Peter Schaar

Datenschutz-Grundverordnung: der neue Goldstandard

Die Datenschutz-Grundverordnung (DSGVO)[1] hat schon vor ihrem Inkrafttreten die weltweite Diskussion über Fragen des Datenschutzes beeinflusst. Die Auswirkungen des neuen Regelungswerks haben sich seither noch intensiviert. Auch außerhalb Europas wurden inzwischen Gesetze beschlossen, die sich am Vorbild der Grundverordnung orientieren. Die Einschätzung des früheren Europäischen Datenschutzbeauftragten Giovanni Buttarelli, die Grundverordnung sei ein Aufruf zur Entwicklung eines neuen weltweiten digitalen „Goldstandards“[2], hat sich nach Ansicht von Peter Schaar bestätigt.

1. Patchwork

Vielfach sind es Krisen oder zumindest die Unzufriedenheit mit dem *Status Quo*, die zu Veränderungen führen. So war und ist es auch mit dem Datenschutz. Das weltweit erste Datenschutzgesetz wurde 1971 in Hessen verabschiedet. Es folgten andere Bundesländer, europäische und außereuropäische Staaten. Von einem einheitlichen Datenschutzrecht konnte dabei keine Rede sein. Es war schließlich der Europarat, der im Jahr 1981 mit der Konvention 108[3] einen ersten internationalen, verbindlichen Datenschutzmindeststandard formulierte. Die Europäische Union folgte diesem Ansatz mit 15jähriger Verspätung, nachdem immer deutlicher geworden war, dass die unterschiedlichen Datenschutzsysteme der Mitgliedstaaten den freien Datenverkehr auf dem gemeinsamen Markt behinderten.

Die EG-Datenschutzrichtlinie von 1995[4] bewirkte zwar, dass alle Mitgliedstaaten eigene Datenschutzgesetze bekamen, doch von einer echten Harmonisierung konnte keine Rede sein. Denn der durch die Richtlinie geschaffene Rahmen war von den Mitgliedstaaten sehr unterschiedlich ausgefüllt worden, so dass das Datenschutzrecht der Mitgliedstaaten weiterhin einen Flickenteppich bildete.

Besonders gravierend waren die Differenzen bei den Durchsetzungsmechanismen: Zwar waren in allen Mitgliedstaaten Datenschutzbehörden eingerichtet worden. Sie

Zitiervorschlag:
Schaar, Peter (2020): Datenschutz-Grundverordnung: der neue Goldstandard, vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik Nr. 231/232 [59(3-4)], S. 7-15.

unterschieden sich jedoch erheblich im Hinblick auf ihre institutionelle Einbindung, ihre Befugnisse und den Grad ihrer Unabhängigkeit. Wiederholt beschäftigte sich der Europäische Gerichtshof mit fragwürdigen Bestimmungen des nationalen Datenschutzrechts.[5]

Schließlich mangelte es an klaren und verbindlichen Regeln für die grenzüberschreitende Zusammenarbeit der Datenschutzaufsicht. Die gem. Art. 29 der Datenschutzrichtlinie eingerichtete Datenschutzgruppe („Artikel 29-Gruppe"), in der alle nationalen Datenschutzbehörden, der Europäische Datenschutzbeauftragte und – allerdings ohne Stimmrecht – die Europäische Kommission vertreten waren, hatte lediglich beratende Funktion. Verbindliche Entscheidungen waren nicht vorgesehen.

Global agierende Unternehmen nutzten das Datenschutzgefälle zwischen den Mitgliedstaaten in ihrem Sinne. Davon profitierten in besonderem Maß Irland und Luxemburg, in denen eine effektive Datenschutzaufsicht nicht stattfand. Die damit verbundene Verwässerung des EU-Datenschutzes wurde in den übrigen Mitgliedstaaten und von den europäischen Institutionen zunehmend kritisch gesehen.

