Humanistische Union

Datenschutz-Grundverordnung – was bewirkt sie für den Datenschutz?

Die DSGVO wurde mit großen Versprechen angekündigt, mit hohen Erwartungen versehen, mit tiefen Enttäuschungen aufgenommen und durch viel Lobby-Arbeit beeinflusst. Sie wird von denen einen als „Meilenstein“, neuer „Goldstandard“ und „Beginn einer neuen Zeitrechnung im Datenschutzrecht“ gepriesen; von den anderen zu „einem der schlechtesten Gesetze des 21. Jahrhunderts“ gekürt und für das Datenschutzrecht als „größte Katastrophe des 21. Jahrhunderts“ bezeichnet.

Alexander Roßnagel wagt eine erste Bilanz der verfehlten Ansprüche und möglicher Innovationen durch die EU-Datenschutz-Grundverordnung ...

Datenschutz-Grundverordnung – was bewirkt sie für den Datenschutz?

Datenschutz-Grundverordnung – ein weiterer Schritt in der Entwicklung des Datenschutzrechts

Das geltende Datenschutzrecht stammt konzeptionell aus den 1960er und 1970er Jahren. In dieser Zeit fand die Datenverarbeitung in Rechenzentren statt. Die Daten wurden in Formularen erfasst und per Hand eingegeben. Die Datenverarbeitung betraf nur einen kleinen Ausschnitt des Lebens und war – soweit die Daten bei der betroffenen Person erhoben worden waren – für diese weitgehend kontrollierbar. Wurde die Zweckbindung beachtet, wusste der Betroffene in der Regel, wo welche Daten über ihn verarbeitet wurden. Für diese erste Stufe der Datenverarbeitung sind die grundlegenden Schutzkonzepte des Datenschutzrechts entwickelt worden. ...

Die zweite, qualitativ neue Entwicklungsstufe wurde mit der – weltweiten – Vernetzung der Rechner erreicht. Dadurch entstand ein eigener virtueller Sozialraum, in den nahezu alle Aktivitäten aus der körperlichen Welt übertragen wurden. Jede Handlung in diesem Cyberspace hinterlässt Datenspuren, die ausgewertet werden können und auch werden. Weder die Erhebung der Daten noch deren – letztlich weltweite – Verbreitung und Verwendung können von der betroffenen Person noch kontrolliert werden. Web 2.0 oder Cloud-Computing sind weitere Ausprägungen dieser Entwicklungsstufe. Für sie versuchten die in den 1990er Jahren erlassenen Multimedia-Datenschutzgesetze die Risiken in den Griff zu bekommen. Sie haben für die Internetdienste die Anforderungen an Transparenz, Zweckbindung und Erforderlichkeit verschärft und vor allem die neuen Prinzipien der Datensparsamkeit und des Datenschutzes durch Technik eingeführt. Diese normativen Vorgaben konnten allerdings nur im Wirkungsbereich des Nationalstaats zur Geltung gebracht werden. Die neue Datenverarbeitung betrifft das komplette Leben im virtuellen Sozialraum, je nach Nutzung des Internet einen großen oder kleinen Ausschnitt des täglichen Lebens. Diesen Risiken zu entgehen, würde voraussetzen, den virtuellen Sozialraum zu meiden – für viele keine realistische Alternative. Jedoch besteht zumindest grundsätzlich die Möglichkeit, bildlich gesprochen, den Stecker zu

ziehen.

In einer weiteren, dritten Entwicklungsstufe gelangt die Datenverarbeitung in die körperliche Welt. Ubiquitous Computing mit seinen Ausprägungen wie z.B. Smart Cars, Smart Health, Smart Home, Smarten Assistenten, Robotern und sonstige Techniken des Internet der Dinge, die auf der Erfassung der Umgebung durch vielfältige Sensoren und auf der Lernfähigkeit der Systeme durch Künstliche Intelligenz aufbauen, führen zu einer allgegenwärtigen Verarbeitung personenbezogener Daten, die potenziell alle Lebensbereiche und diese potenziell vollständig erfasst. In dieser Welt wachsen Körperlichkeit und Virtualität zusammen. Informationen aus der virtuellen Welt werden in der körperlichen Welt verfügbar, Informationen aus der realen Welt in die virtuelle Welt integriert. Aus dieser Welt und der in ihr stattfindenden Datenverarbeitung gibt es aber keinen Ausweg mehr. Insofern verschärft sich das Problem des Datenschutzes radikal und seine Lösung wird existenziell. Für diese neuen Herausforderungen gibt es noch keine datenschutzrechtlichen Regelungen.

