterliegt die Bewertung insbesondere von Personen den Schranken des verfassungsrechtlich garantierten Persönlichkeitsschutzes.[1618] Dabei hat der Bewertete grundsätzlich auch negative Bewertungen, inhaltliche Kritik an seinem Verhalten und sogar pointiert vorgetragene

---

1610 *Paschke*, AnwZert ITR 17/2017 Anm. 2.

1611 *Paschke*, AnwZert ITR 17/2017 Anm. 2.

1612 Vgl. zur alten Rechtslage grundsätzlich zur Prangerwirkung im Internet *Greve/Schärdel*, MMR 2008, 644.

1613 *Roggenkamp*, K&R 2009, 571, 572.

1614 Zur alten Rechtslage BGH v. 23.09.2014 - VI ZR 358/13 - juris Rn. 36 mit Anm. *Starnecker/Tausch*, jurisPR-ITR 1/2015 Anm. 3; *Ernst*, jurisPR-WettbR 12/2014 Anm. 4; *Meyer*, K&R 2014, 807 ff.

1615 Zur alten Rechtslage OLG München v. 17.10.2014 - 18 W 1933/14 mit Anm. *Brennecke/Wilkat*, IPRB 2015, 45 ff.

1616 *Roggenkamp*, K&R 2009, 571, 572.

1617 BGH v. 23.06.2009 - VI ZR 196/08 - MMR 2009, 608, 614 - spickmich.

1618 *Götting/Lauber-Rönsberg*, AL 2013, 165 ff.

© 2019 juris GmbH | www.juris.de

Meinungsäußerungen hinzunehmen. Die **Grenze** solcher Bewertungen ergibt sich wie auch bei ähnlichen Meinungsäußerungen aus dem Recht der persönlichen Ehre als Ausdruck des allgemeinen Persönlichkeitsrechts. Unzulässig sind demzufolge Diffamierungen jeglicher Art, Schmähkritik und ähnliche Äußerungen, die den Bewerteten zum Objekt solcher Bewertungen machen.[1619] Die Abgrenzung Meinungsfreiheit gegen Persönlichkeitsschutz folgt den etablierten verfassungsrechtlichen Grundsätzen.[1620]

VI. Datenschutz und Videoüberwachung

847 Mit § 4 BDSG übernimmt der Gesetzgeber weitestgehend die bislang in § 6b BDSG a.F. normierten Vorgaben zur Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung).[1621] Mit Blick auf die Konzeption der Vorschrift hat der Gesetzgeber insbesondere dem Umstand Rechnung getragen, dass sich die bloße Beobachtung regelmäßig als schwächerer Eingriff darstellt als eine daran anschließende Weiterverarbeitung.[1622] Mithin hat der Gesetzgeber am bereits bekannten **Stufenverhältnis** zwischen der Zulässigkeit der Beobachtung (nunmehr § 4 Abs. 1 BDSG) sowie der Zulässigkeit der Weiterverarbeitung (jetzt insbesondere § 4 Abs. 3 BDSG) festgehalten.[1623]

848 Insbesondere da § 4 BDSG uneingeschränkt sowohl für **öffentliche als auch für nicht öffentliche Stellen** gilt, wird dessen Vereinbarkeit mit den Vorgaben der DSGVO in Frage gestellt.[1624] Im Bereich nichtöffentlicher Stellen soll, mangels entsprechender Konkretisierungsmöglichkeit für die nationalen Gesetzgeber, vielmehr Art. 6 Abs. 1 Satz 1 lit. f DSGVO (vgl. dazu Rn. 335 ff.) zur Rechtfertigung der Videoüberwachung herangezogen werden.[1625]

849 Der Anwendungsbereich der Norm beschränkt sich allerdings auf **öffentlich zugängliche Räume,** bei nicht öffentlich zugänglichen Räumen kann insbesondere im Kontext des Beschäftigtendatenschutzes die Vorschrift des § 26 BDSG einschlägig sein.[1626] Vorausgesetzt wird, dass der zu überwachende Raum entweder dem öffentlichen Verkehr gewidmet ist oder aber dem Zweck nach dazu bestimmt ist, von einer Vielzahl unbestimmter Personen betreten oder genutzt zu werden.[1627] Nicht entscheidend sind dabei Eigentums- oder Besitzverhältnisse, so dass insbesondere auch Eingangsbereiche oder Treppenhäuser öffentlich zugänglich im Sinne der Norm sein können.[1628] Im Umkehrschluss sind solche Räume, welche ausschließlich bestimmten Personen beziehungsweise Personengruppen zugänglich sind, **nicht öffentlich** zugänglich.[1629] Dass eine bestimmte

---

[1619] BGH v. 23.06.2009 - VI ZR 196/08 - MMR 2009, 608, 611 - spickmich.

[1620] Vgl. auch *Roggenkamp*, K&R 2009, 571, 573; *Dix*, DuD 2013, 44; *Schwarz*, JA 2017, 241, *Cremer*, ZRP 2017, 151.

[1621] BT-Drs. 18/11325, S. 81.

[1622] *Frenzel* in: Paal/Pauly, DS-GVO/BDSG, § 4 BDSG Rn. 2.

[1623] BT-Drs. 18/11325, S. 81.

[1624] Vgl. *Kühling*, NJW 2017, 1985, 1987; *Mienert/Gipp*, ZD 2017, 514, 515; *Ziebarth*, ZD 2017, 467, 469; *Lachenmann*, ZD 2017, 407, 410; *Starnecker* in: Gola/Heckmann, BDSG, § 4 Rn. 9 ff.; *Buchner* in: Kühling/Buchner, DS-GVO/BDSG, § 4 BDSG Rn. 2 ff.; *Frenzel* in: Paal/Pauly, DS-GVO/BDSG, § 4 BDSG Rn. 5, 6.

