NomosPraxis

Datenschutz im Internet

Bearbeitet von
Herausgegeben von: Silke Jandt, und Dr. Roland Steidle, RA

1. Auflage 2018. Buch. 532 S. Gebunden
ISBN 978 3 8487 4856 3

NomosPraxis

Jandt | Steidle [Hrsg.]

Datenschutz im Internet

Rechtshandbuch zu DSGVO und BDSG

Nomos

NomosPraxis

Dr. habil. Silke Jandt,
Referatsteilleiterin LfD Niedersachsen, Hannover
Dr. Roland Steidle, Rechtsanwalt, Frankfurt a.M. **[Hrsg.]**

Datenschutz im Internet

Rechtshandbuch zu DSGVO und BDSG

Dr. Jens Ambrock, Referent beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit | **Dr. Ubbo Aßmus,** Rechtsanwalt, Frankfurt a.M., Lehrbeauftragter an der Hochschule RheinMain | **Dr. Christian L. Geminn,** Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG), Universität Kassel | **Dr. Volker Hammer,** Consultant bei Secorvo, Karlsruhe | **Prof. Dr. Felix Hermonies, LL.M.,** Hochschule Darmstadt | **Dr. habil. Silke Jandt,** Referatsteilleiterin bei der Landesbeauftragten für den Datenschutz Niedersachsen, Privatdozentin Universität Kassel | **Dr. Moritz Karg,** Referent und Projektleiter, Digitale Agenda und zentrales IT Management, Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung des Landes Schleswig-Holstein | **Till Karsten, LL.M.,** Syndikus-Rechtsanwalt, Baden-Baden | **Henry Krasemann,** Referatsleiter beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, Jurafunk, Dozent an FH, WAK, Universität Kiel | **Dr. Philipp Richter,** Referent beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz | **Annika Selzer,** Senior Researcher und Datenschutzrechtlerin am Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Darmstadt | **Dr. Roland Steidle,** Fachanwalt für Informationstechnologierecht, Frankfurt a.M. | **Prof. Dr. Thomas Wilmer,** Hochschule Darmstadt

Nomos

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-8487-4856-3

1. Auflage 2018

Zum Geleit

Obwohl das Internet aus dem Alltag jedes Unternehmens, jeder Behörde, jeder sonstigen Organisation oder sogar aus dem Leben jedes Bürgers und jeder Bürgerin in der Europäischen Union nicht mehr hinweg zu denken ist, hat die Datenschutz-Grundverordnung kein einziges der spezifischen Probleme des Datenschutzes im Internet angesprochen. Diese missverstandene Technikneutralität führt dazu, dass im Verordnungstext die Zulässigkeit der Verarbeitung personenbezogener Daten, die Grundsätze der Datenverarbeitung und die Rechte der betroffenen Personen ohne Unterschied danach geregelt werden, ob es sich etwa um eine harmlose Kundenliste einer Änderungsschneiderei oder um eine Vollerfassung aller Kontakte, Beziehungen, Präferenzen, Einstellungen und Kommunikationsakte im Rahmen eines Social Networks handelt.

Zwar erwähnt die Datenschutz-Grundverordnung auch Risiken für die Grundrechte und Freiheiten der betroffenen Person. Diese Bezugnahme auf Risiken beschränkt sich jedoch darauf, bestimmte Pflichten des Verantwortlichen „entsprechend der Risiken von Datenverarbeitungsprozessen“ zu reduzieren. Diese Einschränkung dürfte bewirken, dass nur ein Bruchteil der Verantwortlichen und Auftragsverarbeiter diese Pflichten erfüllen muss. Die Verordnung bestimmt jedoch nicht, was sie unter Risiko versteht und wie dieses festgestellt wird.

Da das Datenschutzrecht aber dazu dient, die Grundrechte und Freiheiten der jeweils betroffenen Personen zu schützen, muss im konkreten Fall immer festgestellt werden, welches Risiko von welchem Verantwortlichen beschränkt, reduziert oder vermieden werden muss und welche Rechte die betroffene Person hat, um ihre Risiken zu verringern. Für diese entscheidende Frage bietet die Datenschutz-Grundverordnung jedoch wenig Hilfestellung. Sie verursacht vielmehr für das Angebot und die Nutzung alltäglicher Internetdienste eine große Rechtsunsicherheit.

