forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

Policy Paper

EVALUATION DER DATENSCHUTZ-GRUNDVERORDNUNG

IMPRESSUM

Autoren:
Alexander Roßnagel[1], Christian Geminn[1], Maxi Nebel[1], Tamer Bile[1],

(1) Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG)

Kontakt:
Michael Friedewald

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, November 2019

Einleitung

Die Datenschutz-Grundverordnung ist nach mehr als vierjährigen Verhandlungen am 24. Mai 2016 in Kraft getreten und seit dem 25. Mai 2018 anzuwenden. Nach Art. 97 Abs. 1 DSGVO ist die Europäische Kommission bereits bis zum 25. Mai 2020 und danach alle vier Jahre dazu verpflichtet, dem Europäischen Parlament und dem Rat einen schriftlichen Bericht über die Bewertung und Überprüfung der Verordnung vorzulegen und zu veröffentlichen. Hierbei hat die Kommission nach Art. 97 Abs. 4 DSGVO die Standpunkte und Feststellungen des Europäischen Parlaments, des Rates sowie anderer einschlägiger Stellen und Quellen zu berücksichtigen. Nach Art. 97 Abs. 5 DSGVO hat die Kommission gegebenenfalls geeignete Vorschläge zur Änderung der Verordnung vorzulegen und dabei insbesondere „aktuelle Entwicklungen der Informationstechnologie und Fortschritte in der Informationsgesellschaft" zu berücksichtigen.

Dieses Policy Paper nimmt die anstehende Evaluation zum Anlass, um auf einige Verbesserungsmöglichkeiten in der Verordnung hinzuweisen und konkrete Verbesserungsvorschläge zu unterbreiten. Hervorzuheben ist, dass die Verordnung eine große Zahl positiver Neuerungen für betroffene Personen mit sich gebracht hat: zum Beispiel die Ausweitung des Anwendungsbereichs des europäischen Datenschutzrechts durch das Marktort- und Beobachtungsprinzip, Vorgaben zum Datenschutz durch Systemgestaltung und datenschutzfreundliche Voreinstellungen, Stärkung der Betroffenenrechte, das Recht auf Datenübertragung oder die erweiterten Sanktionsmöglichkeiten. Dennoch sollte nicht außer Acht gelassen werden, dass die Verordnung – durch Mängel in Konzeption und Normtext – neue Defizite geschaffen und bestehende Defizite nicht beseitigt hat und vor allem durch ihren hohen Abstraktionsgrad wenig geeignet ist, die spezifischen Herausforderungen moderner und zukünftiger Informationstechnologien zu adressieren. Die genannten Defizite sind sowohl praktischer als auch konzeptioneller Natur und werden dementsprechend nachfolgend behandelt.

Das Policy Paper möchte einen Beitrag zur Diskussion um die Verbesserung der Datenschutz-Grundverordnung leisten. Es beschränkt sich auf ausgewählte Aspekte, die bei ihrer anstehenden Evaluation vornehmlich Berücksichtigung finden sollten.

Praktische Defizite

Vier Problemschwerpunkte sind erkennbar, deren Überarbeitung und Klärung insbesondere für die betroffenen Personen deutliche Verbesserungen beim Schutz ihrer grundrechtlich geschützten Rechtspositionen bringen würden. Diese werden im Folgenden vorgestellt und zu ihnen werden konkrete Verbesserungsvorschläge unterbreitet.

Das Verhältnis der Erlaubnistatbestände zueinander

Das Verhältnis der Erlaubnistatbestände zueinander ist im Text der Verordnung ungeklärt. So erweckt Art. 6 Abs. 1 UAbs. 1 DSGVO durch die Verwendung des Begriffs „mindestens“ den Eindruck, dass mehrere Erlaubnistatbestände nebeneinander Anwendung finden können. Die Formulierung in Art. 17 Abs. 1 lit. b DSGVO könnte in Bezug auf die Einwilligung nach Art. 6 UAbs. 1 lit. a DSGVO ebenfalls so verstanden werden, da nach dieser Regelung ein Widerruf der Einwilligung nur dann einen Anspruch auf Datenlöschung begründet, wenn es „an einer anderweitigen Rechtsgrundlage für die Verarbeitung“ fehlt. Nach dieser Lesart könnte sich der Verantwortliche also beispielsweise auf eine Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO berufen, wenn die betroffene Person ihre Einwilligung in die Datenverarbeitung widerrufen hat.