[1625] *Mienert/Gipp*, ZD 2017, 514, 515; *Starnecker* in: Gola/Heckmann, BDSG, § 4 Rn. 11; *Buchner* in: Kühling/Buchner, DS-GVO/BDSG, § 4 BDSG Rn. 4.

[1626] Vgl. *Byers/Wenzel*, BB 2017, 2036, 2039; *Däuber*, NZA 2017, 1481, 1484; *Lachenmann*, ZD 2017, 407, 410; *Buchner* in: Kühling/Buchner, DS-GVO/BDSG, § 4 BDSG Rn. 6.

[1627] *Buchner* in: Kühling/Buchner, DS-GVO/BDSG, § 4 BDSG Rn. 6; *Starnecker* in: Gola/Heckmann, BDSG, § 4 Rn. 23.

[1628] *Frenzel* in: Paal/Pauly, DS-GVO/BDSG, § 4 BDSG Rn. 9.

[1629] *Starnecker* in: Gola/Heckmann, BDSG, § 4 Rn. 23.

© 2019 juris GmbH | www.juris.de

Räumlichkeit allerdings nicht öffentlich zugänglich sein soll, muss durch den Willen des jeweiligen Verfügungsberechtigten zum Ausdruck kommen, wobei sich der Rückgriff auf Verbotsschilder und/oder bauliche Maßnahmen anbietet.[1630]

850 § 4 Abs. 1 Satz 1 BDSG regelt die Zulässigkeit der **Beobachtung** mit optisch-elektronischen Einrichtungen. Wortlaut und Systematik der Norm zwingen dabei zu dem Schluss, dass die bloße **Übertragung** etwaiger Bilder zu einem Monitor ausreichend ist, um das Tatbestandsmerkmal des Beobachtens zu erfüllen. Dafür spricht einerseits, dass allein der Vorgang der Beobachtung keiner Speicherung bedarf, andererseits, dass § 4 Abs. 3 BDSG gesonderte Vorgaben für den Fall der Speicherung und Verwendung trifft.[1631]

851 Zulässig ist die Beobachtung, soweit sie zur Aufgabenerfüllung öffentlicher Stellen (§ 4 Abs. 1 Satz 1 Nr. 1 BDSG), zur Wahrnehmung des Hausrechts (§ 4 Abs. 1 Satz 1 Nr. 2 BDSG) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (§ 4 Abs. 1 Satz 1 Nr. 3 BDSG) erforderlich ist.[1632] Zudem dürfen keine Anhaltspunkte bestehen, dass **schutzwürdige Interessen** der Betroffenen überwiegen. Für den Fall, dass **großflächige Anlagen,** wie beispielsweise Sport- oder Vergnügungsstätten oder aber der öffentliche Schienen-, Schiffs- und Busverkehr überwacht werden sollen, gelten die Schutzgüter Leben, Gesundheit oder Freiheit als besonders abwägungsrelevant, § 4 Abs. 1 Satz 2 BDSG. Sofern die genannten Schutzgüter betroffen sein könnten, geht der Gesetzgeber regelmäßig von einer Abwägungsentscheidung zugunsten der Videoüberwachung aus.[1633]

852 § 4 Abs. 2 BDSG sieht vor, dass der Umstand der Beobachtung sowie der Name und die Kontaktdaten des Verantwortlichen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt **erkennbar** gemacht werden müssen. Der Norm können dabei keine konkreten Formerfordernisse entnommen werden, aus praktischer Perspektive wird sich aber regelmäßig der Einsatz eines Hinweisschildes anbieten.[1634] Bei der Verwendung entsprechender Piktogramme ist darauf zu achten, dass die Betroffenen diese auch tatsächlich wahrnehmen können, wobei insbesondere die Platzierung und formelle Ausgestaltung von Relevanz sind.[1635] Vor dem Hintergrund, dass der europäische Verordnungsgeber mit der Schaffung der DSGVO insbesondere dem Transparenzprinzip einen hohen Stellenwert beigemessen hat, spricht vieles dafür, dass der unterbliebene Hinweis im Sinne des § 4 Abs. 2 BDSG zur Rechtswidrigkeit der Videoüberwachung führt.[1636]

853 Die **Speicherung oder Verwendung** der nach § 4 Abs. 1 BDSG erhobenen Daten ist unter den Voraussetzungen des § 4 Abs. 3 Satz 1 BDSG zulässig. Insbesondere ist die (weiterführende) Verarbeitung nur zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. In der Folge wird gefordert, dass eine Weiterverarbeitung lediglich dann zulässig ist, wenn allein die Aufzeichnung zur intendierten Zweckerreichung der Videoüberwachung nicht ausreichend ist.[1637]

1630 *Starnecker* in: Gola/Heckmann, BDSG, § 4 Rn. 23.

1631 So i.E. auch *Däubler*, NZA 2017, 1481, 1484; *Starnecker* in: Gola/Heckmann, BDSG, § 4 Rn. 29; *Buchner* in: Kühling/Buchner, DS-GVO/BDSG, § 4 BDSG Rn. 7; *Frenzel* in: Paal/Pauly, DS-GVO/BDSG, § 4 BDSG Rn. 7.

1632 Umfassend zu den einzelnen Zulässigkeitstatbeständen *Starnecker* in: Gola/Heckmann, BDSG, § 4 Rn. 33 ff.

1633 BT-Drs. 18/11325, S. 81.

1634 *Starnecker* in: Gola/Heckmann, BDSG, § 4 Rn. 53.

1635 *Frenzel* in: Paal/Pauly, DS-GVO/BDSG, § 4 BDSG Rn. 27.

