Peter Schaar

Deutscher Sonderweg beim Datenschutz?

Lange Zeit wurden Verhandlungen um eine Reform und weitergehende Angleichung der europäischen Datenschutznormen von deutscher Seite mit dem Einwand entgegnet, dem stünde das höhere Datenschutzniveau hierzulande im Wege, das man nicht der Gemeinschaft zuliebe absenken wolle. Die Geschichte des Zustandekommens der Datenschutz-Grundverordnung sowie ihre Umsetzung in Deutschland sprechen jedoch eine andere Sprache: Peter Schaar schildert im folgenden Beitrag die Verhandlungen zur DSGVO, bei der sich deutsche Regierungsvertreter darum bemühten, den europäischen Standard möglichst niedrig zu definieren und mit vielen Öffnungsklauseln zu versehen, die nationale Abweichungen auch nach unten erlauben. Er stellt zudem die Grundzüge des mitterweile reformierten Bundesdatenschutzgesetzes vor, das die Verordnung in deutsches Datenschutzrecht umsetzt und zahlreiche Verschlechterungen gegenüber dem europäischen Referenzrahmen enthält.

„*Wir brauchen ... endlich eine smarte Datenkultur vor allem für Unternehmen. Tatsächlich existiert in Deutschland aber ein Datenschutz wie im 18. Jahrhundert.*“ Dieser Satz stammt nicht etwa von dem Vertreter einer der viel gescholtenen Datenkraken aus den USA, sondern von Dorothee Bär (CSU), der Staatsministerin „für Digitales“ der neu aufgelegten großen Koalition.[1] Was kennzeichnet die „smarte Datenkultur“, die hier gefordert wird? Ganz bestimmt nicht *Datenvermeidung* und *Datensparsamkeit*, also die Minimierung personenbezogener Daten, wie sie in § 3a des bisherigen Bundesdatenschutzgesetzes gefordert werden. An Stelle dieser „Datensparsamkeitsdiktatur“ soll die Digitalisierung dem Leitbild des „*Datenreichtums*“ und der „*Datenvielfalt*“ folgen.[2]

Wer geglaubt hatte, dass das Grundrecht auf informationelle Selbstbestimmung mehr als 30 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts[3] in Deutschland eine Selbstverständlichkeit sei, den haben die Diskussionen der letzten Jahre eines Schlechteren belehrt. Grundlegende Kritik an den angeblich überholten Vorstellungen des an Grundrechten orientierten Datenschutzes wurde insbesondere im Zusammenhang mit der Reform des Datenschutzrechts laut, deren Kernstück, die „Datenschutz-Grundverordnung“ der EU (DSGVO)[4], ab dem 25. Mai 2018 auch in Deutschland anwendbares Recht sein wird.

Auch die immer neuen Sicherheitsgesetze[5] mit ihrer Befugniserweiterung für staatliche Stellen belegen, dass der Datenschutz im Verhältnis zu anderen Rechtsgütern und Interessen vielfach als zweitrangig betrachtet wird und hinter anderen Ge-

staltungszielen zurückstehen müsse, etwa hinter dem vom ehemaligen Bundesinnenminister Friedrich vor fünf Jahren proklamierten „*Supergrundrecht auf Sicherheit*“.[6]

Europa geht voran

Anders als in vielen anderen Politikbereichen hat die Europäische Union beim Datenschutz ihre Handlungsfähigkeit bewiesen. Die mit dem Vertrag von Lissabon 2011[7] erfolgte Aufwertung der EU-Grundrechtecharta (EUGrCh) hat die datenschutzrechtliche Landschaft stark verändert. Art. 7 der Charta verlangt – wie 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.