Diese Situation könnte durch die E-Privacy-Verordnung verbessert werden. Sie greift – zumindest nach den Entwürfen der Kommission und des Parlaments – spezifische Risiken der Datenverarbeitung in der elektronischen Kommunikation, des Trackings von betroffenen Personen und der Werbung im Internet auf. Diese risikoorientierten Regelungen betreffen aber nur Einzelfragen und können die weitgehende Rechtsunsicherheit des Datenschutzes im Internet nur bedingt beseitigen.

In dieser Situation ist es sehr verdienstvoll, dass das vorliegende Handbuch von den unterschiedlichen Diensteangeboten im Internet ausgehend die Rechtsfragen klärt, die die Datenschutz-Grundverordnung und die E-Privacy-Verordnung offenlassen. Sachkundig und risikoorientiert werden die abstrakten und unspezifischen Vorgaben untersucht, um Fragen zu Cloud Computing, zu Big Data, Web-Diensten, Suchalgorithmen, Social Networks sowie zu Datenschutz durch Systemgestaltung, technische Sicherheit sowie zu spezifischen Rechten der betroffenen Person zu beantworten. Damit bietet das Handbuch ein sicheres Fundament für diejenigen, die im Internet ihre Dienste anbieten, und für diejenigen, die sie nutzen und deren Daten im Internet verarbeitet und verwertet werden. Das Handbuch bietet somit eine wertvolle Unterstüt-

zung für die Beantwortung praktischer Fragen und für die dogmatische Durchdringung und Systematisierung des Internetdatenschutzrecht.

Kassel, Mai 2018 *Alexander Roßnagel*

Vorwort der Herausgeber

Am 25. Mai 2016 ist die europäische Datenschutz-Grundverordnung in Kraft getreten. Nach einer zweijährigen Übergangszeit ist sie seit dem 25. Mai 2018 europaweit vorrangig vor dem Datenschutzrecht der Mitgliedstaaten anzuwenden. Die Verordnung ist ein Meilenstein in der Entwicklung des europäischen Datenschutzrechts, das bislang auf der europäischen Datenschutz-Richtlinie aus dem Jahr 1995 basierte. Dem Erlass der Grundverordnung ging eine weit über ein Jahrzehnt dauernde politische und rechtliche Diskussion voraus. Dies verdeutlicht, wie verschieden die Interessen der Mitgliedstaaten aber auch der unterschiedlichen Interessenvertreter bezogen auf eine Datenschutzregulierung waren und sind. Nunmehr gilt jedenfalls ein weitgehend einheitliches europäisches Recht zum Schutz des Grundrechts auf Datenschutz, das die Charta der Grundrechte der Europäischen Union in Art. 8 schützt. Angesichts der bislang mit erheblichen Unterschieden in den Mitgliedstaaten umgesetzten Datenschutz-Richtlinie war dies ein längst überfälliger Schritt. Dies gilt insbesondere mit Blick auf das Internet und grenzüberschreitende Datenverarbeitungen, die wie kaum eine andere Materie im Datenschutzrecht harmonisierte und internationale Regelungen erfordern.

Eine Neuregelung war außerdem überfällig, um Antworten auf die neuen datenschutzrechtlichen Herausforderungen im Internet zu finden. Tatsächlich hat die heutige Realität der Informationstechnologie und der Datenverarbeitung im Internet nur noch wenig mit derjenigen aus dem Jahr 1995 gemein. Erheblich größere Bandbreiten ermöglichen eine performante und zugleich kostengünstige Übermittlung großer Datenvolumen. Dies hat zu zahlreichen neuen Diensten geführt, unter anderem zur Entwicklung von Streaming- und Mediendiensten, die früher so nicht denkbar waren. Die Standardisierung und Flexibilisierung von Speicher- und Infrastrukturleistungen hat eine „Vercloudung“ aller gängigen IT-Services, Internet- und Webangebote gefördert. Kaum mehr eine Anwendung ermöglicht es nicht, Inhalte über Cloud-Dienste und mobile Endgeräte zu verteilen und zu synchronisieren. Dies hat zu weltweit grenzüberschreitenden Verarbeitungen aller möglichen Daten geführt, die nur noch schwer nachvollziehbar, geschweige denn effektiv kontrollierbar sind. Die erheblich gestiegenen Datenmengen haben neue Branchen und Anbieter entstehen lassen, unter anderem im Bereich von Big Data und den damit einhergehenden Datenanalysen. Die daraus folgenden Risiken einer Diskriminierung einzelner Personen über Algorithmen, automatisierte Entscheidungen und statistische Ergebnisse, die – zumindest teilweise – ohne eine Verarbeitung personenbezogener Daten herbeigeführt werden, zwingen dazu, das Konzept des Personenbezugs zu hinterfragen, das bisher alleiniger Anknüpfungspunkt für die Geltung datenschutzrechtlicher Bestimmungen ist. Die Miniaturisierung von Prozessoren und Netzwerkkomponenten wird dazu führen, dass auch kleinste Alltagsgegenstände in absehbarer Zeit netzwerkfähig werden und mehr oder weniger über das Internet miteinander kommunizieren. Das Internet der Dinge wird einen weiteren Entwicklungssprung auf dem Weg zur Digitalisierung des Alltags darstellen. Es stellt sich die Frage, ob ein modernes Datenschutzrecht auch all diese nur flüchtigen und meist nicht längerfristig gespeicherten Daten erfassen soll.