1636 Vgl. dazu m.w.N. *Starnecker* in: Gola/Heckmann, BDSG, § 4 Rn. 57.

1637 *Frenzel* in: Paal/Pauly, DS-GVO/BDSG, § 4 BDSG Rn. 31; *Buchner* in: Kühling/Buchner, DS-GVO/BDSG, § 4 BDSG Rn. 16.

© 2019 juris GmbH | www.juris.de

854 Die **Weiterverarbeitung** zu **anderen Zwecken** ist gem. § 4 Abs. 3 Satz 3 BDSG nur zulässig, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Ob eine derart umfassende Durchbrechung des Zweckbindungsgrundsatzes (vgl. dazu Rn.189 ff.) zugunsten der Sicherheitsbehörden mit den Grundrechten zu vereinbaren ist, bleibt abzuwarten.[1638] Jedenfalls aber ist die Norm dergestalt europarechtskonform auszulegen, dass abseits der Vorgaben des § 4 Abs. 3 Satz 3 BDSG auch weitergehende Erlaubnistatbestände, wie etwa in Art. 6 Abs. 4 DSGVO vorgesehen, eine Zweckänderung im Einzelfall rechtfertigen können.[1639]

855 Für den Fall, dass durch die Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet werden, sieht § 4 Abs. 4 Satz 1 BDSG vor, dass die betroffene Person über die Überwachung gem. Art. 13 beziehungsweise Art. 14 DSGVO **informiert** werden muss. Umfang und Form der Informationspflicht bestimmt sich insbesondere nach den Vorgaben des Art. 13 DSGVO (vgl. dazu bereits Rn. 352 ff.).[1640]

856 Gem. § 4 Abs. 5 BDSG sind die Daten unverzüglich zu **löschen,** wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Bei der Prüfung, ob eine Löschung der Daten erforderlich ist, kommt es stets auf die Vorgaben des **Einzelfalls** an, wobei insbesondere zu prüfen ist, ob der spezifische Überwachungszweck eine weitergehende Speicherung noch rechtfertigen kann.[1641]

VII. Der Datenschutz im Beschäftigungsverhältnis

857 Gestützt auf die Konkretisierungsmöglichkeit des Art. 88 DSGVO hat der nationale Gesetzgeber die **zentralen Vorgaben** zur Datenverarbeitung im Beschäftigungskontext nunmehr in **§ 26 BDSG** normiert.[1642] Im Rahmen des Anwendungsbereichs der Vorschrift treten die Vorgaben der DSGVO zurück.[1643] Die Vorschrift orientiert sich dabei maßgeblich an den Vorgaben des § 32 BDSG a.F., so dass auf die bereits umfassend vorhandene Literatur zum Beschäftigungsdatenschutz, jedenfalls unter Berücksichtigung der Vorgaben der DSGVO, zurückgegriffen werden kann.[1644] Die nachfolgende Darstellung liefert einen prägnanten Überblick über wesentliche Aspekte des § 26 BDSG.

858 Neben der Klarstellung, dass auch die Einwilligung im Beschäftigungskontext herangezogen werden kann, normiert § 26 BDSG **fünf Erlaubnistatbestände** für die Verarbeitung personenbezogener Daten der Beschäftigten.[1645]

859 Insbesondere dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die **Begründung** eines Beschäftigungsverhältnisses oder nach Begründung für dessen **Durchführung** oder **Beendigung** erforderlich ist. Die Verarbeitung im Rahmen des Beschäftigungsverhältnisses kann zudem zulässig

---

1638 Ebenfalls kritisch *Lachenmann*, ZD 2017, 407, 410.

1639 *Starnecker* in: Gola/Heckmann, BDSG, § 4 Rn. 61.

1640 *Starnecker* in: Gola/Heckmann, BDSG, § 4 Rn. 65.

1641 *Starnecker* in: Gola/Heckmann, BDSG, § 4 Rn. 69.

1642 BT-Drs. 18/11325, S. 96.

1643 *Gola*, BB 2017, 1462, 1463; *Gräber/Nolden* in: Paal/Pauly, DS-GVO/BDSG, § 26 BDSG Rn. 2; *Riesenhuber* in: Wolff/Brink, Beck'scher Onlinekommentar, § 26 BDSG Rn. 20.

1644 Vgl. *Ströbel/Böhm/Breunig/Wybitul*, CCZ 2018, 14, 15; *Gola*, BB 2017, 1462, 1464; *Kühling*, NJW 2017, 1985, 1988; *Riesenhuber* in: Wolff/Brink, Beck'scher Onlinekommentar, § 26 BDSG Rn. 1 ff.; *Gräber/Nolden* in: Paal/Pauly, DS-GVO/BDSG, § 26 BDSG Rn. 1.

1645 Ausführlich zu den einzelnen Erlaubnistatbeständen: *Gola*, BB 2017, 1462, 1464; *Gola* in: Gola/Heckmann, BDSG, § 26 Rn. 18 ff.; *Gräber/Nolden* in: Paal/Pauly, DS-GVO/BDSG, § 26 BDSG Rn. 5 ff .;*Maschmann* in: Kühling/Buchner, DS-GVO/BDSG, § 26 BDSG Rn. 17 ff.

© 2019 juris GmbH | www.juris.de

sein, wenn diese zur Ausübung oder Erfüllung der sich aus einem **Gesetz** oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung **(Kollektivvereinbarung)** ergebenden Rechte und Pflichten der Interessenvertretung erforderlich ist. Unter den Voraussetzungen des § 26 Abs. 1 Satz 2 BDSG können Beschäftigtendaten zudem zur **Aufdeckung** von **Straftaten** innerhalb des Beschäftigungsverhältnisses verarbeitet werden. Für den Fall, dass **sensible Daten** der Beschäftigten (vgl. allgemein zum Begriff des sensiblen Datums im Sinne der DSGVO Rn. 115 ff.) im Rahmen des Beschäftigungsverhältnisses verarbeitet werden sollen, sind die Vorgaben des § 26 Abs. 3 BDSG zu beachten.

