ISSN 0178-8930

G 20 141

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

RDV

4/2016

Recht der Datenverarbeitung

Herausgegeben von

Peter Gola · Andreas Jaspers · Rolf Schwartmann · Gregor Thüsing
in Kooperation mit der
Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn

Aufsätze

Kurzbeiträge

Rechtsprechung

Aus dem Inhalt

32. Jahrgang
August 2016
Seiten 171–228

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Zeitschrift für
Datenschutz-, Informations-
und Kommunikationsrecht

32. Jahrgang 2016
Heft 4
Seiten 171–228

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Beilagenhinweis GDD-Mitteilungen 4/2016; Verlag Dr. Otto Schmidt, Köln; DATAKONTEXT GmbH, Frechen; Nomos, Baden-Baden

Schriftleitung
Prof. Peter Gola (federführend)
RA Dr. Georg Wronka
RA Andreas Jaspers
RDV-Schriftleitung@gdd.de

Redaktionsanschrift
Birgit Koppitsch
Heinrich-Böll-Ring 10, 53119 Bonn
Telefon: (02 28) 96 96 75-00
Telefax: (02 28) 96 96 75-25
RDV-Redaktion@gdd.de

Erscheinungsweise
6 x jährlich

Bezugspreis

Jahresabonnement	€ 139,–
Einzelheft	€ 25,–

MwSt. im Preis enthalten
jeweils zzgl. Versandkosten

Bestellungen
DATAKONTEXT GmbH, Frechen
Jürgen Weiß
Augustinusstraße 9d
D-50226 Frechen-Königsdorf
Telefon: (0 22 34) 9 89 49-71
Telefax: (0 22 34) 9 89 49-32
E-Mail: weiss@datakontext.com
www.datakontext.com
Geschäftsführer: Dr. Karl Ulrich
Leitung: Hans-Günter Böse
HRB 337678

Abbestellungen
Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.

Verlag
DATAKONTEXT GmbH, Frechen
Augustinusstraße 9d
D-50226 Frechen-Königsdorf
Telefon: (0 22 34) 9 89 49-30
Telefax: (0 22 34) 9 89 49-32
www.datakontext.com
Geschäftsführung: Dr. Karl Ulrich;
Hans-Günter Böse
HRB 337678

Satz
alka mediengestaltung gmbh
Ottostraße 6, 53332 Bornheim-Sechtem

Druck
AZ Druck und Datentechnik GmbH
Heisinger Straße 16, 87437 Kempten

Anzeigenverwaltung
DATAKONTEXT GmbH, Frechen
Thomas Reinhard-Rief
Hultschiner Straße 8
D-81677 München
Telefon: (089) 21 83-89 35
Fax: (089) 21 83-96 02 33
E-Mail: reinhard@datakontext.com
www.datakontext.com
Geschäftsführer: Dr. Karl Ulrich
Leitung: Hans-Günter Böse
HRB 337678

Zeitschrift für
Datenschutz-, Informations- und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
32. Jahrgang 2016 Heft 4
Seiten 171–228

RDV
Recht der Datenverarbeitung

32. Jahrgang · August 2016 · Seiten 171–228

Editorial

Alles auf Deutsch

Buchbesprechungen stehen in der Regel auf den letzten Seiten der RDV. Heute aber einmal eine Ausnahme. Es geht um das soeben bei Riders Digest erschiene Computerlexikon „Alles auf Deutsch." Auf 288 Seiten werden die 777 wichtigsten Computerbegriffe erläutert: und alles auf Deutsch. Wenn man es liest, wird einem erst bewusst, wie die Digitalisierung unseres Lebens auch unsere Sprache verenglischt. Englische oder eher amerikanische Begriffe fließen in den Sprachgebrauch ein, weil Englisch quasi „Amtssprache" im IT-Bereich ist und keiner auf den Gedanken kommt, über einen deutschen Begriff nachzudenken oder ihn anzuwenden. Englische Begriffe zu digitalen Produkten und Entwicklungen dominieren die Sprache, und die Mehrzahl versteht sie nicht.

Dabei geht es nicht darum, dass man sich fragen mag, was „Spam" mit amerikanischen Dosenfleisch zu tun hat; warum „Phishing" kein Angelsport ist, warum ein „Hotspot" keine Wärme erzeugt oder warum ein „Cookie" kein Keks ist. Die (auch das) „E-Mail" steht für electronic mail und könnte auch simpel E-Post heißen. Wer denkt bei „Firewall" an eine Brandschutzmauer oder dass „online" heißt „auf Leitung" sein.

Vielmehr ist bemerkenswert, dass, wie eine aktuelle Umfrage belegt, diese Sprachwelt von der Mehrzahl nicht beherrscht wird. Von den abgefragten Begriffen hatte „Social Media" den höchsten Bekanntheitsgrad. Immerhin 64 Prozent der Befragten konnten mit dem Wort etwas anfangen. 38 Prozent gelang sogar eine Beschreibung. Vom „Smart Home" hatten 53 Prozent bereits gehört, ein Viertel der Antwortgeber hatte auch eine Definition parat. Eng verknüpft mit dem „Smart Home" ist das „Internet der Dinge", dessen Bekanntheitsgrad mit 21 Prozent deutlich geringer ist. Nur sieben Prozent hatten eine genauere Vorstellung davon, worum es sich dabei handelt. Dann sank der Bekanntheitsgrad. Obwohl Twitter eine vielzitierte Kommunikationsplattform, mit der auch die Bundeskanzlerin zum Volk spricht, ist, kannten nur 34 Prozent der Befragten die Begriffe „Tweet" und „Retweet". 18 Prozent wussten konkret, worum es sich dabei handelt. Andererseits brauchen neue Begriffe ihre Zeit. Von den abgefragten Begriffen am wenigsten bekannt (13 Prozent) waren Wearables – das gilt per se für die Übersetzung dieses englischen Mischworts und auch für seinen Inhalt. Diesen wiederum wussten nur fünf Prozent der Befragten zu erläutern.

Die Verenglischung verleitet aber auch zum Verdenglischen, d.h. der Formulierung deutscher Begriffe in das weltmännerische und IT-synonyme Englisch. Es gibt englische Wörter, die Engländer und Amerikaner gar nicht kennen: Dressman und Showmaster oder Pullover beispielsweise. Auch das Wort Handy gilt als rein deutsche Erfindung. Zumindest wird es so erzählt. So soll die Bezeichnung Handy ihre Geburtsstunde in Deutschland gehabt haben. Den Ruhm des Erfinder gebührt danach dem Postbeamten Josef Kedaj, der 1988 in der Bonner Generaldirektion der Deutschen Bundespost den Vorschlag einer unbekannten Mitarbeiterin genehmigt haben soll, das praktische neue Ding, das die Telekom gerade einführen wollte, Handy zu taufen. Aber wie auch immer, es ist mittlerweile ein deutsches Wort, das sonst niemand für ein Mobiltelefon – man hätte es auch Mobi nennen können – verwendet.

Prof. Peter Gola

Prof. Peter Gola
Mitherausgeber und federführender Schriftleiter der Fachzeitschrift RDV sowie Ehrenvorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn

Termin	Thema	Ort	Kontakt
03.11.2016	Grundlagen der Auftragsdatenverarbeitung	Köln	GDD e.V. und DATAKONTEXT
03.11.2016	Hacker-Tools für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
03.11.2016	Die Datenschutz-Grundverordnung	Nürnberg	GDD e.V. und DATAKONTEXT
07.11.2016	IT-Sicherheit für Dateschutzbeauftragte	Frankfurt/M.	GDD e.V. und DATAKONTEXT
07.-08.11.2016	Datenschutz Management – Teil 3	Berlin	GDD e.V. und DATAKONTEXT
10.11.2016	Verfahrensverzeichnis, Verarbeitungsübersicht, Vorabkontrolle	Stuttgart	GDD e.V. und DATAKONTEXT
16.11.2016	35. RDV-Forum	Köln	GDD e.V. und DATAKONTEXT
17.-18.11.2016	40. DAFTA	Köln	GDD e.V. und DATAKONTEXT
22.11.2016	Repetitorium GDDcert.	Köln	GDD e.V. und DATAKONTEXT
21.-23.11.2016	Das SAP-System für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
24.11.2016	Kontrolle von Auftragnehmern im Rahmen der Auftragsdatenverarbeitung	Köln	GDD e.V. und DATAKONTEXT
29.11.2016	Die Datenschutz-Grundverordnung	Münster	GDD e.V. und DATAKONTEXT
30.11.2016	Big Data-Analysen und der Datenschutz	Köln	GDD e.V. und DATAKONTEXT
28.11.–02.12.2016	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Berlin	GDD e.V. und DATAKONTEXT
05.12.2016	Pflichten bei Datenpannen – Wie Sie das Haftungsrisiko für Ihr Unternehmen reduzieren können	Köln	GDD e.V. und DATAKONTEXT
07.12.2016	ISO 27001 und Datenschutz	Köln	GDD e.V. und DATAKONTEXT
07.12.2016	SAP-Funktionen für den Datenschutz	Köln	GDD e.V. und DATAKONTEXT
12.12.2016	Zertifizierung der betrieblichen Datenschutzbeauftragten (GDDcert.)	Köln	GDD e.V. und DATAKONTEXT
30.-31.01.2017	GDD-Winter-Workshop	Garmisch-Partenkirchen	GDD e.V. und DATAKONTEXT
14.02.2017	Datenschutz und Videoüberwachung – Was geht und was geht nicht?	Köln	GDD e.V. und DATAKONTEXT
15.02.2017	Personalprozesse datenschutzkonform organisieren	Köln	GDD e.V. und DATAKONTEXT
13.-17.02.2017	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Bonn	GDD e.V. und DATAKONTEXT
21.02.2017	Datenschutz Aktuell	Köln	GDD e.V. und DATAKONTEXT
22.-23.02.2017	3. Göttinger Forum IT-Recht	Göttingen	Institut für Wirtschaftsrecht der Universität Göttingen www.goettingen-itrecht.de

DATAKONTEXT GmbH, Telefon: 0 22 34/9 89 49 40

Aufsätze

Sabine Leutheusser-Schnarrenberger

Wie kommt der Datenschutz aus der Defensive?*

Sind die Datenschützer die Spielverderber der Digitalisierung, dieser technologischen Entwicklung, die alle Lebensbereiche durchdringt? Ist das Verteidigen der informationellen Selbstbestimmung des Einzelnen und seiner Privatsphäre heute digital und online nur noch von gestern, aus einer alten Zeit, in der Spießigkeit und Heimlichtuerei weit verbreitet waren und in der den Grundrechten mit ihrer Abwehrfunktion gegenüber staatlichen Eingriffen eine besondere Bedeutung zukam? Ist Datenschutz und Privatsphärenschutz mit dem von einigen Protagonisten verkündeten Post-Privacy-Zeitalter nicht obsolet geworden und einer totalen Transparenz gewichen?

Auch 2016 gilt das Grundgesetz, gelten die Grundrechte in Art. 1 bis 19, und es unterscheidet nicht zwischen digital und analog. Das Internet setzt rechtlich nicht die Grundrechte außer Kraft.

Aber noch nie hat seit der Industrialisierung und Automatisierung eine so umfassende technische Entwicklung stattgefunden, wie es die Digitalisierung ist. Sie führt zu nicht mehr überschaubaren Informationsmassen. Es werden immer mehr Daten der Bürgerinnen und Bürger mit und ohne ihr Wissen erfasst, analysiert, vernetzt und verarbeitet, um das letztendlich auf Werbung basierende Geschäftsmodell vieler global agierender Konzerne zu verfeinern und auszubauen.

Was das tatsächlich für die Arbeitsbedingungen und Arbeitsplätze, für das Autofahren, für das vernetzte und sich selbst vernetzende Home, für die Medizin und Gesundheit und natürlich für die Industrie 4.0. bedeutet, kann heute noch nicht vollständig überblickt werden. Setzen die Algorithmen, setzen die intelligenten Maschinen das Recht außer Kraft? Gibt es einen Wettstreit zwischen Technik und demokratischer Rechtsetzung?

Eric Schmidt, der Vorstandsvorsitzende von Alphabet, der Google Holding, sagt es so:

„ Das Internet ist das größte Anarchismusexperiment aller Zeiten. Die Onlinewelt, in der Hunderte Millionen von Menschen digitale Inhalte produzieren und konsumieren, wird kaum durch Gesetze beschränkt... Das Internet ist der größte unregulierte Raum der Welt“.[1]

I. Das Internet ist kein rechtsfreier Raum

Es ist zwar richtig, dass es für die rasante digitale Entwicklung keinen globalen Rechtsrahmen der Vereinten Nationen gibt, also kein weltweites Datenschutzgesetz, aber es ist nicht zutreffend, dass es keinerlei Recht gäbe, das nicht auch die digitale Entwicklung bindet. Das Internet ist natürlich kein rechtsfreier Raum, diese Binsenweisheit müsste inzwischen jedem bekannt sein. Das Recht wird, da häufig national, nur schwerer durchsetzbar.

Dort, wo die digitale Welt eine Abbildung in der analogen Welt findet, kommen wir mit den bestehenden Gesetzen und unserer gewohnten Art und Weise der Gesetzgebung deshalb ganz gut zurecht.

Es fehlt in Deutschland nicht in erster Linie an strafrechtlichen oder nebenstrafrechtlichen Regelungen, auf deren Basis der Staat seiner verfassungsrechtlichen Verpflichtung nachzukommen im Stande ist, die Grundrechte auch vor Beeinträchtigen durch andere zu schützen. Die dennoch zu konstatierenden Effektivitätsdefizite der schutzrechtlichen Dimension der Grundrechte sind vielmehr auf Spezifika der digitalen Kommunikation zurückzuführen, die eine Anwendung und, vor allem, eine effektive Durchsetzung des bestehenden Rechts erschweren. Denken Sie nur an das Cybermobbing.

Das Recht läuft aber angesichts der Unübersichtlichkeit der Auswirkungen der Digitalisierung zwangsläufig den Entwicklungen in vielen Bereichen hinterher.

1. Disruption als Grundsatz der Digitalisierung

Das der Geschäftspolitik global agierender Konzerne zugrunde liegende Prinzip der Disruption, der Zerstörung des Althergebachten, um etwas Neues, etwas Innovatives aufzubauen – in den Worten von Eric Schmidt ist das der kreative Anarchismus – beinhaltet gerade auch permanente Rechtsverstöße, wie z.B. bei Uber, Airbnb u.a. sehr deutlich geworden ist.

Geht Innovation nur mit Rechtsbruch? Muss, wer die Vision einer virtuellen Welt neben und teilweise anstatt der

* Aufsatz zum Vortrag des 9. GDD-Sommer-Workshops vom 01.-03.08.2016 in Timmendorfer Strand.

1 Die Vernetzung der Welt, S. 13/14.

physischen Welt verfolgt, quasi die Rechtsverletzung billigend in Kauf nehmen?

Wer das bejahen würde, würde den demokratischen Gesetzgeber bewusst missachten und das letzte Vertrauen der Bürgerinnen und Bürger in unseren liberal verfassten Rechtsstaat verlieren. Dann würde wirklich das Recht des wirtschaftlich Stärkeren an die Stelle des Rechts für alle treten. Das wäre die totale Kommerzialisierung des Rechts. Das ist kein Model für Good Old Europe.

Also ist der Gesetzgeber gefordert zu entscheiden, ob er diese auf Big Data, auf Milliarden finanzieller Ressourcen und auf aggressiver Frechheit basierenden Geschäftsmodelle mit allen Mitteln des Rechts bekämpft oder ob er das Recht den neuen technologischen Entwicklungen anpasst.

Da gibt es nur den goldenen Mittelweg: Verstöße gegen die Rechtsordnung müssen geahndet werden, wie das bei Uber und der privaten Ver- bzw Untervermietung von Wohnraum für Touristen in erheblichem Umfang geschieht. Gleichzeitig muss die Politik entscheiden, dass sie den fairen Wettbewerb zwischen den unterschiedlichen Anbietern ermöglichen will, und dann zügig für alle gleich geltende, angepasste Rechtsgrundlagen schaffen.

Eines steht fest: Die digitale Revolution ist unumkehrbar, aber sie ist noch längst nicht abgeschlossen. Die technologische Basis wird immer leistungsfähiger, die Geschwindigkeit der Geräte und die Rechenleistung werden weiter zunehmen. Nach dem Moore`schen Gesetz, einer Faustregel der Technologiebranche, verdoppelt sich die Geschwindigkeit der Prozessoren alle 18 Monate. Demnach wären die Computer im Jahr 2025 etwa 64 Mal schneller als 2013. Speicherkapazitäten kennen also kaum noch Grenzen. Und eine weitere Faustregel sagt, dass sich die Datenmengen, die über die schnellen Glasfaserverbindungen übertragen werden, alle neun Monate verdoppeln.

II. Daten, Daten, Daten

Wie viele nicht müde werden zu betonen, sind Daten das Schmieröl, das Gold oder die Währung der Digitalisierung. Ohne sie wären die Entstehung milliardenschwerer global tätiger Konzerne und die immer neuen Dienstleistungsangebote undenkbar.

Personenbezogene Daten, und das sind die interessanten Daten bei den Geschäftsmodellen der global agierenden IT-Konzerne mit zielgenauen Angeboten, gehören der Person, der sie zuzuordnen sind und die unter anderem über ihre Persönlichkeit (Geburtsdatum, Adresse, Geschlecht), ihr Verhalten (Telekommunikationsdaten, Passagierdaten, Kontodaten) und ihre Internetaktivitäten (Online-Shopping, Chatrooms, soziale Medien) Aufschluss geben. Viele Daten sind mit Zusatzwissen rückverfolgbar auf eine Person wie die IP-Adresse.

In den vergangenen zehn Jahren hat sich die Zahl der mit dem Internet verbundenen Geräte auf sechs Milliarden verdreifacht, sie wird sich in den kommenden Jahren noch einmal verdreifachen. Vor allem rücken diese Geräte immer näher an den Menschen heran, vom Computer in der Ecke über den Laptop in der Tasche bis zum Smartphone in der Hand und zu den Gadgets, die als Wearables bezeichnet werden und immer dicht am Körper dabei sind.

Am Beispiel der Gesundheitsdaten sieht man den tiefgreifenden Wandel. Gesundheitsdaten des Einzelnen werden milliardenfach gespeichert – in Arztpraxen, Krankenhäusern, auf Fitness-Plattformen. Inzwischen gibt es weltweit 40 000 Gesundheitsapps. Die Apple Watch soll vielen Menschen helfen, ein gesünderes Leben zu leben. Herz-Kreislauf-Erkrankungen, Diabetes, Bluthochdruck sowie einige Krebserkrankungen sind verantwortlich für mehr als die Hälfte aller Todesfälle. Die häufigsten Ursachen lassen sich an einer Hand abzählen: Mangel an Bewegung, fehlerhafte Ernährung, übermäßiger Alkoholkonsum und Rauchen erhöhen wesentlich das Risiko für die genannten Erkrankungen. Diese Faktoren sind vermeidbar, aber viele Menschen tun sich schwer, ihren Lebensstil entsprechend zu ändern. Das ist der Ansatz für Überlegungen vieler Anbieter, besonders der Krankenversicherungen, mit innovativen Angeboten zu helfen und die Erfassung der Daten attraktiv zu machen.

Und der Datenumfang ist immens. Ununterbrochen messen Sensoren in der Uhr den Puls des Nutzers, zählen jeden seiner Schritte, errechnen verbrannte Kalorien, Zuckerpegel, Gewichtsveränderungen. Eine Fitness-App sagt jeden Tag, ob der Nutzer sein Soll für das gesunde Leben erfüllt hat. Sämtliche Daten werden in eine Anwendung namens Health App auf dem I-Phone gespeist, die auch Gesundheitswerte aus anderen Apps erfassen und so ein umfangreiches persönliches Vitalprotokoll erstellen kann. Apple will zur zentralen Speicherstelle werden, an der alle Gesundheitsdaten zusammenlaufen. Dazu wird die Health App auf jedem I-Phone vorinstalliert. Dank der Selbstkontrolle per Wearables, Smartwatch und Fitness-App können Versicherungen ihre Kunden mit Bonusleistungen locken, wenn sie sich gesundheitsbewusst verhalten, die nach Umfragen für fast 70 % der Bürgerinnen und Bürger attraktiv sind. Die Generali-Versicherung und der südafrikanische Versicherungskonzern Discovery gehören zu den Anbietern.

Mithilfe dieser riesigen Datenmengen, die zum großen Teil die Betroffenen selbst über die sozialen Medien oder Quantified Self, das sog. Selftracking (pausenlose Körpervermessungsbewegung), geliefert haben, können die Kassen individuelle Risikoprofile erstellen. Wer im Netz stolz über seine neue Leidenschaft „ Fallschirmspringen „ berichtet oder Fotos seiner letzten Sauftour postet, könnte sich mit der Konsequenz konfrontiert sehen, höhere Beiträge zahlen zu müssen. Am Maßstab einer Beitrags- oder Belastungsgerechtigkeit lässt sich gegen eine stärkere individualisierte Zumessung von Risiken wenig einwenden.

Aber Big Data kann und will mehr. Inwieweit führen Risiken, für die ein Individuum nichts kann, zu höheren Prämien? Ob und inwieweit darf Big Data genutzt werden, um Menschen zu kontrollieren und zu manipulieren? Was in an-

deren Staaten bereits erfolgt, ist wegen der Regelungen zur engen Zweckbindung und des Grundsatzes der Direkterhebung beim Kunden in Deutschland so nicht möglich.

Die Gesundheitsapps, das Auto als rollendes Smartphone, das Smart Home, und online Bankgeschäfte jeglicher Art sind nur einige Aspekte des immer transparenter werdenden Verhaltens der Menschen. Mittels Algorithmen werden die erfassten Daten von global agierenden Konzernen für ihre Geschäftszwecke analysiert und vernetzt. Das betrifft gerade nicht nur statistische, technische Daten, sondern vorwiegend Daten mit Bezug zu Personen, die aus ihrem online- und Surfverhalten mit und ohne ihr Wissen gewonnen und zu Profilen zusammengeführt werden, um sie dann z.B. zum Angebot gezielter Werbeplätze zu verwenden. Durch angelegte Verhaltensmuster, also Datenraster, künftiges Verhalten vorhersehbar zu machen und damit dem Nutzer ein auf ihn zugeschnittenes Angebot von Produkten und Dienstleistungen präsentieren zu können, gehört zu einem der immer erfolgreicher werdenden Geschäftsmodelle. An diesem Megatrend der kommenden Jahre wollen viele mitverdienen: die internationalen IT-Konzerne, die Energiewirtschaft, die Gesundheitsbranche, die Automobil- und Transportindustrie, die Medien, die Telefonhersteller und die Versicherungen.

III. Informationelle Selbstbestimmung und Grundrechtsschutz

Die Kehrseite dieser Technik und der auf Daten basierenden Geschäftsmodelle ist die Gefahr für die Selbstbestimmung des Einzelnen und für den Schutz seiner Privatsphäre. Wem gehören die Daten und wer darf unter welchen Voraussetzungen über sie zu welchen Zwecken verfügen?

