Evaluation der Europäischen Datenschutz-Grundverordnung

DSGVO nach einem Jahr

Stand: 18.07.2019 (aktualisierte Version)

Ute Bernhardt
bernhardt@netzwerk-datenschutzexpertise.de
Ingo Ruhmann
ruhmann@netzwerk-datenschutzexpertise.de
beide: Elchdamm 56a, 13503 Berlin
Karin Schuler
schuler@netzwerk-datenschutz-expertise.de
Kronprinzenstraße 76, 53173 Bonn
Thilo Weichert
weichert@netzwerk-datenschutz-expertise.de
Waisenhofstraße 41, 24103 Kiel
www.netzwerk-datenschutzexpertise.de

Inhalt

Art. 97 Europäische Datenschutz-Grundverordnung (DSGVO) sieht vor, dass bis zum 25. Mai 2020 von der Europäischen Kommission ein „Bericht über die Bewertung und Überprüfung" der DSGVO erfolgen soll. Etwas mehr als ein Jahr nach dem Wirksamwerden der DSGVO wird zu dieser Fragestellung hier eine erste Bestandsaufnahme vorgenommen. Die vorliegende Stellungnahme des Netzwerks Datenschutzexpertise untersucht die Wirkungen der DSGVO auf den Schutz der Grundrechte bei der Verarbeitung personenbezogener Daten und macht Vorschläge für Änderungen bzw. für Weiterentwicklungen auf europäischer Ebene.

Allgemeine Hinweise zu dieser Stellungnahme

Die vorliegende Stellungnahme verfolgt nicht den Anspruch, eine umfassende Bewertung der DSGVO vorzunehmen. Die positiven Wirkungen der DSGVO werden vorrangig unter Kap. 2 in allgemeiner Form dargestellt. Der Schwerpunkt wird darauf gelegt, welche besonderen **Defizite sich hinsichtlich des Grundrechtsschutzes** bei der Umsetzung der DSGVO erwiesen haben.

Nicht spezifisch eingegangen wird auf **unzureichende nationale Umsetzungen** der DSGVO, also insbesondere durch die deutschen Gesetzgeber. Etwas anderes gilt, wenn eine unklare Regelung der DSGVO bei der umsetzenden Gesetzgebung dazu geführt hat, dass die Ziele der DSGVO konterkariert werden und dem durch eine Klarstellung auf europäischer Ebene entgegengewirkt werden kann.

Die Stellungnahme knüpft jeweils an der für ein Problem **relevantesten Regelung** für ein spezifisches Defizit an, erfasst aber in der Regel mehrere Bestimmungen der DSGVO, die zu einander einen inhaltlichen Bezug haben. Soweit nicht anders bezeichnet, handelt es sich bei zitierten Regelungen um solche in der DSGVO.

Grundlage der vorliegenden Stellungnahme sind insbesondere Erfahrungen mit der DSGVO in **Deutschland**.

1 Allgemeine Bewertung

Die DSGVO bewährt sich mit ihrem Regelungskonzept und ihren Zielen im Wesentlichen. Die Ziele des verbesserten Grundrechtsschutzes und der Schaffung eines einheitlichen digitalen Binnenmarktes werden durch die DSGVO vorangebracht. Das Wirksamwerden der DSGVO im Mai 2018 hat in Deutschland dazu geführt, dass das seit den 70er Jahren geltende Datenschutzrecht erstmals gesamtgesellschaftlich und von allen beteiligten Stellen nicht nur zur Kenntnis genommen wurde und wird, sondern auch daraufhin überprüft wird, inwieweit es **Änderungen bei bisherigen Verarbeitungsprozessen** notwendig macht. Für diese gesteigerte Aufmerksamkeit waren eine kontrovers geführte öffentliche Diskussion und eine umfangreiche Berichterstattung in den Medien förderlich. Als ein zentraler Aspekt erwies sich hierfür, dass bei Verstößen gegen Datenschutznormen erstmals empfindliche Strafen drohen.

So sehr das Wirksamwerden der DSGVO zu einer Besinnung auf den Datenschutz in der Praxis der Verarbeitung personenbezogener Daten geführt hat, so wenig war die DSGVO Anlass für die **Gesetzgeber auf nationaler Ebene**, ihre bisherigen Datenschutzregelungen daraufhin zu überprüfen, inwieweit auch in ihrem Zuständigkeitsbereich der Datenschutz vorangebracht werden kann. So wurde zumeist nur – zeitlich knapp vor und teilweise auch erst nach dem Wirksamwerden am 24.05.2018 –

eine formale Anpassung des bisherigen Datenschutzrechts an die neuen Vorgaben der DSGVO vorgenommen. Zumindest in Österreich und in Deutschland wurde diese Anpassung an die DSGVO nicht für inhaltliche Weiterentwicklungen beim Datenschutz genutzt. Vielmehr wurden Öffnungsklauseln in der DSGVO genutzt, um den Datenschutz zurückzuschrauben oder zu beschränken, auch wenn dies im Widerspruch zur Intention und manchmal auch zum Wortlaut der DSGVO steht. Der EU-Kommission liegt schon eine Vielzahl von Beschwerden über eine inadäquate nationale Umsetzung der DSGVO vor, die sie nun überprüfen muss.