Und auch die alten Regelungen greifen nicht mehr. In einer Welt allgegenwärtiger Datenverarbeitung laufen die bekannten Anforderungen der Zweckbindung, der Erforderlichkeit, der Transparenz, der Einwilligung und der Betroffenenrechte ins Leere. Wenn die allgegenwärtige Rechnertechnik gerade im Hintergrund und damit unmerklich den Menschen bei vielen Alltagshandlungen unterstützen soll, wird es niemand akzeptieren, wenn er täglich zur Durchsetzung des Transparenzprinzips tausendfach bei meist alltäglichen Verrichtungen Anzeigen, Unterrichtungen oder Hinweise zur Kenntnis nehmen müsste. Wenn die Techniksysteme kontextsensitiv und selbstlernend sein sollen, werden sie aus den vielfältigen Datenspuren, die der Nutzer bei seinen Alltagshandlungen hinterlässt, und seinen Präferenzen, die seinen Handlungen implizit entnommen werden können, entgegen jeder Zweckbindung im Interesse des Nutzers vielfältige und umfassende Profile erzeugen. Wenn die Nutzer auf die Datenspeicher der sie umgebenden Gegenstände zurückgreifen, um ihr eigenes löchriges Gedächtnis zu erweitern, läuft das Erforderlichkeitsprinzip in Leere. Für die Gedächtnisfunktion ist für sehr lange Zeit eine Datenspeicherung auf Vorrat erforderlich, weil niemand wissen kann, an was man sich irgendwann einmal erinnern möchte. Diese Beispiele zeigen: Die allgegenwärtige Datenverarbeitung verursacht nicht nur ein weiteres Vollzugs-, sondern ein grundlegendes Konzeptproblem. Sie stellt die zentralen Schutzkonzepte des Datenschutzrechts in Frage.[15]

Alle drei Entwicklungsstufen bestehen heute parallel und beeinflussen sich gegenseitig. Für jede besteht ein spezifischer Modernisierungsbedarf ... Die Zukunftsfähigkeit neuer Datenschutzregelungen muss daran gemessen werden, ob sie den Herausforderungen auf allen drei Entwicklungsstufen gerecht werden und neue Lösungen für die Gefährdungen der Grundrechtsverwirklichung bieten.

Zielsetzungen der Datenschutz-Grundverordnung

Die DSGVO ... verfolgt drei große Zielsetzungen:

- Zum einen will sie das Datenschutzrecht unionsweit vereinheitlichen und einen soliden, „*kohärenten und durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union*“ schaffen (EG 3, 9 und 13).
- Zum anderen will sie einheitliche Vorgaben für gleiche wirtschaftliche Bedingungen in der Union bieten und damit den Binnenmarkt stärken (EG 5, 10, 13). „*Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden*“ (EG 10).
- Schließlich stellt sie fest, dass „*rasche technologische Entwicklungen und die Globalisierung … den Datenschutz vor neue Herausforderungen gestellt*“ haben (EG 6). Die Verordnung will den Datenschutz angesichts dieser Herausforderungen modernisieren und den Schutz der Grundrechte verbessern (EG 1, 2 und 4).

Wirkungen der Datenschutz-Grundverordnung

Um zu verstehen, warum die DSGVO diese Ziele weitgehend verfehlt, ist der Machtkampf um die Zukunft des europäischen Datenschutzrechts während der Entstehung der Verordnung zu berücksichtigen. Da nahezu alle Lebens-, Wirtschafts- und Verwaltungsbereiche davon abhängig sind, personenbezogene Daten zu verarbeiten, hat derjenige, der über die Fortentwicklung des Datenschutzes bestimmt, ein zentrales Instrument zur Gestaltung der digitalen Gesellschaft in Europa in der Hand. Daher entspann sich ein heftiger Kampf, wer mit welchen Kompetenzen künftig die Datenverarbeitung reguliert (4.1). Er wirkte sich auf die Kontroversen über die Inhalte der Verordnung aus (4.2 – 4.4), mit denen diese Entwicklung begonnen werden sollte. ...

Ko-Regulierung statt Vereinheitlichung des Datenschutzrechts

Die DSGVO hat ein grundlegendes Problem, das durch den Machtkampf verstärkt und nicht beseitigt wurde: die hohe Diskrepanz zwischen der enormen Komplexität des Regelungsbedarfs einerseits sowie die Abstraktheit und damit Unterkomplexität ihrer Vorschriften andererseits. Sie will in 50 Artikeln des materiellen Datenschutzrechts die gleichen Probleme behandeln, für die im deutschen Datenschutzrecht Tausende von bereichsspezifischen Vorschriften bestehen. Wer Datenschutz regelt, verursacht Veränderungen in allen Gesellschaftsbereichen – vom Archivwesen bis zum Zeitungsverlag. Wer meint, die vielen und vielfältigen gesetzlichen Regelungen zum Datenschutz in den Mitgliedstaaten durch wenige generelle und abstrakte Regelungen ersetzen zu können, unterschätzt nicht nur diese Aufgabe gewaltig, sondern übersieht auch die negativen Auswirkungen, die dadurch entstehen, wenn er die Vielfalt und Differenzierung bestehender Regelungen beseitigt und dadurch gewaltige Lücken der Rechtsunsicherheit erzeugt.[22]

Durch diesen unterkomplexen Regelungsansatz muss die DSGVO ihr eigentliches Ziel, einen soliden, kohärenten, einheitlichen Rechtsrahmen für den Datenschutz in allen Mitgliedstaaten der Union zu bilden, verfehlen. Vollzugsfähig und rechtssicher sind die Regelungen der Verordnung nur, wenn sie präzisiert, konkretisiert und ergänzt werden. Dies ist überwiegend Aufgabe der Mitgliedstaaten.[23] Das wichtigste Ergebnis aus dem Machtkampf um die Verordnung sind die 70 Öffnungsklauseln, durch die die Union den Mitgliedstaaten explizit Regelungskompetenzen im Datenschutzrecht überträgt. Diese sind unterschiedlich ausgestaltet. Sie eröffnen den Mitgliedstaaten eigene Regelungsbereiche ohne spezifische Vorgaben – wie in Art. 88[24] für den Beschäftigtendatenschutz.[25] ... Die Öffnungsklauseln verhindern eine unionsweite Vereinheitlichung des Datenschutzrechts. Dies widerspricht zwar den Wünschen und Hoffnungen, die viele mit der Verordnung verbunden haben. Mehr als dieses Nebeneinander von Unions- und nationalem Datenschutzrecht, das im günstigen Fall zu einer Ko-Regulierung führt, hat der Unionsgesetzgeber aber nicht gewollt.

Wie sehr im Ergebnis ein unionsweit einheitliches Datenschutzrecht verfehlt wird, kann in der Anpassung des deutschen Datenschutzrechts an die DSGVO besichtigt werden. Noch in der 18. Legislaturperiode hat der deutsche Gesetzgeber ergänzend zu ihr erste neue Datenschutzgesetze erlassen. ... Der Regulierungsstil dieser nationalen Anpassungsgesetze ist identisch. Sie sind von der Zielsetzung geprägt, das bestehende materielle Datenschutzrecht zu erhalten und nur formelle Anpassungen vorzunehmen. Es entfällt jedoch kein einziges Datenschutzgesetz und auch kein Abschnitt zum Datenschutz in den Fachgesetzen.

