



FORUM PRIVATHEIT UND SELBSTBESTIMMTES
LEBEN IN DER DIGITALEN WELT

Policy Paper

DIE NEUE DATENSCHUTZ- GRUNDVERORDNUNG

**Ist das Datenschutzrecht nun für heutige
Herausforderungen gerüstet?**

IMPRESSUM

Autoren:

Prof. Dr. Alexander Roßnagel
Ass. Iur. Maxi Nebel
Universität Kassel

Kontakt:

Dr. Michael Friedewald
Geschäftsfeldleiter „Informations- und Kommunikationstechnik“

Telefon +49 721 6809-146
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

www.isi.fraunhofer.de
www.forum-privatheit.de

Schriftenreihe:

Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt

ISSN-Print 2199-8906
ISSN-Internet 2199-8914

1. Auflage, Mai 2016



Das Datenschutzrecht war bisher vorrangig geprägt durch die Vorgaben der Datenschutz-Richtlinie aus dem Jahr 1995¹ und der ePrivacy-Richtlinie aus 2002². Seither haben sich die technologischen Rahmenbedingungen fundamental gewandelt. Die Datenschutz-Grundverordnung (DS-GVO)³ hat sich daher zum Ziel gesetzt, neue Grundlagen zu schaffen und Antworten auf die großen Fragen unserer Zeit zu geben. Dabei verfolgt die Verordnung drei große Ziele: eine Harmonisierung der bestehenden Regelungen, eine Wettbewerbsangleichung und eine Modernisierung des Datenschutzrechts. Die Frage ist, ob die Verordnung ihre selbstgesteckten Ziele auch wirklich erreicht.

Harmonisierung

Der europäische Gesetzgeber hat erkannt, dass die Datenschutz-Richtlinie nicht ausreichend zu einer Harmonisierung des Datenschutzrechts zum Schutz der Grundrechte und Grundfreiheiten der betroffenen Personen beigetragen hat, da die Regelungen in den einzelnen Mitgliedstaaten unterschiedlich gehandhabt wurden und sich so ein unterschiedliches Schutzniveau gebildet hat.⁴ Um dies zukünftig zu verhindern, hat er sich für das Instrument der Verordnung entschieden, die in jedem Mitgliedstaat unmittelbar gilt und Anwendungsvorrang vor nationalem Recht genießt. So soll ein solider, kohärenter und durchsetzbarer Rechtsrahmen geschaffen werden, der ein hohes Datenschutzniveau gewährleistet und gleichzeitig der digitalen Wirtschaft Raum zum Wachstum lässt.⁵

Die Ausgestaltung der Verordnung verhindert jedoch eine wirkliche Harmonisierung. Dies liegt an der Abstraktheit der Regelungen im Allgemeinen und den zahlreichen Öffnungsklauseln im Besonderen.

Die Regelungen der Verordnung sind fast durchweg so abstrakt formuliert, dass die einzelnen Regelungsinhalte durch Auslegung und Interpretation erschlossen werden müssen. Da die Verordnung nur sporadisch Auslegungshilfen bereithält, werden in jedem Mitgliedstaat durch die Verantwortlichen und Gerichte nach eigener Rechts tradition Auslegungsgrundsätze entwickelt oder herangezogen werden, um die Verordnung vollziehbar zu machen. Das wird zu einer sehr unterschiedlichen Rechtsanwendung in den einzelnen Mitgliedstaaten führen. Diese Interpretationsfragen können zwar grundsätzlich durch den Gerichtshof der Europäischen Union abschließend geklärt werden,

¹ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, *Amtsblatt der Europäischen Gemeinschaften L 281 vom 23. November 1995*, S. 31-50.

² Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), *Amtsblatt der Europäischen Gemeinschaften L 201 vom 31. Juli 2002*, S. 37-47.

³ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), *Amtsblatt der Europäischen Union vom 04. Mai 2016*, S. 1-88.

⁴ DS-GVO, Erwägungsgründe 3 und 9.

⁵ DS-GVO, Erwägungsgründe 2, 7 und 10.

allerdings sind solche Verfahren aufwendig und langwierig. Auswirkungen einer unterschiedlichen Rechtsanwendung wird es selbst bei so zentralen Punkten wie der Zulässigkeit der Datenverarbeitung geben – etwa bei der Frage, wann für den Verantwortlichen ein „berechtigtes Interesse“ vorliegt, das den Verantwortlichen zur Datenverarbeitung berechtigt, und wann „Interessen der Person“ überwiegen.

Weiterhin enthält die Verordnung 70 Öffnungsklauseln. Diese überlassen den Mitgliedstaaten die selbstständige Regelung einer Materie. Dies betrifft durchaus zentrale Bereiche der Verordnung, etwa einige Erlaubnistatbestände, Beschränkung von Betroffenenrechten oder den Beschäftigtendatenschutz. In diesen Bereichen wird aufgrund der Anwendung mitgliedstaatlichen Rechts keine Harmonisierung erreicht.

Wettbewerbsangleichung

Die Stärkung des Binnenmarkts ist eines der zentralen Ziele der Europäischen Union. Die Datenschutz-Grundverordnung hat daher zum Ziel, durch den Abbau von Hemmnissen für den freien Datenverkehr den Binnenmarkt zu stärken, indem durch einheitliche Regelungen für alle Marktteilnehmer ein einheitlicher Markt geschaffen wird und so eine Wettbewerbsangleichung für alle Marktteilnehmer stattfindet.¹ Die Verordnung bringt erhebliche Verbesserungen im Anwendungsbereich, indem sie vom Niederlassungs- auf das Marktortprinzip umstellt. Dadurch werden auch alle diejenigen Verantwortlichen von der Verordnung erfasst, die keine Niederlassung in der Union haben, aber personenbezogene Daten von betroffenen Personen in der Union verarbeiten, um ihnen Waren oder Dienstleistungen anzubieten oder ihr Verhalten zu beobachten. Damit sind auch große, meist US-amerikanische Unternehmen wie Google und Facebook verpflichtet, die Vorgaben der Datenschutz-Grundverordnung zu Fragen der Zulässigkeit der Datenverarbeitung, zu Betroffenenrechten, Datensicherheit, Datenschutz durch Technikgestaltung, Aufsicht, Zertifizierung etc. einzuhalten.

Aber auch hier steht die Abstraktheit der Regelungen einer echten Wettbewerbsangleichung entgegen. Die einheitlichen Vorgaben werden verwässert, weil vielfach eine weitergehende, nach bisheriger mitgliedstaatlicher Rechtstradition geprägte Auslegung und Interpretation durch Anwender und Gerichte notwendig ist, um die Regelungen vollziehen zu können. So werden sich die Details in der Anwendung der Verordnung von Mitgliedstaat zu Mitgliedstaat unterscheiden. Zwar kann der neu geschaffene Europäische Datenschutzausschuss hier künftig eine bestimmte Auslegung der Grundverordnung festlegen. Dies gilt allerdings nur für die Aufsichtsbehörden: für Gerichte sind diese Beschlüsse nicht verbindlich, sondern allenfalls Empfehlungen, da die Grundverordnung nur vonseiten des Gerichtshofs der Europäischen Union abschließend ausgelegt werden kann. Statt einheitlicher Rahmenbedingungen und mithin einheitlicher Wettbewerbsbedingungen drohen somit im Gegenteil ähnliche Ungleichheiten wie unter der Datenschutz-Richtlinie.

¹ DS-GVO, Erwägungsgründe 5 und 10.

Modernisierung des Datenschutzrechts

Das dritte große Ziel der Verordnung ist die Modernisierung des Datenschutzrechts.¹ Während die Verordnung einige Fortschritte und Verbesserungen im Datenschutzrecht mit sich bringt, steht zu befürchten, dass die vielen Verluste an Datenschutzregeln für Deutschland im Ergebnis zu einer Absenkung des bestehenden Datenschutzniveaus und damit zu einer Schwächung der Grundrechte der betroffenen Personen führen.

Positiv hervorzuheben ist zunächst das bereits erwähnte Marktortprinzip in Art. 3 DS-GVO, das neben der Niederlassung des Verantwortlichen auch die betroffene Person in den Fokus nimmt. Art. 35 DS-GVO stellt Vorgaben für eine Datenschutz-Folgenabschätzung auf, insbesondere für so risikoreiche Verarbeitungstätigkeiten wie die systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen oder bei der Verarbeitung besonderer Kategorien personenbezogener Daten.

Zudem führt die Verordnung einheitliche Sanktionen mit zum Teil drastischen Obergrenzen für Geldbußen ein. So sind je nach Verstoß Geldbußen von 10 oder gar 20 Millionen Euro bzw. 2 oder gar 4 % des gesamten weltweit erzielten Jahresumsatzes fällig. Diese sind, sollten die Behörden sie ausschöpfen, durchaus geeignet, auch große, global agierende Firmen zu datenschutzkonformen Verhalten anzuhalten.

