

Datenschutz im digitalen Zeitalter - global europäisch, national

Vortragsveranstaltung des Instituts für Rundfunkrecht an der Universität zu Köln vom 16. Mai 2014

1. Auflage



Verlag C.H. Beck München 2015

Verlag C.H. Beck im Internet:

www.beck.de

ISBN 978 3 406 67412 9

Zu [Inhaltsverzeichnis](#)

schnell und portofrei erhältlich bei beck-shop.de DIE FACHBUCHHANDLUNG

auch bei der Datenschutzharmonisierung die Frage der Subsidiarität und der Vereinbarkeit mit den jeweils bestehenden nationalen Rechtsrahmen präsent. Bereits Tage vor der Veröffentlichung durch die EU-Kommission warnte der Richter am deutschen *Bundesverfassungsgericht Johannes Masing* in einem Zeitungsartikel vor dem aus seiner Sicht durch die Verordnung drohenden Verlust des Schutzes durch das deutsche Grundgesetz.¹¹ In Deutschland löste er mit dieser sehr einseitigen Betrachtung eine Welle grundsätzlicher Kritik an der Legitimation des Vorschlags aus. Dass auch dem deutschen Datenschutzrecht bisher die EU-Richtlinie von 1995 zugrunde lag, wurde in der Debatte häufig außer Acht gelassen, ebenso die Probleme der Anwendbarkeit des nationalen Rechts in Deutschland, dafür kursierten zahlreiche Missverständnisse im Verhältnis des deutschen Rechts zum EU-Recht. Seine Kritik wiederholte *Masing* in der Folge nicht mehr, sondern schien sie bei Auftritten regelmäßig zu relativieren. Auch ihm war klar, dass an einer stärkeren Harmonisierung des Datenschutzes und einer gemeinsamen Grundrechtsprechung auf EU-Ebene kein Weg vorbei führt. Dieser fehlgeleiteten Grundsatzdebatte setzte dann auch der *Europäische Gerichtshof* im Frühjahr 2014 ein Ende, als er mit den Urteilen zur Richtlinie über die Vorratsdatenspeicherung sowie zu der Datenverarbeitung durch Internetsuchmaschinen wie Google sowohl die Grundrechtsdimension als auch den effektiven Rechtsschutz beim Datenschutzrecht unmissverständlich klarstellte.

VIII. Ausbremsversuche im Rat

Auch in der Debatte einiger EU-Mitgliedstaaten war die Ablehnung nicht von einer substanziellen Auseinandersetzung mit der vorgeschlagenen Verordnung geprägt, sondern von einer grundsätzlichen EU-kritischen Haltung. Die Beratungen im Innen- und Justizministerrat kreisten über fast ein Jahr um die grundsätzlichen Bedenken der deutschen, britischen, dänischen und ungarischen Regierungen, während Mitgliedstaaten wie Spanien, Polen, Österreich und Irland auf die zügige Verabschiedung der Verordnung drängten. Die Bundesregierung stellte über Monate grundsätzlich infrage, ob die Verordnung im Bereich der behördlichen Datenverarbeitung überhaupt gelten sollte. Diese Haltung war absurd, da die prinzipielle Unterscheidung zwischen privater und öffentlicher Datenverarbeitung seit der Richtlinie 95/46/EG nicht mehr bestand. Zudem sieht auch die EU-Datenschutz-Grundverordnung weitgehende Flexibilität für die Gestaltung von Da-

¹¹ Süddeutsche Zeitung vom 9.1.2012, aufrufbar unter: www.datenschutzbeauftragter-online.de/wp-content/uploads/2012/01/20120109_SZ_Masing_Datenschutz.pdf.

tenerhebungs- und Datenverarbeitungsregeln für den behördlichen Bereich vor. Das Europäische Parlament hatte diese gleich zu Beginn der Beratungen noch stärker ausgeweitet. Gerade die von anderen EU-Staaten als datenschutzfreundlich vermutete deutsche Bundesregierung, forderte – damals noch vertreten durch den Innenminister *Hans-Peter Friedrich* – immer wieder, im Bereich der privatwirtschaftlichen Datenverarbeitung vom Prinzip des Erlaubnisvorbehalts der Datenverarbeitung abzurücken, obwohl dies auch im deutschen Datenschutzrecht ein verfassungsrechtlich abgesichertes Grundprinzip ist. Durch diese Exkurse, die von den Lobbyisten und Anwälten international agierender IT-Konzerne mit Freude begleitet wurden, verzögerte sich die Beratung im Ministerrat über viele Monate.