Andererseits verbindet die Datenschutz-Grundverordnung mit den verschiedenen Erlaubnistatbeständen verschiedene Informationspflichten. Zunächst muss sich der Verantwortliche konkret auf einen Erlaubnistatbestand berufen und darüber informieren. Beruft er sich auf eine Interessenabwägung, muss er vor der Datenverarbeitung über seine berechtigten Interessen und deren Überwiegen aufklären sowie über die Möglichkeit des Widerspruchs nach Art. 21 DSGVO. Will er sich demgegenüber auf die Einwilligung der betroffenen Person berufen, muss er vor der Einwilligung über die Möglichkeit und Rechtsfolgen des Widerrufs der Einwilligung informieren, nämlich dass danach eine weitere Datenverarbeitung nicht mehr zulässig ist. Würde sich der Verantwortliche dann aber auf die Interessenabwägung stützen, könnte er den Standpunkt vertreten, dass der Widerruf formell wirkungslos wäre, und es ablehnen, ihn im Sinne eines Widerspruchs nach Art. 21 DSGVO zu interpretieren. Dies könnte auch dazu führen, dass der Verantwortliche im Rahmen seiner Informationspflicht vor Beginn der Datenverarbeitung über alle in Frage kommenden Erlaubnistatbestände, der betroffenen Person widersprüchliche Informationen zur Verfügung stellen würde. Zudem bekäme der Verantwortliche die Möglichkeit, sich anfangs mehrere Erlaubnistatbestände offen zu halten und sich erst im Nachhinein – etwa bei erfolgtem Widerruf oder Widerspruch – auf eine bestimmte Erlaubnis festzulegen.

Dies hat auch Auswirkungen auf das Recht auf Datenübertragung nach Art. 20 DSGVO. Dieses wurde als Neuerung der Grundverordnung gefeiert, kommt allerdings nur zur Anwendung bei personenbezogenen Daten, die aufgrund einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO oder aufgrund eines Vertrags nach Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO verarbeitet werden. Der Wortlaut der Vorschrift ist hier eindeutig und abschließend, sodass zum Beispiel solche personenbezogenen Daten, die aufgrund berechtigter Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO verarbeitet werden, von vornherein nicht umfasst sind. Dieses Recht zu haben oder nicht, könnte für die betroffene Person bei Abgabe der Einwilligung von Bedeutung sein. Wenn der Verantwortliche aber nachträglich seine Datenverarbeitung auf eine Interessenabwägung stützt, nimmt er der betroffenen Person dieses Recht.

Mit dem nachträglichen Wechsel des Erlaubnistatbestands verstieße der Verantwortliche gegen den Grundsatz von Treu und Glauben aus Art. 5 Abs. 1 lit. a DSGVO. Der Grundsatz umfasst die Art und Weise der Rechtsausübung zwischen dem Verantwortlichen und der betroffenen Person. Diese muss im Sinne der englischen Sprachfassung „fair" sein und darf keine der Beteiligten über Gebühr benachteiligen. Eine faire Datenverarbeitung muss daher zumindest umfassen, dass sich die betroffene Person sicher sein kann, dass ein Ausüben ihrer Rechte auch die gewünschten Rechtsfolgen hat, dass also eine Einwilligung das Recht zur Datenübertragung begründet und ein Widerruf der Einwilligung tatsächlich die zukünftige Datenverarbeitung unzulässig macht. Andernfalls würde der betroffenen Person Entscheidungsmacht suggeriert und diese später umgangen werden.

Aufgrund dieser Widersprüche sollte in der Verordnung klargestellt werden, dass ein Verantwortlicher sich neben einer Einwilligung nicht zusätzlich auf einen gesetzlichen Erlaubnistatbestand berufen kann. Wenn er von der betroffenen Person eine Einwilligung einfordert, muss er sich auch auf die Regeln zu einer Einwilligung einlassen. Er muss dann vor allem einen Widerruf der Einwilligung gegen sich gelten lassen und kann nicht trotz des Widerrufs die Datenverarbeitung unter Berufung auf einen anderen gesetzlichen Erlaubnistatbestand fortsetzen; zudem muss er der betroffenen Person eine Übertragung ihrer Daten ermöglichen.

Vermeidung personenbezogener Daten

Das Gebot der Datenvermeidung zählt zu den allgemeinen Datenschutzprinzipien. Vor der Reform des Datenschutzrechts war dieses in Deutschland in § 3a BDSG a. F. gesetzlich verankert. Dieser forderte, die Vermeidung von personenbezogenen Daten bereits bei der Zweckfestlegung zu berücksichtigen, den Zweck also so auszuwählen, dass möglichst wenige personenbezogene Daten für die Verarbeitung erforderlich werden. Die Datenschutz-Grundverordnung regelt indes in Art. 5 Abs. 1 lit. c DSGVO den Grundsatz der Datenminimierung. Dies erscheint auf den ersten Blick gleichbedeutend zu sein, was bei näherem Hinsehen aber nicht der Fall ist. Die Datenminimierung bestimmt, dass Daten nur insoweit verarbeitet werden dürfen, als sie als Mittel zur Erreichung des Zwecks der Verarbeitung erforderlich sind. Anders als im Rahmen der Datenvermeidung ist der Verantwortliche aber frei, den (legitimen) Verarbeitungszweck zu wählen und so auszugestalten, dass alle personenbezogenen Daten, die er erheben will, auch erforderlich sind. Dieser gewählte Zweck wird von der Datenschutz-Grundverordnung nur durch den allgemein gefassten Datenschutzgrundsatz „Verarbeitung nach Treu und Glauben" nach Art. 5 Abs. 1 lit. a DSGVO eingeschränkt. Da offen bleibt, inwieweit dieser Grundsatz Einfluss auf die Zweckwahl durch den Verantwortlichen haben müsste, könnte die aktuelle Formulierung für die betroffene Person bedeuten, dass der Verantwortliche ungleich mehr personenbezogene Daten verarbeiten dürfte, solange er nur den Zweck entsprechend ausrichten würde. Ob das Gebot der Datenvermeidung in Erwägungsgrund 78 Satz 3 DSGVO hineingelesen werden kann, der für Art. 25 DSGVO fordert, die Verarbeitung personenbezogener Daten zu minimieren, kann dahingestellt bleiben, da dieses im Zweifel mit dem kodifizierten Grundsatz der Datenminimierung in Art. 5 Abs. 1 lit. c DSGVO kollidiert. Daher wäre für einen effektiven Grundrechtsschutz die gesetzliche Verankerung der Datenvermeidung in der Grundverordnung wünschenswert. Am besten geschieht dies durch eine Klarstellung in den Datenschutzgrundsätzen, spezifisch in Art. 5 Abs. 1 lit. c DSGVO, dann würden entsprechende Verstöße auch mit Sanktionen belegt werden können.