Nicht nur hinsichtlich ihrer mangelnden Harmonisierungswirkung geriet die Datenschutzrichtlinie in die Kritik. Auch angesichts der stürmischen technischen Entwicklung drängte sich die Frage auf, ob eine Regelung aus dem Jahr 1995 den Anforderungen einer global vernetzten, ubiquitär verfügbaren und immer weitere Lebensbereiche durchdringenden Informationsverarbeitung gerecht zu werden vermochte. Immerhin wurde die formuliert, als das Internet und der Mobilfunk noch Nischentechnologien und viele andere – heute alltägliche – Techniken gänzlich unbekannt waren (etwa Biometrie, Cloud, künstliche Intelligenz).

2. Glücksfall Edward Snowden

Die Europäische Kommission erkannte die Zeichen der Zeit und begann im Jahr 2010 mit Konsultationen über die Fortschreibung des EU-Datenschutzrechts. Anfang 2012 legte sie ein umfassendes Reformpaket vor, dessen Kernstück die Datenschutz-Grundverordnung bildete. Die wichtigste Innovation bestand in der Wahl des Regelungsinstruments: Während die Richtlinie der Umsetzung durch die nationalen Gesetzgeber bedurfte, ist eine Verordnung ein unmittelbar in den Mitgliedstaaten anwendbares Gesetz.

Der Gegenwind gegen ein einheitliches, in allen Mitgliedstaaten direkt anwendbares Datenschutzrecht kam von vielen Seiten. Wie schon in den 1990er Jahren in den Beratungen der Datenschutzrichtlinie hielt sich die Begeisterung über ein weitgehend harmonisiertes europäisches Datenschutzrecht, das die Spielräume für nationale Nischen und Alleingänge reduzieren würde, bei den Regierungen der Mitgliedstaaten in Grenzen. In Deutschland wurde insbesondere das Ende des vermeintlich hohen deutschen Datenschutzniveaus beschworen, das sich jedoch bei näherem Hinsehen allzu oft als Schimäre erwies. Im Zuge des europäischen Gesetzgebungsverfahrens („Trilog") setzten die Regierungen der Mitgliedstaaten schließlich etliche Öffnungsklauseln durch, die sich heute als Schwachstelle der DSGVO erweisen.

Der Widerstand von Wirtschaftsverbänden und Unternehmen richtete sich prinzipiell gegen schärfere Regelungen. Er speiste sich auch aus der Wahrnehmung, dass digitale Geschäftsmodelle in den USA wegen nicht vorhandener gesetzlicher Beschränkungen erfolgreicher waren als in Europa. Schließlich kämpften Vertreter der US-Wirtschaft und der US-Regierung gegen jede Verschärfung des EU-Datenschutzrechts, welche die Geschäftsinteressen der auch auf dem europäischen Markt dominierenden IT-Unternehmen der „GAFAM"-Gruppe (Google, Amazon, Facebook, Apple, Microsoft) behindern könnte.

Der von US-Seite ausgeübte erhebliche Druck auf den europäischen Gesetzgeber blieb nicht ohne Folgen. Anders als beabsichtigt verfestigte er jedoch den (zutreffenden) Eindruck, hier ginge es primär um die Sicherung ihrer datengetriebenen Geschäftsmodelle zu Lasten der EU-Bürgerinnen und Bürger und der europäischen Wirtschaft.

Das weit verbreitete Gefühl der digitalen Abhängigkeit Europas verstärkte sich mit der Aufdeckung globaler Überwachungsaktivitäten durch den Whistleblower Edward Snowden. Es war nicht mehr zu leugnen, dass die US-Geheimdienste die marktbeherrschende Stellung der amerikanischen Digitalunternehmen für ihre Aktivitäten, für ihre auf globale Kontrolle ausgerichteten Überwachungsprogramme nutzten. Vieles spricht dafür, dass die symbiotische Beziehung zwischen Sicherheitsbehörden und Unternehmen mit Wissen und Duldung durch deren Top-Management etabliert wurde, auch wenn die Unternehmen die Geheimdienstaktivitäten sicherlich nicht im Detail kannten.[6] Die Aufdeckung dieses Beziehungsgeflechts wirkte als Katalysator des Gesetzgebungsprozesses zur DSGVO. Edward Snowdens Enthüllungen haben ohne Zweifel dazu beigetragen, dass der ambitionierte Regulierungsansatz schließlich auch von den meisten Europapolitikern befürwortet wurde, die ihm zunächst skeptisch gegenübergestanden hatten.