Die Aufwertung des Datenschutzes durch die Grundrechtecharta hatte Konsequenzen auf unterschiedlichen Ebenen: So hat der Gerichtshof der Europäischen Union (EuGH) in verschiedenen Urteilen verdeutlicht, dass er sich – ebenso wie schon der Straßburger Gerichtshof für Menschenrechte – nun als Hüter der EU-Grundrechte auf Privatsphäre und Datenschutz versteht und sich nicht mehr auf die Rolle eines EU-Verwaltungsgerichtshofs beschränkt. Diese neue Rollenbestimmung des EuGH wurde besonders deutlich in den Urteilen zur Vorratsdatenspeicherung[9] und zu Safe Harbour[10] – eine angesichts der zunehmenden Bedeutung der Informationstechnologie und anschwellender transnationaler Datenströme uneingeschränkt positiv zu beurteilende Entwicklung.

Ohne den Vertrag von Lissabon wäre auch die im Mai 2016 im EU-Amtsblatt verkündete Datenschutzreform – bestehend aus einer Datenschutz-„Grundverordnung“ (DSGVO) und einer Datenschutzrichtlinie für Polizei und Justiz (DS-JIRL)[11] – kaum durchsetzbar gewesen. Die Datenschutz-Grundverordnung hatte den Trilog von Rat, Kommission und Europäischem Parlament vergleichsweise gut überstanden. Dazu beigetragen hat sicherlich auch der Umstand, dass nach den auf Edward Snowden zurückgehenden Erkenntnissen die globalen Überwachungsaktivitäten[12], maßgeblich ins Werk gesetzt von US-Nachrichtendiensten, aber mit tatkräftiger Unterstützung befreundeter Dienste (darunter auch des BND) nicht mehr ernsthaft bestritten werden konnten.

Gleichwohl darf nicht ausgeblendet werden, dass die EU-Datenschutzreform in mancherlei Hinsicht die erhoffte Stärkung des Datenschutzes nicht in vollem Umfang bringen wird. Dies gilt zum einen für Polizei und Justiz, denn hier legt die zeitgleich mit der DSGVO verkündete Richtlinie nur datenschutzrechtliche Mindeststandards fest. Die Richtlinie ermöglicht es den Mitgliedstaaten zwar, strengere nationale Bestimmungen zu erlassen. Andererseits werden die Zugriffsmöglichkeiten von Polizei- und Justizbehörden auf Daten, die in anderen Mitgliedstaaten gespeichert sind, weiter ausgebaut – auch von Behörden aus Staaten, in denen das nach der Rechtsprechung des Bundesverfassungsgerichts geforderte hohe Schutzniveau nicht garantiert ist.

Weiterhin gibt es keine europarechtlichen Beschränkungen für die Tätigkeit der Nachrichtendienste, sofern sie der „nationalen Sicherheit“ dient, denn dieser Bereich fällt nach dem Primärrecht der Europäischen Union weiterhin in die alleinige Verant-

wortung der Mitgliedstaaten.[13] Die Hoffnung, das EU-Recht würde der weltweiten geheimdienstlichen Überwachung zumindest in Europa wirksame Grenzen setzen, wird sich deshalb in absehbarer Zukunft nicht erfüllen.

Bremsen oder beschleunigen?

Welche Rolle hat Deutschland bei der EU-Datenschutzreform eingenommen? Eigentlich hätte man annehmen müssen, dass Deutschland – wie bereits beim Ringen um die Datenschutzrichtlinie von 1995 – erneut eine Vorreiterrolle einnehmen würde. Schließlich war das erste Datenschutzgesetz der Welt – das hessische – „Made in Germany". Und auch sonst beriefen sich manche Politiker und Journalisten immer wieder auf das angeblich „*hohe deutsche Datenschutzniveau*", das bewahrt werden müsse. Hier soll die Frage nicht vertieft werden, ob angesichts der vielfältigen, in den letzten zwei Jahrzehnten vorgenommenen Einschränkungen des Grundrechts auf informationelle Selbstbestimmung von einem besonders hohen deutschen Datenschutzniveau noch ernsthaft die Rede sein kann.