860 § 26 Abs. 2 BDSG bestimmt, dass die **Einwilligung** (vgl. zu den Einzelheiten der Einwilligung nach den Vorgaben der DSGVO Rn. 259 ff.) auch im Kontext des Beschäftigungsverhältnisses herangezogen werden kann. Zugleich normiert § 26 Abs. 2 BDSG allerdings gesonderte Voraussetzungen, welche bei der Einholung der Einwilligungserklärung zu beachten sind. Von besonderer Relevanz sind dabei die gesteigerten Anforderungen an die **Freiwilligkeit**, § 26 Abs. 2 Satz 1 und Satz 2 BDSG, sowie das grundsätzliche **Schriftformerfordernis** in § 26 Abs. 2 Satz 3 BDSG.

861 Bei der Beurteilung der **Freiwilligkeit** der Einwilligungserklärung im Beschäftigungsverhältnis (vgl. allgemein zum Kriterium der Freiwilligkeit im Rahmen der Einwilligung Rn. 259 ff.) sind gem. § 26 Abs. 2 Satz 1 BDSG die bestehende **Abhängigkeit** der beschäftigten Person sowie die **Umstände,** unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Im Sinne eines Regelbeispiels[1646] bestimmt § 26 Abs. 2 Satz 2 BDSG, dass das Kriterium der Freiwilligkeit insbesondere dann gegeben sein kann, wenn die beschäftigte Person durch die Einwilligung einen rechtlichen oder wirtschaftlichen Vorteil erlangt oder der Arbeitgeber und der Beschäftigte bei der Abgabe der Einwilligung gleichgelagerte Interessen verfolgen.

862 Unter Berücksichtigung dessen, dass die Verarbeitung im Beschäftigungsverhältnis regelmäßig auf die gesetzlichen Erlaubnistatbestände des § 26 Abs. 1 sowie Abs. 3 BDSG beziehungsweise ergänzend auf Art. 6 Abs. 1 Satz 1 lit. f DSGVO (vgl. dazu Rn. 308 ff.) gestützt werden kann, ist davon auszugehen, dass die Einwilligung lediglich eine **nachgeordnete Rolle** einnehmen wird.[1647] Der Rückgriff auf die Einwilligungserklärung kommt allerdings im Kontext **freiwilliger Leistungen** des Arbeitgebers in Betracht.[1648] Dabei gilt es allerdings zu beachten, dass auch dann nicht mehr von einer freiwilligen Abgabe der Einwilligung ausgegangen werden kann, wenn die Gratifikation zwingend von der Abgabe der Einwilligungserklärung abhängig gemacht wird.[1649]

863 Im Gegensatz zu § 32 BDSG a.F. normiert § 26 Abs. 3 BDSG nunmehr ausdrücklich einen Erlaubnistatbestand für die Verarbeitung **sensibler Daten** (zum Begriff vgl. Rn. 115 ff.) im Beschäftigungsverhältnis.[1650] Für Zwecke des Beschäftigungsverhältnisses ist die Verarbeitung zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und Sozialschutzes erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen. Vor dem Hintergrund der besonderen Schutzbedürftigkeit sensibler Daten ist allerdings nur in jenen Fällen von einer Zulässigkeit der Verarbeitung auf Grundlage des § 26

1646 So *Riesenhuber* in: Wolff/Brink, Beck'scher Onlinekommentar, § 26 BDSG Rn. 20.

1647 *Gola*, BB 2017, 1462, 1468.

1648 *Gräber/Nolden* in: Paal/Pauly, DS-GVO/BDSG, § 26 BDSG Rn. 27; *Riesenhuber* in: Wolff/Brink, Beck'scher Onlinekommentar, § 26 BDSG Rn. 47.

1649 *Maschmann* in: Kühling/Buchner, DS-GVO/BDSG, § 26 BDSG Rn. 63.

1650 *Gräber/Nolden* in: Paal/Pauly, DS-GVO/BDSG, § 26 BDSG Rn. 40.

© 2019 juris GmbH | www.juris.de

Abs. 3 BDSG auszugehen, in denen die Ausübung des Rechts beziehungsweise die Erfüllung der rechtlichen Pflicht anderenfalls nicht möglich wäre.[1651] Die Verarbeitung muss also konstitutiv für die jeweilige Rechtsausübung sein.[1652]

864 Sofern der Arbeitgeber die Verarbeitung sensibler Daten auf die Grundlage einer Einwilligung stützen möchte, muss sich diese **Einwilligung** ausdrücklich auf die Daten beziehen, § 26 Abs. 3 Satz 2 BDSG.

865 § 26 Abs. 5 BDSG stellt klar, dass der Verantwortliche geeignete Maßnahmen ergreifen muss, um sicherzustellen, dass insbesondere die in **Art. 5 DSGVO** dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden. Allen voran der Verweis auf den in Art. 5 Abs. 1 lit. a DSGVO angelegten **Transparenzgrundsatz** (vgl. allgemein zu dessen Vorgaben Rn. 189 ff.) und dessen Ausgestaltung durch die Informationspflichten der Art. 12 ff. DSGVO (vgl. dazu Rn. 355 ff.) führen zu einem Spannungsverhältnis mit jedenfalls bislang restriktiv zulässigen **verdeckten Mitarbeiterkontrollen.**[1653] Dabei wird vertreten, dass die Vorgaben des § 26 BDSG, insbesondere der Erlaubnistatbestand zur Aufdeckung von Straftaten gem. § 26 Abs. 1 Satz 2 BDSG, nicht ausreichend seien, um heimliche Überwachungsmaßnahmen im Beschäftigungsverhältnis zu legitimieren.[1654] Da es allerdings berechtigte Interessen des Arbeitgebers an einer verdeckten Mitarbeiterüberwachung geben kann und die heimliche Mitarbeiterüberwachung nicht ausdrücklich durch § 26 BDSG adressiert wird, wird der **Rückgriff auf Art. 6 Abs. 1 lit. f DSGVO** vorgeschlagen.[1655] Die durchzuführende Interessenabwägung könnte sodann insbesondere unter Berücksichtigung der bisherigen BAG-Rechtsprechung zur verdeckten Mitarbeiterüberwachung durchgeführt werden.[1656]

