Perspektiven des Datenschutzes nach der Datenschutz-Grundverordnung

Bis vor wenigen Jahren pflegten nicht nur die Politik, sondern auch deutsche Gerichte das Bild, wonach das Datenschutz-Niveau hierzulande vorbildhaft sei und deutlich mehr Schutz biete als die europäischen Gemeinschaftsstandards. Dieses Bild ist mittlerweile überholt, wie nicht zuletzt die beiden Entscheidungen des Bundesverfassungsgerichts und des Gerichtshofs der Europäischen Union zur Vorratsdatenspeicherung zeigen: was in Deutschland noch als verfassungskonform galt, stufte das europäische Gericht als Verstoß gegen die Grundrechte-Charta und weitgehend unzulässig ein. Die Maßstäbe haben sich verschoben, grundrechtliche Schutzstandards (wie etwas das „Recht auf Vergessenwerden") werden in zunehmendem Maß auf europäischer Ebene definiert und durchgesetzt. Umso größer waren und sind die Erwartungen an die neue Datenschutz-Grundverordnung (DSGVO) der EU, die am 25. Mai 2018 auch in Deutschland anwendbar wird. Was beinhaltet das neue europäische Datenschutzrecht? Welche Zugewinne, aber auch welche Verluste für den Schutz der informationellen Selbstbestimmung gilt es zu verzeichnen? Und was ändert sich konkret für Bürger, Verbraucher und private Anbieter? Mit diesen Fragen befasst sich die neue Ausgabe der vorgänge in ihrem Schwerpunkt.

Der erste Beitrag des Themenschwerpunkts stammt von *Thilo Weichert*. Er stellt die Grundzüge der neuen Verordnung vor: ihre Ziele, ihre grundlegenden Prinzipien und Regelungsinhalte sowie ihren Anwendungs- und Geltungsbereich. Die Gewinne der Verordnung sieht er vor allem in einer stärkeren Systematik des Datenschutzrechts (die freilich durch zahlreiche nationale Öffnungsklauseln wieder verschenkt wird), in einigen neuen Betroffenenrechten (z. B. Breach Notification und Übertragbarkeit), in verbesserten Möglichkeiten ihrer Durchsetzung sowie in schärferen Sanktionsmöglichkeiten für die Aufsichtsbehörden.

Eine grundlegende Einordnung des neuen Datenschutzrechts nimmt *Alexander Roßnagel* vor. Er beschreibt die bisherige Entwicklung des Datenschutzrechts seit den 1970er Jahren, das zunächst als Reaktion auf maschinelle Informationsverarbeitungen in Großrechenanlagen entstand. Dabei macht er drei Stufen des Datenschutzrechts aus, die an technologische Entwicklungssprünge der Informationsverarbeitung gekoppelt sind: die Computerisierung von Abläufen; die zunehmende Vernetzung der IT-Systeme; die Durchdringung aller Lebensbereiche mit Smarten Technologien. Die DSGVO ist nach Roßnagels Einschätzung kaum in der Lage, die speziellen Risiken neuer Informationstechnologien adäquat einzuhegen. Von einigen kleinen Neuerungen (etwa dem Recht auf Datenübertragbarkeit oder den Vorgaben zur Systemgestaltung) abgesehen, bleibe die Verordnung auf dem Stand der alten EU-Datenschutzrichtlinie von 1995; eine wirkliche Modernisierung des Datenschutzrechts finde nicht statt. Letztlich beschränken sich die materiellen datenschutzrechtlichen Vorgaben der Grundverordnung auf ein zu allgemeines und formelhaftes Niveau, das den „Bäcker um die Ecke" mit den gleichen Maßstäben wie Facebook behandle. Konkrete Antworten auf spezielle Risiken, wie sie etwa mit Sozialen Netzwerken, mit Cloud Computing, Big Data oder „intelligenter" Videoüberwachung einher gehen, suche man daher in der Verordnung vergebens. Ihren größten Gewinn sieht Roßnagel noch in den teilweise gestärkten Kontrollkompetenzen und den verschärften Sanktionsmöglichkeiten gegen Datenschutzverstöße.