Auch der Blick auf den Werdegang der Datenschutzreform verstärkt den Eindruck, dass es sich beim Hohelied auf den guten deutschen Datenschutz vielfach eher um eine Floskel statt um innere Überzeugung handelt. Nachdem die Europäische Kommission im Januar 2012 nach mehrjährigen Vorarbeiten ihren Entwurf des Datenschutz-Reformpakets[14] auf den Tisch gelegt hatte, setzte ein erbittertes Ringen ein, bei dem über lange Zeit nicht einmal klar war, ob es überhaupt am Ende zu der beabsichtigten Reform kommen würde. Unternehmen und Wirtschaftsverbände liefen Sturm gegen die strengeren Regeln zur Verarbeitung personenbezogener Daten und insbesondere gegen die beabsichtigte Stärkung der Aufsichtsbehörden und die erheblich verschärften Sanktionen bei Datenschutzverstößen. Abgeordnete des EP berichteten darüber, dass große US-Unternehmen ganze Flugzeugladungen an Lobbyanwälten nach Brüssel in Bewegung setzten, um das drohende Unheil für ihre datengetriebenen Geschäftsmodelle abzuwenden. Auf der anderen Seite bemühten sich Datenschutzbehörden, Verbraucherschutz- und Datenschutzverbände und Bürgerrechtsorganisationen erfolgreich um den Aufbau von Gegenpositionen.

Die äußerst intensive Lobbyarbeit in Brüssel und in den Hauptstädten der EU-Mitgliedstaaten blieb nicht ohne Folgen. Eine Vielzahl der mehreren Tausend im Europäischen Parlament eingebrachten Änderungsanträge hatten eine Verwässerung der Kommissionsvorschläge zum Gegenstand. Das Europäische Parlament positionierte sich nach zähem Ringen mit erstaunlich klaren Mehrheiten für eine deutliche Verbesserung des Datenschutzes in der Union[15], nicht zuletzt aufgrund der zähen Arbeit des Berichterstatters Jan-Phillip Albrecht (Grüne) und der Schattenberichterstatter aus den anderen Parlamentsfraktionen, von denen viele aus Deutschland stammen oder zumindest – wie etwa der Berichterstatter zur JI-RL, der griechische Abgeordnete Dimitris Droutsas (S&D Fraktion) – umfassende Kenntnisse des deutschen Rechtssystems hatten. Zudem war es schon auffällig, dass auch maßgebliche Vertreter der Europäischen Kommission, die sich mit der Datenschutzmaterie beschäftigten, aus Deutschland stammen.

Deutlich schwieriger als im EP verlief die Debatte im Rat, der Vertretung der Regierungen der Mitgliedstaaten.[16] Niemanden konnte es verwundern, dass die britische Regierung sich sehr zurückhielt. Für viele Beobachter überraschend war es aber, dass auch die Bundesregierung lange Zeit nicht etwa zu den treibenden Kräften der Reform gehörte, sondern im Bremserhäuschen Platz genommen hatte. Während man einerseits in eher allgemeiner Form Zustimmung signalisiere, wurde bei den Fachdebatten soviel Sand ins Getriebe gestreut, dass der Reformprozess zu scheitern drohte.[17] Die deutsche Verhandlungsführung war dabei gekennzeichnet durch eine eigenartige Melange von fundamentalistischen und opportunistischen Positionen. So wurde beklagt, das Reformpaket der Kommission ginge nicht weit genug. Erforderlich wären vielmehr deutlich klarere, die Datenverarbeitung begrenzende Regelungen. Zum anderen setzten sich die Deutschen in den Gremien, speziell in der Dapix-AG des Rats, dafür ein, statt der vorgeschlagenen, in sämtlichen Mitgliedstaaten direkt anwendbaren Verordnung eine neue Datenschutz-Richtlinie zu beschließen, deren Umsetzung durch nationales Recht erfolgen müsste. Damit wollten die Regierungsvertreter den Änderungsbedarf am deutschen Recht möglichst klein halten. Zugleich bekämpften sie ausdauernd Regelungen, die als „Hindernis“ für die Wirtschaft angesehen wurden, (etwa Vorgaben zur strikten Zweckbindung), obwohl sie dem bisherigen deutschen Datenschutzrecht entsprachen. Besonders erbittert war das Bemühen der Bundesregierung, die öffentlichen Stellen generell von der Verordnung auszunehmen. Erst in der Endphase der Verhandlungen im Rat gab der seinerzeitige Bundesinnenminister de Maizière den grundsätzlichen Widerstand gegen die Verordnung auf, als klar geworden war, dass Deutschland und Großbritannien (anders als offenbar erwartet) für ihre Position kaum Verbündete in den anderen Mitgliedsstaaten gefunden hatten.