Weiter formuliert die Verordnung in Art. 25 und 32 DS-GVO technische und organisatorische Maßnahmen für einen Datenschutz durch Technikgestaltung. Dazu zählt die Verordnung exemplarisch die Verwendung von Pseudonymisierung, Verschlüsselung und datenschutzfreundliche Voreinstellungen, um eine Datenminimierung zu gewährleisten und den Schutz und die Sicherheit personenbezogener Daten sicherzustellen. Leider versäumt es die Verordnung, diese Gestaltungsanforderungen auch unmittelbar an Hersteller zu richten, ohne die ein wirksamer Datenschutz durch Technikgestaltung nicht möglich ist. Zudem unterliegen die Maßnahmen einer umfangreichen Abwägung, die allein dem Verantwortlichen obliegt und die durch die Abstraktheit der Vorgaben nur schwer sanktionierbar sein wird.

Neben positiven Aspekten sind auch einige Verluste und Versäumnisse des europäischen Gesetzgebers zu verzeichnen. Der Grundsatz der Direkterhebung, der dazu dient, die betroffene Person darüber in Kenntnis zu setzen, wer welche Daten über sie erhoben hat, ist in der Verordnung an keiner Stelle verankert. Die grundlegendste Maßnahme, der betroffenen Person Transparenz zu vermitteln, fehlt somit. Andere Maßnahmen zur Sicherung einer transparenten Datenverarbeitung sind insbesondere Informationspflichten gegenüber der betroffenen Person über Verarbeitungsvorgänge. Diese sind jedoch häufig mit Verweis auf Rechte, Grundfreiheiten, Geschäftsgeheimnisse, Urheberrechte und weitere Interessen des Datenverarbeiters oder Dritter beschränkbar.² Somit kann zum Beispiel im Bereich des Scoring auch weiterhin keine Aufdeckung der verwendeten Berechnungsgrundlagen eingefordert werden.

Das so genannte Recht auf Vergessen wurde als große Neuerung und großer Fortschritt zu einem modernen, zeitgerechten Datenschutz gehandelt. Dahinter verbirgt sich jedoch zunächst nur der bekannte Anspruch auf Löschung. Außerdem stellt Art. 17 DS-GVO eine Informationspflicht des Verantwortlichen auf, wenn dieser personenbezogene Daten einer Person weitergegeben hat und diese betroffene Person die Lö-

¹ DS-GVO, Erwägungsgründe 1, 2, 4 und 6.

² DS-GVO, Erwägungsgrund 63.

schung ihrer Daten verlangt. Die tatsächliche Reichweite und Umsetzbarkeit dieses Rechts ist allerdings mehr als fraglich. Art. 17 DS-GVO sieht weitreichende Ausnahmen dieser Pflicht vor, die jedenfalls keine einzelfallbezogene Interessenabwägung zulassen. Zudem werden keine konkreten Kriterien genannt, welche Maßnahmen der Verantwortliche genau zu ergreifen hat und bis zu welcher Grenze diese Maßnahmen gelten sollen. Dies liegt alles im Ermessen des Verantwortlichen. So besteht die Gefahr, dass mit Verweis auf die mangelnde Verhältnismäßigkeit der zu ergreifenden Maßnahmen insbesondere bei umfassenden Datenverarbeitungsvorgängen wie Big Data-Verfahren die Notwendigkeit der Informationspflicht durch den Verantwortlichen abgelehnt werden wird. Schließlich ist auch die technische Realisierbarkeit einer solch umfassenden Informationspflicht fraglich, da insbesondere bei Informationsdiensten im Internet nur mit hohem Aufwand und damit einhergehender umfangreicher Datenerhebung der Abruf und damit die Weitergabe der personenbezogenen Daten verfolgt werden kann, um damit anschließend einem Lösungsbegehren nachzukommen.¹

Als weiterer Verlust ist die Zweckbindung zu nennen. Diese soll sicherstellen, dass die Zweckbestimmungen des Gesetzgebers oder der Einwilligung der betroffenen Person befolgt werden, indem erhobene personenbezogene Daten nur für vorher eindeutig festgelegte, vereinbarte oder eingewilligte Zwecke verarbeitet werden. Sie dürfen nicht auf Vorrat aufbewahrt werden, um sie zu gegebenem Anlass für andere Zwecke weiterzuverarbeiten. In der Verordnung ist die Zweckbindung zwar genannt, ihre beschränkende Wirkung ist aber im Ergebnis ausgehebelt. Nach Art. 5 Abs. 1 lit. b DS-GVO sind personenbezogene Daten grundsätzlich für genau festgelegte, eindeutige und rechtmäßige Zwecke zu erheben und dürfen nicht in einer mit diesem Zweck unvereinbaren Weise weiterverarbeitet werden. Wann eine solche Vereinbarkeit vorliegt, darf nach der Verordnung trotz mangelnder konkreter Vorgaben jedoch nicht der Gesetzgeber entscheiden, sondern nur der Verantwortliche und im Streitfall die Gerichte. Endgültig ausgehebelt wird die Zweckbindung schließlich, indem bei unvereinbaren Zwecken lediglich ein Zulässigkeitstatbestand der Verordnung einschlägig sein muss, durch den die Weiterverwendung der bereits vorhandenen Daten für andere Zwecke zulässig wird.² Für jedes berechnete Interesse des Verarbeiters oder eines Dritten, das die Interessen der betroffenen Person überwiegt, können die Daten für jeden beliebigen Zweck verwendet werden.