Automatisierte Entscheidung im Einzelfall

Die Datenschutz-Grundverordnung enthält Regelungen für die automatisierte Entscheidung im Einzelfall, die jedoch in der derzeitigen Gestaltung die betroffenen Personen über Gebühr benachteiligen. Art. 22 Abs. 1 DSGVO normiert das „Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie ähnlicher Weise erheblich beeinträchtigt". Dies ist grundsätzlich als Verbot von automatisierten Entscheidungen im Einzelfall zu interpretieren. Abs. 2 sieht von diesem Verbot Ausnahmen vor, wenn die automatisierte Entscheidung für den Abschluss eines Vertrags erforderlich war, wenn dies aufgrund von Rechtsvorschriften der Mitgliedstaaten zulässig ist oder wenn die betroffene Person eingewilligt hat. Eine automatisierte Entscheidung im Einzelfall liegt vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch einen Menschen stattgefunden hat. Das ist zum Beispiel dann der Fall, wenn die Zuteilung von Sitzplätzen in Flugzeugen ausschließlich automatisiert erfolgt oder wenn der Score-Wert maßgeblich für die Entscheidung über einen Vertragsschluss ist.

Automatisierte Entscheidungsverfahren können ungleich mehr an Informationen berücksichtigen und verarbeiten als Menschen und versprechen dabei bessere, schnellere, gerechtere und kostengünstigere Ergebnisse. Allerdings bergen diese Verfahren ein hohes Potential für Diskriminierung für betroffene Personen. So kann eine automatisierte Entscheidung im Einzelfall etwa dazu führen, dass ein gewünschter Vertrag abgelehnt wird oder ein höherer Zinssatz als bei optimaler Bonität angeboten wird. Ein hohes Diskriminierungspotential wird insbesondere auch in der modernen Arbeitswelt erwartet, wenn durch automatisierte Entscheidungsverfahren Bewerbungen nach bestimmten Schlagworten „ausgesiebt" werden.

Problematisch ist, dass der Anwendungsbereich des Verbots automatisierter Einzelentscheidungen sehr eng formuliert ist und damit leicht zum Nachteil der betroffenen Person interpretiert und angewendet werden kann. Zum einen erfasst Art. 22 Abs. 1 DSGVO lediglich die Entscheidung selbst, nicht aber die vorhergehende automatisierte Verarbeitung und auch nicht die auf einer automatisierten Verarbeitung beruhende Entscheidung. Die Vorschrift kommt also nicht zum Tragen, sofern am Ende ein Mensch entscheidet. Daher wird die Vorschrift von den Datenverarbeitern vielfach auch so verstanden, dass damit auch Fälle erfasst sind, in denen eine formale Entscheidung durch einen Menschen nachgeschaltet wird, dieser Mensch aber gar keine praktische Möglichkeit oder ausreichendes Fachwissen besitzt, um von den Ergebnissen der automatisierten Entscheidung abzuweichen. Um diesem Defizit zu begegnen und die Einschränkungen des Verbots automatisierter Entscheidungen im Einzelfall für die betroffene Person weniger nachteilig zu gestalten, sollte das Wort "ausschließlich" in Art. 22 Abs. 1 DSGVO gestrichen werden. So würden auch solche automatisierten Entscheidungen unter das Verbot fallen, in denen ein Mensch die Letztentscheidung fällt, ohne diese inhaltlich beeinflussen zu können.