IX. Erschwerte Arbeit im Europäischen Parlament

Diverse Lobbygruppen versuchten, auch im Europäischen Parlament den Prozess durch eine Flut von Änderungsanträgen in die Länge zu ziehen. Wie die Plattform Lobbyplag.eu im Sommer 2013 offenlegte, waren ein großer Teil der 3.999 Änderungsanträge, die durch die Abgeordneten aller Fraktionen eingereicht worden waren, durch den Einfluss präsender Internetkonzerne und ihrer Lobbygruppen motiviert. Die Verschiebung der Abstimmung zunächst auf den Sommer und dann auf den Herbst des Jahres 2013 war den umständlichen Beratungen zwischen den Fraktionen über die Erreichung von Kompromissformulierungen für jeden einzelnen Artikel der Verordnung geschuldet. Nur so konnte sichergestellt werden, dass am Ende des Prozesses ein Ergebnis steht, das in sich schlüssig ist und tatsächlich von einer breiten Mehrheit der Fraktionen im Parlament getragen wird. Das große Interesse für die Arbeit an der Datenschutz-Grundverordnung zeigt am Ende aber auch, dass der Datenschutz als Materie im Zentrum der politischen Auseinandersetzung angekommen ist. Die Abgeordneten im Europäischen Parlament wissen genau, dass eine breite Öffentlichkeit auf ihre Arbeit an dieser Verordnung schaut. Deshalb ist es auch richtig, trotz oder gerade wegen der informellen Verhandlungen mit dem Rat, möglichst viel Öffentlichkeit für die beratenen Vorschläge zu schaffen.

X. Breiter Kompromiss mit vielen Änderungen

Die Parlamentarier wollten vor allem die Definitionen und Prinzipien schärfen: Die neue Kategorie der pseudonymisierten Daten als Unterfall personenbezogener Daten wurde eingeführt. Datenschutzfreundlichere Kommunikation im Internet soll durch die Verordnung befördert wer-

den. Dazu kommt eine zusätzliche Information der Verbraucherinnen und Verbraucher durch leicht verständliche standardisierte Symbole, die die Grundlagen der Datenverarbeitung und die Rechte des Einzelnen anschaulicher darstellen sollen. Bei den Pflichten für die Datenverarbeiter sorgt das Parlament für Entlastungen und reduziert umständliche Vorabgenehmigungen deutlich. Die Kommission wollte sich eine weite Flexibilität bei der weiteren Ausgestaltung und Auslegung des Datenschutzrechts einräumen und hatte breite Kritik von allen Seiten einstecken müssen. So hatte sie sich bei der Frage der Datenschutzaufsicht selbst in eine zentrale Position als letzte Instanz gebracht. Dies wird nun durch das Parlament zurückgewiesen. Stattdessen soll der neu geschaffene Europäische Datenschutzausschuss die Rolle eines Streit-schlichtungsgremiums zwischen den Datenschutzbehörden übernehmen, in letzter Konsequenz auch verbindliche Entscheidungen gegenüber der für die Durchsetzung von Maßnahmen zuständigen Aufsichtsbehörde treffen. Die Enthüllungen durch *Edward Snowden* im Sommer 2013 hatten zumindest eine direkte politische Reaktion zur Folge: Im Europäischen Parlament fand sich schnell eine breite Mehrheit für die Wiedereinführung des ehemaligen „Artikel 42“ eines internen Vorentwurfs der Kommission, den der Berichterstatter des Parlaments als neuen Art. 43a wieder eingeführt hatte. Diese Bestimmung sieht vor, dass die Weitergabe personenbezogener Daten aus der EU an drittstaatliche Behörden nur auf der Grundlage des europäischen Rechts oder darauf beruhender Rechtshilfeabkommen erfolgen darf. Für Unternehmen würde ein Verstoß gegen das so statuierte Weitergabeverbot empfindliche Strafen bedeuten: Mit bis zu fünf Prozent des Jahresweltumsatzes eines Unternehmens wird das neue EU-Datenschutzrecht alles andere als ein zahloser Tiger sein – jedenfalls, wenn es nach dem Europäischen Parlament geht.