Im Ergebnis verfehlt die DSGVO weitgehend ihr Ziel, das Datenschutzrecht in der Union zu

vereinheitlichen. Für Rechtsanwender und Rechtsbetroffene ist die Gemengelage aus DSGVO sowie dem weitgehend unveränderten deutschen Datenschutzrecht schwer zu durchschauen und verursacht ein hohes Maß an Rechtsunsicherheit.

Kontinuität in den Mitgliedstaaten statt einheitlicher Datenschutzpraxis

Stärker kommt die DSGVO im Bereich der Wirtschaft zur Anwendung. Doch auch wenn in allen Mitgliedstaaten die gleichen Vorschriften gelten, führt dies nicht immer zu unionsweit einheitlichen Wettbewerbsbedingungen. Gerade ihre vielen abstrakten und unbestimmten Regelungen bedürfen in der Praxis der Präzisierung und Konkretisierung durch die Verantwortlichen, betroffenen Personen, nationalen Aufsichtsbehörden und Gerichte.

Es ist ein entscheidender Unterschied, ob eine Richtlinie fünf Erlaubnistatbestände als Ziele vorgibt, die eine bereichs- und problemspezifische Konkretisierung durch nationale Gesetze erfahren sollen, oder ob die gleichen fünf Erlaubnistatbestände in einer Verordnung unmittelbare Rechtsgeltung haben und die bestehenden ausdifferenzierten und risikobezogenen nationalen Regelungen ersetzen sollen. Die Auslegung der identischen abstrakten Begriffe wird in jedem Mitgliedstaat nach der jeweiligen Datenschutztradition und -kultur erfolgen. Insbesondere die offene Abwägung berechtigter Interessen der Verantwortlichen mit den schutzwürdigen Interessen der betroffenen Person wird in jedem Mitgliedstaat unterschiedlich sein. Dies ist z.B. für die Videoüberwachung, für Werbung, Auskunfteien, Marktforschung, Scoring, Bonitätsauskünfte oder Internetangebote zu erwarten. Europäischer Datenschutz wird hinsichtlich der Zulässigkeit der Datenverarbeitung in jedem Mitgliedstaat praktisch einen anderen Inhalt haben. Dadurch entsteht kein einheitlich durchgesetztes und gelebtes Recht. Wettbewerbsgleichheit ist so nicht zu erreichen.[30]

Indem die Verordnung die Entscheidung über die Abwägung letztlich auf die Gerichte überträgt, entstehen aber noch viel unterschiedlichere Ergebnisse als unter der DSRL. ... Eine Vereinheitlichung der Rechtsprechung ist allenfalls in einzelnen Fällen bezogen auf die jeweils enge Fallfrage nach jahrelangen Prozessen[33] durch den EuGH zu erwarten.

Keine inhaltliche Modernisierung des Datenschutzrechts

Die DSGVO führt für das materielle Datenschutzrecht die Grundkonzeption der Datenschutz-Richtlinie von 1995 fort. Sie enthält keinen grundlegenden innovativen Ansatz, weist jedoch einige sinnvolle Neuerungen auf: Angesichts der Globalisierung der Datenverarbeitung ist die Ausweitung ihres räumlichen Anwendungsbereichs hilfreich. Danach ist die Verordnung auch anwendbar, wenn ein Datenverarbeiter – egal wo – personenbezogene Daten von Personen verarbeitet, die sich in der Union aufhalten und der er entweder Waren oder Dienstleistungen anbietet oder die er durch seine Datenverarbeitung in ihrem Verhalten beobachtet.[34] Bisher unbekannt ist das Recht für betroffene Personen in Art. 20 DSGVO, ihre Daten, die sie einem Verantwortlichen bereitgestellt haben, auf einen anderen Datenverarbeiter zu übertragen. Innovativ sind auch die Anforderungen an den Datenschutz durch Systemgestaltung und Voreinstellungen in Art. 25 DSGVO[35] und die Datenschutz-Folgenabschätzung in Art. 35 DSGVO.[36]

Inhaltlich verursacht die Verordnung Defizite – auch gegenüber dem bisherigen Datenschutzniveau[37] – und verfehlt ihr Modernisierungsziel vor allem durch ihren spezifischen Ansatz der Technikneutralität.[38] Technikneutralität ist sinnvoll, wenn sie verhindern soll, dass rechtliche Vorschriften technische