Einschränkend wirkt zudem, dass das Recht nach Art. 22 Abs. 1 DSGVO nur gelten soll, wenn die Entscheidung eine Rechtswirkung entfaltet oder die betroffenen Personen auf ähnliche Weise erheblich beeinträchtigt. Nach Erwägungsgrund 71 DSGVO sollen hierzu die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen zählen. Art. 22 Abs. 1 DSGVO soll daher etwa keine Anwendung finden für algorithmengesteuerte Direktwerbung oder die Beschränkung von Zahlungsmöglichkeiten im E-Commerce, soweit dies jeweils automatisiert erfolgt. Um hier Abhilfe zu schaffen, sollte es für das Recht, nicht einer auf automatisierter Verarbeitung beruhenden Entscheidung unterworfen zu

werden, genügen, wenn sie geeignet ist, die betroffene Person in erheblicher Weise zu beeinträchtigen.

Zum anderen kommt das Verbot der automatisierten Entscheidung im Einzelfall nicht zur Anwendung, wenn nach Art. 22 Abs. 2 lit. a DSGVO die automatisierte Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist. Durch diese Ausnahme vom Verbot der automatisierten Entscheidung im Einzelfall wird Verantwortlichen und Auftragsverarbeitern ermöglicht, nach eigenem Ermessen einen Großteil ihrer Entscheidungsprozesse zu automatisieren. Bedenklich ist zudem, dass diese Ausnahme nicht greifen soll, wenn der Verantwortliche beschließt, dass automatisierte Entscheidungen Dritter als Grundlage für seine Entscheidung dienen sollen. Dies ist etwa dann der Fall, wenn eine Bonitätsprüfung von einem Dritten eingeholt wird, die dann über die Vergabe eines Kredits entscheidet. Diese Regelung des Abs. 2 lit. a bevorzugt die Interessen des Verantwortlichen einseitig. Um diese Asymmetrie zu beseitigen, sollte die Regelung des Abs. 2 lit. a gestrichen werden. Diesbezüglich ließe sich ein Ausgleich der Grundrechte des Verantwortlichen und der betroffenen Personen durch die Vorschrift des Abs. 2 lit. c erreichen, nachdem eine Ausnahme vom Verbot automatisierter Entscheidungen im Einzelfall gilt, wenn die betroffene Person in diese Form der Datenverarbeitung eingewilligt hat.

Profiling

Ein großer Mangel der Datenschutz-Grundverordnung besteht darin, dass sie zwar das Profiling punktuell erwähnt, seine besonderen Risiken aber nicht ausreichend regelt. Gegen Profiling kann nach Art. 21 Abs. 1 und 2 DSGVO Widerspruch angemeldet werden, wenn es der Wahrung berechtigter Interessen, insbesondere dem Direktmarketing dient. Es ist außerdem nach Art. 22 Abs. 1 DSGVO verboten, wenn es für eine ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung dient, es sei denn eine der Ausnahmen des Art. 22 Abs. 2 DSGVO erlaubt dies. Alle anderen Formen und Gründe für Profiling bleiben in der DSGVO ungeregelt.

Profiling wird in Art. 4 Nr. 5 DSGVO definiert als „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen".

Ein Anwendungsfall von Profiling ist die Auswertung des Online-Nutzungsverhaltens. So kann auf Grundlage vergangener Suchanfragen eine Sortierung von Suchergebnissen vorgenommen oder die Auswertung früherer Einkäufe für die zielgerichtete Werbung (Predictive Behavioral Targeting), für Produktempfehlungen, Preisgestaltungen oder Sonderangebote genutzt werden. Wer Online-Dienste nutzt, dem werden auf diese Weise nur noch die Suchergebnisse oder die Werbung angezeigt, für die er sich mutmaßlich interessiert.

Profiling ist jedoch mit Risiken für die Rechte der betroffenen Personen verbunden, die über die normale Verarbeitung von personenbezogenen Daten hinausgehen. So kann es in Folge einer automatisierten Entscheidung auf Grundlage eines Profils zu einer Preisdiskriminierung im Internet kommen, wenn etwa Kunden, bei denen aufgrund ihres Profils (Einkommen, Interessen, Präferenzen) eine höhere Zahlungsbereitschaft angenommen wird und daher ein höherer Preis verlangt wird, als dies ohne Profil der Fall wäre.

Um den spezifischen Risiken zu begegnen, die mit Profiling für die Grundrechte der betroffenen Personen einhergehen, sind risikoadäquate Regelungen notwendig. Die Datenschutz-Grundverordnung könnte gesetzlich festlegen, für welche Zwecke Profiling zulässig ist und für welche nicht. Vergleichbar mit der Regelung in Art. 9 DSGVO für besondere Kategorien personenbezogener Daten könnte die Regelung festlegen, dass Profiling grundsätzlich nicht erlaubt ist und nur in den ausdrücklich vorgesehenen Fällen zugelassen ist.

Informationspflichten

Art. 13 und 14 DSGVO enthalten die zentralen Informationspflichten des für die Verarbeitung Verantwortlichen gegenüber der betroffenen Person. Im Gegensatz zu den Vorgängerregelungen der Datenschutzrichtlinie wurden die Informationspflichten mit der Datenschutz-Grundverordnung zwar inhaltlich ausgeweitet, aber teilweise sehr abstrakt umschrieben. Der betroffenen Person sind alle relevanten Informationen, unter anderem der Name und die Kontaktdaten des für die Verarbeitung Verantwortlichen sowie die Zwecke der Verarbeitung, mitzuteilen. Differenziert wird danach, ob personenbezogene Daten bei der betroffenen Person oder bei anderen erhoben werden.