Nach dieser Darstellung des europäischen Standards widmet sich *Peter Schaar* der Umsetzung der europäischen Vorgaben im neuen Bundesdatenschutzgesetz (BDSG). Obwohl die DSGVO als Verordnung in allen Mitgliedstaaten unmittelbar geltendes Recht darstellt, das keiner speziellen Umsetzung in deutsches Recht bedarf, enthält sie 70 Öffnungsklauseln, mit deren Hilfe die nationalen Gesetzgeber einzelne Bereiche des Datenschutzrechts (z. B. für Gesundheitsdaten, die Datenverarbeitung von Berufsgeheimnisträgern oder Kirchen) gesondert regeln können bzw. dort, wo die Verordnung selbst keine Regelungen trifft, sogar erlassen müssen. Mit den Öffnungsklauseln bietet sich die Chance, auf besondere Gefahren einzelner Sachgebiete sowie auf nationale Tradierungen zu reagieren. Von dieser Möglichkeit hat der Bundesgesetzgeber im vergangenen Jahr reichlich Gebrauch gemacht, als er das Bundesdatenschutzgesetz (BDSG) an die Vorgaben der DSGVO anpasste. Schaar geht zunächst auf die Entstehungsgeschichte der Grundverordnung ein, vor deren Hintergrund die Öffnungsklauseln zu verstehen sind. Dann stellt er das neu gefasste BDSG in Grundzügen vor, das nicht nur die bestehenden Öffnungsklauseln exzessiv nutzt, sondern zum Teil sogar darüber hinaus Sonderregeln aufstellt, mit denen der deutsche Datenschutzstandard gegenüber der DSGVO abgesenkt wird: So werden die Rechte der Betroffenen beschnitten,

die Zuständigkeit der Aufsichtsbehörden sowie ihre Sanktionsmöglichkeiten gegenüber staatlichen Stellen deutlich eingeschränkt. Für die Zukunft sieht Schaar sogar die Gefahr, dass sich andere Mitgliedstaaten an der deutschen Umsetzung auf Minimalniveau orientieren und Deutschland zum Negativvorbild eines Unterbietungswettbewerbs im Datenschutz werde.

Nach diesen eher grundsätzlichen Abhandlungen widmen wir uns im Folgenden konkreten Einzelfragen der Datenschutzreform: *Marie-Theres Tinnefeld* diskutiert die Möglichkeiten und Grenzen der selbstbestimmten Einwilligung durch Betroffene, die nach wie vor wichtigste Legitimationsquelle für Datenverarbeitungsvorgänge ist. Tinnefeld schildert zunächst den menschenrechtlichen Kontext des Datenschutzes und der freien Einwilligung, bevor sie die konkreten Anforderungen an die Freiwilligkeit, die Folgenabschätzung, die Transparenz und die Formerfordernisse bzw. Nachweispflichtigkeit der Erteilung darstellt. Zum Schluss ihres Beitrags zeigt sie die Grenzen der Einwilligung auf, d. h. welche Datenverarbeitung auch bei etwaiger Zustimmung der Betroffenen unzulässig ist. Angesichts der immer komplexeren Verarbeitungsprozesse, die gerade bei smarten, global vernetzten Systemen zum Einsatz kommen, bleibt jedoch offen, wie weit das Konzept einer informierten und sachkundigen Entscheidung heute noch realistisch ist, wo die AGB-Texte vieler Angebote fast so umfangreich wie klassische Romane sind und die Konsequenzen selbst für IT-kundige kaum zu überblicken sind.

Marit Hansen und *Sven Polenz* knüpfen an diese grundsätzlichen Betrachtungen an und stellen die wichtigsten Änderungen vor, die sich aus Verbrauchersicht mit der DSGVO ergeben. Sie erläutern die praktischen Voraussetzungen, die für eine wirksame Einwilligung erfüllt sein müssen und geben anschließend einen Überblick über die wichtigsten Neuerungen bei den Verbraucherrechten, etwa den Informations- und Benachrichtigungspflichten. Nach einem kurzen Überblick der technischen und systemischen Vorgaben zum Datenschutz gehen sie auf die Möglichkeiten zur Durchsetzung der Betroffenenrechte sowie die Klage-, Untersagungs- und Sanktionsmöglichkeiten von Verbraucherverbänden bzw. Aufsichtsbehörden ein.