Weiterentwicklungen ausschließen.[39] In der DSGVO wird Technikneutralität aber ideologisch überhöht und im Sinne einer Risikoneutralität[40] genutzt: In keiner Regelung werden die spezifischen Grundrechtsrisiken z.B. von smarten Informationstechniken im Alltag, von Big Data, Cloud Computing oder datengetriebenen Geschäftsmodellen, Künstlicher Intelligenz und selbstlernenden Systemen angesprochen oder gar gelöst. Die gleichen Zulässigkeitsregeln, Zweckbegrenzungen oder Rechte der betroffenen Person gelten für die wenig riskante Kundenliste beim „*Bäcker um die Ecke*“ ebenso wie für diese um Potenzen risikoreicheren Datenverarbeitungsformen. Insbesondere durch abstrakte Zulässigkeitsregelungen wie in Art. 6 Abs. 1 werden die spezifischen Grundrechtsrisiken verfehlt.[41] Damit wird die Verordnung keiner der identifizierten Herausforderungen der zweiten und dritten Entwicklungsstufe der Datenverarbeitung[42] auch nur im Ansatz gerecht. ...

Diese Zielsetzung darf einerseits nicht dazu führen, dass die Vorschriften an technische Detailmerkmale anknüpfen, so dass sie technische Weiterentwicklungen ausschließen. Andererseits dürfen technikunspezifische Regelungen nicht dazu führen, dass der demokratisch legitimierte und zur Regelung berufene Gesetzgeber sich nicht mit den besonderen Interessenlagen und Risiken sowie passenden Lösungen einer Technikanwendung auseinandersetzt. Technikbezogene Regelungen sind gerade in einem so technikgeprägten Bereich wie dem Datenschutz unabdingbar, sollen die rechtlichen Ziele erreicht werden. Daher müssen spezifische Technikfunktionen und die typischen Verarbeitungszwecke, ihre Risiken und Lösungsansätze interessengerecht und risikoadäquat geregelt werden. Nur so kann die notwendige Rechtssicherheit und Interessengerechtigkeit erreicht werden. ...

Innovationen im Vollzug

Die Differenz zwischen Sollen und Sein ist im Datenschutzrecht besonders groß. Daher ist es vor allem relevant, wie die Rechtsdurchsetzung in der DSGVO geregelt ist. Hier dürfte die wirkliche Innovation der Verordnung zu finden sein.

Die Regelung der Unabhängigkeit, der Aufgaben und der Befugnisse der Aufsichtsbehörden sowie deren Zusammenarbeit in der Union umfasst insgesamt 26 Artikel. Die Verordnung hat die Aufgaben und die Befugnisse erheblich ausgeweitet. Wichtig ist vor allem, dass die Aufsichtsbehörde nach Art. 58 Abs. 2 unmittelbare Durchsetzungsbefugnisse hat und z.B. eine rechtswidrige Datenverarbeitung verbieten kann. Eine auffällige Veränderung bringt auch Art. 83, der für Verstöße gegen die Verordnung drastische Sanktionen ermöglicht. Wichtig ist ferner, dass die Aufsichtsbehörde nach Art. 83 Abs. 6 bei Nichtbefolgung ihrer Anweisung Geldbußen von bis zu 20 Mio. Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängen kann, je nachdem, welcher der Beträge höher ist. ...

Wichtig ist aber auch, dass die Zivilgesellschaft in den Vollzug eingebunden wird. Bürger und in ihrer Vertretung Datenschutzverbände können bei der Aufsichtsbehörde Beschwerde einlegen und gegen die Aufsichtsbehörde und gegen den Verantwortlichen Rechtsbehelfe einlegen, wenn sie der Meinung sind, dass gegen die Verordnung verstoßen wird. Haben sie dadurch einen Schaden erlitten, können sie auch Schadensersatz geltend machen.

Ob diese neuen Regelungen die Durchsetzung des Datenschutzrechts in der Wirklichkeit verbessern, hängt davon ab, wie sie in der Praxis angewendet werden. Dies setzt eine den neuen Aufgaben entsprechende Ausstattung der Aufsichtsbehörden voraus,[46] die derzeit noch fehlt. Daran wird der politische Wille zu besserem Datenschutz zu messen sein.[47] Die bisherigen Regelungen im BDSG und in den Landesdatenschutzgesetzen beschränken jedoch die Aufsicht im öffentlichen Bereich im Vergleich zur

Verordnung. ...

PROF. DR. ALEXANDER ROßNAGEL ist Universitätsprofessor für öffentliches Recht, Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnikgestaltung (ITeG) und Sprecher der Forums Privatheit.

Bei dem Text handelt es sich um eine gekürzte Fassung eines Beitrags aus den vorgängen Nr. 221/222 (Heft 1-2/2018) zum Schwerpunkt Datenschutz. Den vollständigen Beitrag erreichen Sie über untenstehenden Link.

Anmerkungen:

15 S. hierzu Roßnagel, Datenschutz in einem informatisierten Alltag, 2007.

22 S. näher Roßnagel/Geminn/Jandt/Richter, Datenschutzrecht 2016 – „Smart“ genug für die Zukunft?, 2016, 176f.

23 S. hierzu näher Roßnagel (Fn. 17), § 1 Rn. 31 ff. und § 2 Rn. 1 ff.

24 Art. und EG ohne Gesetzesbezeichnung sind solche der DSGVO.

25 S. z.B. Maier, DuD 2017, 169; Roßnagel, DuD 2017, 292.

30 So aber Voßhoff, in: BfDI-Info 6: Datenschutz-Grundverordnung, 2016, 7.

33 Das Urteil zur Vorratsdatenspeicherung vom 8.4.2014 erfolgte über acht Jahre nach Erlass der Richtlinie zur Vorratsdatenspeicherung, das Urteil zu Safe Harbor vom 6.10.2015 erging über 15 Jahre nach der Entscheidung der Kommission zur Anerkennung des Safe-Harbor-Systems.

34 Diese Erweiterung sorgt auf dem europäischen Markt für Wettbewerbsgleichheit zwischen Anbietern in der Union und Anbietern außerhalb der Union und vereinfacht die Wahrnehmung von Betroffenenrechten.

35 Die Anforderung richtet sich jedoch an den verantwortlichen Technikanwender, statt an den Hersteller.

36 Die sich hoffentlich nicht in einem Formalismus erschöpfen wird.

37 Entgegen der Zusicherung der damaligen Justizkommissarin Reding, ZD 2012, 197.

38 S. EG 15; Reding, ZD 2012, 198.

39 S. grundsätzlich Roßnagel, Technikneutrale Regulierung: Möglichkeiten und Grenzen, in: Eifert/Hoffmann-Riem (Hrsg.), Innovationsfördernde Regulierung, 2009, 323 ff.

40 Der „Risikoansatz“ der DSGVO – s. z.B. Albrecht, CR 2016, 94 – beschränkt sich darauf, bestimmte Pflichten des Verantwortlichen „entsprechend der Risiken von Datenverarbeitungsprozessen“ zu reduzieren; s. kritisch Roßnagel, DuD 2016, 565, weil dieser Ansatz bewirkt, dass nur ein Bruchteil der Verantwortlichen und Auftragsverarbeiter diese Pflichten erfüllen muss.

41 S. näher Roßnagel, DuD 2016, 565.

42 S. Kap. 2.

46 Roßnagel (Anm. 31), 179 ff.

47 S. zum Datenschutz in der Koalitionsvereinbarung Forum Privatheit, Datenschutz stärken, Innovationen ermöglichen – Wie man den Koalitionsvertrag ausgestalten sollte, Policy Paper, 2018.

---

https://www.humanistische-union.de/publikationen/vorgaenge/221-222/publikation/datenschutz-grundverordnung-was-bewirkt-sie-fuer-den-datenschutz-1/
Abgerufen am: 29.03.2024