Eine an der DSGVO geäußerte zentrale Kritik besteht darin, dass diese unterschiedslos für kleine wie große Datenverarbeiter gilt und davon unabhängig ist, ob diese kommerziell oder gemeinnützig/ehrenamtlich tätig sind. Für **kleine Unternehmen und (ehrenamtlich tätige) Vereine** werden Befreiungen von spezifischen DSGVO-Pflichten gefordert. Der Bürokratismus-Vorwurf wird erhoben, etwa was die Bestellungspflicht von Datenschutzbeauftragten betrifft; die angedrohten Sanktionen werden als existenzgefährdend dargestellt.[1] Diese Kritik berücksichtigt nicht, dass die Risiken personenbezogener Datenverarbeitung nicht durch die Größe der verantwortlichen Stelle und nicht allein von den erklärten Zwecken bestimmt werden, sondern vom Umfang, der Vernetzung und der Sensitivität der tatsächlichen Verarbeitung. Die DSGVO verfolgt durchgängig einen risikobasierten Ansatz. Zudem ist sie dem Verhältnismäßigkeitsgrundsatz verpflichtet (Art. 52 Abs. 1 GRCh). Dies führt dazu, dass die Nichtbeachtung bestimmter Pflichten, wie etwa der Bestellungspflicht von Datenschutzbeauftragten, bei geringem Risiko und im Fall einer Unverhältnismäßigkeit nicht sanktioniert werden darf. Gesetzliche Änderungen sind deshalb nicht zwingend notwendig.[2]

In den letzten 15 Jahren haben sich insbesondere **global agierende US-Unternehmen** in Europa etabliert und teilweise insbesondere bei bestimmten Internet-Anwendungen zu Monopolen entwickelt (z. B. Google, Facebook, Amazon, Microsoft). Deren Geschäftsmodell setzt dabei mehr oder weniger voraus, dass sie den Datenschutz nach europäischem Verständnis ignorieren. So konnten Facebook und Google 2018 global einen Marktanteil bei der Online-Werbung von 56,4% erlangen und eine gewaltige Kapitalmenge anhäufen. Für 2019 wird eine Steigerung auf 61,4% prognostiziert.[3] Die Marktmacht dieses Duopols beim Online-Marketing besteht auch in Europa. Diese Macht basiert hier wesentlich auch darauf, dass bewusst und massenhaft gegen europäisches Datenschutzrecht verstoßen wurde und weiterhin wird. Die Informationstechnik-Konzerne aus den USA und deren Monopolisierungstendenzen werden inzwischen als Bedrohung für die europäische Wirtschaft wahrgenommen[4]. Erst langsam, aber zunehmend entwickelt sich die Bereitschaft in der EU, hiergegen politisch und rechtlich vorzugehen. Als ein geeignetes Instrument zur Begrenzung des Einflusses dieser Unternehmen wird insbesondere von der Politik und der Administration der EU das Datenschutzrecht erkannt. Diese Funktion soll die DSGVO erfüllen. Angesichts der darin geregelten Sanktionsandrohungen ist sie hierfür grundsätzlich auch geeignet (z. B. Art. 83 Abs. 4, 5 mit hohem

[1] Siehe etwa den Antrag des Landes Niedersachsen im Bundesrat, BR-Drs. 144/19 v. 03.04.2019; dazu Presseerklärung der DVD v. 12.04.2019, https://www.datenschutzverein.de/wp-content/uploads/2019/04/2019-04-12-BR-Vorstoss-NDS-DSGVO.pdf; Bayerischer Ministerrat, 05.06.2018, abgedruckt in DANA 2018, 189.
[2] Siehe hierzu die Stellungnahme des Netzwerks Datenschutzexpertise v. 16.07.2018, https://www.netzwerk-datenschutzexpertise.de/dokument/benennungspflicht-datenschutzbeauftragter-bei-kleinstunternehmen
[3] Nötting, Google und Facebook bauen ihre Dominanz aus, www.wuv.de 21.02.2019.
[4] Siehe die Pressemitteilung der EU-Kommission zur Verhängung einer Geldbuße gegen Google wegen Missbrauchs einer beherrschenden Stellung auf dem Markt für Online-Werbung vom 20.03.2019, http://europa.eu/rapid/press-release_IP-19-1770_de.htm.

Bußgeldrahmen). Ob sich das Sanktionenregime der DSGVO auch in der Praxis bewährt, kann nach einem Jahr noch nicht beurteilt werden (s. u. 11). Zugleich wird die DSGVO auch als ein Instrument angesehen, um die Etablierung chinesischer Firmen, die weltweit und auch in Europa immer mehr Einfluss gewinnen und ein ähnliches Geschäftsmodell verfolgen wie die US-Internetkonzerne, zu behindern oder gar zu verhindern. Ob diese Erwartung realistisch ist, kann derzeit auch noch nicht beurteilt werden.

Von vielen wird die DSGVO nicht nur als ein ökonomisches Schutzschild wahrgenommen, sondern auch als eine **wert- und grundrechtsbezogene Alternative** zu den Regulierungskonzepten in den USA und in China, die stark auf eine unternehmerische bzw. staatliche Kontrolle des Internets hinauslaufen.

Die DSGVO erweist sich, in stärkerem Maße als schon zuvor die Europäische Datenschutzrichtlinie (EG-DSRl) als ein **Regulierungsvorbild für Drittstaaten**, die sich einerseits der Dominanz durch chinesische und US-Unternehmen entziehen wollen und die zugleich den Zugang zum europäischen Markt erleichtern wollen. So haben z. B. jüngst Japan und Brasilien Datenschutzregelungen angenommen, die sich an der DSGVO orientieren und welche die Anerkennung durch die EU als „angemessenes Schutzniveau“ anstreben oder erreicht haben (Art. 45 Abs. 1 DSGVO).[5] Auch Kalifornien hat bereits im Juni 2018 ein für US-amerikanische Verhältnisse sehr weitreichendes Datenschutzgesetz verabschiedet.

2 Ziele (Art. 1)

Als Zielsetzung nennt die DSGVO eingangs den Schutz der „Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“. Die Ausrichtung auf den Schutz sämtlicher Grundrechte wird in den weiteren Regelungen der DSGVO immer wieder betont. Dessen ungeachtet beschränken sich sowohl die Wahrnehmung der DSGVO wie auch deren praktische Umsetzung weitgehend auf den Schutz des Grundrechts auf Datenschutz nach Art. 8 GRCh. Die Schutzfunktion für andere in der GRCh garantierten Grundrechte, etwa die Diskriminierungsverbote nach Art. 21 GRCh, wird teilweise nicht, teilweise nur eingeschränkt anerkannt. Dies dürfte auch darauf zurückzuführen sein, dass Art. 8 GRCh bisher das einzige explizite informationelle Abwehrrecht in der GRCh geblieben ist und darüber hinausgehende grundrechtliche Schlussfolgerungen oft nur durch Ableitungen möglich sind. So hat bisher z. B. das deutsche Bundesverfassungsgericht (BVerfG) aus dem allgemeinen Persönlichkeitsrecht ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgeleitet,[6] ohne dass dieses „Computergrundrecht“ bisher europaweit anerkannt ist. Jenseits von personenbezogener Datenverarbeitung ist ein „Recht auf digitale Souveränität“, etwa für juristische Personen in Bezug auf Plattformanbieter, noch nicht etabliert (s. u. 5). Diese Defizite sollten dadurch behoben werden, dass weitere informationelle Grundrechte ausdrücklich normiert und konkretisiert werden, so wie dies im Entwurf einer Charta der **digitalen Grundrechte in Europa** vorgesehen ist.[7]

Die Öffnung des Datenschutzrechts für einen umfassenden digitalen Grundrechtsschutz sollte dadurch verstärkt werden, dass den Datenschutzaufsichtsbehörden eine **umfassendere informationelle**

[5] Zu Japan: Drewes, Japan übernimmt europäische Datenschutz-Standards. www.noz.de 23.01.2019; zu Brasilien: Datenschutzgesetz nach DSGVO-Vorbild verabschiedet, DANA 2018, 214 f.
[6] BVerfG 27.02.2008 – 1 BvR 370 u. 595/07, NJW 2008, 822.
[7] https://digitalcharta.eu/.

Wächterfunktion zuerkannt wird. Dies erfolgt teilweise schon heute dadurch, dass diesen neben den Aufgaben für den Datenschutz solche zur Verwirklichung der Informationsfreiheit zugewiesen sind. Aufgabenzuweisungen bei der Regulierung von Algorithmen bzw. der sog. künstlichen Intelligenz können deren Rolle als unabhängige Grundrechtshüter im digitalen Raum weiter stärken.

3 Öffnungsklausel für öffentliche Stellen (Art. 6 Abs. 3 lit. b i. V. m. Abs. 1 lit. e)

Die DSGVO erlaubt den nationalen Gesetzgebern, Rechtsgrundlagen für Datenverarbeitung zu schaffen, die für die Wahrnehmung einer Aufgabe erforderlich ist, „die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt“. Gemäß der DSGVO muss nur gewährleistet werden, dass die derart geregelte Verarbeitung „in einem angemessenen Verhältnis zu dem verfolgten Zweck“ steht. Diese sowie weitere Öffnungsklauseln (z. B. Art. 9 Abs. 2 lit. b) wurden in Deutschland genutzt, die bisherigen **spezifischen materiellen Regelungen** für öffentliche Stellen weitgehend beizubehalten.

Die Öffnungsklauseln der DSGVO zur Verarbeitung durch öffentliche Stellen ermöglichen neben präzisierenden Regelungen im Recht der Mitgliedstaaten auch **Präzisierungen durch das Unionsrecht**. Hiervon sollte beim Bestehen von europaweiten Bezügen durch den EU-Gesetzgeber Gebrauch gemacht werden, um die Grundprinzipien der DSGVO in harmonisierter Weise bei öffentlichen Stellen weiterzuentwickeln.

4 Gesundheitsdatenverarbeitung (Art. 9)

Anders als die sonstige Datenverarbeitung erfolgt die „Verarbeitung besonderer Kategorien personenbezogener Daten“, also von sog. sensitiven Daten, weitgehend nicht auf der Grundlage der DSGVO selbst. Vielmehr bedarf diese einer speziellen Rechtsgrundlage. Die Regelung der Verarbeitung von Gesundheitsdaten oder von genetischen Daten für Zwecke der Gesundheitsvorsorge, bei der Versorgung und Behandlung im Gesundheits- und Sozialbereich sowie im Rahmen medizinischer Forschung obliegt damit bisher grundsätzlich den **nationalen Gesetzgebern**. Statt der Regulierung durch die Mitgliedstaaten ist aber auch ein Tätigwerden der Union möglich (Art. 9 Abs. 2 lit. h, j). Entsprechendes gilt für die Verarbeitung sensitiver Daten, die zugleich einem speziellen Geheimnis bzw. einem Berufsgeheimnis, also etwa der ärztlichen Schweigepflicht, unterliegen (Art. 9 Abs. 3).

Es ist nachvollziehbar, dass der DSGVO-Gesetzgeber nicht den gesamten Bereich der Gesundheitsdatenverarbeitung in der EU regeln wollte und dies kurzfristig auch nicht konnte. Dies hat aber zur Folge, dass für diesen besonders sensitiven Bereich mit einer hohen Binnenmarktrelevanz bisher keine EU-weite Harmonisierung erreicht wird. Dies gilt insbesondere für den immer weiter zusammenwachsenden Markt von Gesundheitsleistungen, bei dem es sich zunehmend auch um informationelle Angebote handelt. Diese Angebote werden weiterhin durch einen rechtlichen Flickenteppich reguliert. Dies gilt insbesondere für die Bundesrepublik Deutschland als föderalem Staat. Relevante Gesundheitsdienstleistungen wie z. B. die von Krankenhäusern unterliegen der Gesetzgebungszuständigkeit der Bundesländer. Entsprechendes gilt für die Verarbeitung von Gesundheitsdaten durch Universitätskliniken für Forschungszwecke, da auch der Hochschulbereich von den Bundesländern reguliert wird. Wünschenswert ist dagegen auch hier eine **einheitliche materielle Regulierung durch die EU**. Diese ist rechtlich möglich. Datenschutzrechtliche Standards für

die Technik und das Datenschutzmanagement werden ohnehin schon durch die DSGVO vorgegeben. Gründe, die voneinander abweichende Regelungen innerhalb der EU rechtfertigen würden, sind nicht ersichtlich. Die Notwendigkeit einheitlicher Normen ist groß, zumal etwa in den Bereichen medizinischer Behandlung und Medizin länder- bzw. grenzüberschreitende Datenverarbeitungsprozesse stark zunehmen.

5 Automatisierte Entscheidungen im Einzelfall/Profiling (Art. 22)

Die dem Art. 15 EG-DSRl nachempfundene Regelung des Art. 22 DSGVO zu automatisierten Entscheidungen einschließlich Profiling hat nur einen **beschränkten Regelungsgehalt** und wird in der konkreten Auslegung in der Praxis wegen seiner Unbestimmtheit weiter beschränkt.

Der derzeitige Hauptanwendungsfall von Profiling (Art. 4 Nr. 4) ist heute die Profilerstellung auf der Grundlage von Internet-Kommunikations-Inhalten und -Metadaten für Werbezwecke, für personalisierte Preisangebote sowie für **personalisierte Informationsanzeigen**. In all diesen Fällen erfolgen jeweils massive Eingriffe in die Persönlichkeitsrechte der Betroffenen. Viele Juristen meinen aber, dass Art. 22 hier nicht anwendbar sei, weil es sich nicht um „automatisierte Entscheidungen“ handele. Diese hätten keine rechtliche Wirkung und entfalteten keine erheblichen Beeinträchtigungen.[8] Diese Position wird auch von kommerziellen Anwendern vertreten und wurde bisher von der Aufsicht nicht sanktioniert. Tatsächlich erfolgen aber gerade in diesem Bereich gezielte individuelle Manipulationen und Diskriminierungen gewaltigen Ausmaßes.[9] Zugleich erfolgt eine massive Beeinträchtigung des demokratischen Meinungsbildungsprozesses etwa durch algorithmenbasierte Priorisierung von Falschnachrichten. Es bedarf daher der rechtlichen Klarstellung, dass alle Formen eines umfassenden und komplexen Profilings von dem grundsätzlichen Verbot in Art. 22 erfasst werden.

In Art. 15 Abs. 1 lit. h ist geregelt, dass Betroffene das Recht haben, vom Verantwortlichen Auskunft zu erhalten über das „Bestehen einer automatisierten Entscheidungsfindung“ und „– zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung“. Dieser Auskunftsanspruch wurde bisher normativ nicht präzisiert; eine Praxis hierzu ist bisher nicht erkennbar. Vielmehr wird diesem Anspruch – bisher von der deutschen Rechtsprechung bestätigt – das Recht auf Wahrung von Betriebs- und Geschäftsgeheimnissen entgegengehalten.[10] Diese Praxis und diese Rechtsprechung ignorieren sowohl die individuelle und gesellschaftliche Relevanz automatisierter Entscheidungen. Es bedarf daher einer europarechtlichen **Präzisierung der Transparenzpflichten**, wodurch sichergestellt wird, dass automatisierte Entscheidungen sowohl individualrechtlich wie auch demokratisch hinterfragt, kontrolliert und im Bedarfsfall revidiert werden können.

Art. 22 ist bisher die einzige Regelung zu automatisierten Auswertungsprozessen auf der Basis von Algorithmen. Die Komplexität der Algorithmen nimmt zu, die Transparenz und die Kontrollierbarkeit

[8] Deutscher Dialogmarketing Verband, Europäische Datenschutz-Grundverordnung, Auswirkungen auf das Dialogmarketing, 2016; Martini in Paal/Pauly, 2. Aufl. 2018, Art. 22 Rn. 23; Schulz in Gola, 2. Aufl. 2018, Art. 22 Rn. 28.
[9] Weichert in Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Art. 22 Rn. 30 f.
[10] Dazu ausführlich Weichert, DANA 2018, 132.

dieser Prozesse nehmen ab. Zugleich durchdringen Algorithmen immer mehr Lebensbereiche und werden für diese bestimmend. Algorithmen sind die Werkzeuge zur Transformation des „digitalen Rohstoffes“ Daten. Algorithmen legen Prozessschritte in den verschiedensten Anwendungsfeldern fest. In der analogen Welt hat sich die Zertifizierung der Qualität und Zuverlässigkeit von Unternehmensprozessen durch die Reihe der ISO 90.000 Normen durchgesetzt. Ein ähnlicher Ansatz fehlt in der digitalen Welt. Das Instrumentarium des Art. 22 allein ist nicht geeignet, die mit Algorithmen verbundenen Risiken einzuhegen. Es bedarf darüber hinausgehender Vorgaben für die Entwicklung, den Einsatz und die Kontrolle von Algorithmen und der Haftung für deren Ergebnisse. Die Alternative zu einer solchen Prüfung von Algorithmen und deren Ergebnissen könnte nur sein, die Übermittlung von Daten sehr viel stärker einzuschränken. Art. 22 muss, so wie es derzeit in europäischen wie nationalen Gremien, etwa dem im Herbst 2018 eingerichteten Digitalrat, diskutiert wird, weiterentwickelt werden zu einer grundrechtskonformen **Algorithmenkontrolle**, die zugleich vermeidet, dass dadurch unerwünschte Innovationshindernisse aufgebaut werden.

Automatisierte Entscheidungen greifen nicht nur in die Rechte von natürlichen Personen ein, sondern auch in die Rechte von **juristischen Personen**, etwa bei der Verwendung von fremder Software oder bei der Inanspruchnahme von Cloud-Dienstleistungen. Betroffen sind von solchen Entscheidungen immaterielle Rechte wie z. B. Betriebs- und Geschäftsgeheimnisse oder Urheberrechte. Die computergestützten Entscheidungen haben gravierende Effekte auf den eingerichteten und ausgeübten Geschäftsbetrieb. Programmtechnisch vorgegeben werden diese Entscheidungen durch Plattform- und Diensteanbieter, ohne dass die diese Dienste nutzenden Stellen wirksame Einwirkungsmöglichkeiten hätten. Marktstandards oder Monopole führen dazu, dass oft keine freie Wahl der eingesetzten Produkte möglich ist. Dadurch wird deren digitale Souveränität tangiert. Auch juristischen Personen sollten insofern in einem am Konzept des Art. 22 orientierten eigenständigen Rechtsakt zur Wahrung ihrer Autonomie Transparenz- und Einflussrechte zugestanden werden.

6 Beschränkungen der Betroffenenrechte (Art. 23)

Für Betroffene ist es wenig einsichtig, dass ihre Rechte, die in den Art. 12 bis 21 geregelt und Art. 8 GRCh grundrechtlich abgesichert sind, durch nationale Regelungen eingeschränkt werden. Art. 23 räumt den EU-Mitgliedstaaten diese Befugnis ein. Erst recht nicht vermittelbar ist, dass – so wie dies in Deutschland durch den Bund und viele Länder erfolgte – die Betroffenenrechte und insbesondere das **Recht auf Auskunft** nach Art. 15 DSGVO in einem über das zugelassene Maß eingeschränkt werden (z. B. §§ 32-36 BDSG; §§ 32a-32f AO). Es ist wünschenswert, dass im Interesse der Einheitlichkeit und der Verhinderung einer übermäßigen Beschränkung der Betroffenenrechte die wesentlichen Beschränkungen europarechtlich festgelegt werden. Lediglich spezifische Einschränkungen in besonders aufgeführten öffentlichen Bereichen sollten, soweit spezifische nationalrechtliche Belange tangiert sind, den Gesetzgebern der Mitgliedstaaten überlassen bleiben.

7 Gemeinsame Verantwortlichkeit (Art. 26)

Durch die Urteile des Europäischen Gerichtshofs (EuGH) zur gemeinsamen Verantwortlichkeit im Jahr 2018[11] wurde der Rechtspraxis erstmals umfassend vor Augen geführt, welche zentrale Bedeutung dieses in Art. 26 geregelte Instrument für die Durchsetzung des Datenschutzes hat. Während die

[11] EuGH 05.06.2018 – C-210/16, NJW 2018, 2537; EuGH 10.07.2018 – C-25/17, NJW 2019, 285.

Auftragsverarbeitung in Art. 28 eine präzise und konkrete Ausgestaltung in der DSGVO gefunden hat, ist die gleichermaßen relevante gemeinsame Verantwortlichkeit nur sehr allgemein geregelt. Darin wird eine Verpflichtung der gemeinsam Verantwortlichen zum Abschluss einer Vereinbarung begründet. Die nötigen Inhalte und der nötige Detailliertheitsgrad ist der Norm nicht zu entnehmen, ebenso wenig eine Verpflichtung zur gegenseitigen Unterrichtung. Dies führt in der Praxis dazu, dass der marktmächtigere Verantwortliche, also z. B. der Internetplattformbetreiber, einige allgemeine Festlegungen vornimmt, die für die weiteren Verantwortlichen nicht ausreichen, um ihre eigene Verantwortlichkeit wahrzunehmen, weil sie weder den Umfang noch die Art der Verarbeitung des marktmächtigen Verantwortlichen hinreichend kennen, geschweige denn bewerten und beeinflussen können. In Analogie zu Art. 28 ist daher der **Regelungsgehalt der Vereinbarungen** nach Art. 26 zu präzisieren und insbesondere festzulegen, welche Informationen die gemeinsam Verantwortlichen verpflichtend untereinander austauschen müssen und welchen konkreten Inhalt die ebenfalls geforderte Information der Betroffenen über das „Wesentliche der Vereinbarung“ aufweisen muss.

8 Zertifizierung (Art. 42, 43)

Eine unabhängige, kompetente und transparente Zertifizierung von IT-Produkten und -Verfahren ist angesichts von deren Komplexität und der hohen Grundrechtsrelevanz eine zentrale Voraussetzung für den digitalen Grundrechtsschutz. Datenschutzzertifizierungen haben das Potenzial, globale Standards für einen grundrechtskonformen IT-Einsatz zu setzen. Die Umsetzung der Regelungen zur Zertifizierung ist bisher nur sehr schleppend vorangekommen. Es gibt bisher noch keine etablierten Verfahren auf DSGVO-Grundlage, keine anerkannten Zertifizierungsstellen und keine konkret erteilten Datenschutzsiegel bzw. -prüfzeichen. Dies hat seinen Grund darin, dass den Datenschutzaufsichtsbehörden und den Akkreditierungsstellen für die **Schaffung der organisatorischen, prozeduralen und technischen Voraussetzungen** nicht die nötigen Ressourcen zur Verfügung gestellt werden und von Seiten der Politik diesen Stellen insofern bisher weder eine Erwartung geschweige denn die nötige ideelle Unterstützung entgegengebracht wird. Einzige Ausnahme ist insofern die vom deutschen Bundeswirtschaftsministerium unterstützte Entwicklung eines DSGVO-konformen Zertifizierungsverfahrens für Cloud-Anbieter.[12]

Art. 42 Abs. 1 beschränkt Zertifizierungen auf „Verarbeitungsvorgänge von Verantwortlichen oder Auftragsverarbeitern“. Zwar erfolgt beim Einsatz von modernen IT-Produkten zunehmend durch den Hersteller und Anbieter von IT-Produkten auch eine Verarbeitung (personenbezogener) Daten. Dies ist aber auch oft nicht der Fall bzw. nicht der Schwerpunkt, der dann zumeist vorrangig in der Bereitstellung von Hard- und Software liegt. Die Verarbeitung personenbezogener Daten erfolgt oft nur im Rahmen der Administration, der Wartung oder der Erbringung von Services. Im Interesse der Datenminimierung und des Selbstschutzes (Art. 5 Abs. 1 lit. c, 25 Abs. 1, 3) sollte die DSGVO auch **Zertifizierungen von IT-Produkten** vorsehen, die ausschließlich vom Betroffenen genutzt werden, ohne dass es bei dem Produkthersteller zu einer personenbezogenen Datenverarbeitung kommt.

Art. 42 Abs. 3 sieht bisher vor, dass Zertifizierung „freiwillig“ sein muss. Die Regelung setzt darauf, dass sich Grundrechtskonformität bestätigende Zertifikate auf dem Markt allein durch ihre Existenz durchsetzen würden. Diese Erwartung ist nur für spezifische sensitive Anwendungen und nur in begrenzten Maß gerechtfertigt. Tatsächlich gibt es eine Vielzahl von IT-Verfahren, bei denen eine

[12] European Cloud Service Data Protection Certification, AUDITOR, https://www.auditor-cert.de/.

präventive Gewährleistung der Grundrechtskonformität nicht nur wünschenswert, sondern zwingend nötig ist. Dies gilt z. B. für Anwendungen im Bereich von Berufsgeheimnissen, generell bei Gesundheitsanwendungen und insbesondere Medizinprodukten, für den Einsatz automatisierter Entscheidungsverfahren (Art. 22) und insbesondere für solche, die mit Machine Learning, also sog. künstlicher Intelligenz, operieren. In diesen Bereichen bedarf es einer zusätzlichen Regulierung, wonach qualifizierte **Zertifizierungen verpflichtend** sind.

9 Ausstattung der Aufsichtsbehörden (Art. 52 Abs. 4)

Gemäß der DSGVO stellt jeder Mitgliedstaat sicher, dass seine Aufsichtsbehörde mit den Ressourcen, „die sie benötigt", ausgestattet wird. Die Bereitstellung der Ressourcen erfolgt dann in der Regel durch parlamentarische Haushaltsbeschlüsse. Das Inkrafttreten der DSGVO 2016 hatte in Deutschland zunächst keine adäquate Ausweitung der Ressourcenbereitstellung zur Folge, obwohl mit der DSGVO massive Aufgabenausweitungen verbunden sind. Die Ausstattung der Aufsichtsbehörden ist in den meisten Bundesländern auch nach gewissen Aufstockungen **nicht in der Lage, den tatsächlichen Bedarf** zu decken. Dies hat zur Folge, dass Beschwerden über lange Zeit unbearbeitet, Verstöße teilweise unsanktioniert bleiben. Die Glaubwürdigkeit des Datenschutzes sowohl bei Betroffenen wie allgemein in der Öffentlichkeit sowie dessen Akzeptanz werden hierdurch in Frage gestellt.

Es ist nachvollziehbar, dass die Aufsichtsbehörden den Weg vor Gerichte scheuen, um eine angemessene Ausstattung einzuklagen. Um dem gesetzlichen Auftrag zu genügen und von allen Seiten unerwünschte gerichtliche Auseinandersetzungen zu vermeiden, wird vorgeschlagen, verpflichtend für die politischen Träger jeweils ein **unabhängiges Gremium** zu etablieren, das den Ausstattungsbedarf der jeweiligen Aufsichtsbehörde objektiviert. Diese Festlegung sollte dann zur Grundlage der parlamentarischen Festlegungen genommen werden.

10 Abstimmung zwischen den Aufsichtsbehörden (Art. 60 ff.)

Im Kapitel VII der DSGVO ist die Zusammenarbeit und Kohärenz der Aufsichtsbehörden geregelt. Wegen des föderalen Aufbaus der Bundesrepublik gibt es ergänzende Regelungen zur Zusammenarbeit der Aufsichtsbehörden in Deutschland (§§ 18, 40 Abs. 2 BDSG). Die Aufsichtsbehörden haben es bisher weder auf europäischer noch auf deutscher Ebene geschafft, für viele wesentliche Fragen des Datenschutzes **einheitliche Positionen** zu entwickeln, die Datenverarbeitern wie Betroffenen hinreichend Rechtssicherheit schaffen. Ein Grund hierfür liegt unzweifelhaft in der ungenügenden Ausstattung der Aufsichtsbehörden. Doch muss auch in Frage gestellt werden, ob die bisher vorgesehenen Abstimmungsprozesse effektiv und sinnvoll sind.

11 Abhilfebefugnis der Aufsichtsbehörden (Art. 58 Abs. 2)

Zwar sieht die DSVGO einen umfangreichen Strauß von Sanktionsmaßnahmen im Fall von Datenschutzverstößen sowie von Abhilfemaßnahmen vor (vgl. auch Art. 82 ff.). Diese gehen bis zum Verhängen einer endgültigen „Beschränkung der Verarbeitung, einschließlich eines Verbots" (Art. 58 Abs. 2 lit. f). Im Internet sind auch nach dem Wirksamwerden der DSGVO weiterhin bei großen Plattformanbietern Verarbeitungspraktiken üblich und bestimmend, die offensichtlich und unbestreitbar gegen die DSGVO-Regeln verstoßen und bei denen im Interesse des

Grundrechtsschutzes aller Betroffenen nur ein Verbot als angemessene Sanktion in Frage kommt. Zwar ist erkennbar, dass Aufsichtsbehörden gegen massenhafte illegale Praktiken insbesondere auch im Internetbereich vorzugehen bereit sind. Doch konnte innerhalb des ersten Jahres der Geltung der DSGVO bisher noch nicht festgestellt werden, dass wesentliche Verbesserungen bei relevanten Internetplattformen erreicht wurden. Insofern bedarf es möglicherweise mehr Zeit. Dessen ungeachtet sollte schon jetzt geprüft werden, ob für den Fall von **offensichtlichen und massenhaften Datenschutzverstößen** Prozesse nötig sind, die eine zeitnahe Rechtsklärung und Herstellung rechtmäßiger Zustände ermöglicht.

12 Meinungsäußerung und Informationsfreiheit (Art. 85)

Die Verbreitung von Hassnachrichten und sog. Fake-News mit Bezug zu natürlichen Personen hat sich in den letzten Jahren zu einem großen gesamtgesellschaftlichen Problem entwickelt. Die Regulierung des Verhältnisses zwischen Meinungs- und Informationsfreiheit (Art. 11 GRCh, Art. 5 Abs. 1 GG) und Datenschutz (Art. 8 GRCh, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) liegt bisher ausschließlich bei den Mitgliedstaaten. Die EU-Kommission hat allerdings eine Analyseeinheit im EU-Zentrum für Informationsgewinnung und -analyse aufgebaut, die Erkenntnisse zu Fake News als Teil hybrider Bedrohung sammelt und an nationale Stellen weitergibt[13]. Diese aus Grundrechts- und Demokratiesicht äußerst heikle Aufgabe wurde bisher weder normativ noch operativ befriedigend gelöst. An der Aufgabenzuweisung an die Mitgliedstaaten sollte mittelfristig nichts geändert werden, um möglicherweise verschiedene nationale Lösungsversuche miteinander vergleichen zu können. Auf europäischer Ebene muss aber dieser Prozess aktiv begleitet werden mit dem Ziel, einen europaweit möglichst einheitlichen wirksamen Ausgleich zwischen den in Frage stehenden Grundrechten zu finden. Hierzu sollten **Forschungs- und Diskursprozesse** gefördert werden.

13 Beschäftigtendatenschutz (Art. 88)

Zum Beschäftigtendatenschutz enthält die DSGVO bisher lediglich eine Rahmenregelung. Dies ist der Tatsache geschuldet, dass in den Verhandlungen eine Einigung in der Sache nicht möglich schien. Letztlich musste der EU-Gesetzgeber in dieser Frage kapitulieren und hat stattdessen eine Öffnungsklausel formuliert, die die Rechtssetzung im Beschäftigtendatenschutz in die Hände der nationalen Gesetzgeber legt. Diese Öffnungsklausel ist nicht durch die Überzeugung entstanden, dass sachliche Gründe eine nationale Regelung erfordern, sondern sie war die minimale Regelung, auf die man sich einigen konnte. Die auf nationaler Ebene in den EU-Mitgliedstaaten bisher vorhandenen rudimentären Regelungsansätze taugen nicht als Vorbild für eine einheitliche EU-Regelung. Der Bedarf an einer europaweit einheitlichen Regelung steigt jedoch mit der zunehmenden ökonomischen Verflechtung europäischer Arbeitgeber, dem europaweiten Einsatz von IT bei Arbeitgebern und der zunehmenden Mobilität von Beschäftigten. Regulierung und Rechtsprechung sind beim Beschäftigtendatenschutz bisher praktisch vollständig national geprägt. Zumindest besteht – auch im Interesse einer einheitlichen Anwendung des Art. 88 DSGVO – ein starker Bedarf an einem Erfahrungsaustausch in der EU. Wenigstens dieser Bedarf sollte durch EU-weite Forschungs- und Diskursprojekte gestillt werden.

[13] Gemeinsame Mitteilung an das Europäische Parlament und den Rat: Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen – eine Antwort der Europäischen Union, Brüssel, den 6.4.2016 JOIN(2016) 18 final, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016JC0018&from=en

14 Forschung (Art. 85, 89)

In den Erwägungsgründen der DSGVO finden sich mehrere Anknüpfungspunkte zum Datenschutz in der Forschung, die jedoch im Regelungstext der DSGVO nicht aufgegriffen werden. Ebenso wie für den Ausgleich zwischen Meinungs- und Informationsfreiheit mit dem Datenschutz besteht bisher für den Ausgleich zwischen Forschungsfreiheit und Datenschutz eine ausschließliche Zuständigkeit der Mitgliedstaaten. Lediglich hinsichtlich geeigneter Garantien und der forschungsbegründeten Beschränkung von Betroffenenrechten besteht eine begrenzte Gesetzgebungszuweisung an die EU. Forschungsprojekte werden innerhalb der EU zunehmend grenzüberschreitend durchgeführt, auch soweit dabei personenbezogene Daten verarbeitet werden. Derartige Forschungsprojekte stoßen derzeit auf eine unübersichtliche Vielzahl nationaler, ja sogar regionaler Normen.[14] Dies ist für die Realisierung des Datenschutzes wie für die Verwirklichung wissenschaftlicher Forschung hinderlich und erweist sich als schädlich für die Weiterentwicklung des Wirtschafts- und Wissenschaftsstandortes Europa. Um diese Defizite zu beheben bedarf es zunächst eine Bestandsaufnahme der in der EU geltenden Forschungsregelungen. In einem zweiten Schritt ist zu prüfen, in welchen Bereichen personenbezogener Forschung in der EU **vereinheitlichende Regelungen** nötig und möglich sind. Insbesondere im Bereich der medizinischen Forschung dürfte dies der Fall zu sein.

15 Geheimhaltungspflichten (Art. 90)

Die DSGVO erlaubt den Mitgliedstaaten, die Befugnisse der Aufsichtsbehörden bei Stellen zu regeln, für die Berufsgeheimnisse gelten, „um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen“. In Deutschland wurde die Befugnis dafür genutzt, um erstmals im deutschen Recht die Datenschutzkontrolle bei Berufsgeheimnissen vollständig auszuschließen, wenn eine Stelle ihre Geheimhaltungspflicht geltend macht. Es war bis zum Erlass des Art. 90 nicht erkennbar, dass in der Praxis zwischen Datenschutzkontrolle und Geheimschutz relevante Konflikte bestünden. Die Regelung des Art. 90 geht auf massive Lobbyarbeit von Interessenverbänden insbesondere von rechts- und steuerberatenden Berufen zurück. Sie erfasst nicht nur diese Bereiche, sondern auch den gesamten sensitiven und hochgefährdeten Bereich des Patientengeheimnisses bzw. der ärztlichen Schweigepflicht. Unabhängig davon, dass die deutsche Umsetzung des Art. 90 in § 29 Abs. 2 BDSG europarechts- und verfassungswidrig ist, besteht keine Notwendigkeit für die Einschränkung der in Art. 8 Abs. 3 GRCh verankerten Kontrollkompetenz der Datenschutzaufsicht.[15] Art. 90 sollte vollständig gestrichen werden.

16 Elektronische Kommunikationsdienste (Art. 95)

Art. 95 regelt das Verhältnis der DSGVO zur Richtlinie 2002/58/EG, also der Telekommunikations-Datenschutzrichtlinie (TK-DSRl). Diese sollte ursprünglich schon zum 25.05.2018 durch eine **ePrivacy-Regulation**, also eine „Verordnung über Privatsphäre und elektronische Kommunikation“ ersetzt werden, die dann auf die DSGVO Bezug nimmt und den modernen technischen Rahmenbedingungen der elektronischen Kommunikation angepasst ist. Ein Verordnungsentwurf wurde von der Kommission

[14] Zum in Deutschland bestehenden Flickenteppich https://www.netzwerk-datenschutzexpertise.de/dokument/die-forschungsklauseln-im-neuen-datenschutzrecht.
[15] Netzwerk Datenschutzexpertise, https://www.netzwerk-datenschutzexpertise.de/dokument/benennungspflicht-datenschutzbeauftragter-bei-kleinstunternehmen; Weichert in Däubler u. a. (Fn. 8), § 29 Rn. 24-29.

der EU eingebracht und vom Parlament behandelt. Der EU-Rat hat hierzu bisher keine Stellung genommen. Bis zum Wirksamwerden einer neuen ePrivacy-Regulation besteht bei der Anwendung der TK-DSRl und deren Umsetzung durch das deutsche Telekommunikationsgesetz (TKG) und insbesondere durch das Telemediengesetz (TMG) große Verunsicherung. Es ist insbesondere auch nach zwei aktuellen EuGH-Entscheidungen weiterhin unklar, wie sog. Over-the-Top-Kommunikationsdienste (OTT-Dienste), also Internet-Kommunikationsdienste, datenschutzrechtlich zu bewerten sind.[16] Es ist also dringend nötig, dass die ePrivacy-Regulation durch die Gesetzgebungsgremien der EU beschlossen und in Kraft gesetzt wird.

[16] EuGH 5.6.2019 – C-142/18, Skype; EuGH 13.6.2019 (http://curia.europa.eu/juris/liste.jsf?num=C-142/18&language=DE)– C-193/18, Gmail ((http://curia.europa.eu/juris/liste.jsf?num=C-193/18&language=DE); Weichert in Däubler u. a. (Fn. 8), Einleitung TMG Rn. 10.

Abkürzungen

Abs.	Absatz
AO	Abgabenordnung
Art.	Artikel
Aufl.	Auflage
BDSG	Bundesdatenschutzgesetz
BVerfG	Bundesverfassungsgericht
DSGVO	Europäische Datenschutz-Grundverordnung
EG	Europäische Gemeinschaften
EU	Europäische Union
EuGH	Europäischer Gerichtshof
ff.	fortfolgende
GG	Grundgesetz
GRCh	Europäische Grundrechte-Charta
i. V. m.	in Verbindung mit
IT	Informationstechnik
lit.	Buchstabe
Nr.	Nummer
NJW	Neue Juristische Wochenschrift
TK-DSRl	Europäische Telekommunikations-Datenschutzrichtlinie
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
vgl.	vergleiche
z. B.	zum Beispiel