Je mehr personenbezogene Daten aus- und verwertet werden, umso mehr wird die Privatsphäre des Einzelnen eingeschränkt. Auch wenn sich die Grenze zwischen öffentlich und privat durch die Digitalisierung verschieben mag, gehört die Privatsphäre unverzichtbar zur Persönlichkeit eines jeden Menschen. Immerhin messen nach einer repräsentativen Umfrage 56 % der Bürgerinnen und Bürger dem Schutz ihrer Daten und ihrer Privatsphäre in der Digitalisierung große Bedeutung bei. Denn anders als in der analogen Zeit hinterlassen wir digital eine Unmenge an Datenspuren, von denen der Nutzer gar nichts weiß und die vernetzt und analysiert Profilbildungen und Einordnungen zulassen, wie es zu Zeiten der Lochkarten unvorstellbar war.

Privatsphäre und Datenschutz sind in Deutschland Grundrechte und haben deshalb eine große verfassungsrechtliche Bedeutung.

Das Bundesverfassungsgericht hat im Volkszählungsurteil 1983 die grundsätzlichen Kernelemente des Rechts auf informationelle Selbstbestimmung entwickelt. Der Ausgangsfall erscheint rückblickend marginal. Die gesammelten Daten bezogen sich ua auf Wohnungsgrößen, Regionen, aber auch auf eine zentral zu verwendende Personenkennziffer, die ihren Träger, also jedem Menschen in Deutschland, ein Stück gläserner machte.

Das Bundesverfassungsgericht hat mit der Grundsatzentscheidung zur Volkszählung 1983[2] unmissverständlich erklärt, dass zum allgemeinen Persönlichkeitsrecht das Recht des Einzelnen gehört, selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte von ihm preisgegeben werden. Es hat die Gefahren gesehen, die dem Persönlichkeitsrecht unter den Vorzeichen der automatisierten Datenverarbeitung drohen, und reklamiert, dass der einzelne davor besonders geschützt werden muss.

Eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung, in der der Bürger nicht mehr wissen könne, wer was wann und bei welcher Gelegenheit über ihn weiß, ist mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar. Wer unsicher sei, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, werde versuchen, nicht durch solche Verhaltensweisen aufzufallen. ...Dies würde nicht nur die individuellen Entwicklungschancen des einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen, demokratischen Grundordnung sei. Hieraus folge: Freie Entfaltung der Persönlichkeit setze unter den modernen Bedingungen der Datenverarbeitung den Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz sei daher von dem Grundrecht des Art. 2 Abs.1 GG i.V.m. Art.1 Abs. 1 GG umfasst.

Das Datenschutzrecht wird also aus der Unantastbarkeit der Menschenwürde abgeleitet, die alle staatliche Gewalt bindet und als objektive Wertordnung mittelbar Wirkung im Verhältnis der Bürger untereinander und im Verhältnis zu den Unternehmen entfaltet.[3] Das Grundrecht gewährleistet insoweit die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[4]

Ist das eine Entscheidung aus einer anderen Zeit ohne heutige Relevanz? Geht das denn heute überhaupt? Erklärung der notwendigen Einwilligung in die Datenverarbeitung mittels Fax gehören doch in die 90iger Jahre und nicht in das Zeitalter der Digitalisierung.

Weit gefehlt. Damals haben die Richter vorausschauend geurteilt, auch wenn die Dynamik und Dimension der Digitalisierung nicht vorhersehbar war.

Die damals aufgestellten Anforderungen an Eingriffe in das Recht auf informationelle Selbstbestimmung sind heute genauso aktuell, vielleicht sogar noch bedeutsamer. Es geht um die grundgesetzlichen Freiheitsrechte, die die Grundlage

2 BVerfGE vom 15. Dezember 1983 - Az. 1BvR 209/82.

3 Lüth–Urteil des BVerfG.

4 BVerfG 65, 1 - 71.

unserer Demokratie darstellen und die durch technische Entwicklungen nicht ausgehöhlt werden dürfen. Ihnen liegt das Menschenbild des selbstbestimmten Individuums zu Grunde, das nicht Objekt, sondern Subjekt staatlichen und wirtschaftlichen Handels ist. Wenn manche IT-Firmen die Auffassung vertreten, das sei alles eine alte Idee, die Rechte des einzelnen Bürgers hätten sich überholt, mit der neuen Technik wolle man etwas Neues ausprobieren, was nicht so bürokratisch wie die Demokratie sei, dann wird damit das kantische Menschenbild der Aufklärung aufgegeben. Wenn wir nicht wollen, dass schleichend durch diese technologische Entwicklung unsere fundamentalen Werte ausgehöhlt werden, dann brauchen wir den richtigen Gestaltungsrahmen, um Freiheit im digitalen Zeitalter so leben zu können, dass die Rechte des anderen wie sein Persönlichkeitsrecht, sein Recht auf Schutz der Privatsphäre, sein Selbstbestimmungsrecht nicht unverhältnismäßig eingeschränkt werden.

Wie kann dieses Recht durchgesetzt werden? Ist der Gesetzgeber gefordert, sind es die Gerichte oder ist es nicht zu allererst Aufgabe des Nutzers, alles zu tun, um seine eigenen Rechte zu schützen? Verschlüsselung, weniger Posts und Tweets, kein Unterzeichnen der Datenschutzerklärungen der Konzerne? Ist das die Antwort?

Die Antwort ist ein auch ausländische Konzerne bindender europäischer Gestaltungsrahmen, das sind verbindliche Datenschutzstandards und die Stärkung der Grundrechte durch höchstrichterliche Rechtsprechung.

IV. Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH)

Neben dem Bundesverfassungsgericht hat sich besonders der EuGH zum Verteidiger der Grundrechte entwickelt, und damit der EU-Grundrechte-Charta Wirkung verliehen. Drei Entscheidungen aus jüngster Zeit haben den Datenschutz und die Persönlichkeitsrechte der Nutzer gestärkt.

1. Die anlasslose Vorratsdatenspeicherung

Die Entscheidung vom 2014 setzte einen vorläufigen Schlusspunkt unter die unendliche Geschichte der anlasslosen Vorratsdatenspeicherung, das umstrittenste Vorhaben der EU-Kommission der letzten Jahre, eine Geschichte des juristischen Scheiterns des deutschen und europäischen Gesetzgebers. Es geht um die Verpflichtung des Staates, alles zu unterlassen, was die Privatsphäre und das Datenschutzrecht der Bürger unverhältnismäßig einschränkt.

Das am 1. Januar 2008 in Kraft getretene Gesetz zur Speicherung von Kommunikationsverbindungsdaten wurde auf die dagegen eingelegten Verfassungsbeschwerden vom Bundesverfassungsgericht am 2. März 2010 als verfassungswidrig verworfen.[5] Die Daten mussten unverzüglich gelöscht werden, da das Gesetz zur anlasslosen Vorratsdatenspeicherung in dieser Ausgestaltung das Grundrecht auf Schutz des Post- und Fernmeldegeheimnisses und auf Schutz der Vertraulichkeit der Kommunikation verletzt. Bei Beachtung der Vorgaben der Entscheidung ist eine Regelung zur Speicherung dieser Daten nicht grundsätzlich untersagt.

Angesichts der jahrelangen intensiven und streitigen Debatte über die anlasslose Vorratsdatenspeicherung aller Telekommunikationsverbindungsdaten sollte man annehmen, dass die Behauptungen der Unverzichtbarkeit der anlasslosen Vorratsdatenspeicherung durch eindeutige rechtstatsächliche Untersuchungen belegt seien. Denn neben den gravierenden Eingriffen in das Kommunikationsverhalten aller Bürgerinnen und Bürger durch die massenweise Speicherung der dadurch entstandenen Daten verursacht diese gesetzliche Verpflichtung millionenfache Investitionen der Telediensteanbieter, die vom Staat weder teilweise noch ganz erstattet werden. Zudem sind diese Datenberge für den Zugriff von Geheimdiensten und Hackern äußerst interessant, die Missbrauchsgefahr groß.

Vor diesem Hintergrund sollte mit dem bahnbrechenden Urteil der Großen Kammer des EuGH, mit dem die EU-Richtlinie von 2006 für mit der EU-Grundrechte-Charta unvereinbar und deshalb als rechtswidrig aufgehoben wurde, eigentlich ein juristischer Schlusspunkt unter diese politische Debatte und unter diese in der Geschichte der Europäischen Union wohl umstrittenste Gesetzgebung gesetzt worden sein.

Der vom irischen High Court und dem österreichischen Verfassungsgerichtshof wegen der bei ihnen anhängigen Klagen einer NGO, einer Landesregierung und von mehr als 11.000 Einzelpersonen angerufene EuGH stellt unmissverständlich in seiner Entscheidung vom Mai 2014[6] fest, dass die massenweise anlasslose Speicherung von Daten sowohl das Recht auf Schutz der Privatheit gemäß Art. 7 als auch den Schutz der persönlichen Daten gemäß Art. 8 der Charta der Grundrechte berührt und den Verhältnismäßigkeitsgrundsatz nach Art. 52 Abs. 1 der Charta verletzt.

Die in der Richtlinie aufgestellte Verpflichtung zur Speicherung und die Erlaubnis zur Verarbeitung stellen als solche einen besonders schwerwiegenden Eingriff in diese beiden Grundrechte von großem Ausmaß dar. Die immer wieder gern verwandte Argumentation, dass nicht die Speicherung der Daten, sondern erst der Zugang zu ihnen und die weitere Verwendung und Verarbeitung grundrechtsrelevant seien, ist damit vom EuGH klar zurückgewiesen worden. Wie schon das Bundesverfassungsgericht in seiner Rechtsprechung herausgearbeitet hat, entsteht durch die unterschiedslose massenweise Speicherung der Daten auf Vorrat bei den ca. 500 Millionen Bürgerinnen und Bürgern in der Europäischen Union ein diffuses bedrohliches Gefühl der permanenten Überwachung und damit des Vertrauensverlustes in die Vertraulichkeit der Kommunikation informationstechnischer Systeme. Diese Entgrenzung der staatlichen

5 BVerfG, DuD 2010, 409 ff.

6 EuGH Urteil vom 8. April 2014 – C 293/12, C-594/12, DuD 2014, 488 ff.

Überwachungstätigkeit unter Benutzung privater Diensteanbieter macht die Intensität des Eingriffs aus. Auch wenn der EuGH die generelle Geeignetheit bejaht, da es im Interesse des Gemeinwohls liege, organisierte Kriminalität und Terrorismus zu bekämpfen und wegen der wachsenden Bedeutung elektronischer Kommunikationsmittel die Vorratsdatenspeicherung theoretisch ein nützliches Mittel sein könne, lehnt er die in der EU-Richtlinie geregelte anlasslose Speicherung der Telekommunikationsdaten klar ab, da sie nicht auf das unbedingt notwendige Maß beschränkt ist und keinen unmittelbaren oder noch nicht einmal einen mittelbaren Bezug zu einer Handlung hat, die zur Strafverfolgung Anlass gibt. Weiter rügt er zu Recht den fehlenden Zusammenhang zwischen den verpflichtend zu speichernden Daten und der tatsächlichen Bedrohung der öffentlichen Sicherheit. Mit seiner Kritik an der fehlenden geografischen und personellen Beschränkung der zu speichernden Daten erteilt er der anlasslosen Vorratsdatenspeicherung eigentlich eine endgültige Absage. Denn nur wenn es konkrete Kriterien für einen Anhaltspunkt oder konkreten Tatverdacht gibt, kann der Personenkreis eingegrenzt und auch räumlich ein engerer Rahmen gezogen werden.

Die Informationsgesellschaft lebt eben nicht davon, Grundrechte zu verzehren. Die anlasslose staatliche Ausspähung und Speicherung der Kommunikation darf nicht Normalität werden. Das ist die Lehre des Luxemburger Urteils. Der EuGH versteht sich als der Hüter der Grundrechte, dem die Bürgerinnen und Bürger vertrauen können sollen. Mit solcher Rechtsprechung kommt der Datenschutz aus der Defensive.

Das hat die Bundesregierung nicht davon abgehalten, unter der täuschenden Bezeichnung sog. Höchstspeicherfristen einen Gesetzentwurf zur anlasslosen Speicherung der meisten Telekommunikationsverbindungsdaten vorzulegen und zu behaupten, dies sei zum Vorgehen gegen Terrorismus erforderlich. Seit dem 18. Dezember 2015 ist das Gesetz in Kraft. Auch wenn gewisse Vorgaben des Bundesverfassungsgerichtes berücksichtigt werden, handelt es sich wieder um eine ohne jeden Anlass verpflichtende Speicherung für 4 bzw 10 Wochen. Ausgenommen werden lediglich Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitspflichten unterliegen. Für Berufsgeheimnisträger gilt dagegen ein bloßes Abrufverbot der Daten durch die Strafverfolgungsbehörden. Mit dieser Regelung wird verkannt, dass die anwaltliche Verschwiegenheit für die betroffenen Mandanten von vergleichbarer existenzieller Bedeutung ist. Das Speichern der Daten, wann, wer wie lange mit seinem Rechtsanwalt telefoniert hat, widerspricht dem verfassungsrechtlich gebotenen Vertrauensschutz. Der Schutz der anwaltlichen Kommunikation ist mit einem bloßen Verwendungs- und Verwertungsverbot nicht gewährleistet, die bloße Speicherung bietet Missbrauchspotenzial. Es muss der Schutz der Berufsgeheimnisträger deshalb schon „by design„ in die technische Einrichtung der Vorratsdatenspeicherung integriert werden.

Den allgemeinen Äußerungen von Regierungsmitgliedern zu mehr Datenschutz und verbale Bekenntnisse zum Grundrechtsschutz sind nicht wirklich überzeugend, wenn gleichzeitig im Gesetzgebungsverfahren der Datenschutz und der Schutz der Privatsphäre gegenüber dem Vorrang angeblicher größerer Sicherheit zurückstehen müssen.

Dieses nationale Gesetz erlaubt mit Blick auf das Bundesverfassungsgericht die Speicherung von Daten nur auf Servern in Deutschland. Das wiederum wurde von der EU-Kommission kritisiert.

Gegen dieses Gesetz ist von einigen Fraktionen, Verbänden und von einigen Politikern der FDP, vertreten durch Prof. Amadeus Wolff, erneut Verfassungsbeschwerde eingelegt worden. Hauptkritikpunkte sind die Speicherung der Daten auch von Berufsgeheimnisträgern, also von Anwälten, Ärzten, Journalisten, die mit der Speicherung der Funkzellen möglichen Bewegungsprofile unbescholtener Bürger, die Speicherung der SMS, wohl auch ihrer Inhalte und die Verletzung des Bestimmtheitsgrundsatzes.

Eine spannende juristische Frage wird sein, wieweit das Bundesverfassungsgericht die mit der Entscheidung des EuGH konkretisierte EU-Grundrechte-Charta zu beachten hat.

Das Brief-, Post- und Fernmeldegeheimnis darf keine museale Erinnerung an graue Vorzeiten werden, in denen man noch unbefangen Kontakte mit anderen Menschen haben konnte. Es muss seine Kraft gerade auch unter den technischen Bedingungen unserer heutigen Gesellschaft entfalten können. Um dazu die verfassungsrechtlichen Grenzen aufzuzeigen, ist es notwendig, erneut nach Karlsruhe zu gehen.

V. Das sog. Recht auf Vergessenwerden

Das Internet eröffnet weltweiten, weitestgehend grenzenlosen Kommunikationsverkehr und Zugang zu Informationen. Einmal gespeicherte personenbezogene Daten sind immer wieder auffindbar. Was also an den digitalen Kommunikationstechnologien bekümmert und auch bekümmern muss, ist der sorglose und missbräuchliche Umgang mit den Möglichkeiten, die die digitalen Kommunikationstechnologien zur Verfügung stellen. Es geht also eigentlich nicht ums Vergessen. Es geht vielmehr um die Destruktion der Vorhaltbarkeit individuellen oder kollektiven Verhaltens. Dieser Destruktion haftet ein ethisches Moment an, nämlich das der Anerkennung der personalen Würde und Freiheit des einzelnen, wie es in unserem Grundgesetz, in dessen Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 und der EU-Grundrechte Charta seinen normativen positiv-rechtlichen Ausdruck gefunden hat. Anders ausgedrückt: Es ist nicht irgendeine sogenannte Tugend des Vergessens, deren Verlust zu befürchten wäre,

es ist vielmehr die ethische und rechtliche Grenzen überschreitende individuelle und kollektive Handhabung der Möglichkeiten der digitalen Kommunikation, derer wir uns erwehren müssen. Es geht darum, mit den Mitteln des Rechts die Würde, die Freiheit und die Selbstbestimmung des Einzelnen sowie deren grundrechtliche Konkretisierungen gegen Verletzungen zu schützen. Das ist, angesichts der beschränkten Reichweite nationaler Gesetzgebung, angesichts der immensen Widerstände gegen internationale Übereinkünfte und angesichts der starken ökonomischen Interessen, die grundrechtsschützenden Regelungen entgegenstehen, schwer genug.

Und deshalb hat nach meiner Überzeugung das Urteil des Europäischen Gerichtshofs einen deutlichen Schritt in diese, richtige Richtung getan.

Es hat der millionenfachen Verbreitung privater Informationen, auch wenn sie zutreffend sind, mit Hilfe des Datenschutzes einen begrenzt wirkenden Riegel vorgeschoben.

In seiner Entscheidung vom 13. Mai 2014 zum sog. Recht auf Vergessenwerden[7] hat der Gerichtshof der Europäischen Union (EuGH) eine bahnbrechende Weichenstellung vorgenommen: Suchmaschinenbetreiber werden neben den Contentverantwortlichen für den Schutz der Privatsphäre der betroffenen Nutzer und ihren Datenschutz in die Verantwortung genommen. Sie müssen mittels namensbasierter Recherche gefundene Links zu Online-Artikeln dann löschen, wenn die millionenfache globale Verbreitung der Artikel und der damit verbundenen potenzierten Rechtsverletzung im Vergleich zur gedruckten Auflage einer Lokalzeitung den Datenschutz und die Persönlichkeitsrechte der Betroffenen verletzt. Die Zeit, in der man den Eindruck haben konnte, das Recht kapituliere vor den Großen des Internets, geht damit zu Ende.

Ganz einfach heißt das: Google, Apple, Facebook, Twitter, Amazon, Microsoft und viele andere Unternehmen können sich mit ihrem Sitz in den USA nicht länger dem europäischen Datenschutz entziehen.

Das war ein Kulturschock, auch für Google, das mit der EuGH-Entscheidung verurteilte Unternehmen. Seine Philosophie geht von der weltumspannenden Transparenz und von dem Wunsch der Bürgerinnen und Bürger aus, möglichst vieles von vielen Menschen wissen zu wollen und technisch einfach, barrierefrei und zügig Zugang zu Informationen zu haben. Datenschutz stand bisher bei diesen weltweit agierenden IT-Konzernen nicht als wichtiger zu achtender Wert ganz oben. Das von ihnen immer wieder propagierte totale Recht auf Wissen gibt es nicht, sondern es gibt ein Recht auf Zugang zu Informationen, die im öffentlichen Interesse liegen und nicht die Privatsphäre des Bürgers verletzen.

Mit der Einbeziehung von Suchmaschinen in den Schutz der Privatsphäre der Nutzer hat der EuGH deutlich gemacht, dass Suchmaschinen nicht nur unbeteiligte Vermittler, sog. Gatekeeper sind, sondern mit der Erfassung der millionenfachen Daten und ihrer Aufbereitung Beteiligte, und deshalb auch Verantwortung tragen. Aus der Begründung der Entscheidung ist ziemlich deutlich zu entnehmen, dass der Europäische Gerichtshof international agierende Konzerne für ihre Tätigkeit innerhalb der Europäischen Union zur Einhaltung europäischen Rechts verpflichten will. In Auslegung der europäischen Datenschutzrichtlinie hat der Gerichtshof damit bereits das Marktortprinzip entwickelt, das der europäische Gesetzgeber nunmehr in der Ende letzten Jahres verabschiedeten Datenschutzgrundverordnung, die mit Inkrafttreten im Jahr 2018 die europäische Datenschutzrichtlinie ablösen wird, verankert hat. Damit entfällt die beliebte juristische Argumentation, mangels Sitz in der EU gelte das „strenge“ europäische Datenschutzrecht nicht. Und es wird der mit der Sitzwahl eines Konzerns in der EU verbundenen Absicht, sich das auf niedrigstem Niveau bewegende Datenschutzrecht eines EU-Mitgliedstaates auszusuchen, ein Riegel vorgeschoben. Es wird künftig datenschutzrechtlich nichts mehr bringen, sich in Dublin anzusiedeln, wie das derzeit Facebook, Google und viele andere internationale Konzerne tun.

Welche Bedeutung der EuGH dem Datenschutz zumisst, zeigt sich an diesen beiden Grundsätzen:

1. Wirtschaftliche Interessen der Suchmaschinenbetreiber haben bei diesen Löschanträgen generell keinen Vorrang. Die digitale Kommunikation verschiebt zwar die Abgrenzung zwischen privat und öffentlich, aber der Schutz der eigenen Daten und der Privatsphäre werden und dürfen nicht aufgegeben werden. Ihm wird vom EuGH ein grundsätzlicher Vorrang vor den wirtschaftlichen Interessen der Suchmaschinenbetreiber eingeräumt, es sei denn, es liegt ein überwiegendes öffentliches Interesse an dem Zugang zu diesen Daten durch namensbasierte Recherche vor. Damit muss eine Abwägung zwischen dem berechtigten Schutz des Datenschutzsubjekts an einer zweckgebundenen Verwendung seiner Daten und dem Interesse der Öffentlichkeit an Information stattfinden. Nicht die mit teilweiser marktbeherrschender Stellung agierenden IT-Konzerne haben die uneingeschränkte Definitionshoheit darüber, was von ihnen an vorgegebenen Informationenverarbeitet und verbreitet wird, sondern sie sind an die europäisch geltenden Grundrechte gebunden. Es gilt nicht ihr Verständnis von allumfassender Transparenz und des behaupteten Rechts, von jedem alles wissen zu dürfen (so Eric Schmidt, der Vorsitzende des Verwaltungsrates von Alphabet, der Google Holding). Das ist eine neue Erfahrung!
2. Der Antragsteller darf nicht darauf verwiesen werden, zuerst gegen die Journalisten und deren Verlag wegen Verletzung des Persönlichkeitsrechts und des Datenschutzrechtes durch die Publikation vorzugehen. Die Ansprüche auf Delisting gegen die Suchmaschinenbetreiber und auf mögliche inhaltliche Korrektur gegen die Contentverantwortlichen bestehen nebeneinander und haben auch unterschiedliche Voraussetzungen. Sie sind nicht inhaltlich

7 EuGH, Urteil vom 13. Mai 2014 – C 131/12 –, DuD 2014, 559 ff.

voneinander abhängig, denn auch rechtmäßige frühere Berichterstattung kann zu einem berechtigten Löschantrag führen, auch wenn der Artikel selbst online verfügbar bleibt, aber dadurch nicht mehr so leicht auffindbar sein mag.