3. Datenschutz ist Grundrechtsschutz

In vielen Ländern – darunter die USA und die asiatischen Staaten – wird Datenschutz (jedenfalls im Hinblick auf den nicht-öffentlichen Bereich) als Gegenstand privatrechtlicher Aushandlungen gesehen. Ein entscheidendes Manko auch der Datenschutzrichtlinie von 1995 bestand darin, dass es sich bei ihr in erster Linie um ein Instrument der Marktregulierung handelte, mit dem der freie Datenverkehr im europäischen Binnenmarkt sichergestellt werden sollte.[7] Mit der Weiterentwicklung der Europäischen Gemeinschaft zu einer politischen Union stellte sich die Frage nach europäischen Grundrechten, die kurz nach der Jahrtausendwende in der EU-Grundrechtecharta festgeschrieben wurden. Art. 7 der Charta verlangt – wie zuvor schon Art. 8 der Europäischen Menschenrechtskonvention[8] – die Achtung des Privat – und Familienlebens. Art. 8 EUGrCh garantiert den Schutz personenbezogener Daten und schreibt eine unabhängige Datenschutzaufsicht vor. Zudem hatte die Rechtsprechung in den Mitgliedsstaaten seit den 1980er Jahren dem Datenschutz als Grundrecht der Informa-

tionsgesellschaft einen höheren Stellenwert einzuräumen begonnen – zu nennen ist hier besonders das „Volkszählungsurteil" des Bundesverfassungsgerichts von 1983[9].

Durch den Vertrag von Lissabon[10] wurde die Grundrechtecharta zum anwendbaren Recht in der gesamten EU aufgewertet. Mit der Charta war eine echte EU-weite Datenschutzgesetzgebung geboten, weil nur so ein angemessener Grundrechtsschutz sichergestellt werden konnte.

4. Die ersten 2½ Jahre

Angesichts des teils gravierenden, mit der DSGVO verbundenen Anpassungsbedarfs des nationalen Rechts hatte der europäische Gesetzgeber den Mitgliedstaaten und den Rechtsanwendern eine zweijährige Übergangsfrist eingeräumt. Die am 25. Mai 2016 im EU-Amtsblatt veröffentlichte DSGVO wurde erst am 25. Mai 2018 vollständig wirksam. Trotzdem wurden die notwendigen Anpassungs- und Umsetzungsarbeiten bis heute nicht abgeschlossen. Aber selbst dort, wo der nationale Gesetzgeber tätig geworden ist, bestehen weiterhin viele Probleme. Dies gilt etwa für nationale Regelungen zur Videoüberwachung, zur Verarbeitung biometrischer Daten oder für die Datenverarbeitung zu Forschungszwecken. Als Problem erweist sich auch, dass die Mitgliedstaaten die ihnen durch die DSGVO eingeräumten Regelungsspielräume beim Beschäftigtendatenschutz und beim Austarieren des Datenschutzes mit der Informations- und Meinungsfreiheit sehr unterschiedlich gefüllt haben.

Auch die Unternehmen waren vielfach nicht hinreichend auf die DSGVO vorbereitet. So ergab eine im Dezember 2017 veröffentlichte Umfrage, dass mehr als der Hälfte der deutschen Unternehmen die DSGVO nicht bekannt war oder dass sie sich noch nicht mit ihr beschäftigt hätten.[11] Die Rechtsunsicherheiten waren und sind in Deutschland besonders ausgeprägt, weil das hiesige Datenschutzrecht maßgeblich durch Spezialregelungen geprägt ist und sich vielfach die Frage stellt, in welcher Beziehung die bereichsspezifischen Datenschutzvorschriften zu den Vorgaben der DSGVO stehen. Hinzu kommt die föderale Differenzierung des deutschen Datenschutzrechts, die in keinem anderen Mitgliedsland eine Entsprechung findet.