Wenn die rechtlichen Möglichkeiten zur Durchsetzung von Datenschutz-Anforderungen an ihre Grenzen kommen, wird häufig der Ruf nach einem bereits auf technischer bzw. systemischer Ebene verankerten Datenschutz laut. Privacy by design und Privacy by default finden sich als Vorgaben auch in der DSGVO wieder. Inwiefern sie dazu beitragen können, das europäische Schutzniveau anzuheben, ist Thema des Beitrags von *Clemens Heinrich Cap*. Bevor er diese Frage beantwortet, geht er zunächst auf den Stellenwert von Privatheit und informationeller Selbstbestimmung in der heutigen Gesellschaft ein. Daran schließt eine Bestandsaufnahme an, welche Möglichkeiten für einen stärkeren Datenschutz sich ergeben, wenn dessen Anforderungen von Anfang an beim Technik- und Ablaufdesign berücksichtigt werden. Cap warnt jedoch vor zu hohen Erwartungen an einen programmierten Datenschutz, denn die Gestaltung neuer Informationstechniken folge i. d. R. anderen (mutmaßlichen) Nutzerwünschen, und das schwächste Glied in der IT-Systemreihe seien immer noch die nach Bequemlichkeit strebenden Anwender, die Sicherheitsvorkehrungen außer Kraft setzen. Cap fordert deshalb eine digitale Aufklärung 2.0, um den unmündigen Umgang mit IT-Systemen und ihrer Datenverarbeitung zu beenden.

Mit einigen Banalisierungen und Verengungen des Datenschutz-Begriffes befasst sich *Martin Rost*: Seine Kritik wendet sich dagegen, Datenschutz allein auf die Minimierung von technischen Risiken und damit ein Problem der Systemsicherheit zu reduzieren. Das Ziel des Datenschutzes sei nicht die Bewahrung einer ‚idyllischen Privatheit', die sich von der Gesellschaft abschotten will, sondern bestehe darin, den Einzelnen gegenüber staatlicher wie unternehmerischer Übermacht zu bewahren, die sich aus der Verfügbarkeit über Daten ergeben kann. Wenn die DSGVO daher von den Risiken der Datenverarbeitung spreche (wie in Erwägungsgrund 75 der Verordnung), dürfe die Risikoanalyse nicht auf Missbrauchs- und Fehlerszenarien beschränkt bleiben, sondern müsse auch die strukturellen Gefahren für die Betroffenen in den Blick nehmen, die mit einer fehlerfrei funktionierenden Verarbeitung verbunden sind. Rost spannt dazu acht Dimensionen des Risikobegriffs auf, die für eine umfassende Folgeabschätzung, aber auch für eine wirksame Datenschutzkontrolle zu berücksichtigen sind.

Den Themenschwerpunkt schließen wir mit drei Beiträgen ab, die über den Tellerrand der DSGVO hinaus schauen: Parallel zur DSGVO wurde auch eine europäische Richtlinie zur Datenverarbeitung bei Strafverfolgungs- und Strafvollstreckungsbehören verabschiedet (EU-RL 2016/680), die einen einheitlichen Datenschutzstandard in diesem Bereich vorgibt. Mit dem Anwendungsbereich der Richtlinie, den zahlreichen Ausnahmen und ihrer ersten Umsetzung im Bundesdatenschutzgesetz sowie im BKA-Gesetz befasst sich der Beitrag von *Hartmut Aden*.

Florian Glatzer geht auf die Verordnung über Privatsphäre und elektronische Kommunikation (ePrivacy-Verordnung) ein, mit der die Datenschutzstandards für den gesamten digitalen Kommunikationsbereich neu geregelt werden. Mit der Verordnung soll der Schutz vertraulicher Kommunikation, der nach der bisherigen EU-Richtlinie nur für klassische telefoniegestützte Kommunikation (einschließlich SMS) gilt, auf die neuen netzbasierten Angebote von Instant Messenger Diensten (bspw. WhatsApp) und Sozialen Netzwerken (etwa Facebook) erweitert werden. Die neue ePrivacy-Verordnung sollte ursprünglich zeitgleich mit der DSGVO in Kraft treten – bisher liegen aber erst der Kommissionsentwurf und die Stellungnahme des EU-Parlaments vor, im Herbst beginnen voraussichtlich die Trilog-Verhandlungen mit dem Rat.

Martin Kutscha nimmt einen kürzlich erschienenen Sammelband zur „Informationellen Selbstbestimmung im digitalen Wandel" zum Anlass, um die ketzerische Frage zu stellen, ob das Datenschutz-Grundrecht überhaupt noch eine realistische Zukunft habe. Mit seinem Kommentar beenden wir diesen Schwerpunkt.

(*Aus dem Editorial von Sven Lüders*)

Dazu enthält die Ausgabe weitere Hintergrundberichte und Rezensionen. Die Beiträge von Alexander Roßnagel und Marie-Theres Tinnefeld sind mit freundlicher Genehmigung auch in dieser Ausgabe der *FIfF-Kommunikation* enthalten.

vorgänge #221/212 Perspektiven des Datenschutzes nach der Datenschutz-Grundverordnung, 57. Jahrgang, Mai 2018, Hefte 1/2, ISSN 0507-4150