Die Nutzer machen von diesem neuen Anspruch fleißig Gebrauch. Ca 500 000 Anträge auf Löschen von Links mit durchschnittlich jeweils 3 betroffenen URLs (1,5 Millionen URLs insgesamt in ca 2 Jahren) sind seit der Urteilsverkündung am 13. Mai 2014 gestellt worden. Google löscht ca 42 %, 58 % der Anträge werden abgewiesen. Eine relativ ausgewogene Praxis. Zahlen zu den anderen Suchmaschinen liegen nicht vor, so dass kein Gesamtbild gezeichnet werden kann.

VI. Safe Harbor

Mit seiner dritten Entscheidung[8] zum europäischen Datenschutz hat der EuGH die Fiktion beendet, die Datenschutz - Selbstverpflichtung amerikanischer Unternehmen verbunden mit dem Eintrag in eine Liste würde das angemessene Datenschutzniveau i.S. der derzeit noch geltenden europäischen Datenschutzrichtlinie erreichen. Datenschutz hat also doch seinen Platz im digitalen Zeitalter. Unternehmen und der Staat müssen ihn beachten und ihm im Zweifel pauschale Sicherheitsbegründungen oder reine Praktikabilitätserwägungen unterordnen.

Mit der Safe Harbor Entscheidung, die die Angemessenheitserklärung der EU -Kommission iSd Datenschutzrichtlinie für rechtswidrig erklärt, ist die Rechtsunsicherheit für die betroffenen Unternehmen groß. Mögliche Alternativen wie die Einwilligung der Kunden, Verwendung bestehender von der EU-Kommission genehmigter und entsprechend ergänzter Vertragsklauseln oder sog. Binding Corporate Rules (BCR), die konzernweit verbindliche Datenschutzvorschriften enthalten, sind mit Rechtsunsicherheit verbunden. Einmal können sie einen entscheidenden Kritikpunkt der EuGH-Entscheidung nicht ausräumen, dass in den USA die Geheimdienste auf die Server der Unternehmen direkten Zugriff haben, damit auf die personenbezogenen Daten, und dass daraus die Verletzung des Datenschutzrechtes hergeleitet wird. Und außerdem müssten die BCR von der Datenschutzaufsicht vorher genehmigt werden, was die deutschen Datenschutzbehörden abgelehnt haben. Der Hafen bleibt unsicher.

Diese Entscheidung ist auch eine Antwort auf die Enthüllungen von Edward Snowdon seit 2013, die von der Politik auf die rechtsverletzenden Handlungen ausländischer Geheimdienste nicht gegeben wurde. Der umfassende Zugriff auf die auf den Rechnern amerikanischer IT-Konzerne gespeicherten Daten europäischer Bürgerinnen und Bürger und der vollkommen unzulängliche Rechtsschutz von Ausländern in den USA stellen eine Verletzung der informationellen Selbstbestimmung dar, die so nicht weiter hingenommen werden darf.

Das Safe-Harbor-Urteil hat weitreichende Folgen für Unternehmen dies- und jenseits des Atlantiks. Die zur Rechtsunwirksamkeit führenden Grundrechtsverletzungen können nicht in wenigen Wochen behoben werden, weil weder die amerikanische Politik noch die Sicherheitsbehörden dazu bereit und in der Lage sind. Es gilt deshalb eine Schonfrist, die den Unternehmen seitens der Datenschutzbehörden eingeräumt worden war und erst jüngst verlängert wurde. Andernfalls hätten sie bei weiterem Datentransfer Sanktionen verhängen müssen.

Ob das im Februar ausgehandelte Übereinkommen zwischen der EU und den USA , das sog. EU/US Privacy Shield Abkommen eine wirklich angemessene datenschutzrechtliche Antwort gibt, ist mit Fragezeichen zu versehen. Zunächst ist positiv, dass es überhaupt Bewegung gibt und die amerikanischen Sicherheitsbehörden versichern, dass sie nicht mehr wie in der Vergangenheit auf die Rechner der US-Firmen zugreifen werden. Das wird allerdings nicht rechtlich verbindlich abgesichert, sondern basiert auf schriftlichen Zusicherungen der Behörden und damit letztlich auf gegenseitigem Vertrauen. Das ist nach dem NSA-Skandal erschüttert. Das US-Handelsministerium soll die Firmen, die europäische Daten verarbeiten, überwachen und ein Ombudsmann im US-Außenministerium sich um Beschwerden von EU-Bürgern über eine mögliche Überwachung kümmern. EU-Bürger erhalten zudem erstmals Zugang zu US-Gerichten, wenn sie ihre Rechte durch dortige Internetfirmen verletzt sehen.

Neben positiven Bewertungen der Unternehmensverbände und der Regierungen sowie der EU-Kommission äußern Datenschutzbehörden in EU-Mitgliedstaaten, Abgeordnete und auch Max Schrems deutliche Bedenken an diesem transatlantischen Datenaustausch, die sich im Kern darauf beziehen, dass das Abkommen vom Goodwill der amerikanischen Behörden abhängt, die die letzten Jahre eine genau entgegensetzte Praxis aus Überzeugung ausgeübt haben.

Der Privacy Shield ist am 12. Juli von der EU-Kommission gebilligt und damit eine neue Rechtsgrundlage für den transatlantischen Datenfluss geschaffen worden.

VII. Europäische Datenschutzgrundverordnung

Was der EuGH mit dieser Entscheidung schon vorweggenommen hat, hat der europäische Gesetzgeber mit der Verabschiedung der europäischen Datenschutzgrundverordnung (DS-DGV), die 2018 in Kraft treten wird, ausdrücklich festgeschrieben, das Marktortprinzip für die Anwendung europäischen Rechts. Mit seiner Verankerung müssen sich auch global agierende IT-Konzerne, die ihren Hauptsitz außerhalb der EU haben, an das europäische Recht halten, wenn sie Daten von Bürgern in der EU erfassen, analysieren, ver-

8 EuGH, Urteil vom 6. Oktober 2015 – C362/14-, DuD 2015, 823 ff.

netzen und verarbeiten und für ihre Zwecke nutzen, um dann ihre Dienstleistungen in der EU anzubieten. Das schafft gleiche Wettbewerbsbedingungen, mehr Rechtssicherheit und leichtere Rechtsdurchsetzbarkeit. Datenschutz und wirtschaftliche Entwicklung sind keine unvereinbaren Gegensätze.

Diese neuen europäischen Datenschutzstandards sind ein wichtiger Schritt und leiten eine neue Zeitrechnung im Datenschutz ein. Die Zeit, dass sich Konzerne den Standort mit dem niedrigsten Datenschutzstandard, das war häufig Irland, aussuchen konnten, ist vorbei. Deshalb ist es überfällig gewesen, dass die Politik und der europäische Gesetzgeber die gesetzlichen Grundlagen zur Stärkung der Grundrechte der Bürgerinnen und Bürger geschaffen haben. Das Recht auf individuelle Selbstentfaltung kann nur wahrnehmen, wer die Kontrolle über sein Leben hat. Es geht um nicht weniger als die verfassungsmäßig garantierten Rechte, ohne deren Einhaltung die Demokratie nicht funktionieren kann.

Mit diesen europäischen Datenschutzstandards soll das Machtverhältnis zwischen der häufig marktbeherrschenden Stellung der Internetgiganten einerseits und der negativen Freiheit, in Ruhe gelassen zu werden[9], sowie der positiven Freiheit, Datenschutz- und Persönlichkeitsrechte zu leben, wieder besser justiert werden.

Es ist ein umfangreiches, abstrakt formuliertes Gesetzeswerk, das viele unbestimmte Rechtsbegriffe, sog. delegierte Rechtsakte, also Ermächtigungen an die EU-Kommission enthält (insgesamt über 60) und den Mitgliedstaaten mit neuen Vorgaben und zahlreichen Öffnungsklauseln einige Hausaufgaben bis zur Anwendung der Verordnung 2018 aufträgt.

Die Datenschutzgrundverordnung ist ein wichtiger Meilenstein (wie Peter Schaar in der PinG 2.2016 zu recht sagt) auf dem Weg in die globale Informationsgesellschaft. Statt 28 unterschiedlicher Datenschutzgesetze in den Mitgliedstaaten wird es künftig ein europäisches Datenschutzgesetz geben.

Die DS-GVO baut auf den bekannten Datenschutzprinzipien auf, die in der EU-Grundrechte-Charta und im AEUV verankert und damit nicht durch Sekundärrecht veränderbar sind. Art. 8 Abs. 1 GRCh enthält ausdrücklich ein Datenschutzgrundrecht und in Abs. 2 ist die Einwilligung der betroffenen Person oder eine sonstige gesetzliche Grundlage als Legitimation für die Verarbeitung personenbezogener Daten festgeschrieben. Und schließlich verlangt Art. 8 Abs. 3 GRCH unabhängige Stellen zur Überwachung, wie auch noch einmal Art. 16 AEUV.

Vor diesem Hintergrund mussten alle Forderungen nach einer grundsätzlichen Umkehr des Datenschutzrechts, nämlich an Stelle des geltenden Verbots mit Erlaubnisvorbehalt einen risikobasierten Ansatz zu wählen, scheitern. Ich halte diesen Verbotsgrundsatz mit Erlaubnisvorbehalt auch für ein notwendiges Korrektiv, um der mangelnden Überschaubarkeit automatisierter Datenverarbeitung und der damit verbundenen Eingriffe in Persönlichkeitsrechte zu begegnen (so auch die Bundesbeauftragte für den Datenschutz in PinG 2/2016, Seite 57) und nicht die Beweislast auf den Nutzer zu verschieben.

Mit der Ausgestaltung der notwendigen Einwilligung in Art. 7 DSGVO wird die Souveränität des Nutzers gestärkt. Daten können mit ausdrücklicher Einwilligung Dritten für bestimmte Verarbeitungszwecke zur Verfügung gestellt werden. Standardmäßig angekreuzte Kästchen oder Untätigkeit, also stillschweigende Einwilligung, reichen nicht aus (EG 32). Opt-out-Lösungen, die der BGH bisher toleriert hat, dürften damit nicht mehr zulässig sein.

Beim Besuch von Internetseiten kann die Einwilligung auch durch die Auswahl technischer Einstellungen erfolgen, dies ist besonders für Cookies relevant. Möglich dürfte danach auch die Einwilligung durch die Einstellungen des Browsers sein.

Die früheren allgemeinen, häufig unbestimmt formulierten Einwilligungen in alle bekannten und nicht bekannten Nutzungen mit allen Auswirkungen hinsichtlich der Verwendung der Daten zu Werbe- und anderen Geschäftszwecken durch allgemeine Datenschutzerklärungen wird es nach den neuen Regelungen so nicht mehr geben können. Einwilligungserklärungen müssen nach der DS-GVO in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache verfasst und klar unterscheidbar von anderen Erklärungen präsentiert werden (Art. 7 Abs.2 S.2 DS-GVO), und sie dürfen keine missbräuchlichen Klauseln enthalten.

Die Einwilligung muss freiwillig erfolgen. Daran fehlt es, wenn ein klares Ungleichgewicht zwischen dem Betroffenen und dem Verantwortlichen besteht.

Außerdem wird der Gedanke des Koppelungsverbots aufgegriffen, es muss also geprüft werden, ob ein Vertragsabschluss von der Einwilligung zur Verarbeitung von Daten abhängig gemacht werden darf, wenn diese für die Vertragserfüllung nicht gebraucht werden.

Zu Ende gedacht, verhindert es das im Internet gängige Modell der „Bezahlung mit eigenen Daten“ und schießt damit über das Ziel hinaus, die informationelle Privatautonomie des Betroffenen zu gewährleisten. Überzeugender wäre es gewesen, darauf abzustellen, ob es dem Betroffenen zumutbar wäre, auf alternative Anbieter auszuweichen.[10]

VIII. Zukunft des Datenschutzes

Neben dieser Rechtsentwicklung durch Rechtsprechung muss der technische Datenschutz vorangetrieben werden. Wenn Hersteller von Software, Hardware und Betreiber von Webseiten Anonymisierung, Pseudonymisierung und Datenschutzstandards ihren Produkten von vornherein mitgeben, dann wird mit diesem Privacy by Design durch Technik der Schutz der Privatsphäre ermöglicht, den die Nutzerinnen und Nutzer immer stärker wünschen und dessen derzeitiges Fehlen zu deutlichem Vertrauensverlust in die digitale Welt führt.

9 Schirrmacher, in: Yvonne Hofstetter, „Sie wissen alles“, 2014, Bertelsmann Verlag, S. 285.

10 Siehe dazu Schantz, NJW 2016, 1841 ff.

1. Das rollende Smartphone

Kaum eine technologische Entwicklung betrifft das Internet und Recht und Freiheit so sehr wie das rollende Smartphone, also das Internet der Dinge, eingesetzt beim connected car. Es bedarf eines digitalen Ordnungsrahmens, der u.a. die Datensicherheit und die komplexen, neuen Haftungsfragen für das Auto der Zukunft behandelt: das teilweise oder ganz selbst fahrende, selbst kommunizierende Auto gegenüber anderen Autos und der Infrastruktur, das vernetzten Auto gegenüber den verschiedenen Verkehrsträgern (zeitnahe Staumeldung im Auto). Mögliche Daten aus dem Auto gibt es mehr als genug. Angesichts der Vielfältigkeit der Einsatzzwecke von Informationsdaten im Auto und vieler Beteiligter stellen sich mehrere datenschutzrechtliche Frage. Vertrauen in das vernetzte Auto und seine Hersteller wird es nur mit klaren Regeln zur Verantwortung, zur Datensparsamkeit, zum Zugriff auf die Daten und zur Verwendung bei Schäden und Unfällen geben.

Da fordert die Digitalisierung den Gesetzgeber, und er sollte sich angesichts des harten Wettbewerbs ua mit amerikanischen Anbietern nicht zögerlich verhalten und die Risikoverteilung und Auskunftsrechte gesetzlich regeln.

Wir befinden uns mitten in der Gestaltung der Digitalisierung-technisch, gesellschaftlich, politisch und rechtlich. Der Erfolg dieser Entwicklung wird davon abhängen, das richtige Maß an notwendiger europäischer Gesetzgebung und nationalen Anpassungen zu finden.

Das Prinzip der Disruption darf es bei den Grundlagen unseres Zusammenlebens nicht geben. Die Grundrechte, verankert in nationalen Verfassungen der Mitgliedstaaten und in der Europäischen Grundrechtecharta stehen nicht zur Disposition. Das gilt für den abwehrrechtlichen Charakter der Grundrechte besonders mit Blick auf die Verletzung der Grundrechte durch ausländische Geheimdienste und für den schutzrechtlichen Charakter der Grundrechte bei Verletzung durch marktbeherrschende Unternehmen.

Generell wird aus den mit der Digitalisierung einhergehenden Grundrechtsgefährdungen deutlich, dass zukünftig dieser Grundrechtsschutz national und immer stärker europäisch erfolgen muss.

Deshalb wird man, wie vom früheren Präsidenten des Bundesverfassungsgerichts gefordert, vom deutschen Staat verlangen müssen, dass er sich energisch für bilaterale oder unilaterale Datenschutzabkommen einsetzt, in denen ein Standard rechtlicher Regeln entwickelt und normiert wird, der auf einem gemeinsamen Wertekanon gründet, der den im Wesentlichen übereinstimmenden grundrechtlichen Wertentscheidungen des Grundgesetzes, der EU-Grundrechtecharta und den menschenrechtlichen Verbürgungen der Europäischen Menschenrechtskonvention in Fragen des Persönlichkeitsschutzes und des Telekommunikationsgeheimnisses entspricht.

Den guten Beispielen des EuGH mit seiner Grundrechtsrechtsprechung, siehe Vorratsdatenspeicherung und sog. Recht auf Vergessenwerden, muss die Politik folgen.

2. Datenschutz der Zukunft

Anstatt den Datenschutz immer wieder als Täterschutz zu diffamieren oder ihn als lästiges Bürokratiemonster anzusehen, das die schöne neue Welt der Digitalisierung nur stört, sollte der Datenschutz als modernes Gestaltungsmittel verstanden werden. Wer den Datenschutz achtet, hat einen Vorteil. Datenschutz macht den Informationsaustausch, auch mit anderen Sicherheitsbehörden, nicht unmöglich, aber verlangt Restriktionen im Interesse der Grundrechte der Bürgerinnen und Bürger.

Wir brauchen eine liberale Datenpolitik, die Datenschutz angemessen gewährleistet. Wir wollen, dass das Recht auf informationelle Selbstbestimmung die digitale Zukunft prägt. Nutzer und Unternehmen brauchen Klarheit und Rechtssicherheit.

IX. Selbstbestimmung und Freiheit

Wer in der digitalen Welt frei entscheiden will, muss souverän über die Verwendung seiner Daten entscheiden.

Deshalb:

- Persönliche Daten sollen nicht unbegrenzt erhoben, gespeichert, verwendet und weitergegeben werden.
- Für die User muss transparent sein: Welche meiner Daten werden wo, von wem, wie lange und zu welchem Zweck erfasst und verarbeitet?
- Datenschutz- und Einwilligungserklärungen müssen verständlich und einfach sein.
- Es darf keine anlasslose Erhebung und Speicherung von Daten geben (Vorratsdatenspeicherung, Fluggastdatenerhebung, automatische Kennzeichenerfassung mit Speicherung der erfassten Daten).

1. Datenschutz technisch verstehen und verbessern

Der technische Fortschritt spielt nicht nur Datensammlern in die Hände, er kann auch dem Datenschutz dienen.

Deshalb:

- Datenschutz bedeutet auch und gerade, datenschutzfreundliche Technologien zu entwickeln und zu nutzen.
- Zukünftiger Systemdatenschutz setzt bereits im Entwicklungsstadium an. Datensparsamkeit heißt, Big-Data-Modelle zu entwickeln, die mit möglichst wenigen personenbezogenen Daten auskommen. Daten sollen so weit als möglich anonymisiert, verschlüsselt oder pseudonymisiert werden.
- Eine dezentrale Datenverarbeitung erleichtert den Datenschutz. Endgeräte für Verbraucher sollen mit einer Grundeinstellung ausgeliefert werden, die einen starken Datenschutz gewährleistet (privacy by design, privacy by default).

2. Datenschutz gestalten

Die Politik muss gesellschaftliche Debatten aufnehmen und Antworten geben. Das gilt auch beim Datenschutz der Zukunft. Die Datenschutzgrundverordnung der Europäischen Union leistet dazu einen wichtigen Beitrag. Die große Koalition muss die notwendigen Umsetzungen zügig vorlegen.

Deshalb:

- Europäische Datenschutzgrundverordnung und Bundesdatenschutzgesetz müssen synchronisiert werden, um Rechtssicherheit für Nutzer und Planbarkeit für Unternehmen herzustellen.
- Das Internet der Dinge wird ganz neue Haftungsfragen aufwerfen-hier brauchen wir klare Regelungen. Ein Recht auf Abtrennung soll gewährleisten, dass man Gegenstände auch ohne Weitergabe der damit verbundenen Daten benutzen kann.
- Das Recht auf Vergessenwerden muss verfahrensmäßig per Gesetz geregelt werden, um so eine Abwägung zwischen den Rechten des Users und der Meinungs- und Pressefreiheit sicherzustellen.

3. Datenpolitik in internationaler Dimension denken

Datenpolitik hat immer eine internationale Dimension: Digitale Geschäftsmodelle machen nicht an Ländergrenzen halt: Zuliefererketten sind weltweit vernetzt und Absatzmärkte global.

Deshalb:

- Die Vorgaben des Europäischen Gerichtshofs zum Datentransfer zwischen Europa und den USA müssen umgesetzt werden-hier gilt es viel nachzubessern.
- Rechtsdurchsetzung durch „Rechtshilfe 4.0" gilt es zu erleichtern: Jeder muss den Schutz seiner Daten durchsetzen können – auch in den USA.
- Datenschutz nach deutschem Standard sollte als Exportschlager verstanden werden – und in internationalen Abkommen verankert werden.

4. Datenschutz heißt auch Schutz vor Cyberangriffen

Von staatlichen oder nichtstaatlichen Cyberangriffen geht eine große Gefahr für die Datensicherheit aus. Bestmögliche IT-Sicherheit und der Schutz der digitalen Infrastruktur – hier brauchen wir einen starken Staat.

Deshalb:

- Unternehmen müssen angemessene Sicherheitsvorkehrungen wie kryptografische Verschlüsselung, personenbezogene Zertifikate zum Schutz vor Manipulation und Nachweis der Identität einsetzen.
- Es darf keine gesetzlichen Beschränkungen oder Vorgaben bei kryptografischen Sicherungssystemen geben, was verschlüsselt ist, muss ohne Hintertür verschlüsselt sein.
- Die obligatorische Nutzung von Verschlüsselungstechnologien muss durchgesetzt und Omnicloud-Lösungen gefördert werden – so werden Daten verschlüsselt, bevor sie in der Cloud gespeichert werden. Das hilft, das Datenvolumen zu minimieren.
- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sollte zu einem unabhängigen IT-Dienstleister für Bürger und Unternehmen werden – und keine nachgeordnete Behörde des Bundesministeriums des Innern sein.
- Daten- und IT-Sicherheit muss als Schwerpunkt der deutschen und europäischen Spitzenforschung ausgebaut werden.
- Auch Cybersicherheit kann nicht national gedacht werden: Daher muss jetzt ein EU-IT-Sicherheitskonzept entwickelt werden – für mehr Transparenz und Schutz vor Cyberangriffen.

X. Fazit:

Datenschutz ist kein „Nice to Have" und auch kein Relikt längst vergangener analoger Zeiten. Datenschutz setzt Freiheit durch. Eine moderne liberale Digitalpolitik hat ihre grundrechtliche Dimension immer im Blick. Sie versteht Digitalisierung nicht als ein über uns hereinbrechendes Naturereignis, sondern als technologischen, dynamischen Prozess, dessen Herausforderungen erkannt und gestaltet werden können. Vor allem aber: Liberale Digitalpolitik kann zeigen, wie wir uns die digitale Zukunft wünschen und wie wir uns einen digitalen Gestaltungsrahmen vorstellen.

Sabine Leutheusser-Schnarrenberger
ist Bundesministerin der Justiz a.D. und Mitglied der Beirates von Google zum Recht auf Vergessen.

Barbara Broers

Auskunftspflichten von Unternehmen zu Zeiten des Terrorismus*

Die Anschläge vom 11. September 2001 zählen zu den weltweit größten und schwersten terroristischen Angriffen in der Menschheitsgeschichte. International wurden in der Folge Gesetzespakete verabschiedet, um zukünftige Terroranschläge besser aufdecken bzw. verhindern und bereits erfolgte nachträglich aufklären zu können. Im Fokus zur Verhinderung von Anschlägen stehen dabei präventive Maßnahmen zur Kappung der finanziellen und wirtschaftlichen Ressourcen von Terroristen.

I. Einführung

Bereits 17 Tage nach den Anschlägen in New York, Washington und Pennsylvania beschloss der Sicherheitsrat der Vereinten Nationen neue umfangreiche Maßnahmen zur Verhütung und Bekämpfung des Terrorismus. Ziel war dabei vor allem die Verhinderung aktiver und/oder passiver Unterstützung von Terrororganisationen bzw. einzelner Personen in Form von Geldmitteln, Vermögenswerten oder wirtschaftlichen Ressourcen[1].