Werden die personenbezogenen Daten bei der betroffenen Person erhoben, so sind die Informationen nach Art. 13 Abs. 1 und 2 DSGVO unmittelbar zum Zeitpunkt der Erhebung mitzuteilen. Dies wird in der Praxis häufig so verstanden, dass bei Vertragsschluss oder beim ersten Kontakt mit der betroffenen Person in umfangreichen Datenschutzerklärungen oder Allgemeinen Geschäftsbedingungen alle denkbaren Eventualitäten künftiger Datenverarbeitungen beschrieben werden müssen. Dies geschieht oft schon lange Zeit vor der tatsächlichen Erhebung der Daten und vor der Entscheidung der betroffenen Person, ob sie mit der Datenverarbeitung einverstanden ist. Dies hat zur Folge, dass sie sich an die umfassenden Inhalte der – unter Umständen Jahre zuvor erfolgten – Information nicht mehr erinnern wird, wenn ihre Daten (dann irgendwann) tatsächlich erhoben werden. Die Praxis entspricht damit nicht der Zielsetzung der Datenschutz-Grundverordnung, die betroffene Person so zu informieren, dass sie ihre informationelle Selbstbestimmung optimal ausüben kann, und damit der Forderung des Art. 13 Abs. 1 DSGVO, betroffene Personen zum Zeitpunkt der Erhebung zu informieren.

Damit der Zweck der Informationspflicht nicht ausgehöhlt wird, sind Ergänzungen am Wortlaut von Art. 13 Abs. 1 und 2 DSGVO geboten, die klarstellen, dass die Information situationsadäquat erfolgt, nämlich vor der konkreten Datenerhebung und der potentiellen Entscheidung der betroffenen Person.

Art. 14 DSGVO findet Anwendung, wenn die personenbezogenen Daten nicht bei der betroffenen Person, sondern bei Dritten erhoben wurden. Art. 13 und 14 DSGVO unterscheiden sich inhaltlich lediglich hinsichtlich des Zeitpunktes der Information und des Umfangs der Ausnahmen von der Informationspflicht. Dabei nimmt die Datenerhebung bei Dritten der betroffenen Person die Chance, Auskunft über die Datenverarbeitung zu erhalten und sie zu beeinflussen, wenn der Verantwortliche die Quellen der Daten nicht konkret benennt, und macht sie von vornherein intransparent. Um diesem Mangel abzuhelfen, sollte Art. 14 DSGVO diese Information zwingend verlangen.

Recht auf Datenübertragung

Das Recht auf Datenübertragung stellt ein prominentes Novum des neuen Datenschutzrechts dar. Es gibt der betroffenen Person das Recht, Daten, die sie dem Verantwortlichen bereitgestellt hat, einem anderen Verantwortlichen zu übertragen oder

übertragen zu lassen. Diese – insbesondere auf soziale Netzwerke – abzielende Regelung soll sogenannte Lock-in-Effekte mindern und den Wettbewerb zwischen Anbietern steigern.

Die Bezeichnung des Rechts ist missverständlich. Statt „Datenübertragbarkeit" sollte es Datenübertragung heißen, da es das Recht beinhaltet, personenbezogene Daten übertragen zu lassen, und nicht nur die theoretische Möglichkeit der Übertragung herstellen soll. Der Nutzen dieses Rechts ist für Verbraucher durch drei Probleme, die der Normtext verursacht, eingeschränkt.

So ist der Begriff „bereitgestellt" in Art. 20 Abs. 1 DSGVO nicht klar genug und wird unterschiedlich interpretiert. Der Begriff sollte, um sinnvolle Ergebnisse zu erzielen, beispielsweise durch „veranlasst" oder „verursacht" ersetzt werden. Bisher ist der Umfang, was als „bereitgestellt" im Sinne der Vorschrift gilt, umstritten und wird von Verantwortlichen zum Nachteil der betroffenen Personen eingeschränkt. Für eine effektive Gewährleistung des Rechts auf Datenübertragung sollten nicht nur solche Daten unter die Vorschrift fallen, welche die betroffene Person im Sinne einer aktiven Eingabe zur Verfügung gestellt hat, sondern auch alle diejenigen Daten, die durch die Nutzung des Systems oder Gerätes entstehen, beispielsweise Suchverläufe, Playlists, Verkehrs- und Standortdaten, Fitnessdaten, aber auch Daten Dritter, über die die betroffene Person rechtmäßig verfügen kann, beispielsweise Chatverläufe. Letztlich geht es darum, Einflusssphären zwischen Verantwortlichem und betroffener Person abzugrenzen und den Beitrag zum Entstehen der Daten zu würdigen. Aus ihrem Beitrag zum Entstehen der Daten leitet sich die Verfügungsbefugnis der betroffenen Person ab. Soweit die betroffene Person das Entstehen der Daten verursacht hat, der Verantwortliche aber hierzu wenig beigetragen hat, indem er etwa lediglich die Infrastruktur bereitstellt, sollen die entstandenen Daten auch unter der Verfügungs- und Nutzungsgewalt der betroffenen, Person stehen. Aus dieser Logik heraus wird klar, dass eine Erstreckung von Art. 20 DSGVO auch auf Rohdaten erfolgen muss, die vom Verhalten der betroffenen Person verursacht werden.