VIII. Datenschutz im Kontext sicherheitsbehördlicher Befugnisse

1. Allgemeines

a. Spannungsfeld zwischen Freiheit und Sicherheit

866 Seit jeher stehen Freiheit und Sicherheit in einem Spannungsverhältnis. Sie sind aber **keine unversöhnlichen Widersprüche;** sie stehen vielmehr in einem Komplementärverhältnis: Sie setzen sich wechselseitig voraus und stärken einander, wenn beide angemessen zur Entfaltung gelangen.[1657] Dieses Spannungsfeld prägt geradezu das gesamte Polizei-, Strafprozess- und Sicherheitsrecht. Diesen gordischen Knoten zwischen individueller Freiheit und staatlichen Eingriffsbefugnissen zu lösen, ist Aufgabe der Politik, die nach programmatischer Ausrichtung der Regierungsparteien, aber auch dem Zeitgeist entsprechend mal die Sicherheit, mal die Freiheit in den Vordergrund stellt.[1658]

1651 Vgl. dazu m.w.N. *Gola* in: Gola/Heckmann, BDSG, § 26 Rn. 147.

1652 *Gola* in: Gola/Heckmann, BDSG, § 26 Rn. 147.

1653 Vgl. dazu ausführlich *Byers*, NZA 2017, 1086 ff.; *Maschmann* in: Kühling/Buchner, DS-GVO/BDSG, § 26 BDSG Rn. 22; zur Frage der Zulässigkeit etwaiger Predictive Policing-Maßnahmen vgl. *Rudkowski*, NZA 2019, 72 ff.

1654 *Byers*, NZA 2017, 1086, 1089; *Maschmann* in: Kühling/Buchner, DS-GVO/BDSG, § 26 BDSG Rn. 22.

1655 *Byers*, NZA 2017, 1086, 1089.

1656 *Byers*, NZA 2017, 1086, 1090.

1657 Vgl. *Di Fabio*, NJW 2008, 421, 422; *Seidl*, PVT 2010, 276.

1658 *Heckmann*, Öffentliches Recht in Bayern, 7. Aufl. 2017, Teil 3, Rn. 43.

© 2019 juris GmbH | www.juris.de

867 Unter dem Eindruck der Menschenleben verachtenden Terroranschläge von New York, Madrid und London und der auch seitens deutscher Sicherheitskräfte immer wieder betonten akuten Terrorbedrohung läuft der Staat jedoch Gefahr, die angemessene **Balance** zwischen Sicherheit und Freiheit zu verlieren und die Freiheit der Sicherheit zu opfern.[1659]

868 Um der immer globaler werdenden, vernetzten Kriminalität, insbesondere der organisierten Kriminalität, und dem Terrorismus zu begegnen, wurden in den letzten Jahren zahlreiche sicherheitsrechtliche **Eingriffsbefugnisse** für Polizei, Verfassungsschutz und Nachrichtendienste geschaffen beziehungsweise erweitert.[1660] Erwähnt seien hier nur die Online-Durchsuchung und die Vorratsdatenspeicherung als die wohl umstrittensten.

869 In einer ganzen Reihe von grundlegenden Entscheidungen hat das Bundesverfassungsgericht gleichsam als „Hüter der Grundrechte" viele dieser neuen Befugnisse auf ihre **Verfassungsmäßigkeit** beleuchtet und sie häufig für zwar nicht dem Grunde, aber der Art ihrer konkreten Ausgestaltung nach für verfassungswidrig erklärt. Wie eine Auswahl der wichtigsten Urteile des Bundesverfassungsgerichts in diesem Zusammenhang zeigt[1661], standen dabei vor allem informationstechnologische Instrumente moderner Sicherheitspolitik im Mittelpunkt.

870 Dem Traum, in einer globalisierten Welt zu leben, deren vernetzte Infrastrukturen, insbesondere im Telekommunikations- und Internetbereich, dazu beitragen, das Leben zu erleichtern, ist die Gefahr inhärent, dass die **Verletzlichkeit dieser modernen Gesellschaft** bisher unbekannte Dimensionen erreicht. So kann mit geringem Aufwand und verhältnismäßig kostengünstigen Mitteln durch eine einzige Aktion eine Vielzahl von Menschenleben gefährdet werden.[1662]

871 Letztlich darf also, wer über Freiheit redet, über Sicherheit nicht schweigen, denn **mit der Sicherheit beginnt die Freiheit.**[1663]

b. Relevanz

872 Laut der aktuellen deutschen **polizeilichen Kriminalstatistik des Bundeskriminalamts (PKS)** wurden im Jahr 2017 in Deutschland 5.761.984 Straftaten polizeilich registriert.[1664] Im Bereich der Computer-Kriminalität ist ein leichter Zuwachs der registrierten Straftaten gegenüber dem Vorjahr zu verzeichnen (108.510 Fälle; 2016: 107.751 Fälle).[1665]

873 Zu bedenken ist jedoch, dass es sich bei der PKS um eine **reine Arbeitsstatistik** mit beschränktem Aussagewert handelt[1666], die zudem nur das sog. Hellfeld – also die der Polizei bekannt gewordene Kriminalität – erfasst. Aufgrund fehlender statistischer Daten kann das sog. Dunkelfeld – polizeilich nicht bekannt gewordene Kriminalität – in der PKS nicht abgebildet werden. Gerade im Bereich der Internetkriminalität dürfte jedoch das Dunkelfeld nicht unerhebliche Fallzahlen aufweisen.