Die USA benötigten etwas mehr Zeit als der Sicherheitsrat der Vereinten Nationen, um einen Gesetzesentwurf im Kongress einzubringen[2], konnten den USA PATRIOT Act dann aber innerhalb von nur drei Tagen verabschieden[3]. Mittlerweile sind bestimmte Teile des Gesetzes nicht mehr in Kraft oder entschärft worden. Weitreichende Änderungen treffen insbesondere den sogenannten National Security Letter (NSL), eine strafbewehrte behördliche Anordnung ohne Richtervorbehalt[4], mit der Telekommunikationsanbieter, Banken und Finanzunternehmen zur Herausgabe von Kundendaten verpflichtet werden können.

Der NSL ist inhaltlich auf Bestandsdaten beschränkt, Kommunikationsinhalte oder die veranlasste Erhebung personenbezogener Daten sind ausgeschlossen. US-Behörden verstehen unter dem Begriff der relevanten Bestandsdaten allerdings auch Verbindungsdaten (IP-Adressen, Log-Files). Eine häufig enthaltene Geheimhaltungsklausel bei Anordnungen des FBI sieht zudem unter Androhung hoher Strafen vor, dass Unternehmen sowohl über die Zustellung eines NSL als auch über die herausgegebenen Daten schweigen müssen[5]. Da nur der Direktor des FBI diese Schweigepflicht aufheben oder einschränken kann, blieb den Unternehmen die gerichtliche Prüfung des NSL verwehrt.

Seit 2006 ist es Unternehmen erlaubt, die Anordnungen durch das United States District Court prüfen zu lassen. In dem wohl bekanntesten Fall des Unternehmers Nicholas Merryl, Gründer des Internetanbieters Calyx Internet Access, führte der elf Jahre andauernde Rechtstreit zu weitreichenden Erfolgen. Nicht nur Merryl darf mittlerweile offen über seinen NSL sprechen[6], auch andere Unternehmen konnten sich mit Erfolg gegen die FBI- Anordnungen zur Wehr setzen, sodass Anordnungen teilweise oder vollständig zurückgenommen wurden[7].

Noch im Dezember 2001 reagierte der Rat der Europäischen Union mit der EG-Verordnung (EG) 2580/2001 auf die vom UN-Sicherheitsrat geforderten Maßnahmen gegen den Terrorismus. Diese unmittelbar geltende Rechtsvorschrift sieht eine Liste vor, die laufend aktualisiert wird und konkret vom Embargo betroffene natürliche und juristische Personen benennt[8].

Im Mai 2002 folgte die nächste EG-Verordnung (EG) 881/2002, die explizit eine Liste von Personen und Organisationen enthält, die mit Osama bin Laden, dem Al-Qaida-Netzwerk und den Taliban in Verbindung stehen[9] und weder mit finanziellen Mitteln noch mit Vermögenswerten oder wirtschaftlichen Ressourcen unterstützt werden dürfen.

Im August 2011 folgte schließlich die dritte EU-Verordnung (EU) 753/2011, die entsprechend der Situation in Afghanistan eine weitere Liste von Personen, Gruppen, Unternehmen und Einrichtungen enthält, die ebenfalls nicht mit Geld, Vermögenswerten oder wirtschaftlichen Ressourcen unterstützt werden dürfen[10]. Darüber hinaus sind weitere Restriktionen enthalten, die eine unmittelbare oder mittelbare technische Hilfe sowie die Bereitstellung, Herstellung, Instandhaltung und Verwendung der in der Gemeinsamen Militärgüterliste der EU aufgeführten Güter und Technologien verbieten[11].

* Aufsatz zum Vortrag des 9. GDD-Sommer-Workshops vom 01.-03.08.2016 in Timmendorfer Strand.

1 UN-Resolution 1373 vom 28.09.2001.

2 Congressional Record – House, 23.10.2001, H7217.

3 H.R.3162 -- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT).

4 Section 505 USA PATRIOT Act.

5 Sogenannte gag order.

6 Anordnung des United States District Court (Judge Marrero) zur Aufhebung der gag order gegenüber Nicholas Merryl, 14-CV-9763 (VM) vom 28.08.2015.

7 Brad Smith: New success in protecting customer rights unsealed today. Microsoft Technet, 22. Mai 2014.

8 Verordnung (EG) Nr. 2580/2001 vom 27.12.2001, Maßnahmen gegen sonstige Terrorverdächtige.

9 Verordnung (EG) Nr. 881/2002 vom 27.05.2002, Maßnahmen gegen das Al-Qaida-Netzwerk.

10 Verordnung (EU) Nr. 753/2011 vom 01.08.2011, Restriktive Maßnahmen gegen bestimmte Personen, Gruppen, Unternehmen und Einrichtungen angesichts der Lage in Afghanistan.

11 Gemeinsame Militärgüterliste ABl. C 69 vom 18.03.2010, S. 19.

Die EG/EU-Verordnungen sind zwar unmittelbar geltende Rechtsvorschriften, sehen allerdings keine Sanktionen für Verstöße vor, sondern verpflichten die Mitgliedsstaaten, ihrerseits, durch eigene Gesetze wirksame, verhältnismäßige und abschreckende Strafen festzulegen.

Im deutschen Recht sind die Strafen und Ordnungswidrigkeiten für Verstöße gegen die EU-Sanktionsmaßnahmen im Außenwirtschaftsgesetz (AWG) angesiedelt. Irrtümlicherweise wird oft angenommen, dass Straftat- und Bußgeldtatbestände nur von Unternehmen erfüllt werden können, die Außenhandel mit Personen oder Unternehmen außerhalb der Europäischen Wirtschaftsräume betreiben. Der Geltungsbereich des Außenwirtschaftsgesetzes ist jedoch nicht begrenzt, sodass jeder, der gegen die EU-Sanktionsmaßnahmen verstößt, nach den Vorschriften dieses Gesetzes bestraft werden kann. Finanzielle Leistungen oder Warenlieferungen bzw. schuldrechtliche Vereinbarungen mit Personen oder Unternehmen, die einer Sanktionsmaßnahme durch EU-Verordnung unterliegen, können gem. § 18 Abs. 1 Nr. 1 lit. a AWG[12] mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft werden. Bei Fahrlässigkeit liegt eine Ordnungswidrigkeit gem. § 19 Abs. 1 AWG vor, die mit einem Bußgeld bis zu 500.000 Euro geahndet werden kann.

Des Weiteren räumen die Europäischen Verordnungen staatlichen Behörden keine besonderen Befugnisse ein. Aus diesem Grund ist am 01. Januar 2002 das Terrorismusbekämpfungsgesetz als sogenanntes Artikelgesetz in Kraft getreten[13]. Geschaffen wurden vor allem umfangreiche datenschutzrechtliche Grundlagen, insbesondere Auskunftsrechte der Nachrichtendienste gegenüber öffentlichen und nichtöffentlichen Stellen. Einige der enthaltenen Gesetzesänderungen waren zunächst befristet bis zum Ablauf des 10. Januar 2007, wurden allerdings im Januar 2007 durch das Terrorismusbekämpfungserweiterungsgesetz[14] verlängert. Im Dezember 2011 wurden mit dem Gesetz zur Änderung des Bundesverfassungsschutzgesetzes[15] weitere Änderungen festgelegt und Bestimmungen ergänzt.

II. Auskunftspflichten

Unternehmen können behördliche Anfragen zu Auskünften über Beschäftigte, Kunden, Lieferanten oder sonstige Geschäftskontakte erhalten. In diesem Fall sollte die Vorgehensweise ähnlich der Auskunft an den Betroffenen gem. § 34 Bundesdatenschutzgesetz (BDSG)[16] intern klar geregelt sein, eine unzulässige Übermittlung an Dritte kann auch als Ordnungswidrigkeit gem. § 43 Abs. 2 Nr. 4 BDSG Bußgelder bis zu 300.000 Euro nach sich ziehen.

Auskunftsersuchen durch Staatsanwaltschaften oder Polizeibehörden werden am Telefon, per Fax, per E-Mail oder per Post gestellt. Grundsätzlich sollten Unternehmen darauf bestehen, dass Anfragen sowie Auskünfte nur schriftlich erfolgen, um eine nachweisbare Dokumentation zu gewährleisten. Dies kann sich im Einzelfall aber auch aus den jeweiligen Rechtsvorschriften ergeben. Innerhalb des Unternehmens sollte festgelegt werden, durch welche Personen oder Fachabteilungen die Auskunftsersuchen bearbeitet werden. In jedem Fall sind datenschutzrechtliche Kenntnisse erforderlich, da jede Anfrage hinsichtlich der Zulässigkeit einer Übermittlung von der Auskunft gebenden Stelle geprüft werden muss.

Darüber hinaus muss die anfragende Behörde eine Rechtsgrundlage für die Zulässigkeit der Datenübermittlung bzw. die Pflicht zur Auskunft nennen, da solche Übermittlungen nicht dem ursprünglichen Zweck der Datenerhebung entsprechen. Personenbezogene Daten von Beschäftigten werden beispielsweise auf Grundlage des § 32 Abs. 1 BDSG erhoben, verarbeitet und genutzt. Übermittlungen, die nicht für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich sind, entsprechen einer zweckfremden Datenverarbeitung und müssen durch eine gesonderte Rechtsvorschrift erlaubt sein. Wichtig: Verantwortlich für die Beurteilung der Zulässigkeit ist die übermittelnde Stelle.

Da die Daten nicht bei den Betroffenen selbst erhoben werden, muss die jeweilige Rechtsvorschrift explizit die Datenerhebung bei dem zur Auskunft verpflichteten Unternehmen zulassen (§ 4 Abs. 2 Nr. 1 BDSG). Eine Pflicht zur Benachrichtigung der Betroffenen (§ 33 Abs. 1 BDSG) besteht nicht für das auskunftspflichtige Unternehmen, da nur Daten betroffen sein dürfen, die bereits zuvor für andere Zwecke bei der übermittelnden Stelle gespeichert waren.

In Bezug auf den internationalen Terrorismus ergeben sich aus den deutschen Gesetzen zur Terrorismusbekämpfung (s. I) weitere Auskunftspflichten gegenüber Nachrichtendiensten. Rechtsgrundlage für Auskunftsersuchen durch das Bundesamt für Verfassungsschutz ist das Bundesverfassungsschutzgesetz (BVerfSchG)[17]. Für den militärischen Nachrichtendienst (MAD) gilt das Gesetz über den militärischen Abschirmdienst (MADG)[18] und für den Auslandsgeheimdienst (BND) das Gesetz über den Bundesnachrichtendienst (BNDG)[19]. Demnach gelten die Vorschriften des BVerfSchG auch für Auskunftsersuchen durch MAD und BND[20].

Mögliche Rechtsgrundlagen für Auskünfte bestehen gegenüber

a) Unternehmen, die geschäftsmäßig Teledienste erbringen zu Daten, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Teledienste (Bestandsdaten) gespeichert worden sind (§ 8a Abs. 1 BVerfSchG).

12 Außenwirtschaftsgesetz vom 6. Juni 2013 (BGBl. I S. 1482), das zuletzt durch Art. 6 des Gesetzes vom 3. Dezember 2015 (BGBl. I S. 2178) geändert worden ist.

13 BGBl. 2002 I S. 361.

14 BGBl. 2007 I S. 2.

15 BGBl. 2011 I S. 2576.

16 Art. 15 EU-DSGVO (ab 25.05.2018).

17 Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch Art. 1 des Gesetzes vom 17. November 2015 (BGBl. I S. 1938) geändert worden ist.

18 MAD-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2977), das zuletzt durch Art. 2 des Gesetzes vom 17. November 2015 (BGBl. I S. 1938) geändert worden ist.

19 BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch Art. 3 des Gesetzes vom 17. November 2015 (BGBl. I S. 1938) geändert worden ist.

20 Vgl. §§ 4a, 4b MADG, §§ 2a, 2b BNDG.

b) Luftfahrtunternehmen, Betreibern von Computerreservierungssystemen und Globalen Distributionssystemen für Flüge zu Namen und Anschriften des Kunden sowie zur Inanspruchnahme und den Umständen von Transportleistungen, insbesondere zum Zeitpunkt von Abfertigung und Abflug und zum Buchungsweg (§ 8a Abs. 2 Nr. 1 BVerfSchG).

c) Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen zu Konten, Konteninhabern und sonstigen Berechtigten sowie weiteren am Zahlungsverkehr Beteiligten und zu Geldbewegungen und Geldanlagen, insbesondere über Kontostand und Zahlungsein- und -ausgänge (§ 8a Abs. 2 Nr. 2 BVerfSchG).

d) denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, zu Verkehrsdaten nach § 96 Abs. 1 Nr. 1 bis 4 des Telekommunikationsgesetzes und sonstigen zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendigen Verkehrsdaten (§ 8a Abs. 2 Nr. 4 BVerfSchG).

e) denjenigen, die geschäftsmäßig Teledienste erbringen oder daran mitwirken, zu

(a) Merkmalen zur Identifikation des Nutzers eines Teledienstes (§ 8a Abs. 2 Nr. 5 lit. a BVerfSchG),

(b) Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung (§ 8a Abs. 2 Nr. 5 lit. b BVerfSchG) und

(c) Angaben über die vom Nutzer in Anspruch genommenen Teledienste (§ 8a Abs. 2 Nr. 5 lit. c BVerfSchG).

Voraussetzung für die zuvor genannten Rechtsgrundlagen ist jeweils, dass die Auskunft nur im Einzelfall eingeholt werden darf und auf Anordnung ergeht. Auskunftsersuchen nach § 8a Abs. 2 BVerfSchG werden nach schriftlichem Antrag mit Begründung vom Behördenleiter oder dessen Stellvertreter im Falle des Bundesamts für Verfassungsschutz vom Bundesministerium des Inneren bzw. im Falle des BND vom Bundeskanzleramt sowie im Falle des MAD vom Bundesministerium der Verteidigung angeordnet. Das zur Auskunft verpflichtete Unternehmen darf gem. § 8b Abs. 4 BVerfSchG weder den Betroffenen noch Dritte über die Auskunft informieren. Zudem sind gem. § 8b Abs. 5 BVerfSchG einseitige nachteilige Handlungen zu Lasten des Betroffenen, wie die Beendigung oder Einschränkung von Verträgen oder die Erhebung oder Erhöhung von Entgelten, verboten.

Mit Ausnahme von Auskünften über Verkehrsdaten bei Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen (§ 8a Abs. 2 Nr. 4 BVerfSchG), gilt für die Erteilung von Auskünften die Verordnung über die Übermittlung von Auskünften an die Nachrichtendienste des Bundes (NDÜV)[21]. Die Auskunftsersuchen werden schriftlich unter Nennung einer angemessenen Frist angeordnet und sind in den vorgeschriebenen Dateiformaten auf den festgelegten Übertragungswegen zu übermitteln, wobei Ausnahmen möglich sind. Gemäß Anlage 2 NDÜV können auskunftspflichtige Unternehmen eine Entschädigung erhalten. Ein entsprechendes Formblatt liegt der Anordnung zur Auskunft bei.

Deutsche Unternehmen sind zwar nicht mit direkten Auskunftsersuchen US-amerikanischer Behörden konfrontiert, innerhalb eines Konzerns jedoch können Schwester- oder Muttergesellschaften in den USA per Gerichtsbeschluss (Subpoena) oder aufgrund behördlicher Anordnung (NSL) gezwungen werden, Kunden- bzw. Beschäftigtendaten herauszugeben. In der Regel sind dann auch Daten der deutschen Unternehmen betroffen, die vorab zu legitimen konzerninternen Zwecken übermittelt wurden. Für die anschließende Weitergabe sind die US-Unternehmen verantwortlich. Die reine Übermittlung zum Zweck einer angeordneten Auskunftspflicht stellt deutsche Unternehmen hingegen vor große Probleme. Die Mutterkonzerne verpflichten meistens vertraglich zur Kooperation, obwohl es an einer datenschutzrechtlich erforderlichen Rechtsgrundlage für die Übermittlung fehlt. Wird übermittelt, kann ggf. ein Bußgeld durch eine Aufsichtsbehörde erfolgen – wird nicht übermittelt, droht eine Vertragsstrafe der Muttergesellschaft, die nach derzeitiger Rechtslage häufig höher ausfällt als das Bußgeld. Ab Geltung der EU-Datenschutzgrundverordnung dürfte sich dieses Ungleichgewicht mit Geldbußen bis zu 4 Prozent des weltweiten Vorjahresumsatzes ändern.

III. Mitwirkungspflichten

Neben den üblichen Auskunftspflichten können für Unternehmen auch aktive Mitwirkungspflichten bestehen. Derzeit stark in der Diskussion sind die Bewilligungsvoraussetzungen für Zugelassene Wirtschaftsbeteiligte (AEO)[22]. Die Weltzollorganisation (WZO) hat mit einem „Framework of Standard to Secure and Facilitate Global Trade" (SAFE) weltweite Rahmenbedingungen für ein modernes, effektives Risikomanagement in den Zollverwaltungen geschaffen. Mit Einführung des Zugelassenen Wirtschaftsbeteiligten wurden sicherheitspolitische Aspekte des SAFE auf europäischer Ebene umgesetzt. Zu diesem Zweck wurde im Zollkodex (ZK) und in der Zollkodex-Durchführungsverordnung (ZK-DVO) die AEO-Zertifizierung eingeführt.

Es werden drei Varianten des zertifizierten Status unterschieden:

- AEO-C (Zollrechtliche Vereinfachungen)
- AEO-S (Sicherheit)
- AEO-F (Zollrechtliche Vereinfachungen / Sicherheit)

Für die Zertifikate mit dem Status AEO-S sowie AEO-F sind gem. Art. 14k ZK-DVO bestimmte Bewilligungsvoraussetzungen hinsichtlich der Sicherheit zu erbringen. Dazu zählt insbesondere der Nachweis, dass der Antragsteller für Personen, die künftig in sicherheitsrelevanten Bereichen arbeiten, Sicherheits- und Hintergrundüberprüfungen durchführt (Art. 14k lit. f ZK-DVO). Entsprechend der Leitlinien für Zugelassene Wirtschaftsbeteiligte[23] betrifft dies sämtliche Personen, die an zollrechtlichen Prozessen beteiligt sind. Die Leitlinien empfehlen explizit, dass Beschäftigte nicht auf schwarzen Listen stehen sollten[24] und nennen

21 Nachrichtendienste-Übermittlungsverordnung vom 11. Oktober 2012 (BGBl. I S. 2117).

22 Authorised Economic Operator.

23 Leitlinien AEO – TAXUD/B2/047/2011 – Rev. 5 vom 11.06.2014 der Europäischen Kommission, Generaldirektion Steuern und Zollunion.

24 (EG) 2580/2001, (EG) 881/2002, (EU) 753/2011.

beispielhaft die drei EU-Verordnungen, wobei jede nationale oder supranationale Liste herangezogen werden kann[25].

Darüber hinaus muss die Verarbeitung personenbezogener Daten zu Zwecken der Sicherheits- und Hintergrundüberprüfungen im Einklang mit jeglichen europäischen oder nationalen Rechtsvorschriften stehen. Der Wortlaut der Leitlinien klingt nun nach einer wohlwollenden Kann-Option – ohne eine entsprechende Rechtsgrundlage der Datenverarbeitung ist kein Listenabgleich zulässig. Die Empfehlungen aus den Leitlinien sehen in der Praxis allerdings wie folgt aus: Ohne Nachweis, dass geprüft wird, ob Beschäftigte auf einer Sanktionsliste stehen, wird kein AEO-S bzw. AEO-F Zertifikat erteilt. Fehlt es an einer gesetzlichen Rechtsgrundlage für die Datenverarbeitung, verweisen die Leitlinien auf die Einwilligung der Betroffenen.

Was zunächst einfach klingt, stellt deutsche Unternehmen allerdings vor große Hürden, da die Einwilligung im Beschäftigungsverhältnis nach Ansicht deutscher Aufsichtsbehörden in der Regel mangels fehlender Freiwilligkeit abgelehnt wird. Bei Beschäftigten kommt daher zunächst nur § 32 BDSG als vorrangige Rechtsvorschrift zur Datenverarbeitung in Frage. Demnach muss die Datenverarbeitung für die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses mit dem Betroffenen erforderlich sein.

Der Gesetzgeber wollte mit der Formulierung des § 32 Abs. 1 BDSG erreichen, dass der Umfang der Verarbeitung von Beschäftigtendaten den bisher von der Rechtsprechung aus dem allgemeinen Persönlichkeitsrecht abgeleiteten Grundsätzen zum Datenschutz im Beschäftigungsverhältnis entspricht[26]. Die Datenverarbeitung im Sinne des § 32 BDSG soll dann erforderlich sein, wenn sie den arbeitsrechtlichen Grundsätzen der Verhältnismäßigkeit entspricht, indem die berechtigten Interessen des Arbeitgebers an dem Umgang mit den Personaldaten gegen die maßgeblichen Rechtsgüter der betroffenen Beschäftigten abgewogen werden[27]. Die Verarbeitung von Beschäftigtendaten muss daher geeignet, erforderlich und angemessen sein.

Geeignet ist eine Maßnahme, wenn sie den vom Arbeitgeber angestrebten, von der Rechtsordnung gebilligten Zweck fördern kann[28]. Die AEO-Zertifizierung ermöglicht dem Arbeitgeber zollrechtliche Vereinfachungen auf Grundlage europäischer Rechtsverordnungen und stellt somit einen legitimen Zweck dar. Der Abgleich bestimmter Beschäftigter mit den Sanktionslisten ist im Rahmen der AEO-Zertifizierung eine der geforderten Bewilligungsvoraussetzungen und demnach geeignet.

Nach arbeitsrechtlicher Rechtsprechung ist eine Maßnahme erforderlich, wenn kein anderes, gleich wirksames und die Persönlichkeitsrechte der Betroffenen weniger einschränkendes Mittel zur Verfügung steht[29]. Die Feststellung, ob ein Beschäftigter auf einer der Sanktionslisten steht, lässt sich allerdings einzig und allein durch einen Abgleich treffen. Lediglich die Art und Weise, wie abgeglichen wird (manuell oder automatisiert), lässt einen gewissen Spielraum für Abwägungen zu.

Angemessen ist eine Maßnahme schließlich, wenn die berechtigten Interessen des Arbeitgebers die schutzwürdigen Interessen des Betroffenen überwiegen[30]. Dabei ist eine Gesamtabwägung der Intensität des Eingriffs und des Gewichts der ihn rechtfertigenden Gründe vorzunehmen[31]. Im Rahmen der AEO-Zertifizierung sind grundsätzlich nur bestimmte und nicht alle Arbeitnehmer von einem Listenabgleich betroffen. Die Intensität des Eingriffs beschränkt sich auf den Vergleich von Stammdaten der Betroffenen (Name, ggf. Anschrift, Geburtsdatum, Geburtsort) mit einer im Amtsblatt der Europäischen Union veröffentlichte Liste, die für jedermann einsehbar ist. Demgegenüber stehen nicht nur wirtschaftliche Vorteile des Arbeitgebers durch eine AEO-Zertifizierung, sondern auch erhebliche Strafandrohungen (§§ 18, 19 AWG) für den Fall, dass ein Beschäftigter auf einer Sanktionsliste aufgeführt ist[32]. Kritisiert wird allerdings, dass die Entscheidung, wer auf der Liste steht, weder nachvollziehbar ist noch rechtstaatlichen Grundsätzen entspricht[33].

Tatsächlich würde ein Listenabgleich bei Personen, die zu Unrecht auf einer Sanktionsliste stehen, zu einem *deutlich* überwiegenden Interesse seitens des Beschäftigten führen. Neben dem Versagen des Verdienstes würden auch keine sozialen Hilfen wie Arbeitslosengeld II, Sozialhilfe, Rente o.ä. mehr gezahlt werden. Im Übrigen überwiegen allerdings die Interessen des Arbeitgebers, sodass es mangels bestätigter Fälle zu Unrecht gelisteter Personen sowie mangels Beurteilungsmöglichkeiten des Arbeitgebers unter dem Strich zu einer Würdigung zugunsten des Unternehmens kommen wird.

Der Bundesfinanzhof hat 2012 entschieden, dass der Sanktionslistenabgleich im Rahmen der AEO-Zertifizierung (AEO-S, AEO-F) auf Grundlage des § 32 Abs. 1 BDSG zulässig ist[34]. Indem der Arbeitgeber zollrechtliche Vereinfachungen mit erhöhten Sicherheitsanforderungen beantragt, muss er auch nachweisen, dass die Bewilligungsvoraussetzungen erfüllt werden. Da es keine andere Möglichkeit gibt herauszufinden, ob ein Bewerber oder ein bereits Beschäftigter auf einer Sanktionsliste steht, wird ein Listenabgleich unmittelbar für die Begründung oder die Durchführung bzw. Beendigung des Beschäftigungsverhältnisses erforderlich. Fragwürdig ist, ob der Bundesfinanzhof von dieser Schlussfolgerung selbst überzeugt ist, da die Richter Unternehmen im Zweifel die Einholung einer Einwilligung bei den Betroffenen empfehlen.

Zur Art und Weise eines zulässigen Abgleichs äußert sich der Bundesfinanzhof leider nicht. Es wurde lediglich bestätigt, dass die Verarbeitung von Beschäftigtendaten für die

25 Vgl. Leitlinien AEO, S. 57.

26 BT-Drs. 16/13657, S. 21.

27 BAG, 18.08.1987 – 1 ABR 30/86, BB 1987, 1461, Rn. 31; BAG, 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187, Rn. 17.

28 BAG, 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 Rn. 19.

29 BAG, 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 Rn. 20.

30 BVerfG, 04.04.2006 – 1 BvR 518/02 – NJW 2006, 1939 Rn. 88.

31 BAG, 26.08.2008 – 1 ABR 16/07, NZA 2008, 1187 Rn. 21.

32 BFH, Urt. v. 19.06.2012, Az. VII R 43/11.

33 Vgl. Birgit Kruse, „Zivile Todesstrafe", Süddeutsche Zeitung, SZ.de, 17.05.2010, http://www.sueddeutsche.de/politik/dick-marty-bericht-zu-terrorlisten-zivile-todesstrafe-1.344886.

34 BFH, Urt. v. 19.06.2012, Az. VII R 43/11.

Bewilligung eines AEO-Zertifikats auf Grundlage des § 32 Abs. 1 BDSG zulässig sein kann und solche Maßnahmen Teil der Bewilligungsvoraussetzungen sein dürfen. Auch wenn zwischen Datenschützern und Gerichten keine Einigkeit hinsichtlich der Zulässigkeit derartiger Datenverarbeitung bestehen mag, sind die Aufsichtsbehörden an die Entscheidung gebunden. Das bedeutet allerdings nicht, dass Sanktionslistenabgleiche, die im Rahmen der AEO-Zertifizierung durchgeführt werden, nicht rechtswidrig sein können. Die konkrete Umsetzung des Abgleichs muss ebenfalls der Zulässigkeitsprüfung des § 32 BDSG unterzogen werden und verhältnismäßig sein. Der Einsatz technischer Hilfsmittel, die Datenverarbeitung im Auftrag durch Dienstleister sowie die Transparenz gegenüber den Betroffenen müssen den Grundsätzen der Geeignetheit, Erforderlichkeit und Angemessenheit folgen.

IV. Handlungspflichten

Für viele Unternehmen stellt sich auch ohne AEO-Zertifizierung die Frage nach der Pflicht bzw. dem Recht zum Sanktionslistenabgleich von Beschäftigten, aber auch von Lieferanten oder von Kunden. Grundsätzlich gilt, dass natürliche oder juristische Personen sanktionierten Personen oder Organisationen weder Geldmittel, noch Vermögenswerte oder wirtschaftliche Ressourcen zur Verfügung stellen dürfen.Anderenfalls drohen Bußgelder (§ 19 AWG) oder bei Vorsatz sogar Freiheitsstrafen (§ 18 AWG). Die Bundesregierung sieht die EU-Verordnungen als unmittelbare Rechtsgrundlage für die Durchführung von Sanktionslistenabgleichen[35].

Für die Datenschutz-Aufsichtsbehörden ist ein Abgleich von Beschäftigtendaten mit Sanktionslisten generell nicht mit dem Bundesdatenschutzgesetz vereinbar, da die Rechtsstaatlichkeit dieser Listen angezweifelt wird[36]. Es ist nicht nachvollziehbar, auf welche Weise Betroffene auf die Listen gelangen und welche Rechtsmittel gegen die Sanktionslisten vorhanden sind. Da Banken gem. § 25c Kreditwesengesetz bereits Screenings durchführen müssen, sehen die Aufsichtsbehörden im unbaren Zahlungsverkehr für Unternehmen keine Veranlassung, zusätzlich abzugleichen und fordern, solche Prüfungen nicht pauschal und anlasslos zu betreiben[37]. Problematisch ist hierbei, dass ohne pauschalen Abgleich die Gefahr einer unwissentlichen Zahlung besteht und der Arbeitgeber eine Ordnungswidrigkeit begeht.

Zur Klärung der Unsicherheiten tragen weder die Ansichten des Düsseldorfer Kreises noch die der Bundesregierung oder das Urteil des Bundesfinanzhofes bei, die betroffenen Unternehmen versuchen in eigener Regie die Schaffung von Rechtsgrundlagen. So zeigt der Daimler-Konzern anhand einer Konzernbetriebsvereinbarung, wie gesetzesähnliche Rechtsvorschriften geschaffen werden können, die nicht nur Abgleiche mit EU-Listen, sondern auch mit US-Listen ermöglichen[38]. Zumindest bis zur Geltung der EU-Datenschutzgrundverordnung könnten Betriebsvereinbarungen als Rechtsgrundlagen für Mitarbeiterscreenings dienen.

Interessanterweise beschäftigen sich Aufsichtsbehörden wie auch öffentliche Diskussionen dabei fast ausschließlich mit der Frage nach Mitarbeiterscreenings. Kunden und Lieferanten werden nicht gleichermaßen berücksichtigt. Gleiches gilt für Abgleiche mit US-Listen, die nicht von den Vorschriften des Außenwirtschaftsgesetzes erfasst sind. Deutsche Unternehmen, die mit den USA handeln, müssen allerdings befürchten, selbst auf einer der Listen zu gelangen, falls Leistungen an Personen oder Organisationen erbracht werden, die auf den Listen aufgeführt sind. Ein umfassender Abgleich von Kunden und Lieferanten wäre dementsprechend erforderlich, um existenzbedrohende Folgen für das Unternehmen zu vermeiden.

Ungeachtet der Rechtsgrundlagen für Screenings stellt sich auch die Frage nach der Art und Weise der Abgleiche. Die EU stellt mittlerweile eine umfassende Datenbank zur Verfügung, die sämtliche Personen oder Organisationen aus den EU-Verordnungen erfasst. Darüber hinaus gibt es gemeinsame Datenbanken der US-Sanktionslisten. Anbieter von Compliance-Software bieten ebenfalls unterschiedliche Produkte zu Abgleichen von CRM-Systemen mit verschiedenen Sanktionslisten an.

V. Fazit

Zusammenfassend lässt sich feststellen, dass es mangels Rechtsvorschrift weder eine Pflicht noch ein Recht zu anlasslosen oder pauschalen Listenabgleichen gibt. Im Gegenzug gibt es allerdings die unmissverständliche Pflicht, Geldmittel, Vermögenswerte und/oder wirtschaftliche Ressourcen nicht an Personen zu leisten, die auf Sanktionslisten geführt sind. So hat der EUGH beispielsweise 2007 entschieden, dass eine Grundstücksübertragung an eine Gesellschaft bürgerlichen Rechts (GbR) nicht möglich ist, wenn einer der Gesellschafter auf einer Sanktionsliste steht. Dies gilt selbst dann, wenn die Person erst ***nach*** *Unterzeichnung des Kaufvertrages auf die Liste gelangt ist*[39]*. Aufgrund der mangelnden Rechtsvorschrift erfordert der anlasslose oder pauschale Listenabgleich zumindest die eingehende Interessenabwägung, also die Einschätzung, ob die Interessen oder Grundrechte und Grundfreiheiten der Betroffenen nicht überwiegen.*

Barbara Broers
Barbara Broers ist Geschäftsführerin der Datenschutzberatung Broers sowie Leiterin des ERFA-Kreises NORD der Gesellschaft für Datenschutz und Datensicherheit e.V..

35 BT-Drucksache 17/388 vom 04.01.2010.

36 Beschluss des Düsseldorfer Kreises vom 23./24.04.2009 in Schwerin.

37 Beschluss des Düsseldorfer Kreises vom 22./23.11.2011.

38 http://www.spiegel.de/wirtschaft/unternehmen/daimler-ueberprueft-mitarbeiter-wegen-angst-vor-terror-a-1011135.html.

39 EuGH, 11.10.2007 – C-117/06.

Felix Bieker/Marit Hansen/Dr. Michael Friedewald

Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung*

Die Europäische Union verfügt seit dem Inkrafttreten des Vertrags von Lissabon im Jahr 2009 über die rechtlich verbindliche Grundrechtecharta (GRC), die das Recht auf Privatsphäre, wie es seit den fünfziger Jahren aus Art. 8 der Europäischen Menschenrechtskonvention (EMRK) bekannt ist, um ein eigenständiges Recht auf den Schutz personenbezogener Daten erweitert. Allerdings klafft eine Lücke zwischen dem Schutz dieser Rechte und der Umsetzung neuer Technologien. Einen Ansatz, um die Lücke zu schließen, bietet die in der neuen Europäischen Datenschutz-Grundverordnung (DS-GVO) erstmals verbindlich geregelte Datenschutz-Folgenabschätzung (DSFA).[1]

Um Unternehmen und Behörden für die Einhaltung dieser Rechte zu sensibilisieren, schreibt Art. 35 DS-GVO die Durchführung einer DSFA vor, die dazu dient, Risiken für Individuen, die sich aus der Verwendung einer bestimmten Technologie oder eines bestimmten Systems ergeben, zu erkennen und zu analysieren. Auf der Grundlage dieser Analyse sind angemessene Maßnahmen auszuwählen und umzusetzen, um die festgestellten Risiken zu bewältigen.

Seit der Einführung von Folgenabschätzungen gab es immer wieder Ansätze, diese auch auf dem Gebiet des Privatsphären- und Datenschutzes fruchtbar zu machen.[2] *Auf freiwilliger Basis wurden diese jedoch in der Praxis oft nicht umgesetzt oder eher als Form des Produkt-Marketings verstanden. Wenn die Grundverordnung im Mai 2018 anwendbar wird, müssen Unternehmen und Behörden im Fall eines voraussichtlich hohen Risikos ihrer Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen den Datenschutzaufsichtsbehörden auf Anfrage ihre Datenschutz-Folgenabschätzungen vorlegen.*

I. Eine grundrechtskonforme Datenschutz-Folgenabschätzung

Der im Folgenden dargestellte Prozess für eine DSFA orientiert sich an den in Art. 35 DS-GVO formulierten Anforderungen und basiert auf ausführlichen Analysen bestehender Verfahren[3]. Er stellt sicher, dass die Ergebnisse reproduzierbar und überprüfbar sind. Zudem erlaubt er den Vergleich verschiedener möglicher Lösungen und ist technologieneutral formuliert.

Der Prozess ist in vier Phasen unterteilt (siehe Abb. 1): In der Vorbereitungsphase (1) ist zunächst das geplante Verfahren zur Datenverarbeitung zu beschreiben, das anschließend in der Bewertungsphase (2) aus der Perspektive der Betroffenen zu beurteilen ist. Sodann werden in der Maßnahmenphase (3) Vorkehrungen getroffen, um die identifizierten Risiken einzudämmen. Schließlich werden in der Berichtsphase (4) die Ergebnisse des DSFA-Verfahrens dokumentiert. Die anlassbezogen und regelmäßig erforderliche Fortschreibung der DSFA wird durch die Einbindung in das Datenschutz-Management des Verantwortlichen sichergestellt.

1. Vorbereitungsphase

1.1 Relevanzschwelle

Zunächst ist festzustellen, ob eine DSFA notwendig ist. Nach Art. 35 DS-GVO ist dies der Fall, wenn voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Die Formulierung „Rechte und Freiheiten" lehnt sich an Art. 52 Abs. 1 GRC an, der wiederum, der französischen Rechtstradition folgend, auf den Gebrauch in der EMRK zurückgeht.[4] Es besteht zwischen beiden kein qualitativer Unterschied; sie beziehen sich auf die europäischen Individualgrundrechte.[5]

Von den Verantwortlichen wird also die Einschätzung von Risiken gefordert, um festzustellen, ob es einer DSFA bedarf. Allerdings ist dabei zu beachten, dass es sich bei einer DSFA nach DS-GVO nicht um das im Bereich der Informa-

* Aufsatz zum Vortrag des 9. GDD-Sommer-Workshops vom 01.-03.08.2016 in Timmendorfer Strand.

1 Das in diesem Text vorgestellte Verfahren einer Datenschutz-Folgenabschätzung beruht in Teilen auf einem White Paper des Forums Privatheit für die Digitale Welt, an dem die Autoren mitgewirkt haben: Friedewald u.a., Datenschutz-Folgenabschätzung. Ein Werkzeug für einen besseren Datenschutz, Fraunhofer ISI, Karlsruhe, 2016. Die Ausgestaltung der DSFA wird zurzeit auf europäischer Ebene zwischen den Aufsichtsbehörden diskutiert; der vorliegende Text ist daher „work in progress" und gibt den Stand vom 08.07.2016 wieder.

2 Vgl. etwa ICO (Information Commissioner's Office), Conducting privacy impact assessments code of practice, 2014, https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf; CNIL (Commission Nationale de l'Informatique et des Libertés), Privacy Impact Assessment: Methodology (how to carry out a PIA), 2015, http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf; Wright/De Hert (Hrsg.), Privacy Impact Assessment, Dordrecht u.a. 2012.

3 Wright u.a., Privacy Impact Assessment and Smart Surveillance. A State of the Art Report, Deliverable 3.1 SAPIENT Project, 2013; Venier u.a., A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies. Deliverable 4 PRESCIENT Project, 2013, http://prescient-project.eu/prescient/inhalte/download/PRESCIENT_deliverable_4_final.pdf; Wright/Friedewald, Integrating privacy and ethical impact assessment, Science and Public Policy Bd. 40, 2013, S. 755.

4 Borowsky, in: Meyer (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, Art. 52, Rn. 19.

5 Becker, in: Schwarze u.a. (Hrsg.), EU-Kommentar, 3. Aufl. 2012, Art. 52, Rn. 2.

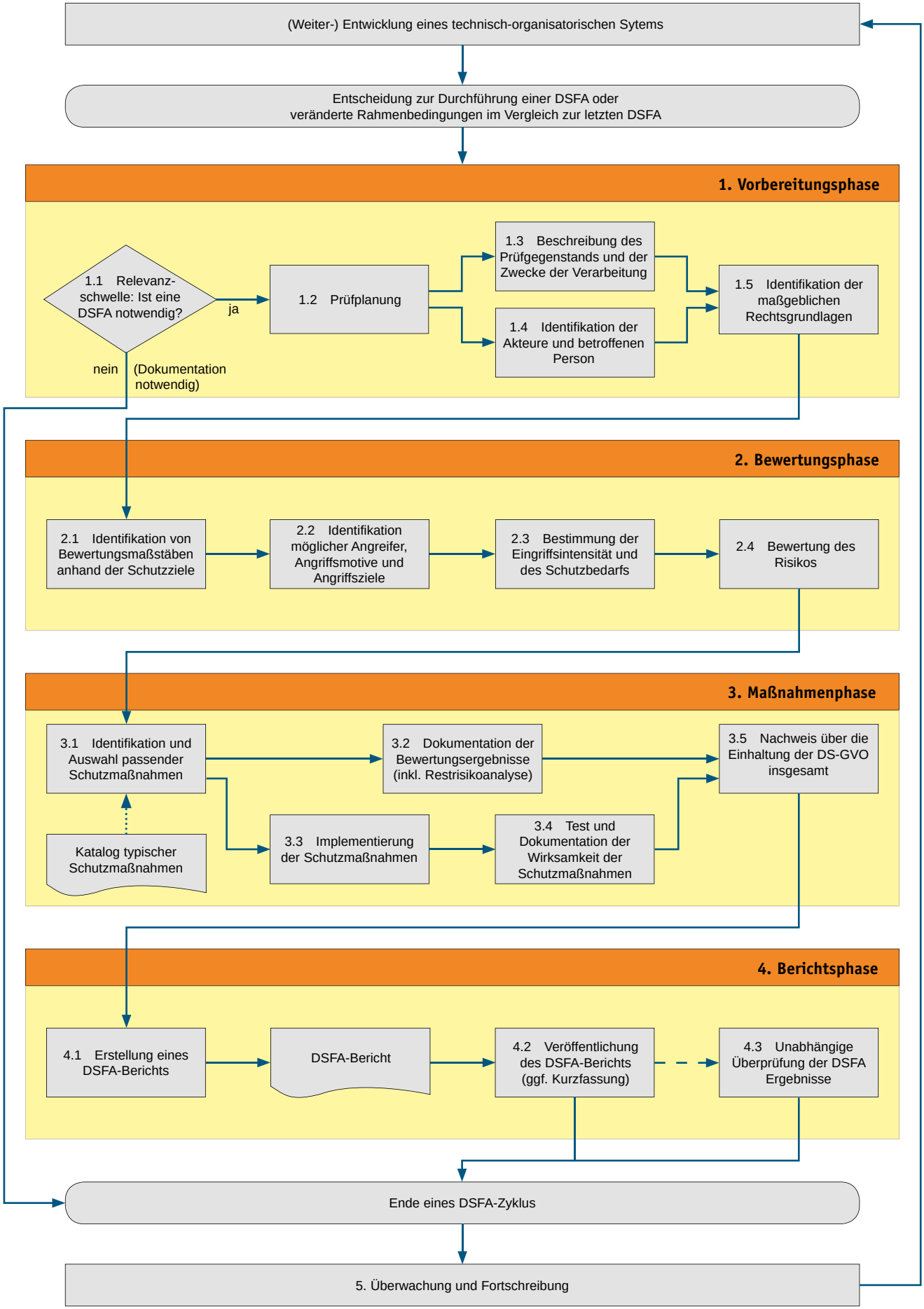

Abb. 1: Prototypischer Ablauf einer Datenschutz-Folgenabschätzung

tionssicherheit übliche Verfahren des Risikomanagements handelt. Dieses befasst sich mit Risiken für eine Organisation und ihren Aktivitäten. Art. 35 Abs. 1 DS-GVO liegt eine andere Art von Risikobeurteilung zugrunde: Im Fokus steht eine Bewertung des Risikos für die Rechte von Individuen. Damit ist insbesondere das Grundrecht auf den Schutz personenbezogener Daten gemeint.[6] Nach ständiger Rechtsprechung des Gerichtshofs der EU (EuGH) stellt jede Verarbeitung von personenbezogenen Daten einen Eingriff in Art. 8 GRC dar, der gerechtfertigt werden muss.[7] Folglich ist jeder Eingriff ein Risiko für die Rechte der betroffenen Personen. Den identifizierten Risiken müssen Maßnahmen entgegengesetzt werden. Können etwa bestimmte Risiken nicht (vollständig) beseitigt werden, müssen diese verbleibenden Restrisiken dokumentiert und gerechtfertigt werden. Sind diese allerdings als zu hoch einzustufen, darf das Verfahren nicht eingesetzt werden.

Die DS-GVO selbst gibt verschiedene Anhaltspunkte, wann ein solches hohes Risiko besteht. Nach der nicht abschließenden Aufzählung des Abs. 3 besteht ein solches Risiko insbesondere

- bei systematischer und umfassender Bewertung persönlicher Aspekte von Personen, die auf automatisierter Verarbeitung beruht und Grundlage von Entscheidungen ist, die diese Personen in erheblicher Weise beeinträchtigen;
- wenn besondere Kategorien personenbezogener Daten oder solche zu strafrechtlichen Verurteilungen oder Straftaten umfangreich verarbeitet werden;
- bei der systematischen und umfangreichen Überwachung öffentlich zugänglicher Bereiche.

Zudem sind die von den Aufsichtsbehörden nach Art. 35 Abs. 4 u. 5 DS-GVO zu erstellenden Listen zu beachten, in denen diese Verarbeitungsvorgänge benennen, die stets einer DSFA bedürfen oder von einer solchen explizit ausgenommen sind. Allerdings ist die Aufstellung der Letzteren in das Ermessen der Datenschutzaufsichtsbehörden gestellt. Bei bestimmten Arten von Datenverarbeitungen generell und ohne weitere Prüfung von einer DSFA abzusehen, wäre jedoch dem umfassenden Grundrechtsschutz, den die DS-GVO ausdrücklich beabsichtigt, abträglich, so dass dieser Ansatz nicht weiter verfolgt werden sollte.

Unabhängig von der Entscheidung, ob eine DSFA durchgeführt werden soll, ist dieser Schritt in jedem Fall mit einer Begründung zu dokumentieren. Dies dient auch der Absicherung des Verantwortlichen gegenüber der zuständigen Aufsichtsbehörde, der eine Überprüfung so zudem erleichtert wird.

1.2 Prüfplanung

Zu den Zielen der DSFA nach der DS-GVO gehört es zu bewerten[8], ob ein definiertes Datenverarbeitungssystem die datenschutzrechtlichen Anforderungen erfüllt, und geeignete Schutzmaßnahmen für dieses System zu identifizieren. Die Überprüfbarkeit für die Öffentlichkeit und Aufsichtsbehörden kann durch den Rückgriff auf einen vordefinierten Katalog an Bewertungskriterien und -maßstäben sowie Schutzmaßnahmen erleichtert werden. Dies dient auch der Sicherstellung der von Art. 35 Abs. 9 DS-GVO geforderten Transparenz des Verfahrenlegts. Der Katalog sollte nicht mit einer einfachen Checkliste verwechselt werden, bei der einzelne Punkte abgehakt werden – vielmehr müssen die einzelnen Risiken detailliert in Bezug auf die konkreten Verarbeitungsvorgänge geprüft werden.

Das Team zur Durchführung der DSFA sollte über ausreichende Ressourcen und – idealerweise auch interdisziplinäre – Kompetenz verfügen, um eine objektive Analyse zu ermöglichen. Der für die Entwicklung und Umsetzung Verantwortliche sollte, mit der Unterstützung einer neutralen Partei, wie etwa aus der Qualitätssicherung, die DSFA durchführen. Zudem ist gem. Art. 35 Abs. 2 DS-GVO der Rat der/des Datenschutzbeauftragten einzuholen, soweit ein(e) solche(r) benannt ist.

1.3 Beschreibung des Prüfgegenstands und der Zwecke der Verarbeitung

Der Prüfgegenstand (engl. target of evaluation) bestimmt den Umfang der DSFA. Um einzuschätzen, ob voraussichtlich ein hohes Risiko besteht, muss der Verantwortliche einen Überblick über die geplante Datenverarbeitung haben. Aus diesem Grund fordert Art. 35 Abs. 7 Buchstabe a DS-GVO eine systematische Beschreibung der Verarbeitungsvorgänge, ihrer Zwecke sowie der berechtigten Interessen des Verantwortlichen. Dies beinhaltet insbesondere die Daten, ihre Formate beim Speichern oder Transferieren (Kommunikationsprotokolle), die verwendeten IT-Systeme und deren Schnittstellen sowie Prozesse und Funktionsrollen.

Eine DSFA nach Art. 35 DS-GVO darf sich dabei nicht auf eine einzelne Komponente oder Funktion beschränken, sondern muss das gewählte Prüfobjekt in seiner Gesamtheit, inklusive der technischen und organisatorischen Umsetzung bei dem Verantwortlichen prüfen. Die datenschutzrechtlichen Regeln zur Zweckbindung nach Art. 5 Abs. 1 Buchstabe b DS-GVO und der Datenminimierung gem. Art. 5 Abs. 1 Buchstabe c DS-GVO erfordern dabei eine abschließende Definition der verfolgten Zwecke und eine Güterabwägung zur Gewährleistung des Grundrechtsschutzes, die im nachfolgenden Verfahren bereits berücksichtigt ist. Bei dieser Verhältnismäßigkeitsprüfung ist zu beachten, dass sich auf das Europarecht als autonomer Rechtsordnung nicht einfach Instrumente des nationalen Rechts übertragen lassen. Folglich gibt es eine eigenständige europarechtliche Verhältnismäßigkeitsprüfung, die den Schwerpunkt auf die Prüfung der Erforderlichkeit und nicht, wie im deutschen Recht, auf die Angemessenheit legt.[9] Die Verarbeitung selbst unter-

6 Vgl. Erwägungsgründe 1 u. 2 DS-GVO.

7 EuGH v. 09.11.2010 – C-92/09 und C-93/09 (Schecke und Eifert); EuGH v. 08.04.2014 – C-293/12 und C-594/12 (Digital Rights Ireland und Seitlinger).

8 Obwohl alle Sprachfassungen von EU-Rechtsakten in gleichem Maße verbindlich sind, enthalten die englische und französische Version mit dem Begriff „assessment" / „évaluation" einen umfassenderen Begriff, als die deutsche Übersetzung. Die Ersteren beinhalten auch eine Beurteilung.

9 Trstenjak/Beysen, EuR 2012, 265.

liegt dem Zweckbindungsgrundsatzes des Art. 5 Abs. 1 Buchstabe b DS-GVO. Daher muss begründet werden, warum die Datenverarbeitung gerade für die verfolgten Zwecke notwendig ist.

1.4 Identifikation der Akteure und betroffenen Personen

Ebenso bedeutend wie die korrekte Beschreibung des Prüfgegenstands ist in dieser Phase die Identifikation der Akteure und betroffenen Personen. Die Rolle jeder dieser Gruppen bei der Datenverarbeitung, ihre rechtlichen Beziehungen und Interessen sind zu bestimmen. Relevant sind insbesondere

- der Hersteller[10] des Prüfgegenstands;
- der Betreiber des Prüfgegenstands, etwa als Dienstleister im Rahmen einer Auftragsverarbeitung (Rechenzentrum, Internet-Provider);
- Mitarbeiter der für den Einsatz des Prüfgegenstands verantwortlichen Organisation;
- Dritte, die im Zuge des Einsatzes des Prüfgegenstands Kenntnis von personenbezogenen Daten nehmen, entweder zufällig (etwa zufällig anwesende, mithörende Dritte) oder absichtlich (Sicherheitsbehörden);
- die betroffenen Personen gem. Art. 35 Abs. 9 DS-GVO in ihren (vom Anwendungskontext abhängigen) Rollen als Bürger, Patient, Kunde, Arbeitnehmer etc.

1.5 Identifikation der maßgeblichen Rechtsgrundlagen

Wie in Art. 5 Abs. 2 DS-GVO festgelegt, muss der Verantwortliche im Rahmen seiner Rechenschaftspflicht nachweisen können, dass die Verarbeitung der Daten rechtmäßig ist. Dies ist eine Voraussetzung für sämtliche Datenverarbeitungen und muss daher noch vor Beginn des DSFA-Verfahrens geprüft werden. Als Grundrechtseingriff ist die Datenverarbeitung nur zulässig, wenn einer der in Art. 6 Abs. 1 DS-GVO abschließend aufgezählten Gründe einschlägig ist. Zunächst muss die Verarbeitung der personenbezogenen Daten dazu geeignet sein, den damit verfolgten Zweck zu erreichen. Das ist der Fall, wenn sie der Erreichung des Zwecks jedenfalls dienlich ist. Dies ermöglicht eine Überprüfung, ob der Zweck systematisch und in einer kohärenten Weise verfolgt wird.[11]

Weiterhin muss die Verarbeitung erforderlich sein; es darf also keine weniger eingriffsintensive Maßnahme geben, die gleich geeignet zur Erreichung des verfolgten Zwecks sind. Die Erforderlichkeit umfasst das Schutzziel der Datensparsamkeit;[12] es dürfen also nicht mehr personenbezogene Daten verarbeitet werden, als für die Erreichung des Verarbeitungszwecks erforderlich ist.

Obwohl die wesentlichen Vorschriften zum Datenschutzrecht in der DS-GVO enthalten sind, lassen zahlreiche Regelungen den Mitgliedstaaten einen Spielraum bei der Umsetzung, etwa im öffentlichen Bereich gem. Art. 2 Abs. 2 DS-GVO oder im Gesundheitsbereich sowie den Sozialversicherungssystemen gem. Art. 9 Abs. 2 Buchstabe h DS-GVO. Daneben können auch sektorspezifische europäische oder nationale Regelungen zu beachten sein, zum Beispiel im Telekommunikationsbereich, bezüglich Berufsgeheimnissen oder dem Schutz von Minderjährigen. Soweit diese Vorschriften sich auf die Datenverarbeitungsvorgänge beziehen – auch in Bezug auf die Frage der Rechtmäßigkeit der Verarbeitung – sind sie im Verfahren der DSFA zu berücksichtigen.

2. Bewertungsphase

Die Bewertungsphase deckt die Anforderungen von Art. 35 Abs. 7 Buchstaben b und c DS-GVO an die Bewertung der Verhältnismäßigkeit und des Risikos für die betroffenen Personen ab.

2.1 Identifikation von Bewertungsmaßstäben anhand der Schutzziele

Die datenschutzrechtlichen Anforderungen sind in Form des Standard-Datenschutzmodells[13] operationalisiert und haben sich in der IT- und Informationssicherheit bewährt.[14] Mithilfe dieser Methode können Risiken durch angemessene Maßnahmen und Verfahrensgestaltung behandelt werden.

Im Rahmen des Standard-Datenschutzmodells haben sich sieben Schutzziele etabliert: Vorgeschaltetes Schutzziel ist die Datensparsamkeit. Dazu gehören die klassischen drei Schutzziele der Informationssicherheit, nämlich Verfügbarkeit, Integrität und Vertraulichkeit, die allerdings in dem DSFA-Kontext aus der Perspektive der betroffenen Personen zu interpretieren sind.[15] Diese werden ergänzt durch drei zusätzliche datenschutzspezifische Schutzziele: Nichtverkettbarkeit, Transparenz und Intervenierbarkeit.

10 Der Hersteller könnte den Verantwortlichen auch mit einem „Beipackzettel", der bereits die wesentlichen Elemente einer DSFA benennt, unterstützen, s. unten II.

11 Trstenjak/Beysen, EuR 2012, S. 271.

12 Insofern ist die deutsche Fassung der DS-GVO missglückt: Während der deutsche Wortlaut („Notwendigkeit und Verhältnismäßigkeit") scheinbar ein weiteres Kriterium einführt, beziehen sich die englische und französische Fassung auf die „necessity"/„nécessité" und damit eigentlich die Erforderlichkeit, die ein Teil der Verhältnismäßigkeitsprüfung ist, vgl. Trstenjak/Beysen, EuR 2012, S. 269. Der Wortlaut von Art. 35 Abs. 1 DS-GVO ist dabei ebenfalls an Art. 52 Abs. 1 GRC angelehnt: „Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind […]".

13 AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder/Schulz/Rost, Das Standard-Datenschutzmodell – der Weg vom Recht zur Technik. Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen, Hannover 2015, https://www.datenschutzzentrum.de/uploads/sdm/SDM_Tagungsband2015_Hannover.pdf.

14 Hansen/Jensen/Rost, Protection Goals for Privacy Engineering, in: 2015 International Workshop on Privacy Engineering (IWPE), Security and Privacy Workshops (SPW), 2015, S. 159; Rost/Pfitzmann, DuD 2009, S. 353; Rost/Bock, DuD 2012, 743; Hansen, Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals, in: Camenisch u.a. (Hrsg.) Privacy and Identity for Life. IFIP AICT, Bd. 375, Springer, 2012, S. 14; Danezis u.a., Privacy and Data Protection by Design – from policy to engineering, ENISA 2014, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design/at_download/fullReport.

15 Daneben erwähnt Art. 32 Abs. 1 Buchstabe b DSVGO neben den klassischen Sicherheitszielen der Vertraulichkeit, Integrität und Verfügbarkeit auch die Belastbarkeit der Systeme und Dienste.

Datensparsamkeit, die in der DS-GVO in Art. 5 Abs. 1 Buchstabe c DS-GVO als Prinzip der Datenminimierung ausdrücklich normiert ist, konkretisiert den Grundsatz der Erforderlichkeit, nach dem personenbezogene Daten nur in dem Umfang verarbeitet werden dürfen, wie es für das Erreichen des Zwecks erforderlich ist.[16] Danach gilt es, dass Erheben von personenbezogenen Daten von vornherein weitestgehend zu vermeiden und vorhandene personenbezogene Daten schnellstmöglich zu löschen. Dies betrifft die Gestaltung der Verarbeitung insgesamt, d.h. nicht nur Technik und organisatorische Verfahren, sondern auch das Geschäftsmodell oder Geschäftsprozesse in der Organisation.

Verfügbarkeit bedeutet, dass personenbezogene Daten für die Berechtigten rechtzeitig zur Verfügung stehen und ordnungsgemäß verwendet werden können. Integrität beinhaltet die Anforderung, dass die Prozesse und Systeme der Datenverarbeitung gemäß Spezifikation funktionieren und die personenbezogenen Daten unversehrt, vollständig und aktuell sind. Vertraulichkeit betrifft Anforderungen an Geheimhaltung, das heißt, dass kein Unbefugter die personenbezogenen Daten zur Kenntnis nehmen kann. Nichtverkettbarkeit stellt sicher, dass Daten nicht zwischen verschiedenen, getrennt zu haltenden Bereichen verknüpft und nicht für andere als die ursprünglichen Zwecke verarbeitet werden. Transparenz bedeutet, dass die betroffenen Personen erkennen können, welche Umstände und Faktoren für die Verarbeitung der personenbezogenen Daten gelten. Intervenierbarkeit umfasst die Möglichkeit der betroffenen Person zur Kontrolle der sie betreffenden Daten und Verarbeitungen, beispielsweise durch effektive Wahrnehmung der Betroffenenrechte wie Auskunft, Berichtigung, Sperrung oder Löschung sowie Widerruf einer Einwilligung o.ä. Bei der Arbeit mit Schutzzielen ist stets zu berücksichtigen, dass sie und die sie umsetzenden Maßnahmen nicht unabhängig voneinander sind, sondern Wechselwirkungen bestehen und die Schutzziele in ihren Ausprägungen – je nach Kontext – unterschiedlich priorisiert werden müssen.

Für den Bewertungsmaßstab, den die Schutzziele setzen, ist es im Rahmen der DSFA essenziell, die Perspektive der betroffenen Personen, deren Rechte geschützt werden müssen, einzunehmen. Wenn etwa die Transparenzanforderung verletzt wird, weil der Verantwortliche die betroffene Person nicht den gesetzlichen Anforderungen entsprechend informiert hat, muss eine DSFA auf diesen Mangel reagieren. Dies bedeutet: Nicht nur Sicherheitslücken stellen ein Risiko für die betroffene Person und ihre Daten dar, sondern auch andere datenschutzrechtliche Mängel. In dem Fall der fehlenden Information ist beispielsweise der betroffenen Person die Möglichkeit zur Intervention genommen, wenn sie nicht weiß, zu welchen Zwecken welche ihrer Daten verarbeitet werden.

2.2 Identifikation möglicher Angreifer, Angriffsmotive und Angriffsziele

Da die DSFA, wie Art. 35 Abs. 1 DS-GVO ausdrücklich regelt, die Perspektive der von der Datenverarbeitung betroffenen Person einnimmt, können Angriffe nicht nur seitens Dritter, sondern selbst durch regelkonform handelnde interne Anwender der Organisation erfolgen. Anders als in der Informationssicherheit, die die Perspektive der betroffenen Organisation einnimmt, ist das Ziel einer DSFA daher nicht der Schutz der Geschäftspraktiken, sondern der Schutz der Rechte der betroffenen Personen, also der zum Beispiel der Kunden oder auch der Beschäftigten in der Organisation. Folgerichtig muss in diesem Schritt des DSFA-Verfahrens jeder Eingriff in die Rechte der betroffenen Personen durch die Organisation ebenso betrachtet werden wie die Angriffe durch Unbefugte. Insoweit gehören also staatliche Stellen, wie Sicherheitsbehörden oder auch die Leistungsverwaltung, und Unternehmen, etwa IT-Dienstanbieter, Banken oder Interessenvereinigungen sowie Gesundheitsdienstleister oder Forschungsstellen, zu der Menge der potenziellen Angreifer, deren Motive und Angriffsziele zu analysieren sind. Beispielsweise bestünde in diesem Sinne ein Angriff darin, dass eine Abteilung der Organisation eine Nutzung der personenbezogenen Daten zu nicht kompatiblen Zwecken beabsichtigen würde.

Da die Organisation, die die DSFA durchführt, selbst als Risiko zu sehen ist, besteht natürlich ein Interessenskonflikt. Um tote Winkel in der Betrachtung auszuschließen, sollte es daher zumindest eine nachträgliche externe Aufsicht geben. Außerdem ist von der/dem Datenschutzbeauftragten, soweit ein(e) solche(r) ernannt ist, zu erwarten, dass sie/er den Standpunkt der von der Verarbeitung betroffenen Personen einnimmt.

2.3 Bestimmung der Eingriffsintensität und des Schutzbedarfs

Für die Abwägung der Rechte und Interessen der betroffenen Person und des Verantwortlichen ist die Intensität des Eingriffs festzustellen. Der Schutzbedarf ist dabei eng mit der Eingriffsintensität verknüpft: Die Eingriffsintensität blickt von außen auf die betroffene Person und bewertet die Folgen des Eingriffs für diese. Der Schutzbedarf wird aus Sicht der betroffenen Person, unabhängig davon, ob ein Eingriff tatsächlich erfolgt, festgestellt. Hat eine Person etwa eigene, sensible Daten auf einem System, so ergibt sich für sie ein hoher Schutzbedarf, unabhängig davon, was mit diesen Daten geschieht. Wie bereits einleitend ausgeführt, stellt jede, auch rechtmäßige, Verarbeitung personenbezogener Daten einen Eingriff in das Grundrecht auf Datenschutz gem. Art. 8 GRC der betroffenen Personen dar. Daher kann man im Falle einer DSFA den Eintritt eines Schadens – im Unterschied zum für den Bereich der Informationssicherheit entwickelten IT-Grundschutz des BSI[17] – nicht einfach nach Eintrittswahrscheinlichkeit und Schwere des

16 AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder/Schulz/Rost, Das Standard-Datenschutzmodell – Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V.0.9, Darmstadt 2015, S. 9.

17 BSI (Bundesamt für Sicherheit in der Informationstechnik), BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise (Version 2.0), Bonn 2008, https://www.bsi.bund.de/gshb.

Schadens beurteilen. Stattdessen muss ein Eingriff in das Recht auf Datenschutz gem. Art. 8 Abs. 2 und Art. 51 Abs. 1 GRC gerechtfertigt werden. Daraus ist abzuleiten, dass der Schutzbedarf standardmäßig als normal eingestuft werden muss. Aufgrund der hervorgehobenen Stellung des Grundrechtsschutzes im Datenschutzrecht kommt ein niedriger Schutzbedarf nicht in Betracht. Der Datenschutz befasst sich mit der Machtasymmetrie zwischen der betroffenen Person, deren Daten verarbeitet werden, und dem Verantwortlichen, der diese Verarbeitung vornimmt, und kann daher keine geringeren Anforderungen stellen. Allerdings kann bei Verarbeitung besonderer Kategorien von Daten oder bei fehlender Transparenz oder Intervenierbarkeit für die betroffene Person der Schutzbedarf auf hoch oder sehr hoch steigen. Die drei Schutzbedarfsabstufungen werden daher wie folgt beschrieben:

- „Normal“: Personenbezogene Daten werden verarbeitet, und es gibt keine Anwendungsszenarien, bei denen die Verarbeitung eine hohe Eingriffsintensität erwarten lässt.
- „Hoch“:
  - Besondere Kategorien von Daten i.S.v. Art. 9 DS-GVO werden verarbeitet, so dass gesetzlich ein höheres Schutzniveau gefordert ist, oder
  - die betroffenen Personen sind auf die Entscheidungen/Dienste der Organisation angewiesen, soweit
    - die hohe Eingriffsintensität der Datenverarbeitung ernsthafte Folgen für die betroffenen Personen haben kann und/oder
    - es keine effektiven Sicherungsmaßnahmen oder Interventionsmöglichkeiten für die betroffenen Personen gibt (einschließlich der Möglichkeit Rechtsschutz zu erlangen).
- „Sehr hoch“: Personenbezogene Daten, die einen hohen Schutzbedarf aufweisen, werden verarbeitet und die betroffene Person ist in existenziellem Maße von der Entscheidung/dem Dienst der Organisation abhängig, und es bestehen weitere Risiken aufgrund mangelnder Datensicherheit oder unrechtmäßiger Zweckänderungen, die die betroffene Person nicht bemerken und/oder verhindern kann.

Zudem kann ein hoher Schutzbedarf aufgrund kumulativer Effekte verschiedener Aspekte bestehen, die allein keinen hohen Schutz erfordern. Dies kann etwa der Fall sein, wenn personenbezogene Daten über eine große Personengruppe gesammelt werden oder wenn personenbezogene Daten für verschiedene Zwecke erfasst und analysiert werden und die betroffenen Personen in verschiedenen Rollen betroffen sind.

2.4 Bewertung des Risikos

Kern der DSFA ist die Risikobewertung. Diese erfordert nach Art. 35 Abs. 7 Buchstabe c DS-GVO die Bewertung der Risiken für die Rechte der betroffenen Personen. In der Bewertung sind nach Erwägungsgrund 90 DS-GVO für jedes identifizierte Risiko auch die spezifische Eintrittswahrscheinlichkeit und die Schwere zu berücksichtigen. Dafür werden die in Phase 1 benannten Angriffsszenarien und der ermittelte Schutzbedarf aus Phase 2 miteinander in Beziehung gesetzt.

In der Informationssicherheit kennt man die formelhafte Kalkulation des Gesamtrisikos für ein System:
$Risk = \sum_{i=1}^{n} Impact_i \times p_i$ mit $Impact_i$ für das Schadensausmaß des Risikos i und p_i für dessen Eintrittswahrscheinlichkeit.

Die Verwendung dieser Formel ist allerdings weder für Datenschutz- noch Informationssicherheitsrisiken praktikabel. So können in der Informationssicherheit üblicherweise keine exakten Werte angegeben werden: Beispielsweise würde die Eintrittswahrscheinlichkeit für ein Risiko eine ausreichende statistische Datenbasis für das betrachtete System erfordern. Für Datenschutzrisiken und die Perspektive der betroffenen Person gilt dies umso mehr. Während das Schadensausmaß aus Sicht der Organisation häufig zumindest grob kalkulierbar ist, da finanzielle Auswirkungen abgeschätzt werden können, ist ein Risiko für Rechte der betroffenen Person oft kaum zu beziffern und nur in Ausnahmefällen seriös in einer Einheit wie Euro ausdrückbar. Auf Pseudo-Berechnungen sollte in der DSFA verzichtet werden. Stattdessen muss der Verantwortliche eine nachvollziehbare Argumentation für seine Bewertung in Abhängigkeit der Angriffsszenarien und Schutzzielanforderungen liefern.

Als Risiko für die Rechte natürlicher Personen wird in der DS-GVO insbesondere angeführt, dass aus der Verarbeitung personenbezogener Daten physische, materielle oder immaterielle Schäden resultieren könnten. Dabei ist zu berücksichtigen, dass bereits der Eingriff in das Recht auf Schutz der Daten der betroffenen Person aus Art. 8 GRC, wenn dieser nicht gerechtfertigt ist, einen immateriellen Schaden darstellt. Erwägungsgrund 75 nennt als Beispiele Diskriminierung, Identitätsdiebstahl oder -betrug, finanziellen Verlust, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, unbefugte Aufhebung der Pseudonymisierung oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile. Auch das Risiko, dass die betroffenen Personen um ihre Rechte gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wird benannt. Zudem wird ein hohes Risiko dann angenommen, wenn personenbezogene Daten besonderer Kategorien (Art. 9) verarbeitet werden, wenn persönliche Aspekte (Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel) bewertet oder prognostiziert werden, oder wenn personenbezogene Daten schutzbedürftiger natürlicher Personen (z.B. von Kindern) verarbeitet werden. Mit Blick auf die Datensicherheit ergänzt Erwägungsgrund 83 „Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte“.

Nach Erwägungsgrund 76 sollen die Eintrittswahrscheinlichkeit und Schwere des Risikos in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das gesamte Verfahren (also Daten, Systeme und Prozesse) muss dabei im Blickfeld stehen und vom Verantwortlichen in Bezug auf die möglichen Risiken beurteilt werden. Soweit der in Phase 1 definierte Prüfgegenstand bereits implementierte oder geplante technisch-organisatorische Maßnahmen umfasst, wie sie auch in Art. 32 DS-GVO gefordert sind, unterfallen diese ebenfalls der Bewertung. Dies ist auch sinnvoll, da bestimmte Maßnahmen bereits in den verbreiteten Datenverarbeitungssystemen enthalten sind, beispielsweise Rollen- und Rechtekonzepte in Datenbanken und Betriebssystemen.

Bei der Bewertung des Risikos ist aber wesentlich, dass die vorhandenen Maßnahmen richtig umgesetzt werden, da singuläre Maßnahmen nicht ausreichen. So kann etwa die Vertraulichkeit eines Systems durch Rollen- und Rechtekonzepte gestärkt werden. Allerdings kann dies allein die Anforderungen der Vertraulichkeit nicht erfüllen. Denn wenn die eingeräumten Rechte zu weitgehend sind oder es keine klare Rollentrennung gibt, ist das Konzept nicht effektiv. Der Verantwortliche muss daher in der Risikobewertung darlegen, inwiefern das Rechte- und Rollenkonzept des konkreten Systems die Vertraulichkeit der Daten garantiert.

3. Maßnahmenphase

In der Maßnahmenphase werden die Ergebnisse der Risikobewertung umgesetzt und passende Schutzmaßnahmen identifiziert. Nach Art. 35 Abs. 7 Buchstabe d DS-GVO muss die DSFA Maßnahmen enthalten, die die identifizierten Risiken bewältigen, und es muss der Nachweis erbracht werden, dass die DS-GVO in ihrer Gesamtheit erfüllt wird, wobei die Rechte und berechtigten Interessen der betroffenen Personen sowie auch sonstiger Betroffener zu berücksichtigen sind. Hier ist die Angemessenheit der Datenverarbeitung zu beurteilen, wobei das Interesse des Verantwortlichen an der Datenverarbeitung zu den genannten Zwecken mit den Rechten und Interessen der betroffenen Person abgewogen werden muss.

3.1 Identifikation und Auswahl passender Schutzmaßnahmen

Die Auswahl der Maßnahmen lässt sich durch einen Katalog von Referenzschutzmaßnahmen unterstützen, wie er zurzeit vom AK Technik der Konferenz der unabhängigen Datenschutzbehörden entwickelt wird.[18] Allerdings ist zu beachten, dass es sich dabei um keine Checkliste handelt, auf der man Maßnahmen abhakt. Dies wäre auf Basis der Risikobewertung unzureichend. Stattdessen müssen das gesamte Verfahren und die Schutzziele des Standard-Datenschutzmodells mit ihren Wechselwirkungen berücksichtigt werden. Dafür ist eine Soll-Ist-Betrachtung hilfreich, durch die deutlich wird, inwieweit die geplanten Maßnahmen den Vorgaben des Standard-Datenschutzmodells entsprechen (siehe Abb. 2). Im Rahmen der Auswahl der Maßnahmen sind die Rechte und Interessen der betroffenen Personen sowie sonstiger Betroffener zu berücksichtigen.

18 AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder/Schulz/Rost, Das Standard-Datenschutzmodell – Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V.0.9, Darmstadt 2015, Kapitel 7.

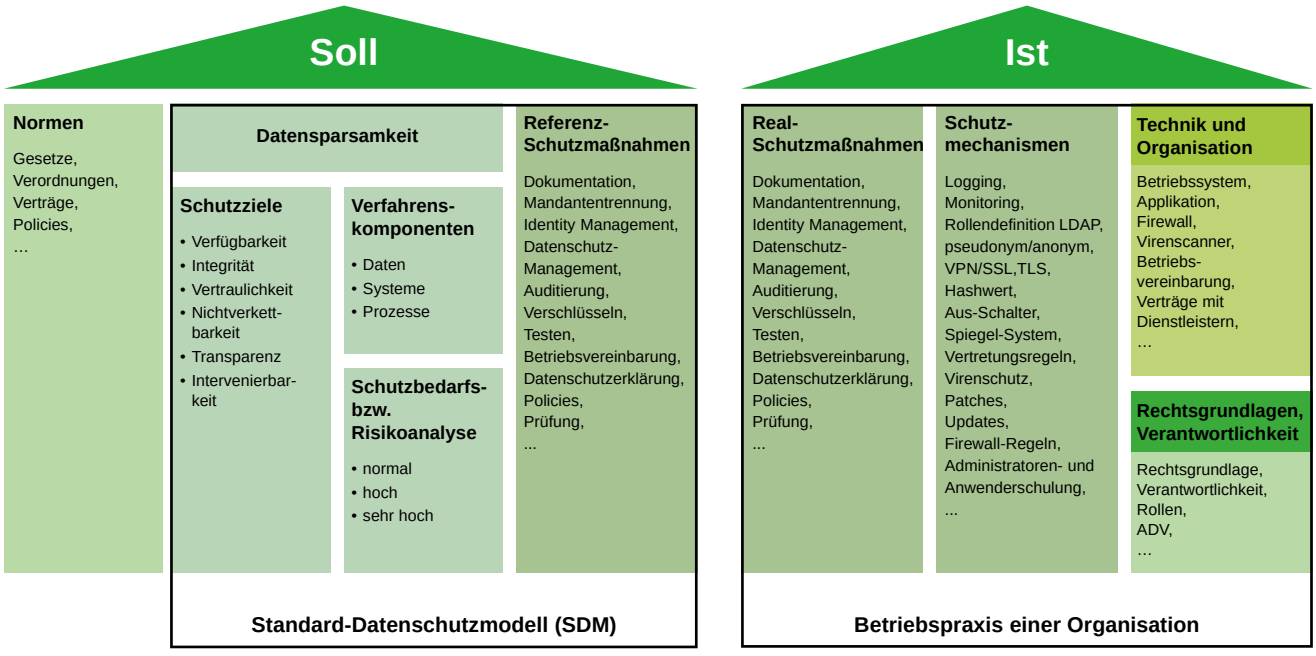

Abb. 2: Soll-Ist-Abgleich gemäß Standard-Datenschutzmodell

Auch in der Praxis erleichtert der Soll-Ist-Vergleich die Überprüfung der Risikobewertung. Hat ein Verantwortlicher zum Beispiel gar kein Rechte- und Rollenkonzept eingeplant, ist die Abweichung offensichtlich und muss begründet werden. Aber auch wenn es ein solches gibt, muss dies mitsamt seiner Funktion schlüssig dargelegt werden. Die ausgewählten Maßnahmen müssen dem Stand der Technik entsprechend gem. Art. 25 Abs. 1 u. Art. 32 DS-GVO regelmäßig aktualisiert werden.

Da die DSFA den Schutz von Individualrechte bezweckt, ist es nicht hinnehmbar, ein identifiziertes Risiko mit einer geringen Anzahl von betroffenen Personen als akzeptabel einzustufen und nur Maßnahmen zur Schadensminderung zu ergreifen. Es besteht jedoch die Möglichkeit, Risiken zu priorisieren und die Maßnahmen zu ergreifen, die den höchsten Nutzen für die betroffenen Personen haben und mit den rechtlichen Anforderungen übereinstimmen. Bei der Auswahl der Maßnahmen sollte der Verantwortliche insbesondere darlegen, welche Maßnahmen zur Verringerung oder Vermeidung von Eingriffen in die Rechte der betroffenen Personen oder um Schäden von ihnen abzuwenden, getroffen werden. Zudem sollte festgelegt sein, wer für die Umsetzung der Maßnahmen verantwortlich ist und welche Personen dabei einzubeziehen sind. Außerdem sollte der Verantwortliche bestimmen, bis wann die Maßnahmen umgesetzt sein sollen und welche Mittel dafür zur Verfügung stehen. Auch die Zuständigkeit für die Durchführung der Tests und Dokumentation der Wirksamkeit der Schutzmaßnahmen sind zu regeln.

3.2 Dokumentation der Bewertungsergebnisse

Nach der Bewertungsphase und Identifikation passender Schutzmaßnahmen müssen die Bewertungsergebnisse und die getroffene Auswahl dokumentiert werden. Diese Dokumentation umfasst nicht nur die erfolgreich eindämmbaren Risiken. Können etwa bestimmte Risiken nicht (vollständig) durch die Maßnahmen beseitigt werden, müssen diese verbleibende Restrisiken gerechtfertigt werden: Es muss dargestellt werden, aus welchen Gründen sie nicht oder nur zum Teil ausgeschlossen werden können. Sofern es sich bei den verbleibenden Restrisiken um hohe Risiken handelt, darf das untersuchte System nicht freigegeben werden und damit nicht zum Einsatz kommen. In dem Fall wären die Anforderungen der DS-GVO nicht erfüllt. Art. 36 der DS-GVO sieht jedenfalls in einem solchen Fall vor, dass der Verantwortliche vor der Verarbeitung die Aufsichtsbehörde kontaktiert („vorherige Konsultation"), die die DSFA überprüfen und Empfehlungen abgeben muss.

3.3 Implementierung der Schutzmaßnahmen

Sofern die DSAF nicht nur ein Konzept für einen möglichen Einsatz, sondern ein konkretes Verarbeitungssystem betrifft, müssen die vorher ausgewählten Maßnahmen umgesetzt werden. Dies kann parallel zu der Dokumentation der Bewertungsergebnisse erfolgen. Die Umsetzung betrifft in der Regel technisch-organisatorische Maßnahmen, beispielsweise hardware- oder softwarebasierte Funktionalität für einen besseren Schutz der personenbezogenen Daten, Konfigurationsanpassungen, Konzepte mit Festlegungen der Rollen und Rechte, die in die Praxis umzusetzen sind, oder Prozesse zum Umgang mit Beschwerden der betroffenen Personen. Es ist auch möglich, dass dem Risiko dadurch begegnet wird, dass bei geeigneter technischer Realisierung auf personenbezogene Daten verzichtet werden kann oder dass bestimmte risikoträchtige Funktionalität abgeschaltet wird.

3.4 Test und Dokumentation der Wirksamkeit der Schutzmaßnahmen

Die Implementierung der Schutzmaßnahmen allein reicht nicht aus. Zusätzlich muss die Wirksamkeit der Maßnahmen getestet und dokumentiert werden. Auch die Durchführung der Tests und die Testergebnisse sind zu dokumentieren.

3.5 Nachweis über die Einhaltung der DS-GVO insgesamt

Für den Nachweis, dass der betrachtete Prüfgegenstand – erweitert um die getroffenen Schutzmaßnahmen – die DS-GVO in ihrer Gesamtheit erfüllt, ist neben der Umsetzung der gewählten Schutzmaßnahmen eine Dokumentation der Verarbeitungsvorgänge, Risiken und Maßnahmen nötig. Die Gesamtheit der Dokumente dient nicht nur als Grundlage für den DSFA-Bericht, sondern auch der Freigabe der Datenverarbeitung durch den Verantwortlichen.[19] Datenverarbeitungssysteme für personenbezogene Daten sollten nicht eingesetzt werden, bevor die Freigabe auf Basis einer nachvollziehbaren Dokumentation erfolgt ist.

Änderungen der Maßnahmen können zu Änderungen des Prüfgegenstands oder der Akteure und betroffenen Personen führen. Es ist daher zu beachten, dass bei der Durchführung der DSFA nicht lediglich linear von Phase 1 bis 4 vorgegangen werden kann, sondern dass eine Rückkoppelung der jeweiligen Ergebnisse, im Sinne eines iterativen Vorgehens, sinnvoll ist. Beispielsweise kann es durch die Wahl entsprechender Maßnahmen zu einer weiteren Verarbeitung personenbezogener Daten kommen, für die wiederum die etwaigen Risiken zu betrachten sind. Eine ergebnisoffene Vorgehensweise wird daher üblicherweise verschiedene Maßnahmen-Sets beleuchten, bis das die DSFA durchführende Team davon überzeugt ist, dass die DS-GVO in ihrer Gesamtheit eingehalten wird und mit dem Ergebnis zufrieden ist.

19 So hat es etwa der Gesetzgeber in der Datenschutzverordnung Schleswig-Holstein geregelt, die auf dem Landesdatenschutzgesetz Schleswig-Holstein beruht.

4 Berichtsphase

4.1 Erstellung eines DSFA-Berichts

Für den Bericht zur DSFA bietet es sich die Orientierung an den einzelnen Phasen an, so dass der Prüfgegenstand, die Kriterien, die Bewertung und die Maßnahmenwahl in getrennten Abschnitten nachvollziehbar dargestellt werden. Die umfassende Dokumentation der Bewertungsergebnisse in einem DSFA-Bericht gewährleistet, dass die Ziele der DSFA erreicht werden. Dieser Bericht muss den Datenschutzaufsichtsbehörden gem. Art. 58 Abs. 1 Buchstabe a DS-GVO auf deren Verlangen vorgelegt werden.

4.2 Veröffentlichung des DSFA-Berichts

Der DSFA-Bericht sollte im Sinne der Transparenz veröffentlicht werden, zumindest in einer Kurzversion, die Geschäftsgeheimnisse sowie die Restrisikoanalyse, die sonst als Angriffsvorlage missbraucht werden könnte, schützt. Es sollten aber alle wesentlichen Informationen enthalten sein und keine (negativen) Ergebnisse der Untersuchung verschwiegen werden.

4.3 Unabhängige Überprüfung der DSFA-Ergebnisse

Um zu gewährleisten, dass die DSFA ordnungsgemäß durchgeführt wurde, sollte die DSFA anhand des DSFA-Berichts von einem unabhängigen Dritten, etwa der zuständigen Datenschutzaufsichtsbehörde, überprüft werden können. Dies umfasst insbesondere den Umgang mit Interessenskonflikten, die ausreichende Berücksichtigung der Rechte und Interessen der betroffenen Personen bei der Identifikation der Risiken, die Angemessenheit der ausgewählten Maßnahmen, genügende Information der Öffentlichkeit und die Sicherstellung, dass die gewählten Maßnahmen auch tatsächlich umgesetzt werden.

5. Überwachung und Fortschreibung

Eine DSFA ist kein strikt linearer oder abgeschlossener Prozess, sondern muss während des gesamten Lebenszyklus eines Projekts fortlaufend überwacht werden. Dementsprechend legt Art. 35 Abs. 11 DS-GVO fest, dass die DSFA jedenfalls dann zu wiederholen ist, wenn sich das mit der Verarbeitung verbundene Risiko ändert. Solche Änderungen können sich durch Veränderung der organisatorischen oder rechtlichen Rahmenbedingungen oder neue Risiken für den Datenschutz im Allgemeinen ergeben. Es gilt stets sicherzustellen, dass die Maßnahmen an solche Veränderungen angepasst werden können. Um auf Veränderungen der Rahmenbedingungen möglichst effizient reagieren zu können, ist eine Einbindung in das allgemeine Datenschutz-Management der Organisation ratsam.

II. Übergang in die neue Welt der DS-GVO

Die Datenschutz-Folgenabschätzung ist zwar in ihrer Beschreibung in der DS-GVO ein neues Instrument. Allerdings ist es auch gemäß der heutigen Rechtslage erforderlich, dass die Datenverarbeitung den Prinzipien der Zweckbindung und Erforderlichkeit genügt, dass die Verarbeitungsvorgänge dokumentiert vorliegen (z.B. im Verfahrensverzeichnis, das die/der Datenschutzbeauftragte führt) und dass die erforderlichen technisch-organisatorischen Maßnahmen getroffen und dokumentiert werden. Ziel ist die Beherrschbarkeit des Risikos, das mit der Datenverarbeitung einhergeht. Risikoanalysen sind zudem aus der Informationssicherheit bekannt.

Neu ist die Betonung der Rechte und Freiheiten der betroffenen Personen, die in herkömmlichen Risikoanalysen aus Organisationssicht zumeist unterreflektiert sind. Wer sich als verantwortliche Stelle heute datenschutzkonform aufgestellt hat, sollte auf Basis der vorhandenen Dokumente (Verfahrensverzeichnis, Sicherheitskonzept, Restrisikoanalyse, Test- und Freigabedokumente, sonstige Dokumentation) relativ schnell eine Datenschutz-Folgenabschätzung durchführen können – auch wenn der Fokus der DSFA deutlicher auf den Grundrechten statt auf Informationssicherheit liegen muss. Da die DS-GVO keine Meldepflicht der Datenverarbeitung (außer bezüglich der Informationspflicht im Fall von Datenpannen) an die Aufsichtsbehörde vorsieht,[20] besteht die Motivation für die Durchführung der DSFA darin, Risiken für die betroffenen Personen und indirekt auch für die Organisation (Sanktionierung durch Aufsichtsbehörden, Reputationsverlust) zu vermeiden und sich abzusichern.

Eine weitere interessante Nutzungsmöglichkeit der DSFA wird in Art. 35 Abs. 10 der DS-GVO angesprochen: Auch Rechtsgrundlagen, die Verarbeitungsvorgänge konkret regeln, können im Gesetzgebungsverfahren einer Folgenabschätzung unterzogen werden, in der die Anforderungen aus der DS-GVO berücksichtigt werden. In diesen Fällen können die Mitgliedstaaten regeln, dass eine nachfolgende DSFA durch den Verantwortlichen entbehrlich ist. Besser als ein Verzicht auf die DSFA ist es jedoch, wenn der Verantwortliche eine eigene DSFA für seinen Anwendungskontext mit seinen spezifischen Maßnahmen durchführt, die auf der abstrakten Gesetzes-DSFA beruht und sie konkretisiert. Eine solche DSFA wäre zügig durchführbar und hätte den Vorteil, dass die Einsatzbedingungen vor Ort geprüft werden und sich der Verantwortliche damit ein Bewusstsein über die Risiken und ihre Behandlung verschafft.

Ohnehin wäre es sehr sinnvoll, wenn die Datenverarbeitungssysteme – mindestens alle zertifizierten Produkte – als „Beipackzettel“ bereits die für die DSFA nötigen Informationen beinhalten würden. Beispielsweise könnte ein Muster für eine DSFA beigefügt sein, das die Anwender darauf hinweisen würde, welche Einsatzbedingungen zu garantieren sind, wo für die Durchführung der eigenen DSFA Angaben ergänzt werden müssen und wie die Risiken vor Ort zu bewerten sind.

20 Vgl. Erwägungsgrund 89 DS-GVO.

III. Fazit

Die DSFA hat großes Potenzial, den Schutz der Rechte von betroffenen Personen zu verbessern. Dabei ist insbesondere die Identifikation von Risiken durch neue Datenverarbeitungstechnologien für den Einzelnen hilfreich. Die Datenschutz-Folgenabschätzung dient dabei als Frühwarnsystem, dass alle Beteiligten in die Lage versetzt, potenzielle Schwachstellen in einem Verfahren systematisch zu finden und zu beseitigen. Das vorgestellte Verfahren bietet die Möglichkeit, den Schutz von Individuen, wie er von der DS-GVO beabsichtigt ist, im DSFA-Verfahren praktisch umzusetzen. Der Schutz der Grundrechte als das Leitmotiv des Datenschutzes, wie es auch in Art. 1 Abs. 2 DS-GVO normiert ist, rückt dabei endlich in den Vordergrund.

Felix Bieker, LL.M. Eur. (Edinburgh)
ist juristischer Mitarbeiter im Projektreferat des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD).

Dipl.-Inform. Marit Hansen
ist seit 2015 die Landesbeauftragte für Datenschutz Schleswig-Holstein und leitet das ULD.

Dr. Michael Friedewald
leitet am Fraunhofer-Institut für System- und Innovationsforschung in Karlsruhe das Geschäftsfeld Informations- und Kommunikationstechnik und koordiniert das BMBF Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt.

Dr. Niels Lepperhoff

Dokumentationspflichten in der DS-GVO

Bisher galt das Prinzip, dass die Aufsichtsbehörde Verstöße eines Unternehmens gegen Datenschutzvorschriften belegen muss. Ein Unternehmen war nicht verpflichtet, anlasslos eine Dokumentation zu erstellen und zu pflegen, mit der es sein gesetzeskonformes Handeln nachweisen konnte. Dies wird sich mit dem Inkrafttreten der Datenschutz-Grundverordnung grundlegend ändern. Dann müssen Unternehmen jederzeit in der Lage sein, die Rechtmäßigkeit ihrer Verarbeitung nachweisen zu können. So kann zukünftig auch eine fehlende Dokumentation mit einem Bußgeld belegt werden – sogar dann wenn die dazugehörige Verarbeitung rechtskonform erfolgt ist. Vor diesem Hintergrund sollte jedes Unternehmen ein Dokumentationssystem einführen oder das bereits vorhandene an die neue Rechtslage anpassen.

I. Einleitung

Der Dokumentation kommt in der Datenschutz-Grundverordnung (DS-GVO) eine größere Bedeutung zu als bisher. Die Bedeutung speist sich primär aus der in Art. 5 Abs. 2 DS-GVO eingeführten „Rechenschaftspflicht“:

„(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).“

Art. 24 Abs. 1 S. 1 DS-GVO konkretisiert die Anforderungen zur Erfüllung der Rechenschaftspflicht wie folgt:

„(1) Der Verantwortliche setzt […] geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. […]“

Die Nachweispflicht bezieht sich explizit auf die gesamte Verordnung und umfasst somit auch die die Grundsätze der DS-GVO (Art. 5 Abs. 1 DS-GVO):

- Rechtmäßigkeit, Verarbeitung[1] nach Treu und Glauben und Transparenz,
- Zweckbindung,
- Datenminimierung,
- Richtigkeit,
- Speicherbegrenzung sowie
- Integrität und Vertraulichkeit.

Diese Grundsätze werden durch die weiteren Vorschriften der DS-GVO konkretisiert, so dass ein nicht geführter Nachweis

1 Art. 4 Nr. 2 DS-GVO fasst unter „Verarbeitung“ alle Phasen von der Erhebung über die Nutzung bis zur Löschung zusammen. Die Trennung von Erhebung und Verarbeitung aus § 3 Abs. 3 und 4 BDSG wird aufgegeben.

gemäß Art. 24 Abs.1 DS-GVO regelmäßig auch den Nachweis nach Art. 5 Abs. 2 DS-GVO scheitern lässt. Ein Verstoß gegen Art. 5 DS-GVO ist mit einem Bußgeld bis zu 20 Mio. Euro oder – sofern höher – 4 % des weltweiten Jahresumsatzes bewehrt.[2] Gelingt der Nachweis der Einhaltung nicht, ist bereits von einem Verstoß gegen Art. 5 Abs. 2 DS-GVO auszugehen. Die Frage, ob ein weitergehender Verstoß wie bspw. eine unzulässige Datenverarbeitung tatsächlich begangen wurde, kann dahinter zurücktreten.

Zusätzlich haften Auftraggeber und Auftragnehmer in einer Auftragsverarbeitung gesamtschuldnerisch, sofern ihnen der Nachweis des Unbeteiligtseins nicht gelingt.[3] Die DS-GVO bezeichnet mit dem Begriff „Auftragsverarbeitung"[4] die aus § 11 BDSG bekannte „Auftragsdatenverarbeitung".

Die Dokumentation der Befolgung der DS-GVO in ihrer Gesamtheit wird von zentraler Bedeutung sein. Eine Betrachtung der DS-GVO, die sich auf wenige Artikel der DS-GVO konzentriert, neigt zum Verkennen der Sachlage.[5]

Dieser Beitrag will die Anforderungen an die Dokumentation insbesondere für Unternehmen und andere nichtöffentliche Stellen beleuchten. Der Schwerpunkt der Betrachtung liegt auf den für alle Branchen geltenden Vorschriften, d.h. Bereichsregelungen bspw. aus Art. 89 DS-GVO bleiben unberücksichtigt. Für Unternehmen aus Drittstaaten gelten zusätzlich die Vorschriften nach Art. 27 DS-GVO zur Benennung eines Vertreters.