Das Recht auf Datenübertragung besteht nach Art. 20 Abs. 1 DSGVO nur, wenn die Verarbeitung auf einer Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO oder auf einem Vertrag gemäß Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO beruht. Ungeklärt ist die Frage, ob dieser Anspruch auch noch zu dem Zeitpunkt besteht, wenn die Einwilligung widerrufen oder der Vertrag beendet worden ist. Ohne Einwilligung oder ohne Vertrag müssen die Daten nach Art. 17 Abs. 1 lit. a, b oder d DSGVO gelöscht werden. Eine Datenübertragung wäre dann nicht mehr möglich. Zwar wird gemeint sein, dass die Datenübertragung auch noch nach Beendigung der Verarbeitungserlaubnis möglich ist, solange der Verantwortliche die Daten noch nicht gelöscht hat. Hier wäre jedoch eine textliche Klarstellung geboten, wobei auch festgelegt werden könnte, dass dieser Anspruch in einem angemessenen zeitlichen Zusammenhang zum Widerruf oder zur Vertragsbeendigung geltend zu machen wäre.

Schließlich bleibt in der Formulierung offen, in welcher Form die betroffene Person die Datenübertragung fordern darf. Diese ist durch unbestimmte Rechtsbegriffe wie „gängig", „maschinenlesbar" und „strukturiert" gekennzeichnet, die von Verantwortlichen höchst uneinheitlich und für die betroffene Person nachteilig ausgelegt werden und zu nicht sachgerechten Ergebnissen führen. Konkrete Formate werden hingegen nicht vorgegeben. Die – in Erwägungsgrund 68 DSGVO am Rande erwähnte – Interoperabilität würde bewirken, dass Daten nur in einem solchen Format übertragen werden dürfen, dass ein anderer Verantwortlicher diese auch weiterverarbeiten kann. Hier bietet sich eine gesetzliche Verankerung an. In jedem Fall wäre es von Vorteil, wenn der Europäische Datenschutzausschuss konkrete technische Bedingungen der Interoperabilität festlegen würde.

Konzeptionelle Defizite der DSGVO

Neben den oben angesprochenen praktischen Defiziten weist die Datenschutz-Grundverordnung weitere, teilweise gravierende konzeptionelle Defizite auf. Diese letzteren Defizite dürften dazu führen, dass die Datenschutz-Grundverordnung ihre selbstgesteckten Ziele nicht erreicht, nämlich das Datenschutzrecht unionsweit zu vereinheitlichen, einheitliche Vorgaben für gleiche wirtschaftliche Bedingungen in der Europäischen Union zu bieten und damit den Binnenmarkt zu stärken und schließlich zur Modernisierung des Datenschutzes beizutragen.

Ein zentrales Problem der Datenschutz-Grundverordnung liegt in der großen Diskrepanz zwischen der hohen Komplexität des Regelungsbedarfs einerseits und der Abstraktheit ihrer Vorschriften andererseits. Mit nur 51 materiellrechtlichen Regelungen versucht sie, den datenschutzrechtlichen Herausforderungen gerecht zu werden, für die vor Anwendbarkeit der Datenschutz-Grundverordnung im deutschen Datenschutzrecht tausende bereichsspezifische Vorschriften existierten. Die zum Teil hochabstrakten Vorgaben der Datenschutz-Grundverordnung erzeugen bei den Adressaten hohe Rechtsunsicherheit.

Ihr Ziel, das Datenschutzrecht unionsweit zu vereinheitlichen, verfehlt die Datenschutz-Grundverordnung dadurch, dass sie trotz ihres Anwendungsvorrangs viele implizite und explizite Gestaltungsspielräume für mitgliedstaatliche Regelungen lassen muss, um der Komplexität ihres Regelungsgegenstandes gerecht zu werden. Diese Freiräume führen konsequenterweise dazu, dass die Vorgaben der Datenschutz-Grundverordnung in den Mitgliedstaaten unterschiedlich konkretisiert, präzisiert oder ergänzt und nach der jeweiligen nationalen bisherigen Datenschutzkultur ausgelegt werden (bspw. bezüglich Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO). Zwar koordinieren die Aufsichtsbehörden ihre rechtlichen Auffassungen zu vielfältigen Themen im Europäischen Datenschutzausschuss, jedoch gewährleistet dies allein noch keine einheitliche Auslegung des Datenschutzrechts, zumal die Gerichte in den Mitgliedstaaten daran nicht gebunden sind. Durch unterschiedliche Konkretisierungen und Präzisierungen der Vorgaben der Datenschutz-Grundverordnung in den Mitgliedstaaten verfehlt die Datenschutz-Grundverordnung auch ihr Ziel, gleiche wirtschaftliche Bedingungen in der Europäischen Union zu bieten.