Wesentliche Elemente des Reformpakets, die während des mehr als vierjährigen Verhandlungsmarathons immer wieder in Frage gestellt worden waren, blieben bei der im April 2016 vom EP gebilligten Datenschutzreform erhalten oder wurden sogar gegenüber dem Anfang 2012 vorgelegten Entwurfstext[18] stärker akzentuiert. Dies gilt etwa für die Ausdehnung des Anwendungsbereichs auf Anbieter elektronischer Dienste mit Sitz in einem Drittland („Marktortprinzip“) oder die sehr deutliche Verschärfung der Sanktionen bei Datenschutzverstößen.

Auf den Rat ist es allerdings zurückzuführen, dass die beschlossene Datenschutzgrundverordnung viele – je nach Zählart bis zu 70 – Klauseln enthält, die den nationalen Gesetzgebern Regelungskompetenzen belassen. Zwar beharrt die Europäische Kommission darauf, dass es sich dabei nicht um „Öffnungsklauseln“ handele, sondern lediglich um Möglichkeiten zur Konkretisierung der Bestimmungen der DSGVO durch nationales Recht. Festzustellen ist jedenfalls, dass diese Klauseln herangezogen wurden, um erhebliche Abweichungen des neu gefassten deutschen Datenschutzrechts[19] von der DSGVO zu rechtfertigen.

Deutscher Sonderweg?

Spätestens im September 2016, als der Blog „Netzpolitik" einen ersten Referentenentwurf des Bundesinnenministeriums für ein neues Bundesdatenschutzgesetz veröffentlichte,[20] wurde klar, dass es dem BMI in erster Linie nicht darum ging, das „hohe deutsche Datenschutzniveau" zu erhalten, sondern vorrangig um dessen Absenkung.

Staatliche Stellen sollten mehr Befugnisse zur Verarbeitung personenbezogener Daten erhalten. An die Stelle spezifischer Vorgaben für die Erhebung, Speicherung, Änderung und Nutzung sollten Generalermächtigungen zur Verarbeitung treten. Spezifische Zweckbindungsregeln sollten durch biegsame Verwendungsregeln abgelöst werden, die den Vorgaben des Bundesverfassungsgerichts (und der DSGVO) Hohn sprachen. Bei den Nachrichtendiensten – die ja durch das EU-Reformpaket gar nicht berührt waren[21] – sollten nach dem Referentenentwurf die Schwellen zur Erhebung von Daten weiter abgesenkt werden. Die Betroffenenrechte und die Kontrollbefugnisse der Datenschutzbehörden sollten dagegen eingeschränkt werden, wo immer es die EU-Vorgaben zulassen und teils sogar dort, wo solche Spielräume nicht bestehen. Bemerkenswert waren die vorgesehenen Lockerungen der Zweckbindung für die Verwendung personenbezogener Daten. Zugleich sollten Unternehmen erheblich von lästigen Auskunfts- und Löschungspflichten entbunden werden, etwa wenn damit ein „*unverhältnismäßiger Aufwand*" verbunden wäre. Letztlich zog das Bundesjustizministerium aus verfassungsrechtlichen und handwerklichen Gründen die Notbremse und stoppte die offizielle Versendung des Entwurfs.