2018 setzte insbesondere in Deutschland eine teils aufgeregte öffentliche Diskussion darüber ein, was nun verboten und was erlaubt ist. Anstatt den Datenschutz als Chance zu begreifen und so das Vertrauen in digitale Prozesse in Staat und Wirtschaft zu stärken, wurde der Eindruck erzeugt, Datenschutz bedrohe den Wohlstand, verhindere sinnvolle IT-Projekte und erschwere das Leben von Vereinen und kleinen Unternehmen unverhältnismäßig. Die Wahrnehmung der DSGVO als „Innovationsbremse" oder „Bürokratiemonster" wurde verstärkt durch vielfach unbegründete Behauptungen und zweifelhafte Rechtsauslegungen. Eine bevorstehende „Abmahnwelle"[12] wurde beschworen. Es wurde in Frage gestellt, ob die namentliche Begrüßung als Erhebung personenbezogener Daten noch zulässig sei.[13] Die Bild-Zeitung titelte auf ihrer Frontseite: „*Datenschutz-Irrsinn: Unsere Klingelschilder sollen weg!*"[14] Inzwischen hat sich die Aufregung weitgehend gelegt. Kunden werden weiterhin namentlich begrüßt, kein Klingelschild wurde abmontiert und die beschworene Abmahnwelle ist ausge-

blieben.[15] Zur Beruhigung hat sicherlich beigetragen, dass die Datenschutzbehörden in Deutschland und Europa eine Vielzahl von Auslegungs- und Orientierungshilfen zur DSGVO vorgelegt haben, um Unsicherheiten bei den Rechtsanwendern auszuräumen.[16]

Inzwischen ist auch deutlich geworden, dass die Datenschutzbehörden nicht mehr dem Bild des „zahnlosen Tigers" entsprechen. Sie haben seit dem Wirksamwerden der DSGVO hunderttausende Beschwerden bearbeitet und eine Vielzahl von Bußgeldern – einige davon in Millionenhöhe – gegen Verantwortliche für Datenschutzverstöße verhängt. Dass das Engagement und die Konfliktbereitschaft der nationalen Datenschutzbehörden recht unterschiedlich ausgeprägt sind, ist jedoch auch nicht zu übersehen. Während viele Datenschutzbehörden schwerwiegende Datenschutzverstöße mit hohen Bußgeldern geahndet haben, tun sich andere Datenschutzbehörden hier deutlich schwerer. So hat die irische Datenschutzbehörde bis Ende November 2020 nicht eine der vielen Tausend Beschwerden gegen US-amerikanische Internetunternehmen abschließend entschieden, die ihre Europazentralen in Irland haben (s. dazu den Beitrag von Caspar in diesem Heft).

5. Evaluation

Die Europäische Kommission ist verpflichtet, die Anwendung und Wirkungsweise der Verordnung laufend zu überprüfen und erforderlichenfalls Vorschläge zur Änderung und Weiterentwicklung vorzulegen. Die Evaluations- und Berichtspflicht soll verhindern, dass der neue Rechtsrahmen und die technische und soziale Realität auseinanderfallen. Im Rahmen des Konsultationsprozesses haben Wirtschaftsverbände, Datenschutz- und Verbraucherschutzorganisationen sowie Wissenschaftler[17] Bewertungen der Erfahrungen mit der DSGVO vorgenommen. Auch wenn die Stellungnahmen erwartungsgemäß widersprüchliche Bewertungen einzelner Vorschriften enthielten, sehe ich es als positives Signal, dass die DSGVO grundsätzlich in keiner Stellungnahme in Frage gestellt wurde. Fast alle Teilnehmer des Konsultationsprozesses traten für eine verstärkte EU-weite Harmonisierung und eine bessere Zusammenarbeit der Datenschutzbehörden ein. Die Vielzahl der von den Regierungen der Mitgliedstaaten durchgesetzten Öffnungsklauseln in der DSGVO müsse reduziert werden. Das Regelungspatchwork des nationalen Rechts stehe im Widerspruch zur angestrebten EU-weiten Harmonisierung und beeinträchtige die Datenfreizügigkeit. Die Zusammenarbeit der Aufsichtsbehörden habe sich zwar deutlich verbessert, müsste aber noch effektiver gestaltet werden.

Wirtschaftsverbände und einige Mitgliedstaaten forderten unter der Überschrift „Bürokratieabbau" weitere Erleichterungen für kleinere und mittlere Unternehmen, speziell im Hinblick auf die Reduktion von Dokumentations- und Meldepflichten. Dagegen konzentrierten sich Datenschutz- und Verbraucherschutzverbände auf Verbesserungen bei den Betroffenenrechten, speziell beim *Profiling* und automatisierte Entscheidungen. Systeme, welche für den einzelnen Menschen oder für die Gesellschaft wichtige Entscheidungen treffen oder solche vorbereiten, müssten konsequenter re-

guliert werden, speziell im Hinblick auf den Einsatz von „Künstlicher Intelligenz“ (KI). Daten- und Verbraucherschützer forderten zudem, Hersteller von Hard- und Software datenschutzrechtlich in die Verantwortung zu nehmen.

Der am 24. Juni 2020 veröffentliche erste Bericht der EU-Kommission[18] zog ein positives Fazit und verzichtet auf den Vorschlag konkreter Änderungen des Verordnungstextes. Die DSGVO habe die meisten ihrer Ziele erreicht. Bei der Unterstützung digitaler Lösungen in unvorhersehbaren Situationen wie der COVID-19-Krise habe sich die DSGVO als flexibel erwiesen. Ferner hätten die Unternehmen eine Compliance-Kultur entwickelt und sähen einen starken Datenschutz immer häufiger als Wettbewerbsvorteil.

Aus Sicht von Datenschützern hat die Kommission die Gelegenheit verpasst, mit neuen Vorschlägen erkennbare Fehlentwicklungen zu korrigieren.[19] Unübersehbar bestünden nach zwei Jahren Erfahrung weiterhin massive aufsichtsbehördliche „Ladehemmungen“ bei der Kontrolle der grenzüberschreitenden Datenverarbeitung. Gerade gegenüber global agierenden großen Internetdiensten und Plattformen, deren Nutzer die DSGVO effektiver schützen sollte, hätte sich die DSGVO bislang als stumpfes Schwert erwiesen (s. dazu den Beitrag von Caspar in diesem Heft).

6. Datenschutz-Grundverordnung als weltweites Referenzmodell

Trotz mancher Unzulänglichkeiten der DSGVO orientieren sich immer mehr Staaten bei der Regulierung des Umgangs mit personenbezogenen Daten an diesem Regelungswerk. Zu nennen sind beispielsweise die neuen bzw. geänderten Datenschutzgesetze von Brasilien, Thailand, Japan[20], Singapur und Indien. Selbst in China wurden in verschiedenen Bereichen Regelungen in Kraft gesetzt, die der DSGVO in mancher Beziehung ähneln.[21]

Der wichtigste Hebel für die Durchsetzung der europäischen Datenschutzanforderungen auf internationaler Ebene ist die schon in der Datenschutzrichtlinie von 1995 enthaltene Anforderung, dass personenbezogene Daten in Staaten außerhalb der Europäischen Union nur übermittelt werden dürfen, wenn beim Empfänger ein angemessener Datenschutz gewährleistet wird. Dafür sieht die DSGVO verschiedene Instrumente vor, speziell einen „Angemessenheitsbeschluss“ der Europäischen Kommission, genehmigte Standarddatenschutzklauseln und verbindliche Unternehmensregelungen (*Binding Corporate Rules*).

Im Regelfall beziehen sich Angemessenheitsbeschlüsse auf ein Land. Allerdings ist es auch möglich, die Angemessenheit des Datenschutzes für bestimmte Regionen oder Sektoren festzustellen. Solche partiell wirksamen Angemessenheitsbeschlüsse wurden etwa zwischen der EU und den Vereinigten Staaten vereinbart. Diese Beschlüsse annullierte jedoch der Europäische Gerichtshof.[22] Sowohl das „*Safe Harbor*“-Abkommen aus dem Jahr 2001 als auch das Nachfolgeabkommen „*Privacy Shield*“ von 2016 scheiterten vor dem EuGH am unzureichenden Schutz personenbezogener Daten gegen einen Zugriff amerikanischer Sicherheitsbehörden. In beiden Urteilen ging es speziell um Datenübermittlungen zwischen *Facebook Europa* und dem amerikanischen Mutter-

unternehmen. Der EuGH hat nicht nur über die Beschwerden gegen konkrete Datentransfers entschieden, sondern auch über die zugrundeliegenden Abkommen. Das oberste EU-Gericht hielt die von der EU-Kommission bei der US-Regierung ausgehandelten rechtlichen Garantien nicht für ausreichend. Insbesondere sei es nicht hinzunehmen, dass EU-Bürgerinnen und -Bürger keinen effektiven Rechtsschutz gegen die Überwachungsmaßnahmen amerikanischer Behörden haben.

Die Gewichte in dem in den 1970er Jahren begonnenen Wettbewerb zwischen dem europäischen und dem amerikanischen Datenschutzmodell haben sich verschoben. Der US-Ansatz sah Datenschutz primär als Gegenstand eines Aushandlungsprozesses auf dem Markt. Dementsprechend verzichtete er weitgehend auf eine Regulierung der Datenverarbeitung im privatwirtschaftlichen Sektor. Dagegen setzte Europa frühzeitig auf gesetzliche Regelungen und unabhängige Datenschutzaufsicht.

Inzwischen ist nicht mehr zu übersehen, dass sich die DSGVO zu *dem* internationalen Referenzmodell entwickelt, an dem sich die Datenschutzgesetze weltweit orientieren. Mit der gegenseitigen Anerkennung der jeweiligen Datenschutzbestimmungen als „angemessen" durch die Europäische Kommission[23] und die japanische Regierung ist der weltweit größte Datenraum entstanden, in dem personenbezogene Daten unter Wahrung eines hohen Datenschutzniveaus verarbeitet werden.

Die Wirkungen der DSGVO haben längst auch die Vereinigten Staaten selbst erreicht. So greift der kalifornische *Consumer Privacy Act* (CCPA) wichtige Elemente des EU-Datenschutzrechts auf. Mit dem erfolgreichen, zeitgleich mit der US-Präsidentschaftswahl am 3. November 2020 durchgeführten Referendum („*Proposition 24*") wurden u.a. eine kalifornische Datenschutzbehörde eingeführt und die Betroffenenrechte gestärkt.[24] Auch andere US-Bundesstaaten haben inzwischen eigene Datenschutzgesetze. Dem US-Kongress liegen mehrere Entwürfe für US-Bundesgesetze zum Datenschutz vor bzw. werden gegenwärtig in ungewohnter Kooperation von demokratischen und republikanischen Mitgliedern des US-Senats und des Repräsentantenhauses erarbeitet.[25]

Selbst die großen Internet-Konzerne haben ihren früheren Widerstand gegen DSGVO-ähnliche US-Gesetze aufgegeben und fordern mittlerweile ein US-Bundesgesetz zum Datenschutz in der Wirtschaft.[26] So hat Marc Zuckerberg vor dem US-Kongress und vor dem Europäischen Parlament die europäische Datenschutz-Grundverordnung als vorbildlich bezeichnet. Unabhängig von der Glaubwürdigkeit solcher Aussagen, die in der Folge des *Cambridge Analytica*-Skandals[27] gemacht wurden, ist unverkennbar, dass der Druck der Wirtschaft auf den US-Kongress zunimmt, ein Datenschutzgesetz zu erlassen, das ein der Grundverordnung entsprechendes Datenschutzniveau gewährleistet und eine unabhängige Datenschutzaufsicht vorsieht, aber zugleich die Datenschutzgesetzgebung in den Bundesstaaten deckelt.[28]

Trotz aller positiven Signale ist es heute immer noch alles andere als sicher, ob die DSGVO ihre eigentliche Bewährungsprobe besteht: Die Einhegung der mit der Digitalisierung verbundenen Überwachung und Manipulation und des darin zum Ausdruck kommenden Machtmissbrauchs. Trotz verbaler Zustimmung zur DSGVO sind die GAFAM-Unternehmen bis heute nicht bereit, ihre Geschäftsmodelle den Grundsätzen des europäischen Datenschutzrechts anzupassen. Die bereits während der Beratungen des Europäischen Parlaments zur DSGVO zu Höchstform aufgelaufenen Bemühungen

von Lobbyisten, als geschäftsschädigend betrachtete EU-Datenschutzvorgaben zu verhindern, werden fortgesetzt. Sie konzentrieren sich derzeit auf die *E-Privacy*-Verordnung, die den Umgang mit personenbezogenen Daten durch Telekommunikations- und Internetdiensten EU-weit einheitlich regulieren soll.

Angesichts dessen ist zu wünschen, dass Europa sich nicht von dem eingeschlagenen Weg abbringen lässt und die dringend nötige Regulierung nicht nur im Hinblick auf den Datenschutz, sondern auch im Verbraucherschutz- und Kartellrecht weiter voranbringt. Neben der E-Privacy-Verordnung betrifft dies insbesondere Vorgaben für digitale Plattformen und zur Herstellung eines gemeinsamen europäischen Datenraums.

PETER SCHAAR Jahrgang 1954, ist gelernter Ökonom. Er war ab 1980 in der Verwaltung der Hansestadt Hamburg tätig und wechselte 1986 zum Hamburger Landesdatenschutzbeauftragten. 2003 wurde er auf Vorschlag der rot-grünen Bundesregierung vom Deutschen Bundestag zum fünften Bundesbeauftragten für Datenschutz gewählt. Seine Amtszeit endete am 16. Dezember 2013. Seit 2013 steht Schaar der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) vor.

Anmerkungen:

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rats vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) - EU Amtsblatt v. 4.5.2016, L119/1.
2 Buttarelli, The EU GDPR as a clarion call for a new global digital gold standard, IDPL 2017, 77.
3 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention 108, 28.01.1981.
4 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, EG-Amtsblatt 23.11.1995, L 281.
5 Vgl. etwa EuGH, Urteil zur Unabhängigkeit der deutschen Datenschutzbehörden v. 09.03.2010 - C-518/07.
6 Vgl. Schaar, Überwachung total - Wie wir in Zukunft unsere Daten schützen, 2014, S. 14ff.
7 Simitis, Hornung, Spiecker (Hg.), Datenschutzrecht (1. Aufl. 2019), Einleitung Rndnr. 133.
8 Konvention zum Schutz der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention) v. 4. 11.1950.
9 Bundesverfassungsgericht, Urteil vom 15.12.1983, BVerfGE 65, 1, S. 1.
10 EU-Amtsblatt v. 13.12.2007 - 2007/C 306/01.
11 ZEW, Dezember 2017
12 Vgl. etwa Ärzte-Zeitung v. 22.6.2018; BfDI, 27. Tätigkeitsbericht, S. 29.

13 Berliner Morgenpost, 14.12.2018, https://www.morgenpost.de/vermischtes/article215988685/Datenschutz-DSGVO-Metzgerei-Kundin-wehrt-sich-gegen-namentliche-Begruessung.html (abgerufen am 10.5.2019).
14 Bild-Zeitung v. 18.10.2018 (Titelseite).
15 Zu den angesprochenen Fragen vgl. Schaar/Dix, Umsetzung der Datenschutz-Grundverordnung (DSGVO) – Bilanz ein Jahr nach Inkrafttreten. Gutachten im Auftrag der Fraktion Bündnis 90/Die Grünen im Deutschen Bundestag, 16.5.2020; https://www.gruene-bundestag.de/fileadmin/media/gruenebundestag_de/themen_az/datenschutz/PDF/Gutachten_DSGVO.pdf.
16 European Data Protection Board, DSGVO: Leitlinien, Empfehlungen, bewährte Verfahren, https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de; Datenschutzkonferenz (DSK), https://www.datenschutzkonferenz-online.de.
17 GDD: Stellungnahme zur Evaluierung der DS-GVO v. 27.6.2019; Deutscher Industrie- und Handelskammertag: Position Paper of 2.7.2019; Netzwerk Datenschutz Expertise: Evaluation der DSGVO vom 18.7.2019; Mitgliedstaaten: DAPIX 286 (12756/1/19 Rev. 1) v. 9.10.2019; Konferenz der unabhängigen Datenschutzbehörden Deutschlands, Erfahrungsbericht v. 13.11.2019; Roßnagel/Geminn: Evaluation der DSGVO aus Verbrauchersicht, 26.11.2019; Verbraucherzentrale Bundesverband: Evaluation der DSGVO aus Sicht der Verbraucher, 27.11.2019; Bundesrat: Entschließung v. 29.11.2019, Drs. 570/19 (Beschluss); Rat: DAPIX 364 (14994/1/19 Rev.1) Council Position and Findings of 19.12.2019; Europ. Akademie für Informationsfreiheit und Datenschutz: Stellungnahme v. 27.1.2020.
18 COM(2020) 264 final.
19 Vgl. Stellungnahme des Hamburgischen Datenschutzbeauftragten zum Evaluationsbericht der Kommission, https://datenschutz-hamburg.de/%2Fpressemitteilungen%2F2020%2F06%2F2020-06-25-dsgvo-evaluation.
20 Japanese Amended Act on the Protection of Personal Information v. 30. Mai 2017, https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf; im Jahr 2020 beschlossene Änderungen vgl. https://www.ppc.go.jp/files/pdf/overview_amended_act.pdf.
21 Chinese Personal Information Security Specification vom 01.10.2020; https://www.wzr-china.com/news/neue-entwicklungen-im-chinesischen-datenschutzrecht.
22 EuGH, Urteile in der Rechtssache C-362/14 v. 06.10.2015 (Safe Harbor, „Schrems „I) und Urteil v. 16.07.2020 in der Rechtssache C-311/18 (Privacy Shield„Schrems II“).
23 European Commission, EU Japan Adequacy Decision, January 2019; https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
24 California Proposition 24, Consumer Personal Information Law and Agency Initiative (2020) https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020)#Measure_design
25 Eine Gruppe von Senatoren (Republikaner und Demokraten) erarbeitet gegenwärtig einen Gesetzentwurf für den Datenschutz im Online-Bereich; siehe auch das Schreiben des Electronic Privacy Information Center (EPIC) an den Handelsausschuss vom 29.4.2019, https://epic.org/testimony/congress/EPIC-SCOM-ConsumerPerspectives-Apr2019.pdf.
26 Der *U.S. Privacy Act* von 1974 gilt nur für die öffentliche Verwaltung.
27 Vgl. ICO investigation into use of personal information and political influence, Letter of 02 October 2020; https://ico.org.uk/media/action-weve-taken/2618383/20201002_ico-o-ed-l-rtl-0181_to-julian-knight-mp.pdf
28 Vgl. *Data Protection Act of 2020*, https://www.congress.gov/bill/116th-congress/senate-bill/3300/text.