Auch dem Ziel, den Datenschutz zu modernisieren, wird die Datenschutz-Grundverordnung nicht gerecht. Sie führt – abgesehen von wenigen Ausnahmen – grundsätzlich die Konzeptionen der Datenschutzrichtlinie von 1995 weiter und kann den gegenwärtigen und künftigen Herausforderungen der Informations- und Kommunikationstechnologie schon allein deshalb nicht gerecht werden.

So hält sie etwa an Datenschutzprinzipien fest, die weitgehend aus einer Zeit stammen, in der weder PCs noch das Internet bekannt waren. In Zeiten von Ubiquitous Computing, Big Data, lernfähigen Algorithmen und der Erfassung der Welt durch Systeme der Künstlichen Intelligenz geraten diese Prinzipien jedoch unter einen massiven Druck, der ihre künftige Anwendbarkeit in Frage stellt. So wird das Prinzip der Zweckbindung etwa durch Smart-Car, Smart-Home oder Smart-Health-Anwendungen ausgehöhlt, da diese Anwendungen eine möglichst breite Datengrundlage über Verhalten, Interessen und Vorlieben benötigen. Das eigentliche Ziel der Zweckbindung, Datenverarbeitungen auf das erforderliche Maß zu begrenzen, wird dabei sowohl von der Idee einer unbemerkten, komplexen und spontanen technischen Unterstützung als auch von dem Ziel, durch Zusammenführen und Auswerten möglichst vieler Daten aus vielfältigen Quellen neue Erkenntnisse zu gewinnen, konterkariert.

Auch ein Systemdesign, in dem Privatpersonen arbeitsteilig Verarbeitungsvorgänge als Teil einer Infrastruktur vornehmen können (z. B. Blockchain, Mix-Netze, Crowd-Sensing, Peer-to-Peer-Kommunikation), wird in der Datenschutz-Grundverordnung noch nicht aufgegriffen. In diesen Fällen sind die Verantwortlichkeitsgrenzen nicht klar oder könnten beteiligte Privatpersonen unangemessen benachteiligen. Weiterhin wäre eine Weiterentwicklung der Datenschutz-Grundverordnung im Sinne kollektiver Aspekte, auch bei der Rechtewahrnehmung, zu überlegen.

Zudem sollten Hersteller stärker in die Pflicht genommen werden können. Insbesondere bei der Anforderung von Datenschutz durch Technikgestaltung und datenschutzfreundlicher Voreinstellungen (Art. 25 DSGVO) wird zurzeit lediglich der Verantwortliche verpflichtet; ihm obliegt es, die Umsetzung dieses Prinzips von Auftragsverarbeitern, Herstellern und Dienstleistern einzufordern. In der Praxis hat dies jedoch erst wenig sichtbare Effekte gezeigt; so bleibt die gute Idee des eingebauten Datenschutzes noch deutlich hinter ihren Möglichkeiten zurück.

Exemplarisch sei noch das Transparenzgebot genannt, das auf Grund gegenwärtiger und künftiger Informations- und Kommunikationstechnologien an subjektive und objektive Grenzen stößt. Subjektiv übersteigt die zu erwartende Vervielfachung der Datenverarbeitungsvorgänge in allen Lebensbereichen die mögliche Aufmerksamkeit, die zur Effektivität der Transparenz erforderlich ist, um ein Vielfaches. Objektiv setzen hohe Komplexität, vielfältige Zwecke und lernfähige Systeme der möglichen Transparenz enge Grenzen. Um den gegenwärtigen und künftigen Herausforderungen der Informations- und Kommunikationstechnologien gerecht zu werden, sind neue, ergänzende und präzisere Datenschutzprinzipien erforderlich.

Ihr Modernisierungsziel verfehlt die Datenschutz-Grundverordnung aber auch insbesondere durch ihren spezifischen Ansatz der Technologieneutralität. Der Ansatz der Technologieneutralität ist insoweit sinnvoll, als er bewirkt, dass rechtliche Vorschriften so formuliert werden, dass sie technische Weiterentwicklungen nicht ausschließen. Die Datenschutz-Grundverordnung nutzt diesen Ansatz jedoch im Sinne einer Risikoneutralität, das heißt, in nicht einer einzigen Regelung wird auf die besonderen Grundrechtsrisiken moderner Informationstechnik wie zum Beispiel smarten Informationstechniken im Alltag, von Big Data oder Cloud Computing eingegangen. Die Vorgaben der Datenschutz-Grundverordnung gelten im gleichen Maße für die Kundenliste beim ,,Bäcker um die Ecke" wie auch für die um Potenzen risikoreicheren Datenverarbeitungen weltweit agierender Großkonzerne. Es ist gerade dieser Umstand, der erhebliche Akzeptanzprobleme der Datenschutz-Grundverordnung auf Seiten der gesamteuropäischen Bevölkerung – und damit Skepsis gegenüber Politik und Rechtsetzung der Europäischen Union insgesamt – hervorzurufen droht. Dass es im Unionsrecht durchaus möglich ist, technikneutrale als auch funktions- und risikobezogene Datenschutzregelungen vorzusehen, zeigt Art. 6 der eCall-Verordnung (EU) 2015/758, der klare Datenschutzanforderungen an die Zulässigkeit des automatisierten Notrufs stellt.