Ausblick auf die weiteren Verhandlungen

Die Debatten über die Enthüllungen des Whistleblowers *Edward Snowden* und die Frage nach den Unterschieden des Datenschutzrechts auf transatlantischer und internationaler Ebene sorgen derzeit dafür, dass der Sinn und die Notwendigkeit eines einheitlichen EU-Datenschutzgesetzes einer breiten gesellschaftlichen Mehrheit offenbart werden. Nicht umsonst gab es einschlägige Entscheidungen im Europäischen Parlament sowie auf mitgliedstaatlicher Ebene, sich stärker mit EU-weiten Standards beim Datenschutz, der IT-Sicherheit und den Regeln für die sogenannte Cloud zu beschäftigen. Die Entscheidung der EU-Kommission, die Safe-Harbour-Vereinbarung mit der U.S.-Wirt-

schaft grundlegend auf den Prüfstand zu stellen, wird durch die unmissverständliche Aussage des Abschlussberichts zur Untersuchung der Massenüberwachung im Europäischen Parlament besonders akut: Die Safe-Harbour-Vereinbarung soll nach Ansicht der großen Mehrheit im Parlament aufgekündigt werden. Auch die Anwendung grundlegender Rechtsprinzipien der EU-Staaten gegenüber drittstaatlichen Unternehmen, die die Daten europäischer Bürgerinnen und Bürger sowie aus dem EU-Binnenmarkt verarbeiten, wird offen thematisiert. Angesichts der umfassenden Chancen einer EU-Datenschutz-Grundverordnung in dieser und vieler anderer Hinsicht hat die Bundesregierung mit ihrem Spiel auf Zeit viel Vertrauen der Bürgerinnen und Bürgern verspielt. In den kommenden Monaten wird sich zeigen, wohin sich die Reform des europäischen Datenschutzrechts entwickelt. Entscheidend ankommen wird es insoweit auf die öffentliche Debatte. Von herausgehobener Bedeutung ist dabei, dass dort nicht etwa die Frage des „Ob“, sondern vielmehr die Frage des „Wie“ einheitlicher europäischer Datenschutzregeln im Mittelpunkt steht.

DISKUSSION^{*}

^{*} Stellvertretend für *MdEP Jan Philipp Albrecht, LL.M.* referierte und diskutierte sein wissenschaftlicher Mitarbeiter *Ralf Bendrath*. Die Diskutanten werden im Einzelnen im Anhang vorgestellt.

HAIN:

Wir danken Ihnen ganz herzlich für den Bericht über wesentliche Inhalte und Prozessuales zur Datenschutz-Grundverordnung. Gerne möchte ich Fragen aus dem Auditorium zulassen.

TILLMANN:

Herr *Bendrath*, herzlichen Dank für den interessanten Überblick über die geplanten EU-Regeln. Wir befinden uns heute beim WDR, einer deutschen Rundfunkanstalt, und deshalb sei es mir erlaubt, erneut auf die journalistischen Standards und journalistische Datenverarbeitung im Kontext der EU-Novellierung einzugehen. Könnten Sie hier noch eine kurze Erläuterung zu Art. 80 des Entwurfs geben? Diesem ähnlich gibt es bereits eine spezifische Regelung auf der Basis der EU-Richtlinie von 1995 für die Mitgliedstaaten – auch die Selbstregulierung betreffend –, die in den einzelnen Ländern funktioniert, insbesondere auch hier in Deutschland. Wird eine Selbstregulierung für die journalistisch redaktionelle Datenverarbeitung jetzt auch im Entwurf der Datenschutz-Grundverordnung sichergestellt sein?