Während des Gesetzgebungsverfahrens zum deutschen Datenschutzanpassungsgesetz konnten eine Reihe besonders problematischer Vorschläge entschärft werden. Dennoch trägt das vom Bundestag im Sommer 2017 beschlossene neue Bundesdatenschutzgesetz (BDSG-neu)[22] der im Gesetzgebungsverfahren vorgebrachten Kritik an dem Regierungsentwurf[23] nur unzureichend Rechnung. Das neue BDSG belegt die anhaltende Distanz der Bundesregierung und der sie tragenden Parteien zur Europäischen Datenschutzreform, unbeschadet der Tatsache, dass Deutschland dem EU-Datenschutzpaket im Rat letztlich doch zugestimmt hatte. Die Unhandlichkeit der neuen deutschen Regelungen – allein das neue BDSG ist mit 85 Paragraphen fast doppelt so umfangreich wie das bisherige Gesetz – ist ein Indiz dafür, dass die Bundesregierung in vielen Punkten mit der Europäischen Datenschutzreform unzufrieden ist. Den ganzen Text durchzieht das Bemühen, soviel vom alten BDSG zu „retten" wie möglich.

Noch gravierender war es, das in der Substanz des neuen BDSG von den europarechtlichen Vorgaben abgewichen werden sollte, deutlich über die von der DSGVO eingeräumten Regelungsspielräume für die nationalen Gesetzgeber hinaus. Dies gilt in besonderem Maße für diejenigen Regelungen, die sich auf Unternehmen beziehen.

So enthält das neue BDSG deutliche Einschränkungen der Betroffenenrechte. Abweichend von den Vorgaben der DSGVO muss der Betroffene nicht über die Datenverarbeitung informiert werden, soweit „*die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben ... gefährden würde ...*" oder „*... die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde ...*" (§ 32 Abs. 1 BDSG-neu). Auch die Auskunftsrechte der betroffe-

nen Person werden eingeschränkt. Kritisch zu sehen ist auch die gegenüber der DSGVO abgeschwächte Zweckbindung personenbezogener Daten.

Im Zuge des Gesetzgebungsverfahrens wurde eine brisante Neuregelung nur wenig thematisiert, die von zentraler Bedeutung für den Schutz der Privatsphäre ist: Die Einschränkung der Datenschutzkontrolle bei „Berufsgeheimnisträgern" (§ 29 Abs. 3 BDSG-neu). Die Mitarbeiter der Aufsichtsbehörden haben danach keinen Anspruch mehr, Krankenhäuser, Arztpraxen, Anwalts- oder Notariatskanzleien, Apotheken, Steuerberatungs- und Buchführungsbüros oder Suchtberatungsstellen zu betreten, um vor Ort die Datenverarbeitung zu kontrollieren, wenn dadurch der Bruch eines strafbewehrten Berufsgeheimnisses zu befürchten sei. Nicht mehr effektiv prüfbar wären auch Unternehmen der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle. Die Aufsichtsbehörden hätten auch keinen Zugang mehr zu den sensiblen Daten, die in diesen Bereichen verarbeitet werden.

Die bisherige einschlägige Regelung, welche die Datenschutzbehörden ausdrücklich zur Prüfung entsprechender Daten ermächtigte, wurde nicht ins neue Gesetz übernommen („*die Kontrolle der oder des Bundesbeauftragten erstreckt sich auf ... personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis ... unterliegen.*")[24]. Die neue Rechtslage bedeutet, dass sich Berufsgeheimnisträger nach § 203 StGB strafbar machen würden, wenn sie den Aufsichtsbehörden entsprechende Daten zugänglich machen. In diesen für den Datenschutz zentralen Bereichen – hier werden besonders sensible Daten verarbeitet – könnten die Datenschutzbehörden nur noch allgemeine Befragungen hinsichtlich der Datenverarbeitung durchführen, aber keinen Einblick in Datenbanken oder übertragene Informationen nehmen; und sie können Behauptungen zum konkreten Umgang mit personenbezogenen Daten nicht mehr nachprüfen. Da ein derartiger aufsichtsfreier Raum den Vorgaben des Bundesverfassungsgerichts und den Maximen der Datenschutz-Grundverordnung widerspricht, wonach eine lückenlose Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften durch unabhängige Datenschutzbehörden unverzichtbar ist, bleibt abzuwarten, wie die entsprechenden Regelungen durch das Bundesverfassungsgericht oder durch den EuGH bewertet werden.

Paradoxer Weise werden trotz der hohen Regelungsintensität der deutschen Bestimmungen zur Umsetzung der DSGVO – neben dem BDSG wurden inzwischen zahlreiche weitere, bereichsspezifische Gesetze novelliert – die in der Verordnung enthaltenen Gestaltungsspielräume für konkretisierende nationale Datenschutzbestimmungen bisher nur unzureichend ausgefüllt. Dies gilt in besonderem Maß für den Beschäftigtendatenschutz, der durch das neue BDSG nur unzureichend geregelt wird.

Auch fehlen im Bundesrecht Bestimmungen zum Ausgleich zwischen den Rechtsgütern Datenschutz und Meinungsfreiheit. Diese schwierige Materie hat der Bund vollständig den Ländern überlassen. Diese beschränken sich allem Anschein nach darauf, Regelungen für Medienunternehmen auszuarbeiten, nicht jedoch für die immer wichtigeren sozialen Netzwerke. Solche Konkretisierungen wären aber dringend erforderlich. Die vielleicht wichtigste Länderregelung zum Datenschutz in den Medien ist der 21. Rundfunkänderungsstaatsvertrag, der den Landesparlamenten seit Ende letzten Jahres zur Ratifizierung vorliegt.[25] Danach sollen der Rundfunk und die von

Rundfunkanstalten angebotenen Mediendienste bei ihrer redaktionellen Datenverarbeitung von sämtlichen materiellen Datenschutzbestimmungen, der Kontrolle durch die Datenschutzbehörden und den Rechten der betroffenen Personen ausgenommen bleiben. Auch bei den Ländern dominiert offensichtlich eine Haltung, den bisherigen, teils unbefriedigenden deutschen Rechtszustand unverändert beizubehalten, obwohl der europäische Gesetzgeber hier eine genaue Interessenabwägung gefordert hat. Es darf bezweifelt werden, dass die vorgesehene vollständige Suspendierung der materiellen Datenschutzbestimmungen und der Betroffenenrechte diese Mindestanforderungen des europäischen Rechts erfüllt.

Fazit

Angesichts der neuen deutschen Datenschutzbestimmungen und der DSGVO wird viel Arbeit auf die Datenschutzbehörden zukommen, welche die Bestimmungen auszulegen und anzuwenden haben. Die nationalen Gerichte und letztlich auch der EuGH werden sich in den nächsten Jahren verstärkt mit dem Datenschutz befassen müssen, um Auslegungsprobleme zu klären. So wird es voraussichtlich viele Jahre dauern, bis die wesentlichen Streitfragen geklärt sind, die sich aus den widersprüchlichen Vorgaben des europäischen und des nationalen Rechts ergeben.

Problematisch ist zudem die Perspektive, dass sich die Gesetzgeber anderer Mitgliedstaaten am deutschen Beispiel orientieren und eigene Sonderwege beim Datenschutz einschlagen. Entsprechende Gesetzgebungsverfahren sind in verschiedenen Mitgliedstaaten bereits auf den Weg gebracht, zum Teil schon abgeschlossen. Statt des angestrebten einheitlichen EU-Datenschutzrechts besteht deshalb die Gefahr, dass es in der Europäischen Union weiterhin einen datenschutzrechtlichen Flickenteppich geben wird – mit allen Problemen, die eigentlich durch die mit der Datenschutzreform angestrebten Vollharmonisierung überwunden werden sollten. Dies wäre insbesondere für diejenigen Unternehmen eine schlechte Nachricht, die grenzüberschreitende Dienste anbieten wollen. Es wäre aber vor allem eine schlechte Nachricht für die Bürgerinnen und Bürger, deren Grundrechte auf Privatsphäre und Datenschutz auch weiterhin nur unzureichend geschützt würden.

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 Bundesbeauftragte für Datenschutz gewählt. Seine zweite Amtszeit endete am 16. Dezember 2013. Seit September 2013 steht Schaar der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) vor.

Anmerkungen:

1 S. „Die neue Digital-Ministerin Dorothee Bär im Bild-Interview“, Bild v. 5.3.2018.
2 Vgl. Bundesministerium für Wirtschaft und Energie, Leitplanken Digitaler Souveränität, 2015, S. 5.
3 Bundesverfassungsgericht, Urteil v. 15.12.1983 (= BVerfGE 65, 1, S. 1).
4 Verordnung (EU) 2016/679 v. 27.4. 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 L 119/1 v. 4.5.2016.
5 Vgl. Schaar, Peter, Trügerische Sicherheit – Wie die Terrorangst uns in den Ausnahmezustand treibt, Hamburg 2017, S. 231 ff.
6 Die Welt v. 16.7.2013, „Friedrich erklärt Sicherheit zum ‚Supergrundrecht‘“.
7 Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft, unterzeichnet in Lissabon, EU-Amtsblatt C 306, 13.12. 2007.
8 Konvention zum Schutz der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention) v. 4. 11.1950.
9 EuGH, Urteil vom 8.4.2014, (verbundene Rechtssachen C-293/12 und C-594/12); Urteil v. 21.12.2016 (verbundene Rechtssachen 203/15 und 698/15).
10 EuGH, Urteil vom 6.10.2015 (Rechtssache C-362/14).
11 Richtlinie (EU) 2016/680 vom 20.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (EU-Amtsblatt L 119, S. 89).
12 Vgl. Rosenbach/Stark, der NSA Komplex, München 2014; Schaar, Überwachung total, Berlin 2014.
13 Art. 3a Abs. 2 Vertrag über die Europäische Union (AEUV), vgl. Anm. 7.
14 Europäische Kommission, Mitteilung „Der Schutz der Privatsphäre in einer vernetzten Welt – ein europäischer Datenschutzrahmen für das 21. Jahrhundert“, KOM (2012) 0009 v. 25.1.2012.
15 Legislative Entschließung des Europäischen Parlaments vom 12. März 2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE.
16 Vgl. Berichte der „Gruppe Informationsaustausch und Datenschutz (DAPIX)“ des Rats, Parlamentsdokumentation der Republik Österreich, https://www.parlament.gv.at.
17 Vgl. Spiegel online v. 2.12.2013, „EU-Ministerrat Deutsche Beamte bremsen Europas Datenschutz aus“, http://www.spiegel.de/netzwelt/netzpolitik/deutsche-beamte-bremsen-europas-datenschutz-aus-a-936704.html.
18 Europäische Kommission, Vorschlag für eine Verordnung zum Schutz natürlicher Personen Datenschutz-Grundverordnung), Mitteilung KOM (2012) 0011 v. 25.1.2012.
19 Vgl. insb. den Entwurf der Bundesregierung v. 1.2.2017 für ein Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DSGVO) und zur Umsetzung der Richtlinie (EU) 2016/680 (JI-RL) - Datenschutz-Anpassungs- und -Umsetzungsgesetz EU DSAnpUG-EU).
20 Netzpolitik.org v. 7.9.2016, „Innenministerium will rechtswidrige Datenverarbeitung bei Geheimdiensten sanktionsfrei machen“, https://netzpolitik.org/2016/innenministerium-will-rechtswidrige-datenverarbeitung-bei-geheimdiensten-sanktionsfrei-machen/.
21 Vgl. Anm. 13.
22 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) v. 30.6.2017, BGBl. I S. 2097).
23 Vgl. Stellungnahme der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) vom 23.11.2016, https://www.eaid-berlin.de/wp-content/uploads/2016/12/EAID-Stellungnahme-zum-DSAnpUG-EU_final.pdf.

24 § 24 Abs. 2 Satz 1 BDSG-alt. Diese Bestimmung galt gem. Abs. 6 auch für die zuständigen Landesdatenschutzbehörden.

25 Einundzwanzigster Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge (Einundzwanzigster Rundfunkänderungsstaatsvertrag), Bremische Bürgerschaft, Drs. 19/1282 vom 2.11.2017.