Der risikoneutrale „One Size Fits All"-Ansatz, den die Datenschutz-Grundverordnung verfolgt, macht bereichsspezifische Konkretisierungen und Ergänzungen des Datenschutzrechts unumgänglich, um auf die Herausforderungen moderner Informations- und Kommunikationstechnologien angemessen reagieren zu können. Für die Konkretisierungen und Ergänzungen kommen dabei unterschiedliche Akteure in Betracht: der Europäische Unionsgesetzgeber, der bereichs- oder technologiespezifische europäische Verordnungen oder Richtlinien erlassen kann, die Mitgliedstaaten, die im Rahmen des von der Datenschutz-Grundverordnung belassenen nationalen Gestaltungsspielraumes die Verordnung ergänzen und konkretisieren können, der europäische Datenschutzaus-

schuss, der Leitlinien und Empfehlungen veröffentlichen kann, die nationalen Aufsichtsbehörden, die alle Beteiligten durch Leitlinien insbesondere zum richtigen Umgang mit den Innovationen der Verordnung unterstützen können, sowie private Akteure (wie zum Beispiel wirtschaftliche Verbände oder Normungsorganisationen), die branchenspezifische Verhaltensregeln erarbeiten können.

Zusammenfassung und Fazit

Die Datenschutz-Grundverordnung hat die Stellung von betroffenen Personen bei der Verarbeitung personenbezogener Daten verbessert. Sie bleibt jedoch noch an vielen Stellen hinter ihren Möglichkeiten zurück. Angesichts der teilweise abstrakten Vorgaben führt sie dazu, dass ihre Vorschriften so ausgelegt werden, dass sie den Datenschutz beschränken. Durch die Abstraktheit der Normen besteht die Gefahr, dass die Normadressaten die Spielräume zum Nachteil von betroffenen Personen nutzen. Aus diesem Grund werden in diesem Policy Paper Vorschläge unterbreitet, die im Rahmen der Evaluation der Datenschutz-Grundverordnung im Jahr 2020 für eine konstruktive Weiterentwicklung der Verordnung genutzt werden können.

Bei der Erarbeitung der Vorschläge wurde der Fokus auf betroffene Personen gerichtet. Deren Stellung zu stärken und Machtasymmetrien zwischen Anbietern und betroffenen Personen abzubauen, steht im Einklang mit dem intendierten Ziel der Datenschutz-Grundverordnung, die Verarbeitung personenbezogener Daten in die Dienste der Menschheit zu stellen und die Rechte und Freiheiten der betroffenen Personen – unter Berücksichtigung der Rechte der Datenverarbeiter – zu wahren. Dabei hat die Untersuchung gezeigt, dass schon kleine Veränderungen des Wortlauts im Normtext der Datenschutz-Grundverordnung zu einer deutlichen Verbesserung des Datenschutzes und der Rechtssicherheit für die Beteiligten führen können.

Dort, wo kleine Veränderungen des Normtextes nicht möglich sind, müssen neben dem Unionsgesetzgeber vor allem die Gesetzgeber der Mitgliedstaaten, der Europäische Datenschutzausschuss, die nationalen Datenschutzaufsichtsbehörden und private Akteure tätig werden und die zum Teil unbestimmten Vorgaben der Datenschutz-Grundverordnung konkretisieren.

Auch mit der anstehenden Evaluation der Datenschutz-Grundverordnung im Jahr 2020 ist die Aufgabe der Weiterentwicklung des Datenschutzes nicht beendet. Der datenschutzrechtliche Diskurs darf mit Blick auf das hohe Transformationstempo im Bereich der Datenverarbeitung nicht stehen bleiben. Die Datenschutzprinzipien sind in der Europäischen Union in ihren Grundzügen seit den 1970er Jahren weitgehend unverändert geblieben. Die seitdem realisierten und absehbaren künftigen Innovationen der Informations- und Kommunikationstechnologien erfordern, diese zu hinterfragen und weiterzuentwickeln.

Weitere Informationen

Simitis, S., Hornung, G., Spiecker gen. Döhmann, I. (Hg.) (2019), Datenschutzrecht – DSGVO mit BDSG, Kommentar.

Roßnagel, A. (Hg.) (2018). Das neue Datenschutzrecht. Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze.

Roßnagel, A., Friedewald, M., Hansen, M. (Hg.) (2018). Die Fortentwicklung des Datenschutzes.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

PROJEKTPARTNER

Fraunhofer

Natur Technik Kultur Gesellschaft
UNIKASSEL VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

EBERHARD KARLS UNIVERSITÄT TÜBINGEN
INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein