forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

Policy Paper

NATIONALE IMPLEMENTIERUNG DER DATENSCHUTZ-GRUNDVERORDNUNG

HERAUSFORDERUNGEN – ANSÄTZE – STRATEGIEN

IMPRESSUM

Autoren:
Alexander Roßnagel, Tamer Bile, Michael Friedewald, Christian Geminn, Olga Grigorjew, Murat Karaboga, Maxi Nebel

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, Januar 2018

Problemaufriss

Mit dem Geltungsbeginn der Datenschutz-Grundverordnung am 25. Mai 2018 wird der europäische Datenschutz auf eine neue Grundlage gestellt. Mit dieser grundlegenden Reform verfolgt die Verordnung drei große Ziele: eine unionsweite Vereinheitlichung des Datenschutzrechts, eine Wettbewerbsangleichung und eine Modernisierung des Datenschutzrechts.

Der Wechsel vom Instrument der Richtlinie zum Instrument der Verordnung hat dabei weitreichende Folgen. Er macht eine umfassende Anpassung und Bereinigung des nationalen Rechts erforderlich. Mangels Geltungsvorrang verlieren zwar lange etablierte und bewährte nationale Regelungen nicht ihre Gültigkeit, dürfen aber wegen des Anwendungsvorrangs der Verordnung nicht angewendet werden, wenn sie im Widerspruch zur Verordnung stehen.

Entstehungsprozess der Datenschutz-Grundverordnung

Nahezu alle Lebens-, Wirtschafts- und Verwaltungsbereiche sind abhängig von der Verarbeitung personenbezogener Daten und jeder, der über den Vollzug des Datenschutzrechts bestimmt, hält ein zentrales Instrument zur Gestaltung der digitalen Wirtschaft und Gesellschaft in der Europäischen Union in Händen. Nachdem die Mitgliedstaaten eine ausreichende Harmonisierung des Datenschutzrechts auf Grundlage der Datenschutzrichtlinie nicht verwirklichen konnten, schlug die Europäische Kommission eine neue Lösung für die notwendige Modernisierung des Datenschutzrechts vor. Durch die Wahl einer Verordnung wollte sie die Mitgliedstaaten weitgehend von der weiteren Gesetzgebung im Bereich des Datenschutzes ausschließen und deren – zumindest in einigen Mitgliedstaaten – teils sehr ausdifferenzierte und risikoorientierte Regelungen zum Datenschutz durch wenige abstrakte und weitestgehend unbestimmte Regelungen ersetzen. Dabei behielt sie sich selbst die Kompetenz vor, mittels Durchführungsakten und delegierter Rechtsakte die Entscheidungsgewalt über notwendige und nützliche Maßnahmen des Datenschutzes zu behalten.

Diese Konzentrierung der Datenschutzgesetzgebung bei der Kommission wurde durch das Europäische Parlament und den Rat verhindert. Von den vielen Kompetenzen, die sich die Kommission selbst zuschreiben wollte, blieben am Ende des Trilogs nur zwei Ermächtigungen für delegierte Rechtsakte und sieben für Durchführungsakte. Im Gegensatz zur vom Parlament vorgeschlagenen abschließenden Ausgestaltung von im Kommissionsentwurf noch unbestimmten Regelungen im Verordnungstext konnte der Rat durchsetzen, dass ein signifikanter Teil der abstrakten Vorgaben der Verordnung durch mitgliedstaatliche Regelungen angepasst werden kann, oder die in den Mitgliedstaaten bereits bestehenden bereichsspezifischen Datenschutzregelungen beibehalten oder durch die Mitgliedstaaten neue Regelungen erlassen werden können. Letztlich hat jedoch der politische und zeitliche Druck im Trilog verhindert, dass durch weitere Beratungen ein in sich stimmiger Regelungskomplex zum Datenschutz in der Union entstehen konnte.

Defizite der Datenschutz-Grundverordnung

Da die Verordnung abstrakt gehalten ist und signifikanten Raum für mitgliedstaatliche Abweichungen lässt, gefährdet sie das selbstgesteckte Ziel einer unionsweiten Vereinheitlichung des Datenschutzrechts.

Fehlende Vereinheitlichung

Der Regelungsbedarf eines unionsweiten Datenschutzrechts ist äußerst komplex. Dies verkennt die Verordnung, wenn sie in wenigen hochabstrakten Regelungen diese Komplexität einfangen will. Die Vorschriften der Verordnung weisen einen hohen Abstraktionsgrad auf und leiden daher an Unterkomplexität. Die Verordnung will in 51 Artikeln des materiellen Datenschutzrechts die gleichen Probleme behandeln, für die in den Mitgliedstaaten zum Teil tausende bereichsspezifische Vorschriften bestehen (so z.B. in Deutschland). Datenschutz ist zu einem zentralen Querschnittsthema der Informationsgesellschaft geworden. Die automatisierte Verarbeitung personenbezogener Daten tangiert heutzutage nahezu alle Lebensbereiche. Alle Verfahrensabläufe in Verwaltung, Wirtschaft, Wissenschaft und Kultur sind durch sie geprägt. Der Versuch der Verordnung, die gewaltige Bandbreite vielfältiger datenschutzrechtlicher Regelungen in 28 Mitgliedstaaten durch nur 51 materielle Vorschriften zu ersetzen, wird dem nicht gerecht.

Eine komplette Ersetzung des nationalen Datenschutzrechts ist indes in der Verordnung nicht angelegt. Ganz im Gegenteil sind ihre abstrakten Regelungen hochgradig ausfüllungsbedürftig. Die Kommission hatte diese Ausfüllungen selbst vornehmen wollen; das Parlament wollte sie direkt im Verordnungstext verankern. Der Rat hat hier schließlich im Wesentlichen die Mitgliedstaaten in die Pflicht nehmen wollen und sich mit dieser Haltung letztlich auch durchgesetzt. Den Mitgliedstaaten bleibt deshalb ein vergleichsweise breiter Handlungsspielraum, unbestimmte Begriffe der Verordnung zu präzisieren, ausfüllungsbedürftige Vorgaben konkretisieren, unvollständige Regelungen ergänzen oder Regelungslücken schließen – freilich ohne dabei das Regelungsziel der Verordnung zu verletzen. Hierzu treten die an die Mitgliedstaaten gerichteten Regelungsaufträge und -optionen der Verordnung. Bestehende nationale Regelungen können damit durchaus anwendbar bleiben und neue Regelungen geschaffen werden.

Mängel bei der Bereinigung des nationalen Rechts können indes zu erheblicher Rechtsunsicherheit führen. Die Europäische Union hat weder die Kompetenz, mitgliedstaatliches Recht zu verändern oder außer Kraft zu setzen, noch hat Unionsrecht diesem gegenüber Geltungsvorrang. Das bedeutet, dass ohne ein Tätigwerden des nationalen Gesetzgebers die datenschutzrechtlichen Regelungen dieses Mitgliedstaats unverändert weiter gelten. Kommt es zu einem Konflikt zwischen dem mitgliedstaatlichen Recht und dem Unionsrecht, ist die Datenschutz-Grundverordnung vorrangig anzuwenden.

Fehlende Angleichung des praktizierten Datenschutzes

Aber auch dort, wo die Verordnung und nicht mitgliedstaatliches Recht anwendbar ist, führt dies nicht immer zu einheitlichen Wettbewerbsbedingungen innerhalb der Union. Die abstrakten und unbestimmten Regelungen der Verordnung müssen in der Praxis durch nationale Aufsichtsbehörden und Gerichte konkretisiert werden. Zwar hat der Europäische Datenschutzausschuss die Aufgabe, die einheitliche Anwendung der Verordnung sicherzustellen und entsprechende Leitlinien, Empfehlungen und Stellungnahmen zu veröffentlichen. Diese binden aber nur die Aufsichtsbehörden und setzen kein allgemeinverbindliches Exekutivrecht. Die Interpretation der Verordnung durch die Aufsichtsbehörden kann durchaus zu unterschiedlichen Ergebnissen gelangen; die Überprüfung der Auslegung obliegt weiterhin den örtlichen Gerichten. Diese können jeden vereinheitlichenden Versuch einer Auslegung verhindern, so dass eine einheitli-

che Rechtsprechung allenfalls in Einzelfragen und nur nach jahrelangen Prozessen durch den Europäischen Gerichtshof erwartet werden kann.

Von einer Vereinheitlichung des Datenschutzrechts in der Union und Rechtssicherheit kann ferner nicht gesprochen werden, da insbesondere die Konkretisierung der Abwägung berechtigter Interessen der für die Datenverarbeitung Verantwortlichen mit den schutzwürdigen Interessen der betroffenen Person nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO in dem jeweiligen Mitgliedstaat nach der bisher gelebten Datenschutzkultur erfolgen wird. Dadurch wird dies in der Praxis zu unterschiedlichen mitgliedstaatlichen Ergebnissen führen. In der Folge werden im Rahmen der Interessenabwägung zum Beispiel für die Videoüberwachung unterschiedliche Konkretisierungen in den Mitgliedstaaten vorgenommen, je nachdem wie in der bisherigen Praxis damit umgegangen wurde. Darüber hinaus wird man sich für die Interessenabwägung zum Beispiel im Kontext von Werbung, Marktforschung und Auskunfteien an den jeweiligen hergebrachten nationalen Regelungen ausrichten. Die Zulässigkeit der Datenverarbeitung wird in jedem Mitgliedstaat einen anderen Inhalt aufweisen, was dazu führt, dass kein unionsweit einheitliches Datenschutzrecht entstehen kann. Einheitliche wettbewerbsrechtliche Bedingungen im Binnenmarkt sind damit nicht zu erreichen.

Das Problem wird auch dadurch verstärkt, dass die Verordnung die Entscheidung über die Abwägung der betroffenen Interessen auf die Gerichte überträgt. Dadurch werden die Ergebnisse noch mehr voneinander abweichen als unter der Datenschutzrichtlinie. Es wird letztlich möglich sein, dass selbst innerhalb eines Staates wie zum Beispiel in Deutschland, in dem die Typisierung der Interessenabwägung durch den Gesetzgeber erfolgte und einheitlich war, Entscheidungen über Interessenabwägungen von Gerichtsbezirk zu Gerichtsbezirk unterschiedlich ausfallen können, was eine erhebliche Rechtsunsicherheit nach sich zieht. Die obersten Gerichte können zwar für Rechtsklarheit sorgen, wie einzelne Interessenabwägungen vorzunehmen sind. Allerdings können solche Entscheidungen erfahrungsgemäß sehr lange dauern.

Fehlende Modernisierung

Auch ihr drittes Ziel – den Datenschutz zu modernisieren und diesen für die Herausforderungen der Zukunft fit zu machen – erreicht die Verordnung an vielen Stellen nicht. Dafür gibt es vor allem zwei Gründe: Die Verordnung führt – von wenigen Ausnahmen abgesehen – die Konzeption der Datenschutzrichtlinie weiter und knüpft damit an Lösungen an, die bereits vor über 20 Jahren im Europarecht verankert wurden und schon damals teils als überholt oder unzureichend galten. Damit wird die Verordnung den künftigen Herausforderungen technisch-ökonomischer Entwicklungen nicht gerecht. Das Festhalten an überholten und unzureichenden Lösungen wirkt jedoch besonders schwer, da die Mitgliedstaaten von diesen grundlegenden Richtungsentscheidungen der Verordnung nicht abweichen dürfen.

Inhaltlich verfehlt die Verordnung ihr Modernisierungsziel, weil sie auf einen spezifischen Ansatz von Technikneutralität abstellt. Richtig verstandene Technikneutralität soll verhindern, dass rechtliche Vorschriften aufgrund ihrer Formulierung technische Weiterentwicklungen ausschließen oder umgekehrt nicht mehr anwendbar sind. Daher vermeidet sie spezifische technische Gestaltungsmerkmale und beschränkt sich auf die Regulierung technischer Funktionen, die nicht an bestimmte technische Ausgestaltungen gekoppelt sind. Die Verordnung bedient sich jedoch eines spezifischen Verständnisses von Technikneutralität und regelt überhaupt keine technischen Risiken. Damit bewirkt sie eine Risikoneutralität ihrer Regelungen zur Zulässigkeit, zu Rechten der betroffenen Person und zu Schutzvorkehrungen. In keiner ihrer Regelungen geht die Verordnung die spezifischen grundrechtlichen Risiken moderner Informationstechnik an oder löst sie. Solche Risiken resultieren zum Beispiel spezifisch aus der allgegenwärtigen Datenverarbeitung, dem Internet der Dinge, Big Data, Cloud-Computing oder datenzentrierten Geschäftsmodellen, Automatisierung, Künstlicher Intelligenz und selbstler-

nenden Systemen. Die Verordnung unterscheidet auch nicht zwischen den Formen der Datenverarbeitung. Die Zulässigkeitsregeln, Zweckbegrenzungen oder Betroffenenrechte gelten für alle Datenverarbeiter gleichermaßen, sei es der „Bäcker um die Ecke" mit seiner „kleinen" Kundenliste oder große Konzerne wie Google oder Facebook, die mit risikoreichen Techniksystemen massenhaft personenbezogene Daten verarbeiten. Durch solche Regelungen wird man den spezifischen grundrechtlichen Risiken nicht wirksam begegnen können. Dass dies im Unionsrecht aber durchaus möglich ist, zeigen Art. 6 der eCall-Verordnung (EU) 2015/758 oder Art. 8, 10 und 16 des Entwurfs der ePrivacy-Verordnung der Kommission.

Ko-Regulierung, Regelungsauftrage und Regelungsoptionen

Letztlich etabliert die Verordnung – entgegen den ursprünglichen Erwartungen – eine Ko-Regulierung zwischen der Europäischen Union und den Mitgliedstaaten, indem sie Zielsetzungen und Grundsätze, grundlegende Rechte und Pflichten und fundamentale Strukturen der Durchsetzung von Datenschutzrecht in der Union einheitlich regeln will, die Präzisierung und Ausfüllung der Regelungen aber vielfach den Mitgliedstaaten überlässt. Dazu hält die Verordnung durch zahlreiche Öffnungsklauseln Regelungskompetenzen für die Mitgliedstaaten bereit. Zu unterscheiden ist dabei zwischen Regelungsaufträgen und Regelungsoptionen. Letztere sind es, bei denen sich die genannten Gefahren, aber auch wesentliche Chancen ergeben.

Regelungsaufträge sind Öffnungsklauseln, die die Mitgliedstaaten verpflichten, bestimmte Regelungen zu erlassen. Dazu zählen etwa Art. 51 ff. DSGVO zur Errichtung einer Aufsichtsbehörde, Art. 84 DSGVO zur Festlegung weiterer Sanktionen sowie Art. 85 DSGVO zur Sicherung der Meinungsäußerung und Informationsfreiheit bei der Verarbeitung personenbezogener Daten.

Regelungsoptionen sind hingegen Öffnungsklauseln, die den Mitgliedstaaten die Möglichkeit eröffnen, eigene Regelungen zu schaffen oder bereits bestehende Regelungen beizubehalten, sofern diese der Verordnung nicht widersprechen. Hierzu zählen etwa Art. 6 Abs. 2 und 3 DSGVO. Nach Art. 9 Abs. 2 lit. a, b, g, h, i, j DSGVO können die Mitgliedstaaten für bestimmte besondere Kategorien personenbezogener Daten Regelungen erlassen oder aufrechterhalten; nach Abs. 4 gilt dies ausdrücklich auch für genetische, biometrische oder Gesundheitsdaten. Art. 23 DSGVO ermöglicht die Beschränkung der Rechte der betroffenen Person im dort genannten Umfang und zu den dort genannten Zwecken. Art. 37 Abs. 4 DSGVO erlaubt den Mitgliedstaaten, eine Pflicht zur Benennung eines Datenschutzbeauftragten vorzusehen. Art. 80 Abs. 2 DSGVO ermöglicht die Etablierung eine Popularklage für Einrichtungen, Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht. Zudem sieht die Verordnung Regelungsoptionen für Mitgliedstaaten für besondere Verarbeitungssituationen vor, zum Beispiel nach Art. 88 DSGVO für Datenverarbeitung im Beschäftigungskontext oder nach Art. 89 DSGVO für im öffentlichen Interesse liegende Datenverarbeitungen zu Archiv-, Forschungs- und statistischen Zwecken.

Insbesondere die Regelungsoptionen bergen die Gefahr der Rechtsunsicherheit, da sie zu einer schwer zu durchschauenden Gemengelage führen können, in der Rechtsanwender und betroffene Personen nur schwer erkennen können, welche Regelungen konkret für sie relevant sind. Zudem stehen sie einer Harmonisierung der Rechtslage in den Mitgliedstaaten im Wege. Gerade die Regelungsoptionen sind aber auch geeignet, nicht nur nationale Besonderheiten im Datenschutz zu berücksichtigen, sondern zudem erst eine risikoadäquate Rechtslage abzubilden. Nur so ist die notwendige Komplexität der Datenschutzregelungen angesichts einer gesellschaftsweiten Verarbeitung personenbezogener Daten zu erreichen. Die Reichweite der Regelungen kann im Einzelnen unklar sein, insbesondere aufgrund ihrer abstrakten, oberflächlichen Vorgaben. Hier

müssen sich die Mitgliedstaaten nun erst einmal vorwagen und mit eigenen Regelungen experimentieren.

Ko-Regulierung, Regelungsauftrage und Regelungsoptionen

Eine Verordnung, die die schwierigen Fragen des Datenschutzrechts abschließend regelt oder eine Richtlinie, die eine klarere Aufgabenteilung zwischen Union und Mitgliedstaaten bewirkt, wären der aktuellen Situation vorzuziehen gewesen. Doch dadurch, dass eine Monopolisierung und Zentralisierung in der Weiterentwicklung des Datenschutzrechts verhindert werden konnten, bietet die gegenwärtige Situation immerhin die Chance, dass Möglichkeiten einer sinnvollen Arbeitsteilung zwischen Union und Mitgliedstaaten erprobt werden können. Angesichts der Vielfalt und Dynamik der zukünftigen, heute noch unbekannten Herausforderungen der Informationstechnik und ihrer Anwendungen für die Grundrechte ermöglicht die beschlossene Verordnung an vielen Stellen, dass mit unterschiedlichen Regelungskonzepten experimentiert werden kann. Dadurch können vielfältige Quellen dazu beitragen, dass sich in der Union ein lebendiger Datenschutz entwickelt. Statt einer Vereinheitlichung der Datenschutzpraxis ermöglichen unbestimmte Rechtsbegriffe und ihre situationsgerechte Konkretisierung, dass in den einzelnen Mitgliedstaaten Datenschutz den lokalen Bedingungen angepasst werden kann. Schließlich bieten die vielen Regelungsmöglichkeiten den Mitgliedstaaten Chancen für eine Modernisierung des Datenschutzrechts, indem dort versucht wird, durch risikoadäquate Regelungen einen ausreichenden Schutz der Grundrechte gegen künftige Herausforderungen zu gewährleisten.

Bezogen auf die hier aufgeführten Regelungsoptionen ist es Aufgabe der Mitgliedstaaten, Rechtssicherheit und Sachgerechtigkeit, Vollzugsfähigkeit und Effektivität des Datenschutzes sicherzustellen. Für die Wahrnehmung der Aufgabe gibt es drei denkbare Konzepte:

- Die Minimallösung erfüllt die Regelungsaufträge, behält geltende nationale Regelungen in begrenztem Maße bei und erhält das bestehende Datenschutzniveau im Mitgliedstaat.
- Die Maximallösung erfüllt die Regelungsaufträge und nutzt aber sowohl die Regelungsoptionen als auch die impliziten Regelungsmöglichkeiten, um mehr Rechtsklarheit, Risikoorientierung und Aufwandsreduktion zu erreichen.
- Die vielleicht optimale Lösung versucht angesichts des Zeitdrucks, die Regelungsaufträge zu erfüllen und die Regelungen zu treffen, die einerseits die Vollzugsfähigkeit wichtiger Vorgaben der Verordnung sicherstellen und Mängel beseitigen, andererseits aber wenig umstritten sind. Regelungen mit einem höheren Beratungsbedarf werden zunächst zurückgestellt. Im Zweifel werden ab Mai 2018 die bestehenden Regelungen fortgeführt.

Neben diesen Umsetzungsmöglichkeiten der Datenschutz-Grundverordnung zugunsten eines kohärenten und starken Datenschutzrechts besteht allerdings auch die Gefahr, dass die Mitgliedstaaten ihre Regelungsspielräume ausnutzen, um das Datenschutzniveau abzusenken.

Umsetzung der Datenschutz-Grundverordnung

Um die Rechtssicherheit, Vollziehbarkeit und Effektivität der Verordnung zu gewährleisten, sind neben den Regelungen der Verordnung auch mitgliedstaatliche Regelungen erforderlich. Die Verordnung sieht hierfür viele implizite und explizite Regelungsspielräume für die mitgliedstaatlichen Gesetzgeber vor. Diese können die Mitgliedstaaten auf unterschiedliche Weise nutzen.

Weitere Anwendbarkeit mitgliedstaatlicher Regelungen

Die Mitgliedstaaten können erstens abstrakte Vorgaben der Verordnung präzisieren und damit Handlungs- und Bewertungsmaßstäbe bieten, die in der Verordnung fehlen. Solche präzisierenden Regelungen sind zulässig, soweit sie nicht im Widerspruch zur Verordnung stehen. Ein Widerspruch liegt nur vor, wenn eine nationale Regelung das Regelungsziel der Verordnung verletzt. Soweit sie nur einen unbestimmten Rechtsbegriff präzisiert, dessen Präzisierung nicht einem bestimmten Akteur vorbehalten ist, ist sie zur Unterstützung der Verordnung anwendbar, auch wenn ihr Wortlaut sich von dem der Verordnung unterscheidet.

Zweitens können die Mitgliedstaaten die Vorgaben der Verordnung konkretisieren, die eine lückenhafte Regelung der Verordnung erst vollzugsfähig machen. Das ist oft dann der Fall, wenn ursprünglich eine Konkretisierung der Verordnung durch delegierte Rechtsakte oder Durchführungsrechtsakte der Kommission vorgesehen war, diese aber ersatzlos entfallen ist. Dann ermöglicht erst die Ausfüllung lückenhafter Vorgaben, die Ergänzung unvollständiger Regelungen oder die Schließung von Regelungslücken den Vollzug der Verordnung durch die nationalen Behörden oder Gerichte. Gleiches gilt, wenn die nationale Regelung den für die Umsetzung notwendigen Rechtsrahmen schafft oder die Vorschrift der Verordnung an die Systematik und den Sprachgebrauch anpasst.

Die Mitgliedstaaten können drittens jede der 70 Öffnungsklauseln der Verordnung ausfüllen, die den Mitgliedstaaten einen Spielraum einräumen, eigene Regelungen unionsrechtskonform anzuwenden oder neue zu erlassen. Solche Öffnungsklauseln für ganze Bereiche enthalten die Rahmensetzungen für besondere Verarbeitungssituationen in Art. 85 bis 91 DSGVO. Vielfach bestehen Öffnungsklauseln, um Regelungen der Verordnung an spezifische Umstände in den Mitgliedstaaten anzupassen – etwa in Art. 9 DSGVO für die Verarbeitung besonderer Kategorien personenbezogener Daten oder in Art. 23 DSGVO zur spezifischen Beschränkung von Rechten der betroffenen Person. Ein weiteres bedeutsames Beispiel ist Art. 6 Abs. 2 DSGVO.

Beispiele für die Umsetzung der Verordnung

Bisher haben nur Deutschland und Österreich Gesetze zur Umsetzung der Verordnung und Anpassung des nationalen Datenschutzrechts verabschiedet. Deutschland hat sein Bundesdatenschutzgesetz (BDSG) im Mai 2017 an die Verordnung angepasst. Österreich hat im Juli 2017 das neue Datenschutzgesetz (DSG) verkündet. Beide treten am 25. Mai 2018 in Kraft. Nachfolgend soll an ausgewählten Beispielen aufgezeigt werden, wie der deutsche und der österreichische Gesetzgeber mit ihren Gestaltungsspielräumen umgegangen sind.

Es sei dabei angemerkt, dass Österreich als einziger Mitgliedstaat im April 2016 im Rat gegen die Annahme der Datenschutz-Grundverordnung votierte. Als Grund wurden ungelöste Probleme genannt, verbunden mit der Erwartung, dass diese Probleme aufgrund der Wahl einer Verordnung nicht durch die Mitgliedstaaten angegangen werden könnten.

Ergänzung der Verordnung

Der deutsche Gesetzgeber ist den expliziten Regelungsaufträgen der Verordnung nachgekommen: Ein wichtiges Beispiel sind ergänzende Regelungen für einen einheitlichen Vollzug der Verordnung in der Union bezüglich der Zusammenarbeit der Aufsichtsbehörden, hinsichtlich des Kohärenzverfahrens und der Vertretung im Europäischen Datenschutzausschuss. Diese Regelungen sind erforderlich, weil die Verordnung viele Aufgaben zur Durchführung der Regelungen und die Aufgabe, ihre Anwendung zu vereinheitlichen, den Aufsichtsbehörden übertragen hat. Der deutsche Gesetzgeber hat diesen expliziten Regelungsauftrag erfüllt, indem er die Vertretung Deutschlands im Datenschutzausschuss und die Willensbildung unter den Aufsichtsbehörden im föderalen System in den §§ 17 bis 19 BDSG geregelt hat. Unverständlich ist hierbei jedoch, warum die Bundesbeauftragte, die von allen Aufsichtsbehörden am wenigsten von den im Ausschuss verhandelten Themen betroffen ist, die Vertreterin Deutschlands sein soll, und warum die Übertragung der Verhandlungsführung und des Stimmrechts auf einen Ländervertreter nur zu Themen erfolgen darf, in denen die Länder „alleine das Recht zur Gesetzgebung haben", wo es doch auf die Vollzugskompetenz ankommt.

Für den österreichischen Gesetzgeber sind ergänzende nationale Vorschriften, die die Zusammenarbeit der Aufsichtsbehörden regeln, nicht erforderlich, da die Einhaltung des Datenschutzes in Österreich nur durch eine Datenschutzbehörde (vormals Datenschutzkommission) gewährleistet wird.

Weiter erfordert die Verordnung implizit zusätzliche Regelungen, um ihre Ziele zu erreichen. Viele wurden im neuen BDSG jedoch nicht aufgegriffen: So fehlen etwa Regelungen, die festlegen, wann eine Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 7 DSGVO für Verarbeitungen nach Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO zu erfolgen hat. Auch sollte eine Regelung festlegen, wann Datenschutz-Folgenabschätzungen zu wiederholen sind. Zu den Vorgaben für Verhaltensregeln in Art. 40 DSGVO sind ergänzende Regelungen zum Verfahren der Erarbeitung notwendig, die ein Mindestmaß an Fairness und Interessensberücksichtigung gewährleisten, sowie Regelungen zur Beteiligung von maßgeblichen Interessenträgern, zur Verbindlichkeit der genehmigten Verhaltensregeln und zur zeitlichen Begrenzung der Genehmigung. Für die Zertifizierung von „Verarbeitungsvorgängen" nach Art. 42 DSGVO sind z.B. Regelungen zu dem „transparenten Verfahren" gemäß Abs. 3 und zu den erforderlichen Informationen gemäß Abs. 6 notwendig. Auch für die Zusammenarbeit mit Aufsichtsbehörden anderer Mitgliedstaaten nach Art. 60 DSGVO, für die gegenseitige Amtshilfe nach Art. 61 DSGVO und für die gemeinsamen Maßnahmen nach Art. 62 DSGVO bedarf es ergänzender Regelungen.

Solche impliziten, jedoch nicht verpflichtenden Ergänzungen, die das Datenschutzniveau weiter anheben würden, hat jedoch weder der deutsche noch der österreichische Gesetzgeber vorgenommen.

Präzisierung der Verordnung

Präzisierungen hat der deutsche Gesetzgeber im BDSG etwa in § 1 für den Anwendungsbereich des Art. 2 DSGVO, in § 2 für öffentliche und nichtöffentliche Stellen als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO, in § 19 für die „federführende Aufsichtsbehörde" aus Art. 60 DSGVO vorgenommen sowie in § 22 Abs. 2 für „geeignete Garantien" oder „angemessene und spezifische Maßnahmen" im Sinne des Art. 9 Abs. 2 lit. b, g und h DSGVO.

Auch der österreichische Gesetzgeber hat etwa in § 26 DSG den Begriff des Verantwortlichen nach Art. 4 Nr. 7 DSGVO präzisiert. Im Gegensatz zum deutschen Anpassungsgesetz enthält das österreichische Anpassungsgesetz jedoch keine Präzisierungen für die in Art. 9 Abs. 2 lit. b, g und h DSGVO normierten unbestimmten Begriffe „geeignete Garantien" oder „angemessene und spezifische Maßnahmen".

Vergleichbare Präzisierungen wären aber auch im Hinblick auf die Betroffenenrechte, wie etwa für „geeignete Maßnahmen" zur Unterrichtung der betroffenen Person nach Art. 12 Abs. 1 Satz 1 DSGVO, oder die Pflichten der Verantwortlichen und Auftragsverarbeiter, wie beispielsweise für „geeignete technische und organisatorische Maßnahmen" nach Art. 24 Abs. 1 DSGVO, notwendig, die jedoch weder der deutsche noch der österreichische Gesetzgeber geregelt haben.

Für die Verhaltensregeln und die Zertifizierung sollte etwa konkretisiert werden, wie diese zu fördern und wie die Interessen der kleinen Unternehmen zu berücksichtigen sind. Gleiches gilt auch für die Pflichten des Auftragsverarbeiters, um für dessen Tätigkeit die Rechtssicherheit zu erhöhen.

Präzisierungen sind auch notwendig hinsichtlich der unbestimmten Rechtsbegriffe in Art. 32 DSGVO. So ist derzeit ungeklärt, was „Belastbarkeit der Systeme" in Art. 32 Abs. 1 lit. b DSGVO umfasst. Art. 32 Abs. 1 DSGVO nennt beispielhaft Anforderungen an die Datensicherheit. Diese Aufzählung ist nicht abschließend; den Mitgliedstaaten bleibt es daher unbenommen, weitere Anforderungen zur Datensicherheit zu normieren, so lange diese der Verordnung nicht widersprechen.

Der Rechtssicherheit wäre es zudem zuträglich, wenn abstrakte Vorgaben wie in Art. 36 Abs. 1 DSGVO präzisiert würden, wonach der Verantwortliche verpflichtet ist, die Aufsichtsbehörde zu konsultieren, wenn „die Verarbeitung ein hohes Risiko zur Folge hätte" und „der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft". Hilfreich wäre, die Kriterien für ein „hohes Risiko" gesetzlich zu normieren, um dem Verantwortlichen eine gewisse Sicherheit bei der Einschätzung der Situation zu verschaffen. Das neue Bundesdatenschutzgesetz sieht hierfür keine Regelungen vor.

Als letztes Beispiel seien die Aufgaben der Aufsichtsbehörden in Art. 57 DSGVO und ihre Befugnisse in Art. 58 DSGVO angeführt. Die Verordnung hält ein breites Bündel an Aufgaben und Befugnissen für Aufsichtsbehörden bereit. Den Mitgliedstaaten bleibt nur wenig Möglichkeit der Anpassung, jedoch bedürfen viele Regelungen einer Konkretisierung, Präzisierung oder Ergänzung. Der deutsche Gesetzgeber hat dies nur vereinzelt vorgenommen, insbesondere hinsichtlich der föderalen Zuständigkeitsverteilung oder zur Akkreditierung.

Der österreichische Gesetzgeber war in diesem Kontext zurückhaltender und hat in einem weitaus geringeren Umfang die Aufgaben und Befugnisse der Aufsichtsbehörde in § 21 f. DSG präzisiert.

Nutzung von Öffnungsklauseln

Der deutsche Gesetzgeber hat die Möglichkeiten, die ihm die vielen Öffnungsklauseln der Verordnung bieten, nur einseitig genutzt. Die Neuregelungen passen vielfach nicht nur das mitgliedstaatliche Recht an die DSGVO an, sondern setzen eigene Akzente, indem sie die Vorgaben der Verordnung und des bisherigen Bundesdatenschutzgesetzes korrigieren. Sie sind dadurch gekennzeichnet, dass sie den bestehenden Interessenausgleich zu Gunsten der Datenverarbeiter und zu Lasten der betroffenen Personen verschieben. Dies gilt insbesondere für die Einschränkungen der Rechte der betroffenen Person gemäß Art. 23 DSGVO in §§ 32 bis 37 BDSG.

So wird in § 32 BDSG etwa die Informationspflicht bei der Erhebung von personenbezogenen Daten bei der betroffenen Person eingeschränkt, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung zu anderen Zwecken im Fall einer öffentlichen Stelle die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Art. 23 Abs. 1 lit. a bis e DSGVO gefährden würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen. Gleiches gilt für die Informationspflicht nach § 33 BDSG, wenn die personenbezogenen Daten nicht bei der be-

troffenen Person erhoben wurden sowie für das Auskunftsrecht der betroffenen Person in § 34 BDSG.

Das Recht auf Löschung nach Art. 17 DSGVO hat der deutsche Gesetzgeber in § 35 BDSG zu Lasten der betroffenen Person dahingehend eingeschränkt, dass dieses Betroffenenrecht z.B. dann entfällt, wenn eine Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und das Interesse der betroffenen Person als gering anzusehen ist. Das in Art. 21 DSGVO normierte Widerspruchsrecht wurde in § 36 BDSG dahingehend eingeschränkt, dass der Widerspruch gegenüber einer öffentlichen Stelle entfällt, soweit an der Datenverarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Personen überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet. Schließlich wurde auch das in Art. 22 DSGVO geregelte Betroffenenrecht eingeschränkt, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden. Dieses Betroffenenrecht besteht gemäß § 37 BDSG nicht, wenn die Entscheidung im Rahmen eines Versicherungsvertrags ergeht und dem Begehren der betroffenen Person stattgegeben wurde.

Im Bereich des Beschäftigtendatenschutzes hat der deutsche Gesetzgeber von der Öffnungsklausel des Art. 88 DSGVO Gebrauch gemacht und die Regelungen des alten Bundesdatenschutzgesetzes mit nur kleinen Änderungen und Ergänzungen übernommen. Das ist grundsätzlich begrüßenswert, da diese ein verhältnismäßig hohes Datenschutzniveau aufweisen. Auch der österreichische Gesetzgeber hat die Öffnungsklausel des Art. 88 DSGVO genutzt, indem er in § 11 DSG für Verarbeitungen personenbezogener Daten im Beschäftigungskontext auf seine bisherigen Regelungen im Arbeitsverfassungsgesetz verweist.

Der österreichische Gesetzgeber hat im Gegensatz zum deutschen Gesetzgeber Gebrauch von der Öffnungsklausel in Art. 8 Abs. 1 Satz 2 DSGVO gemacht. Nach § 4 Abs. 4 DSG kann ein Kind, abweichend von der in der Verordnung festgelegten Altersgrenze von 16 Jahren, nun wirksam einwilligen, wenn das Kind das vierzehnte Lebensjahr vollendet hat.

Weiter hat der österreichische Gesetzgeber etwa Gebrauch von der Öffnungsklausel in Art. 85 Abs. 2 DSGVO gemacht, die es den Mitgliedstaaten erlaubt, den Schutz personenbezogener Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.

Am Beispiel der Ermächtigung zur Videoüberwachung wird deutlich, welche Fehler die Mitgliedstaaten vermeiden sollten, um zu verhindern, dass der EuGH ihre neu erlassenen Regelungen als unionsrechtswidrig erklärt. Deutschland – wie etwa auch Österreich – haben umfangreiche Regelungen beibehalten bzw. erlassen, unter welchen Voraussetzungen Videoüberwachung rechtlich zulässig sein soll. Der nationale Gesetzgeber ist damit jedoch über das Ziel hinausgeschossen. Die Verordnung legt in Art. 6 Abs. 1 UAbs. 1 lit. a bis f DSGVO abschließend fest, unter welchen Voraussetzungen Datenverarbeitung zulässig ist. Nur für den öffentlichen Bereich dürfen die Mitgliedstaaten nach Art. 6 Abs. 2 DSGVO spezifischere Bestimmungen erlassen. Sowohl Deutschland als auch Österreich haben jedoch – ohne eine entsprechende Ermächtigung durch die Verordnung – umfangreiche Regelungen zur Videoüberwachung etwa zur Wahrnehmung des Hausrechts erlassen oder zur Wahrnehmung berechtigter oder anderer Interessen privater Verantwortlicher. Für die Zulässigkeit der privaten Datenverarbeitung haben die Mitgliedstaaten jedoch keine Gesetzgebungskompetenzen. Außerdem sind diese Vorschriften unionsrechtswidrig, soweit sie neben den konkreten Vorgaben der Verordnung grundlegende Rechtsgrundsätze des Europarechts (z.B. Anwendungsvorrang und Normwiederholungsverbot) außer Acht lassen. Zukünftige Gesetzesentwürfe anderer Mitgliedstaaten sollten hier sehr viel genauer auf die Vorgaben der Verordnung achten.

Umsetzung der Datenschutz-Grundverordnung

Um den Herausforderungen moderner Datenverarbeitung auch zukünftig gerecht zu werden, sollten die Mitgliedstaaten die verschiedentlichen Öffnungsklauseln etwa im Bereich des Beschäftigtendatenschutzes und des öffentlichen Bereichs verstärkt dazu nutzen, um mit Hilfe risikoadäquater Regelungen Voraussetzungen für eine zulässige Datenverarbeitung aufzustellen. Dazu gehören zum Beispiel Anforderungen an die Gestaltung der informationstechnischen Systeme in dem spezifischen Bereich, um eine transparente, datensparsame Datenverarbeitung zu ermöglichen, der insbesondere die Bildung von Profilen und die unnötige Lokalisierung von Beschäftigten vermeidet sowie möglichst ausschließlich anonymisierte oder pseudonymisierte Daten verarbeitet. Zudem bedarf es Vorgaben zur ausnahmsweise zulässigen Deanonymisierung anonymisierter Daten, zu Zweckbestimmung und Zweckbindung und eventueller Auftragsdatenverarbeitung. Da auch von der Verarbeitung anonymer Daten Gefahren für die informationelle Selbstbestimmung ausgehen können, sollten auch anonyme Daten bestimmten Verarbeitungsgrundsätzen unterliegen. Weiterhin sollten Anforderungen zur Datensicherheit sowie Maßnahmen des Selbstdatenschutzes der betroffenen Personen konkretisiert werden. Für eine zulässige Datenverarbeitung essentiell sind weiterhin spezifische Vorgaben zu einer wirksamen Einwilligung einerseits und Anforderungen an Interessenabwägungen von betroffener Person und Verantwortlichen andererseits. Schließlich sind konkrete Vorgaben notwendig, ob und unter welchen Voraussetzungen Profiling zulässig sein soll und unter welchen Voraussetzungen besondere Kategorien personenbezogener Daten verarbeitet werden dürfen. Im Hinblick auf die Rechte der betroffenen Personen sind weiterhin Anforderungen zu Speicherzeiträumen und Löschpflichten des Verantwortlichen zu formulieren. Auch hinsichtlich anonymer Daten sollten Vorsorgepflichten des Verantwortlichen formuliert werden, falls diese personenbeziehbar werden.

Schlussfolgerungen

Die Verordnung verfehlt selbstgesteckte Ziele und trägt nicht zu einem systematischen, umfassenden und einheitlichen Neubeginn des Datenschutzrechts in allen Mitgliedstaaten der Union bei. Vielmehr führt sie künftig zu einer Gemengelage an Unions- und nationalen Vorschriften. Dies verursacht viele schwierige Rechtsfragen, wie diese Rechtsbereiche zusammenwirken und welches Recht künftig anwendbar sein wird. Angesichts dieser offenen Fragen entsteht eine hohe Rechtsunsicherheit für Verantwortliche und betroffene Personen.

Einen relevanten Beitrag zur Erhöhung der Rechtssicherheit können die Empfehlungen der Artikel-29-Gruppe und Leitlinien des Europäischen Datenschutzausschusses leisten, um bei entscheidenden Rechtsfragen eine einheitliche Interpretation der unionsrechtlichen Vorgaben zu erreichen. Die Rechtssicherheit könnte auf Unionsebene zudem erhöht werden, indem der EuGH häufiger über Einzelfragen hinaus auch zu grundsätzlichen Problemen Stellung beziehen würde.

Die Mitgliedstaaten können der Rechtsunsicherheit begegnen, indem sie an vielen Stellen ihr allgemeines und besonderes Datenschutzrecht an die Verordnung anpassen oder entsprechend stärken und weiterentwickeln. Im Gegenteil senken die künftigen Regelungen zur Umsetzung der Verordnung das Niveau des Datenschutzes jedoch gegenüber dem geltenden Bundesdatenschutzgesetz, teils sogar unter das Niveau der Datenschutz-Grundverordnung. Auch der österreichische Gesetzgeber hat die Chance zur Modernisierung des Datenschutzrechts nicht ergriffen und viele Regelungsspielräume ungenutzt gelassen.

Eine gründliche Überarbeitung der Datenschutz-Grundverordnung und damit des Fundaments des europäischen Datenschutzes ist auf längere Zeit nicht zu erwarten. Die Europäische Union kann allerdings bereichs- und technikspezifischen Datenschutz regeln. Ein gutes Beispiel ist Art. 6 der eCall-VO (EU) 2015/758. Auch im Entwurf einer ePrivacy-VO ist die Kommission von der Technikneutralität der Verordnung abgewichen und wendet die allgemeinen Regeln der Verordnung gerade nicht an, sondern sieht risikospezifische Regelungen für die besonderen Techniken der elektronischen Kommunikation vor. Sollte die Kommission weitere bereichsspezifische Regelungen angehen, wäre dies sehr zu begrüßen.

Die Union wird moderne, risikobezogene Regelungen indes nur erlassen, wenn die relevanten Stakeholder ausreichend Druck entfalten. Hierzu wären vorbildhafte Regelungen der Mitgliedstaaten, die insbesondere der Ergänzung und Präzisierung der abstrakten und ausfüllungsbedürftigen Vorgaben der Verordnung dienen, ein geeignetes Mittel. Die Mitgliedstaaten sollten Gebrauch von den mehr als 70 Öffnungsklauseln machen, die ihnen die Verordnung lässt. In diesem Zusammenhang hatte die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in Deutschland zu Recht gefordert, dass die Mitgliedstaaten die Öffnungsklauseln zu einer Modernisierung des Datenschutzrechts nutzen müssen. Nichtsdestotrotz sollte aber gerade auch der Europäische Datenschutzausschuss von seinen weitreichenden Kompetenzen Gebrauch machen, um zur Angleichung und Anhebung des Datenschutzniveaus beizutragen, indem er eine unionsweite Einigung insbesondere bei schwierigen Fragen zeitnah herbeiführt und durch gewissenhafte Entscheidungen den Mitgliedstaaten wie auch den Anwendern Lösungen für einen modernen und einheitlichen Datenschutz bietet.

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