Der Alltag würde dann nicht nur durch Datenverarbeitungen, sondern auch durch Datenschutzregelungen durchdrungen, deren Ursprung aus der Zeit der Großrechner und zentralen Datenverarbeitungen mit klar identifizierbaren Verantwortlichen stammt. Ob diese Datenschutzregelungen in einem künftigen Umfeld praktisch überhaupt noch anwendbar oder gar kontraproduktiv sind, ist diskussionswürdig. Dies betrifft etwa Fragen der Verortung datenschutzrechtlicher Verantwortung in komplexen Geschäftsmodellen mit mehreren Beteiligten oder die Forderung nach umfangreichen Informationspflichten und Dokumentationen mit den damit einhergehenden zusätzlichen Datenspeicherungen. Fragen der Verwendung sensitiver Daten, wie der von Biometriedaten zur Authentifizierung an Endgeräten oder bei Webdiensten, fordern ebenfalls Antworten. Ebenso wird das Verhältnis des Datenschutzrechts zur Meinungsfreiheit eine der großen Rechtsfragen der kommenden Jahre sein – nicht zuletzt wegen des Einflusses von Meinungen, Fakten oder „Fake News" auf gesellschaftliche Entwicklungen und Wahlen. Letztlich zeigen sich die massiven Herausforderungen des Datenschutzrechts in einer digitalen Gesellschaft anhand vergangener und aktueller Datenschutzskandale, wie insbesondere den durch die Snowden Veröffentlichungen bekanntgewordenen Maßnahmen amerikanischer Geheimdienste, der Einflussnahme auf Wahlen über Social Networks und anhand intransparenter Datenverwertungen wie im Falle von Facebook und Cambridge Analytica.

Betrachtet man die europäische Datenschutz-Grundverordnung vor dem Hintergrund dieser Entwicklungen ist das Ergebnis freilich äußerst ernüchternd. Fast alle aktuellen und drängenden Fragen des Datenschutzrechts bleiben unbeantwortet. Meist werden sie nicht einmal in den Erwägungsgründen angesprochen. Die Verordnung übernimmt überwiegend das Bewährte und enthält nur wenige Neuerungen. Viele materiellrechtliche Regelungen der europäischen Datenschutz-Richtlinie aus 1995 wurden fast eins zu eins in die Verordnung geschrieben. Darüber hinaus enthält sie einige halbherzige Anpassungen, beispielsweise zur Auftragsverarbeitung und den Formerfordernissen, um klarzustellen, dass ein solcher Vertrag auch ohne die Verwendung von Papier abgeschlossen werden kann. Der große Innovationssprung ist ersichtlich nicht gelungen. Ergänzt wurde die Verordnung durch einen stark bürokratischen Ansatz mit insbesondere erheblichen Dokumentationspflichten, die viele kleine und mittlere Unternehmen überfordern und zudem in erster Linie Papier produzieren werden, aber keine aktuellen Datenschutzfragen lösen. Dazu treten zweifelhafte Haftungsregelungen und die Anforderung an Datenverarbeiter, sich zu rechtfertigen, wenn sie ihren – ebenfalls grundrechtlich geschützten – Gewerbebetrieb ausüben. Letztlich wird das Konzept einer selbstbestimmten Einwilligung durch ein strenges Kopplungsverbot begrenzt. Eine moderne, die Nutzer schützende und zugleich innovationsfreundliche Regulierung, die die Interessen von Nutzern und Anbietern berücksichtigt und in Einklang bringt, enthält die Verordnung bedauerlicherweise nicht.

Positiv hervorzuheben ist jedoch, dass es überhaupt gelungen ist, eine europaweite Regelung in Form einer Verordnung zu finden. Darauf muss in Zukunft aufgebaut werden, wenngleich die Innovationszyklen des europäischen Gesetzgebers nachdenklich stimmen. Schließlich wurde die europäische Datenschutz-Grundverordnung erst über zwanzig Jahre nach der europäischen Datenschutz-Richtlinie realisiert. Positiv

ist weiterhin, dass durch eine Verordnung zumindest versucht wurde, die schon in einzelnen Mitgliedstaaten nicht mehr überschaubare Zersplitterung des Datenschutzrechts zu beenden. Allerdings führen die zahlreichen Öffnungsklauseln, die dem europaweiten Harmonisierungsprozess geschuldet sind, nach wie vor dazu, dass es in allen Mitgliedstaaten eine Fülle spezifischer nationaler Datenschutzvorschriften geben kann. Voraussichtlich für einen längeren Zeitraum besteht zudem erst einmal eine unübersichtliche, vom europäischen Verordnungsgeber allein freilich nicht lösbare Parallelgeltung zwischen den Bestimmungen der Verordnung und dem nicht an diese angepassten Datenschutzrecht der Mitgliedstaaten. Dies führt zu neuen Abgrenzungsfragen und zu einer erheblichen Unsicherheit bei der Rechtsanwendung. Dazu treten in Deutschland gesetzgeberische Aktivitäten mit dem Ziel, das alte Datenschutzrecht in die Gegenwart hinüberzuretten. Dafür werden die Öffnungsklauseln der Verordnung denkbar weit ausgelegt, wenn nicht sogar europarechtswidrig überdehnt. Die ersten Versionen des neuen Bundesdatenschutzgesetzes lasen sich in Teilen wie eine Kopie seines Vorgängers. Dieses Ansinnen ist vor dem Hintergrund verständlich, dass dieselben Personen und Organisationen in Politik, Behörden und Unternehmen mit der Anwendung des neuen Datenschutzrechts betraut sind. Es verwundert daher nicht, dass einerseits politisch versucht wird, das hohe Datenschutzniveau in Deutschland zu erhalten, und dass andererseits selbst Unternehmen, die in der Vergangenheit einige Datenschutzregelungen kritisiert haben, angesichts der aktuellen Rechtsunsicherheit lieber auf festem Grund und nach bewährtem Konzept fortfahren möchten. Es steht allerdings zu erwarten, dass der Europäische Gerichtshof und der Europäische Datenschutzausschuss dem einen Riegel vorschieben werden. Der Preis der europaweiten Harmonisierung und notwendigen Internationalisierung ist auch im Datenschutzrecht, dass die Rechtsauslegung künftig nach europäischen Maßstäben zu beurteilen ist und nicht nach den Vorstellungen eines einzelnen Mitgliedstaats oder dessen Ländern.

Noch ungelöst, aber dem Prinzip einer Verordnung immanent, ist der Verlust an konkreten, vorhersehbaren Detailregelungen. Die damit erzeugte Rechtsunsicherheit dürfte noch auf Jahre bestehen bleiben. Kurzfristig ist weder mit Urteilen des Europäischen Gerichtshofs zu rechnen, noch mit konkretisierenden Empfehlungen und Leitlinien des Europäischen Datenschutzausschusses in größerem Umfang. Selbst die sehr zu begrüßenden Auslegungshilfen der Datenschutzkonferenz und einzelner deutscher Landesaufsichtsbehörden stehen unter dem Vorbehalt einer später abweichenden europäischen Rechtsauslegung. Aus Sicht der datenverarbeitenden Unternehmen ist es damit in vielen Bereichen der Informationstechnologie und der Internetnutzung praktisch unmöglich, sich gerichtsfest rechtskonform zu verhalten, insbesondere in innovativen Projekten. Angesichts des erheblich erweiterten Bußgeldrahmens zur Sanktionierung von – gegebenenfalls nicht eindeutig erkennbaren – Verstößen ist dies wirtschaftlich riskant. Für die Forschung und Entwicklung bleibt zu hoffen, dass Innovationen vor diesem Hintergrund nicht vermehrt in Drittländer und damit ohne direkte Einflussnahmemöglichkeit der europäischen Institutionen ausgelagert werden. Denn alle erfolgreichen Entwicklungen und Webangebote aus Drittländern, insbeson-

dere den USA, haben bislang zu tatsächlichen Auswirkungen auch in der Europäischen Union geführt, allein aufgrund der großen Anzahl betroffener Nutzer.

Die nun anstehenden ersten Jahre mit der neuen Datenschutz-Grundverordnung werden daher äußerst spannend. Aus Sicht der datenverarbeitenden Anbieter von Internet- und Webdiensten ist es angesagt, „auf Sicht zu fahren". Viele Bereiche sind „rechtliches Neuland" und entweder in der Rechtspraxis unklar oder von der Verordnung gleich gar nicht erfasst. Dies betrifft auch die Auswirkungen der noch anstehenden E-Privacy-Verordnung sowie nationale Ergänzungen oder Konkretisierungen der europäischen Datenschutz-Grundverordnung. Insofern haben einzelne Auslegungsfragen auch dieses Handbuchs noch einen gewissen Prognosecharakter. Aus Sicht der Herausgeber und der Autoren bedeutet dies, dass sie die Rechtspraxis mit Blick auf Neuerungen und weitere Auflagen des Handbuchs laufend beobachten und dies in künftigen Auflagen berücksichtigen werden.

Gerade wegen der beschriebenen Herausforderungen sind allerdings Auslegungs- und Argumentationshilfen wichtig für die künftige Rechtsanwendung. Das Handbuch soll dieses Bedürfnis befriedigen und Rechtsanwendern aus Wissenschaft, Behörden, Unternehmen sowie Nutzern von Internet- und Webangeboten eine praktische Hilfestellung im Alltag geben. Dazu enthält es fundierte und wissenschaftlich untermauerte Beiträge zu fast allen relevanten Bereichen des Datenschutzrechts im Internet. Die Autoren haben verschiedene berufliche Hintergründe, alle lange Jahre Erfahrung im Datenschutzrecht und prägen die Materie in ihren Bereichen mit. Es sind Erfahrungen aus Wissenschaft, Aufsichtswesen und Unternehmen in das Handbuch eingeflossen. Der daraus folgende Mehrwert prägt dieses Handbuch und macht seinen Reiz aus.

Die Herausgeber und Autoren bedanken sich bei den Lesern für kritische Anmerkungen und wünschen Ihnen viel Freude beim Lesen.

Göttingen, Frankfurt, Mai 2018 *Silke Jandt und Roland Steidle*

Inhaltsübersicht

Inhaltsverzeichnis

Verzeichnis der Autoren

Dr. Jens Ambrock	Referent beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit
Dr. Ubbo Aßmus	Rechtsanwalt für Datenschutz- und IT-Recht bei Heuking Kühn Lüer Wojtek, Frankfurt aM, Lehrbeauftragter an der Hochschule RheinMain
Dr. Christian L. Geminn	Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel
Dr. Volker Hammer	Consultant bei der Secorvo Security GmbH, Karlsruhe
Prof. Dr. Felix Hermonies	Mag. rer. publ. LL.M. (R.L.), Professor für Datenschutz- und Medienrecht an der Hochschule Darmstadt
Dr. habil. Silke Jandt	Referatsteilleiterin bei der Landesbeauftragten für den Datenschutz Niedersachsen, Privatdozentin an der Universität Kassel
Dr. Moritz Karg	Referent und Projektleiter, Digitale Agenda und zentrales IT Management, Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung des Landes Schleswig-Holstein
Till Karsten, LL.M.	Syndikus-Rechtsanwalt bei der infoscore Consumer Data GmbH, part of Arvato Financial Solutions
Henry Krasemann	Referatsleiter beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, Jurafunk, Dozent an FH, WAK, Universität Kiel
Dr. Philipp Richter	Referent beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
Annika Selzer	Senior Researcher und Datenschutzrechtlerin am Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
Dr. Roland Steidle	Fachanwalt für Informationstechnologierecht und Partner bei SWM Rechtsanwälte in Frankfurt am Main
Prof. Dr. Thomas Wilmer	Professor für Informationsrecht an der Hochschule Darmstadt