Neben diesen grundlegenden Defiziten eines zeitgerechten Datenschutzrechts ist das größte Manko der Verordnung, dass sie keine einzige Regelung enthält, die die großen Herausforderungen moderner Informationstechniken wie Big Data, Ubiquitous Computing, Cloud Computing und viele weitere Grundrechtsrisiken anspricht oder gar löst. So gelten etwa die gleichen Zulässigkeitsregelungen wie für die Datenverarbeitung „beim Bäcker um die Ecke“ auch für diese risikoreichen Datenverarbeitungsformen. Selbst die Regelung zum Profiling in Art. 22 DS-GVO wurde nicht modernisiert, sondern lediglich wie in der Datenschutz-Richtlinie von 1995 wiederholt, umfasst jedoch Personalisierungsmaßnahmen als eine der zentralen Datenverwendungsformen bei Informationsdiensten im Internet nicht.

¹ Ausführlich Jandt, S.; Kieselmann, O.; Wacker, A. (2013): Recht auf Vergessen im Internet, Diskrepanz zwischen rechtlicher Zielsetzung und technischer Realisierbarkeit? *DuD - Datenschutz und Datensicherheit* 37, Nr. 4, S. 235-241.

² Ausführlich dazu Roßnagel, A.; Geminn, C.; Jandt, S.; Richter, P. (2016): *Datenschutzrecht 2016 - "Smart" genug für die Zukunft? Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts*. Kassel (im Erscheinen).

Verbleibende Aufgaben

Die Datenschutz-Grundverordnung ist ein ambitioniertes Gesetz, um den Datenschutz des 21. Jahrhunderts zentral zu regeln. Die selbstgesteckten Ziele Harmonisierung, Wettbewerbsangleichung und Modernisierung werden jedoch nur unzureichend erfüllt. Insbesondere fehlen der Verordnung bedingt durch technikneutrale Formulierungen konkrete Regelungen zu allen wichtigen Risiken moderner Informationstechnologie.

Die Defizite bewirken eine große Verantwortung für die Mitgliedstaaten, Aufsichtsbehörden, Verbände und den Europäischen Datenschutzausschuss für Regelungen, die den Grundrechtsrisiken moderner Informationstechniken gerecht werden und rechtssichere Lösungen gewährleisten müssen. Die weitreichenden Öffnungsklauseln und die vorhandenen, jedoch abstrakten Regelungen der Verordnung bieten hierfür große Handlungsspielräume. Die Bundes- und Ländergesetzgeber sollten das bestehende nationale Datenschutzrecht daraufhin überprüfen, dieses mit den zahlreichen Öffnungsklauseln der Verordnung in Einklang zu bringen sowie Interpretationsspielräume der abstrakten Verordnungsvorschriften unionsrechtskonform auszugestalten. Bestehende Verfahren und Best-Practice-Methoden sollten so weit wie möglich beibehalten und in unionsweite Prozesse überführt werden. Der Europäische Datenschutzausschuss sollte im Rahmen seiner Kompetenzen schnellstmöglich umfassende Empfehlungen zu offenen Fragen geben, an denen sich die Verantwortlichen, aber auch Behörden und Gerichte orientieren können. Dies betrifft insbesondere den Umgang mit den auf europäischer Ebene neu eingeführten Prinzipien wie Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sowie die Instrumente der Datenschutz-Folgenabschätzung und der Zertifizierung: Bei geeigneter Ausgestaltung haben diese das Potenzial, einer Absenkung des Datenschutzniveaus entgegenzuwirken und sogar bessere Lösungen für den Datenschutz voranzubringen.

Vor allem ist jedoch der Unionsgesetzgeber gefragt, die Verordnung in einem nächsten Schritt zeitnah durch risikoadäquate Regelungen zu modernisieren und wichtige Entscheidungen selbst zu treffen, statt diese jedem Anwender selbst zu überlassen. Nur dann können die mitgliedstaatlichen Gesetzgeber auf eigene weitergehende Regelungen verzichten, um ihrem Schutzauftrag für Grundrechte gerecht zu werden.

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung

PROJEKTPARTNER



UNIVERSITÄT HOHENHEIM
LEHRSTUHL FÜR MEDIENPSYCHOLOGIE



EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN



INTERNATIONALES ZENTRUM
FÜR ETHIK IN
DEN WISSENSCHAFTEN