1659 *Heckmann*, Öffentliches Recht in Bayern, 7. Aufl. 2017, Teil 3, Rn. 43.

1660 Vgl. dazu umfassend *Heckmann*, Öffentliches Recht in Bayern, 7. Aufl. 2017, Teil 3, Rn. 44 ff.

1661 BVerfG v. 04.04.2006 - 1 BvR 518/02 zur Rasterfahndung; BVerfG v. 27.02.2008 - 1 BvR 370/07 und 1 BvR 595/07 zur Online-Durchsuchung; BVerfG v. 11.03.3008 - 1 BvR 2074-05, 1254/07 zur Kennzeichenerfassung und BVerfG v. 11.03.2010 - 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 zur Vorratsdatenspeicherung.

1662 *Schmidbauer/Steiner*, Bayerisches Polizeiaufgabengesetz, 3. Aufl. 2011, Vorwort.

1663 *Di Fabio*, NJW 2008, 421, 422.

1664 Vgl. Bundesministerium des Innern, für Bau und Heimat, Bericht zur Polizeilichen Kriminalstatistik 2017, S. 10; abrufbar unter: www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2017/pks2017_node.html;jsessionid=513636DE01C892917D066575752AF0B3.live0612 (abgerufen am 01.03.2019).

1665 Bundesministerium des Innern, für Bau und Heimat, Bericht zur Polizeilichen Kriminalstatistik 2017, S. 17.

1666 Vertiefend *P.-A. Albrecht*, Kriminologie, 4. Aufl. 2010. S. 173 ff.

874 Auch die aktuellen Zahlen vom 18.07.2017 aus der Übersicht über die Telekommunikationsüberwachung für 2016 (Maßnahmen nach § 100a StPO) des Bundesamtes für Justiz belegen die große **Relevanz des Persönlichkeitsrechts- und Datenschutzes** bei den Sicherheitsbehörden. So wurden im Jahr 2016 in der Bundesrepublik allein 17.510 Erstanordnungen nach § 100a StPO getroffen.[1667] Massiv erhöhen dürfte sich die Zahl der Telekommunikationsüberwachungsmaßnahmen noch durch die Vielzahl der von den einzelnen Bundesländern präventiv nach den jeweiligen Landespolizeigesetzen durchgeführten Telekommunikationsüberwachungen.

875 Um einem weiteren Anstieg in diesen Deliktsfeldern entgegenzuwirken, wird verstärkt auch eine **Anpassung der Befugnisse und der Vorgehensweisen der Polizei-, Sicherheits- und Strafverfolgungsbehörden gefordert.** Diese sollten mit effektiven und auch hinreichend dynamisch ausgestalteten Ermittlungsbefugnissen ausgestattet werden. Jedoch darf in diesem Zusammenhang nicht außer Acht gelassen werden, dass die Schaffung derartiger Befugnisse und deren zumeist heimliche, verdeckte Anwendung zu einer Vielzahl von Daten führen und somit einen schweren Grundrechtseingriff darstellen.

876 Diesbezüglich lässt sich insbesondere die **Gesichtserkennung** anführen, die über die sozialen Netzwerke hinaus (vgl. dazu auch Rn. 757 ff.) auch verstärkt von der Polizei zur Gefahrenabwehr eingesetzt werden soll, so etwa in Sachsen[1668] und Bayern[1669]. Auch die Bundespolizei, das BKA und die LKA setzen die Gesichtserkennung immer mehr ein: Während 2010 lediglich 1.673 Fälle verzeichnet wurden, wurden 2017 bereits 27.436 Fälle registriert.[1670]

877 Einer BITKOM-Untersuchung[1671] zufolge werden **staatliche Eingriffe** von **Internetnutzern** je nach Bereich und Anlass **unterschiedlich bewertet.** Während sich eine klare Mehrheit der Internetnutzer bei der vorbeugenden Gefahrenabwehr (78% der User), z.B. bei Terrorgefahr und bei Aufklärung und Verfolgung von Straftaten (74% der User), einen stärkeren staatlichen Eingriff ins Internet wünscht, wird im Hinblick auf die Speicherung von Internet-Verbindungsdaten für polizeiliche Zwecke mehrheitlich (62% der User) eine stärkere Zurückhaltung des Staates erbeten. Bei der Überwachung von Nachrichten und Gesprächsinhalten für polizeiliche Zwecke erhoffen sich 62% der Internetnutzer weniger starke Eingriffe des Staates.

2. Verfassungsrechtliche Rahmenbedingungen

878 Verfassungsrechtliche Grundlage für den Datenschutz bei den Polizei-, Sicherheits- und Strafverfolgungsbehörden ist in Deutschland das **Grundrecht auf informationelle Selbstbestimmung.** Dieses wurde vom Bundesverfassungsgericht im Volkszählungsurteil aus dem Allgemeinen Persönlichkeitsrecht, Art. 2 Abs. 1 und Art. 1 Abs. 1 GG, entwickelt und genauer bestimmt: Es gewährt dem Einzelnen die Befugnis, „grundsätzlich selbst über die Verwendung und Preisgabe seiner

[1667] Bundesamt für Justiz, Übersicht Telekommunikationsüberwachung (Maßnahmen nach § 100a StPO für 2016). Abrufbar unter: www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2016.pdf?__blob=publicationFile&v=2 (abgerufen am 01.03.2019).

[1668] Vgl. *Krempl*, Sachsen: Polizei soll mit Gesichtserkennung und präventiver Überwachung Verbrecher jagen. Abrufbar unter: www.heise.de/newsticker/meldung/Sachsen-Polizei-soll-mit-Gesichtserkennung-und-praeventiver-Ueberwachung-Verbrecher-jagen-4029067.html (abgerufen am 01.03.2019).

[1669] Vgl. Bayerische Staatsregierung, Biometrische Gesichtserkennung bei Täterfahndung. Abrufbar unter: www.bayern.de/biometrische-gesichtserkennung-bei-taeterfahndung/ (abgerufen am 01.03.2019).

[1670] Vgl. Heise Online, Polizei setzt immer mehr automatische Gesichtserkennung ein, Datenschützer besorgt. Abrufbar unter: www.heise.de/newsticker/meldung/Polizei-setzt-immer-mehr-automatische-Gesichtserkennung-ein-Datenschuetzer-besorgt-4000106.html (abgerufen am 01.03.2019).

[1671] Bitkom, Datenschutz im Internet, 2011. Abrufbar unter: www.bitkom.org/Bitkom/Publikationen/Studie-Datenschutz-im-Internet.html (abgerufen am 01.03.2019).

© 2019 juris GmbH | www.juris.de

persönlichen Daten zu bestimmen“[1672] und zu wissen, wer was wann und bei welcher Gelegenheit über ihn weiß[1673]. Dabei unterstrich das Bundesverfassungsgericht, das Grundrecht auf informationelle Selbstbestimmung bedürfe unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes.[1674] Eingriffe in den Schutzbereich der informationellen Selbstbestimmung sind deshalb nur gerechtfertigt, wenn sie im überwiegenden Allgemeininteresse geschehen, auf einer verfassungsmäßigen, gesetzlichen Grundlage beruhen und dem Grundsatz der Verhältnismäßigkeit genügen.[1675] Organisatorische und verfahrensrechtliche Vorkehrungen sollen dabei eine Verletzung des Persönlichkeitsrechts verhindern.[1676]

879 Relativ neu – und gerade für die präventiven und repressiven Ermittlungsmaßnahmen, aber auch in besonderer Weise für die Geheimdienste relevant – ist das vom Bundesverfassungsgericht im Beschluss zur Online-Durchsuchung neu formulierte **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.**[1677] Auch dieses Grundrecht entspringt dem allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

880 Den **Schutzbereich** dieses „IT- bzw. Computergrundrechts“ fasst das Bundesverfassungsgericht wie folgt:

„Geschützt vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.“[1678]

881 Eingriffe in das sogenannte IT-Grundrecht“[1679] sind zwar grundsätzlich möglich, erfordern aber das **Bestehen von tatsächlichen Anhaltspunkten für eine konkrete Gefahr für ein überragend wichtiges Rechtsgut** sowie die Gewährung von verfahrensrechtlichem Schutz durch Richtervorbehalt.[1680]

882 Eingriffe durch Ermittlungsmaßnahmen können aber auch andere Grundrechte betreffen. Insbesondere sind dies **Art. 10 GG** und **Art. 13 GG.**[1681] Telekommunikationsvorgänge wie das Versenden einer E-Mail, das Telefonieren auf klassischem Wege oder über das Internet (VoIP), der Zugriff auf Internetseiten und das Herunterladen von Webseiten-Inhalten fallen in den Schutzbereich des Fernmeldegeheimnisses.[1682] Nicht von Art. 10 GG erfasst sind allerdings lokal abgespeicherte Daten, die sich nicht mehr im Übertragungsvorgang befinden.[1683] Im Telekommunikationsbereich

---

1672 BVerfG v. 15.12.1983 - 1 BvR 209/83 - NJW 1984, 419, Leitsatz Nr. 1 - Volkszählung.

1673 BVerfG v. 15.12.1983 - 1 BvR 209/83 - NJW 1984, 419, 422 - Volkszählung.

1674 BVerfG v. 15.12.1983 - 1 BvR 209/83 - NJW 1984, 419, 421 - Volkszählung.

1675 BVerfG v. 15.12.1983 - 1 BvR 209/83 - NJW 1984, 419, Leitsatz Nr. 2 - Volkszählung.

1676 BVerfG v. 15.12.1983 - 1 BvR 209/83 - NJW 1984, 419, Leitsatz Nr. 2 - Volkszählung.

1677 BVerfG v. 27.02.2008 - 1 BvR 370, 595/07 - NJW 2008, 822.

1678 BVerfG v. 27.02.2008 - 1 BvR 370, 595/07 - NJW 2008, 822, 827.

1679 *Luch*, MMR 2011, 75, 75.

1680 *Fink* in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, Erster Teil, C. Verfassungsrecht, Rn. 65.

1681 *Kudlich*, GA 2011, 194, 195.

1682 *Kudlich*, GA 2011, 194, 196.

1683 BVerfG v. 02.03.2006 - 2 BvR 2099/04 - NJW 2006, 976; mit Besprechung *Jahn*, JuS 2006, 491 ff.

© 2019 juris GmbH | www.juris.de

findet demnach im Wesentlichen das Fernmeldegeheimnis des Art. 10 Abs. 1 Alt. 3 GG Anwendung, das insoweit spezieller ist gegenüber dem Recht auf informationelle Selbstbestimmung und dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als spezielle Ausprägungen des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Es greift dann, wenn die Datenverarbeitung im Telekommunikationsbereich betroffen ist. Dies ist immer dann der Fall, wenn Telekommunikationsdaten (dazu gehören jedoch nicht nur die Inhaltsdaten der Kommunikation, sondern auch die zugehörigen Verkehrs- und Nutzungsdaten[1684], nicht aber die Bestandsdaten) beim Telekommunikationsmittler betroffen sind, denn insoweit greift das besondere Schutzbedürfnis des Fernmeldegeheimnisses. Auch ein Eingriff in die Unverletzlichkeit der Wohnung (Art. 13 GG) ist denkbar, sobald Überwachungsmaßnahmen nicht ausschließlich während der Datenübertragung stattfinden.[1685]

883 Eine heimliche Erhebung von Daten durch die Sicherheitsbehörden ist nur auf Grundlage von Befugnisnormen zulässig, die klar und bestimmt gefasst sind, weil sie zu schwerwiegenden Grundrechtseingriffen ermächtigen. Das Gebot der Normenklarheit ist verletzt, wenn eine Vorschrift die Befugnisse so ausgestaltet, dass die Polizei die Voraussetzungen und die Reichweite ihres Handelns selbst festlegen muss, um ihren verfassungsrechtlichen Schutzauftrag erfüllen zu können.[1686]

884 Darüber hinaus kommt im Anwendungsbereich der Umsetzungsvorschriften der **JI-Richtlinie** eine zusätzliche Geltung der europäischen Grundrechte in Betracht (vgl. dazu bereits Rn. 14 ff.).[1687] Jedenfalls soweit der nationale Gesetzgeber auf Grund der Vorgaben der JI-Richtlinie keinen eigenständigen Umsetzungsspielraum wahrnehmen konnte, sind die europäischen Grundrechte, also insbesondere die Vorgaben der **Grundrechtecharta** als auch der **EMRK** zu berücksichtigen.[1688]

3. Einfachgesetzliche Vorgaben unter besonderer Berücksichtigung der JI-RL

885 Für den Bereich des Datenschutzes im Kontext der Sicherheitsbehörden ist insbesondere die JI-RL[1689] sowie deren Umsetzung im nationalen Recht von besonderer Relevanz. Die JI-RL enthält Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (also die Bereiche Polizei und Justiz), Art. 1 Abs. 1 JI-RL. Sie dient dem Schutz der natürlichen Personen, insbesondere im Hinblick auf deren informationelle Selbstbestimmung in diesem Bereich, Art. 1 Abs. 2 lit. a JI-RL. Andererseits soll unter dem statuierten Datenschutzniveau der freie Verkehr personenbezogener Daten zwischen den Behörden

1684 BVerfG v. 02.03.2006 - 2 BvR 2099/04 - NJW 2006, 976; ebenso *Kudlich*, GA 2011, 194, 196.

1685 *Kudlich*, GA 2011, 193, 196 f., mit Gegenargumenten zum BVerfG, das in der Online-Durchsuchungsentscheidung ein Eingreifen von Art. 13 GG abgelehnt hatte.

1686 VerfGH Thüringen v. 21.11.2012 - 19/09 - ZD 2013, 79.

1687 So auch *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, Rn. 29.

1688 *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, Rn. 31.

1689 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rats vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

© 2019 juris GmbH | www.juris.de

zu den genannten Zwecken innerhalb der Union und die Übermittlung solcher personenbezogener Daten an Drittländer und internationale Organisationen erleichtert werden, Art. 1 Abs. 2 lit. b JI-RL.[1690]

886 Die JI-RL gilt als europäische Richtlinie nach Art. 288 Abs. 3 AEUV grundsätzlich nicht unmittelbar in den Mitgliedstaaten, sondern muss vom Gesetzgeber erst in nationales Recht umgesetzt werden. Sie ist gem. Art. 1 Abs. 3 JI-RL insoweit **mindestharmonisierend,** als die Mitgliedstaaten strengere Garantien zum Schutz der Rechte und Freiheiten der betroffenen Person bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden ergreifen können. Die Bundesrepublik Deutschland hat die JI-Richtlinie im Wesentlichen **im dritten Teil des BDSG (§§ 45 ff. BDSG) umgesetzt.**[1691] Bei der Auslegung des BDSG ist dabei stets die JI-RL im Auge zu behalten, denn das nationale Recht muss weitestgehend richtlinienkonform ausgelegt werden.

887 § 47 BDSG normiert dabei die **allgemeinen Verarbeitungsgrundsätze** bei den betroffenen Behörden. Die §§ 48-54 BDSG enthalten Rechtsgrundlagen zur Verarbeitung von personenbezogenen Daten, wobei insbesondere die Verarbeitung besonderer Kategorien personenbezogener Daten (§ 48 i.V.m. § 46 Nr. 14 BDSG), die Zulässigkeit der Zweckänderung (§ 49 BDSG) sowie die Einwilligung (§ 51 i.V.m. § 46 Nr. 17 BDSG) im Anwendungsbereich der Richtlinie geregelt werden.

888 Dabei ist zu beachten, dass zudem **bereichsspezifische Vorschriften** einschlägig sein können.[1692] Auch die Länder müssen bzw. mussten im Rahmen ihrer Kompetenzen die Richtlinie umsetzen.[1693] Den Anwendungsbereich für die bereichsspezifischen Vorgaben beschreibt § 45 BDSG. Dieser ist zunächst nur für öffentliche Stellen (Sätze 1-4) sowie (bei gesetzlicher Anordnung) deren Auftragsverarbeiter (Satz 5) eröffnet. Jedoch sind nicht sämtliche öffentliche Stellen umfasst, sondern nur solche, die personenbezogene Daten zu den in § 45 Sätze 1-4 BDSG genannten Zwecken verarbeiten.[1694]

[1690] Erwägungsgrund 4 JI-RL.

[1691] BT-Drs. 18/11325, S. 110.

[1692] BT-Drs. 18/11325, S. 1.

[1693] Vgl. *Wolff* in: Wolff/Brink, Beck'scher Onlinekommentar, § 45 BDSG Rn. 4.

[1694] Die genaue Abgrenzung zur DSGVO erweist sich in diesem Punkt bisweilen als unklar, vgl. hierzu ausführlich *Wolff* in: Wolff/Brink, Beck'scher Onlinekommentar, § 45 BDSG Rn. 10 ff.

© 2019 juris GmbH | www.juris.de

www.juris.de/internetrecht