BENDRATH:

Im Prinzip verbleibt es bei der geltenden Regelung. Art. 80 des Entwurfs besagt: Die Mitgliedstaaten haben den Auftrag, durch nationale Gesetze dafür zu sorgen, dass das Recht auf Datenschutz und das Recht auf freie Meinungsäußerung und Pressefreiheit in eine Balance gebracht werden. Allerdings haben wir im Zuge unserer legislativen Arbeit die explizite Nennung von Journalisten aus dem Gesetzestext gestrichen, was zu einigen Missverständnissen bei Journalisten und Pressevertretern geführt hat. Damit sollte mitnichten ihr Privileg aufgehoben werden; vielmehr sollte der enge Wortlaut erweitert werden, sodass auch Blogger und andere, die von ihrem Recht auf freie Meinungsäußerung Gebrauch machen, dem Schutz unterfallen. Im Übrigen bleibt es weiterhin den Mitgliedstaaten vorbehalten, im Detail zu regeln, wie diese Balance zu gestalten ist.

SCHUNICHT:

Private Nutzer sollen nach Ihrer Darstellung des Entwurfes vom Anwendungsbereich ausgeschlossen bleiben, da für privat verarbeitete Daten kein allzu großer Verwendungsbereich bestehe, in dem den Betroffenen Schaden zugefügt werden könne. In sozialen Netzwerken im

Internet beispielsweise liegt der Fall jedoch anders. Wenn dort fremde Daten durch private Nutzer „gepostet“ werden, kann das zu einem sehr hohen Verbreitungsgrad führen. Warum wurde dieser Bereich vom Entwurf ausgenommen, obwohl das Problem doch seit Jahren bekannt ist und sicherlich diskutiert wurde? Ferner möchte ich gerne fragen, inwieweit die Verordnung vollharmonisierend sein soll. Dies knüpft an den ersten Teil der Veranstaltung an, in dem ebenfalls die Frage aufgeworfen wurde, inwieweit Mitgliedstaaten strengere bereichsspezifische Regelungen neben dieser Grundverordnung erlassen können, sollen oder eben nicht dürfen.

BENDRATH:

Gerne gehe ich zunächst auf Ihre letzte Frage ein, weil sie sich an die Frage nach dem Journalisten-Privileg fügt. Art. 80 ff. belassen den Mitgliedstaaten einen mit Leben zu füllenden Umsetzungsspielraum. Allerdings wird seitens der Bundesregierung, des BMI und zum Teil auch der Bundesländer bedauerlicherweise argumentiert, es gäbe im öffentlichen Bereich eine Vielzahl an speziellen Regelungen für Landes- und Bundesbehörden, die mit der bundesweiten Geltung der Grundverordnung hinfällig würden. Dem ist auch nicht zu widersprechen. Doch kann das Vorteile bringen, auch wenn ich um die Bedenken gerade der Landesvertreter weiß, die ihre Hände über dem auf Landesebene gewachsenen Sonderrecht halten. Als Beispiel sei nur die Befürchtung genannt, das Abendland würde untergehen, wenn es die Datenschutzregelung im Berliner Theatergesetz für Theaterkartenabonnenten nicht mehr geben würde. Die im Jahr 2001 von der rot-grünen Bundesregierung in Auftrag gegebene Studie zur Modernisierung des Datenschutzrechts von *Roßnagel*, *Pfitzmann* und *Garstka*¹ macht zwei Punkte deutlich: Vonnöten sind einerseits ein Mehr an technischem Datenschutz und andererseits ein Zurückschneiden des undurchdringlichen Gestrüpps an Spezialregelungen, um Rechtssicherheit zu schaffen. Ersteres wurde nun durch „Privacy by Design“ umgesetzt. Letzterem kann dadurch Abhilfe geschaffen werden, dass in ganz vielen Bereichen das Bundesdatenschutzgesetz angewendet werden kann. Extra Datenschutzregeln für das bayerische Waffenregistergesetz beispielsweise sind dafür nicht erforderlich.

Nun zu Ihrer ersten Frage nach dem Anwendungsbereich der Verordnung für private Nutzer und soziale Netzwerke. Selbstverständlich ist der Betreiber des sozialen Netzwerks im Geltungsbereich der Ver-

¹ Abrufbar unter www.bfdi.bund.de/SharedDocs/VortraegeUndArbeitspapiere/2001/GutachtenModernisierungDSRecht.pdf?__blob=publicationFile.