II. Anforderungen an ein Dokumentationssystem

Mit Blick auf eine praktische Umsetzung stellt sich die Frage nach Inhalt und Grenzen der Dokumentationspflicht. Art. 24 Abs. 1 DS-GVO umreißt die Grenzen mittels einer Abwägung zwischen

- den Implementierungskosten auf der einen Seite und
- der Verarbeitungsart,
- dem Verarbeitungsumfang,
- den Umständen und den Zwecken der Verarbeitung sowie
- der Wahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen (Mitarbeiter, Nutzer, Kunden, Lieferanten usw.) auf der anderen Seite.

Wo genau die Grenze verläuft hängt folglich vom Einzelfall ab. Weiter spielt die Haftungsvermeidung, d.h. das Risiko, den Nachweis der Normbefolgung nicht erbringen zu können, zu minimieren, eine nicht unerhebliche Rolle.

Aus den Vorschriften der DS-GVO lassen sich Mindestinhalte der Dokumentation ableiten. Diese speisen sich aus zwei Quellen:

- Explizite Vorschriften wie z.B. das „Verzeichnis von Verarbeitungstätigkeiten" nach Art. 30 DS-GVO und
- Implizite Anforderungen.

Unter eine implizite Anforderung fallen Normen,

- deren Befolgung entweder durch eine Einzelvorschrift aus Haftungsgründen nachweisbar sein sollte oder
- deren Ergebnis von anderen Normen benötigt wird.

Ein Beispiel für den ersten Fall ist die Einhaltung der Reaktionsfrist bei einer Betroffenenanfrage von grundsätzlich einem Monat gemäß Art. 12 Abs. 3 DS-GVO. Eine Fristüberschreitung stellt einen bußgeldbewehrten Verstoß dar.[6]

Die Informationspflichten nach Art. 13 und 14 DS-GVO sind ein Beispiel für den zweiten Fall, da sie auch die Nennung der Rechtsgrundlagen umfassen, die deshalb bei der Umsetzung von Art. 6 DS-GVO dokumentiert werden sollten. Abbildung 1 zeigt – ohne Anspruch auf Vollständigkeit – zur Illustration eine Übersicht der Normen, die Auswirkungen auf die Dokumentation haben.

2 Art. 83 Abs. 5 Lit. a) DS-GVO.
3 Art. 82 Abs. 3 DS-GVO.
4 Art. 28 DS-GVO.
5 So Hansen-Oest, Datenschutzrechtliche Dokumentationspflichten nach dem BDSG und der Datenschutz-Grundverordnung, PinG 2016, 84.
6 Art. 83 Abs. 5 Lit. b DS-GVO.

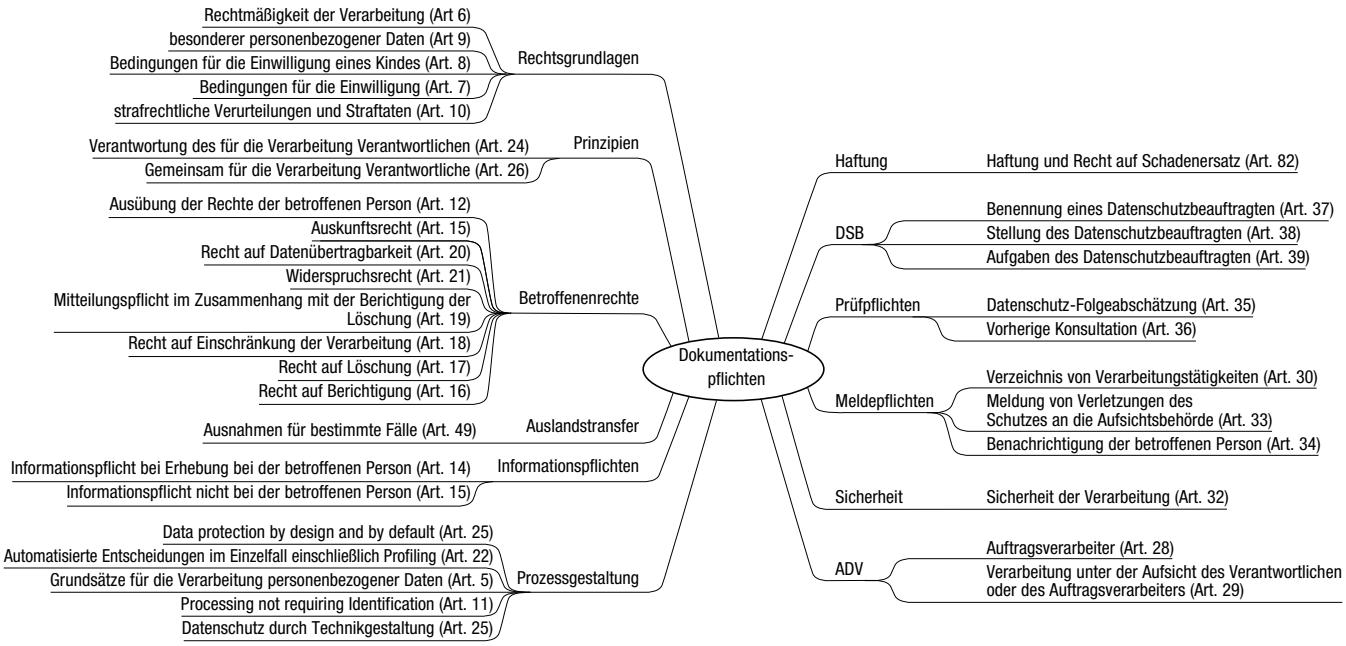

Abb. 1: Übersicht über Normen mit Auswirkungen auf die Dokumentation

III. Inhalte der Dokumentation

Die DS-GVO trifft keine Aussagen, wie eine Dokumentation ausgestaltet sein soll. Das eröffnet Unternehmen Spielräume, vorhandene Systeme und Normen wie z.B. ISO 9001 für das Qualitätsmanagement oder ISO 27001 für das Informationssicherheitsmanagement einzubeziehen und im Rahmen eines unternehmensweiten Dokumentationssystems zu harmonisieren.

Im Folgenden wird exemplarisch der PDCA-Zyklus[7] aus dem Standard BSI 100-1 und der ISO 27001 zur Strukturierung der Dokumentation verwendet. Der hier dargestellte Zyklus bezieht sich auf das Unternehmen als Ganzes. Abbildung 2 zeigt beispielhaft, welche Arten von Dokumenten welcher Phase zugeordnet werden können. Im Folgenden wird erläutert, welche Mindestinhalte sich für die einzelnen Phasen aus der DS-GVO ableiten lassen.

1. Phase Planung

Die Planung legt das Fundament dafür, dass die Verarbeitung im Einklang mit der DS-GVO erfolgt, sofern den Vorgaben der Planung entsprechend gehandelt wird. Aus Sicht der DS-GVO ist insbesondere Folgendes zu dokumentieren:

- Zwecke,
- Rechtsgrundlagen insbesondere nach Art. 6-10 und die Datenübermittlung in Drittstatten nach Art. 44-50 DS-GVO,
- etwaige Interessensabwägungen,
- das Sicherheitskonzept und
- Beschreibungen von Unternehmensprozessen.

1.1. Zwecke und Rechtsgrundlagen

Die Zwecke und Rechtsgrundlagen werden nicht nur zum Nachweis der Rechtmäßigkeit benötigt, sondern u.a. auch im Rahmen der Informationspflicht nach Art. 13 Abs. 1 Lit. c) und 14 Abs. 1 Lit. c) DS-GVO sowie für die Erstellung des Sicherheitskonzepts nach Art. 32 Abs. 1 DS-GVO. Weiterhin legen die Zwecke und Rechtsgrundlagen fest, ab wann die Löschpflicht nach Art. 5 Abs. 1 Lit. e) DS-GVO greift.

7 „P“ steht für Planung („plan“ im Englischen), „D“ für Umsetzung („do“), „C“ für Kontrolle („check“) und „A“ für Mängelbeseitigung („act“).

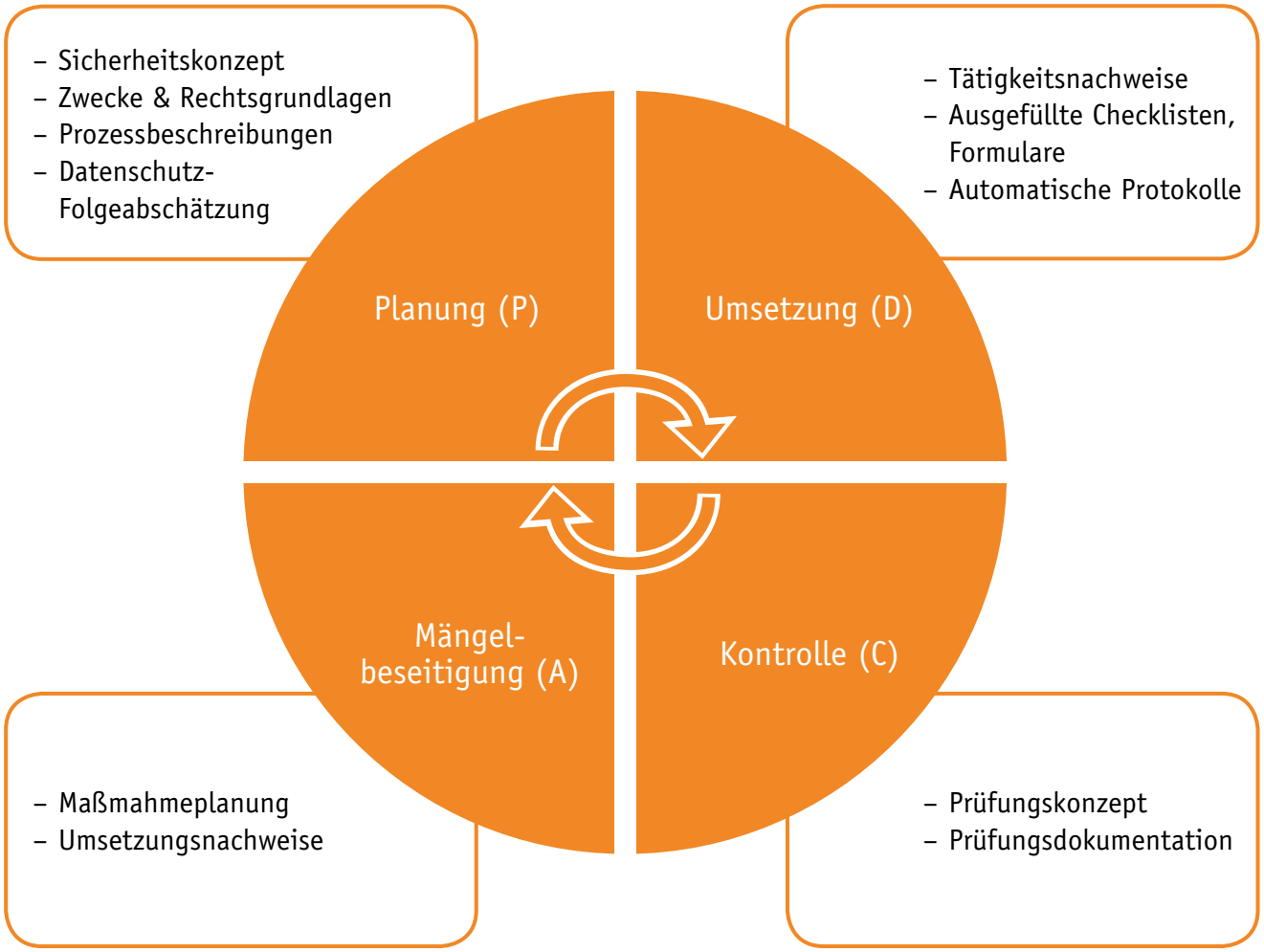

Abb. 2: PDCA-Zyklus als Strukturierungshilfe

1.2 Interessensabwägung

Eine Interessensabwägung sollte aus Nachweisgründen dokumentiert werden. Die Interessen des Verantwortlichen sind im Rahmen der Informationspflichten nach Art. 13 Abs. 1 Lit. d) und Art. 14 Abs. 2 Lit. b) DS-GVO offenzulegen.

1.3 Sicherheitskonzept

Das Sicherheitskonzept nach Art. 32 Abs. 1 DS-GVO gehört ebenfalls zur Planungsphase. Ein Element des Sicherheitskonzepts, um nach Art. 32 Abs. 4 DS-GVO „[...] sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten [...]“ ist das Berechtigungskonzept. Für Auftragsverarbeiter normiert Art. 29 DS-GVO mit Bezug zur Weisungsgebundenheit eine vergleichbare Vorgabe.

Das Protokollkonzept ist ein weiteres Element des Sicherheitskonzepts (siehe Abschnitt 3.2).

1.4 Beschreibung der Unternehmensprozesse

Eine Beschreibung der Unternehmensprozesse ist aus zwei Gründen angeraten: Erstens verlangt Art. 32 Abs. 4 DS-GVO sicherzustellen, dass Mitarbeiter oder andere Personen mit Zugang zu personenbezogenen Daten diese nur innerhalb der Weisungen des Unternehmens verarbeiten, sofern das europäische oder nationale Recht nicht zur Verarbeitung verpflichtet. Die spiegelbildliche Vorschrift in Art. 29 DS-GVO stellt ebenfalls die Weisungen ins Zentrum, indem sie den mit der Datenverarbeitung betrauten Personen eine Verarbeitung ohne Weisung untersagt. Prozessbeschreibungen und Arbeitsanweisungen stellen solche „Weisungen“ zur Verarbeitung dar. Damit der Nachweis des „Sicherstellens“ gelingen kann, empfiehlt es sich, alles zu dokumentieren, was als „Weisung“ gewertet werden kann.

Zweitens gelten die in Art. 5 DS-GVO formulierten Prinzipien sowie die Regelungen des Art. 25 DS-GVO („Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“) für elektronisch ablaufende Prozesse. Eine entsprechend gestaltete Prozessbeschreibung hilft, die Einhaltung nachweisen zu können.

Für die Planung der Überwachung der Einhaltung von Datenschutzvorschriften nach Art. 39 Abs. 1 Lit. b) DS-GVO muss der Datenschutzbeauftragte eine Risikobetrachtung durchführen.[8] Im Rahmen der Prozessbeschreibung kann eine solche Risikobewertung zumindest vorbereitet werden.

Um die Betroffenenrechte auf Einschränkung der Verarbeitung[9] und Widerspruch[10] umsetzen zu können, bietet es sich an zu dokumentieren, wie Sperrmöglichkeiten für die jeweiligen Verarbeitungen auf Feld- und Personenebene umgesetzt werden.

Für automatische Einzelfallentscheidungen und Profiling sind weiterhin die Vorschriften aus Art. 22 DS-GVO im Rahmen der Dokumentation zu beachten.

Die DS-GVO setzt die Existenz einiger Prozesse zur Erfüllung ihrer Anforderungen voraus. Sowohl diese Prozesse sollten aus den obengenannten Gründen dokumentiert werden, als auch als Nachweis, dass die Anforderungen aus der DS-GVO umgesetzt werden. Aus Platzgründen muss auf Detailbeschreibungen der folgenden Prozesse verzichtet werden:

- Umsetzung der Betroffenenrechte auf Information[11], Auskunft[12], Berichtigung[13], Löschung[14] und Einschränkung der Verarbeitung[15], Datenportabilität[16], Widerspruch und Information der Datenempfänger[17] und die korrespondierenden Meldepflichten[18],
- Umsetzung der Sicherheitsanforderungen hinsichtlich Wirksamkeitsprüfung aller technischen und organisatorischen Maßnahmen[19], Dokumentation von Sicherheitsvorfällen[20], Meldung von Sicherheitsvorfällen an die Aufsichtsbehörde[21] und an den Betroffenen[22],
- Überprüfung der technischen und organisatorischen Maßnahmen zur Technikgestaltung und durch datenschutzfreundliche Voreinstellungen[23],
- Durchführung von Datenschutz-Folgenabschätzungen[24] ggf. mit vorheriger Konsultation der Aufsichtsbehörde[25],
- Information der Aufsichtsbehörde über Drittstaatentransfer[26],
- Information der Aufsichtsbehörde über und Veröffentlichung der Bestellung eines Datenschutzbeauftragten[27] und
- Dokumentation der erteilten Weisungen an den Auftragnehmer im Rahmen einer Auftragsverarbeitung durch Auftraggeber[28].

Im Rahmen von Auftragsverarbeitungen nach Art. 28 DS-GVO, im BDSG Auftragsdatenverarbeitungen genannt, kommen auf Seiten des Auftragnehmers folgende Prozesse zusätzlich zu den oben genannten hinzu:

8 Art. 39 Abs.2 DS-GVO.

9 Art. 18 DS-GVO.

10 Art. 21 DS-GVO.

11 Art. 12 mit generellen und Art. 13 und 14 DS-GVO mit spezifischen Vorgaben.

12 Art. 12 mit generellen und Art. 15 DS-GVO mit spezifischen Vorgaben.

13 Art. 12 mit generellen und Art. 16 DS-GVO mit spezifischen Vorgaben.

14 Art. 12 mit generellen und Art. 17 DS-GVO mit spezifischen Vorgaben.

15 Art. 12 mit generellen und Art. 18 DS-GVO mit spezifischen Vorgaben.

16 Art. 12 mit generellen und Art. 20 DS-GVO mit spezifischen Vorgaben.

17 Art. 12 mit generellen und Art. 21 DS-GVO mit spezifischen Vorgaben.

18 Art. 12 mit generellen und Art. 19 DS-GVO mit spezifischen Vorgaben.

19 Art. 24 Abs. 1 DS-GVO und Art. 32 Abs. 1 Lit. d) DS-GVO.

20 Art. 33 Abs. 5 DS-GVO. Die Dokumentationspflicht erstreckt sich auch auf Sicherheitsvorfälle, die keine Meldepflicht auslösen, da Abs. 5 keine Einschränkung wie Abs. 1 vorsieht.

21 Art. 33 Abs. 1-4 DS-GVO.

22 Art. 34 DS-GVO.

23 Konsequenz aus der in Art. 25 Abs. 1 und 2 DS-GVO genannten Forderung nach Sicherstellung.

24 Art. 35 DS-GVO.

25 Art. 36 DS-GVO.

26 Art. 49 Abs. 1 DS-GVO.

27 Art. 37 Abs. 6+7 DS-GVO.

28 Art. 28 Abs. 3 Lit. a) DS-GVO verlangt „dokumentierte“ Weisungen und Art. 29 DS-GVO bindet den Auftragsverarbeiter an diese Weisungen; im Rahmen der gesamtschuldnerischen Haftung können dokumentierte Weisungen zu einer Freistellung führen (Art. 82 Abs. 2 DS-GVO).

- Meldung von Sicherheitsvorfällen an den Auftraggeber[29],
- Auswahl eines (Unter-)Auftragnehmers[30],
- Information des Auftraggebers über neuen Unterauftragnehmer[31] und
- Dokumentation der erhaltenen Weisungen[32].

Da sich die Anforderungen gegenüber dem BDSG bspw. im Bereich der Betroffenenrechte oder Meldepflichten verändert haben, empfiehlt es sich, bestehende Prozesse auf Übereinstimmung mit den Vorgaben aus der DS-GVO zu überprüfen.

2. Phase Umsetzung

Prozessbeschreibungen, Arbeitsanweisungen aber auch in Softwaresystemen hinterlegte Workflows lassen sich als Weisungen i.S.v. Art. 29 DS-GVO auffassen, die die mit der Verarbeitung der personenbezogenen Daten betrauten Personen – typischerweise Mitarbeiter – binden. Eine Verarbeitung ohne Weisung stellt einerseits einen Verstoß der Person gegen Art. 29 DS-GVO dar, aber auch einen Verstoß der Sicherstellungspflicht nach Art. 32 Abs. 4 DS-GVO durch das Unternehmen. Es ist zudem nicht ausgeschlossen, dass Auftragsverarbeiter mit dem Verstoß über Zwecke oder Mittel der Datenverarbeitung bestimmen, wodurch diese nach Art. 28 Abs. 10 DS-GVO zum für die Verarbeitung Verantwortlichen mit allen damit verbundenen Pflichten werden. Insofern ist es wesentlich, belegen zu können, dass die durch Prozessbeschreibungen, Arbeitsanweisungen und in Softwaresystemen hinterlegten Workflows gegebenen Weisungen befolgt werden. Solche Belege werden im Weiteren Protokolle und Protokollierung genannt.

Zu den Protokollen zählen weiterhin eingeholte Einwilligungen nach Art. 7 DS-GVO und die Prüf- und Nachweispflichten bei der Einwilligung von Kindern im Rahmen des Angebots von Diensten der Informationsgesellschaft nach Art. 8 DS-GVO. Die erfolgten Informationen nach Art. 13 und 14 DS-GVO sollten genauso für jeden Betroffenen protokolliert werden wie die Einhaltung der Meldepflichten nach Art. 33 und 34 DS-GVO. Diese Aufzählung ließe sich fortsetzen. Verallgemeinert zählt jeder Beleg im Rahmen der operativen Tätigkeit zu den Protokollen.

Protokolle werden häufig durch Protokollierungsfunktionen der verwendeten Programme, abgehakte Checklisten oder gespeicherte E-Mail-Korrespondenz auch heute schon bspw. im Rahmen von Qualitätsmanagementsystemen gesammelt. Auch Logfiles und andere Protokolle, die im Rahmen der IT-Sicherheit verarbeitet werden, sind zu berücksichtigen. Sie dienen einerseits der Umsetzung der Sicherheitsmaßnahmen nach Art. 32 DS-GVO und andererseits auch als Grundlage für die Wirksamkeitsüberprüfung nach Art. 32 Abs. 1 Lit. d) DS-GVO.

Eine Protokollierung benötigt regelmäßig selber einen Personenbezug, da für jede Person nachweisbar sein sollte, dass sie innerhalb der Weisungen handelt. Der Gesetzgeber hat zwar die Nachweispflicht – wie gezeigt – in der DS-GVO verankert, aber keine korrespondierende Rechtsgrundlage zur Protokollierung geschaffen. Somit verbleibt der Rückgriff auf die allgemeinen Normen des Art. 6 DS-GVO. Theoretisch denkbar wäre auch eine Einwilligung nach Art. 7 oder in bestimmten Fällen auch Art. 8 DS-GVO. In der Praxis ist eine Einwilligung jedoch keine geeignete Rechtsgrundlage für eine Dokumentation, da sie jederzeit widerrufen werden kann. Sie würde die Nachweisbarkeit damit in das Belieben der überwachten Person stellen. Es empfiehlt sich deshalb, in einem Protokollierungskonzept die für die einzelnen Protokolle einschlägigen Rechtsgrundlagen festzuhalten.

3. Phase Kontrolle

Die Notwendigkeit zur Kontrolle, ob und in welchem Maß die datenschutzrechtlichen und unternehmensinternen Vorgaben eingehalten werden, ergibt sich bereits sachlogisch aus der Überlegung, dass Vorgaben, deren Einhaltung nicht überprüft, und Protokolle, die nicht ausgewertet werden, wirkungslos und damit überflüssig sind. Die Überwachung der Einhaltung gehört zu den gesetzlich festgelegten Überwachungsaufgaben des Datenschutzbeauftragten.[33] Für die Sicherheitsmaßnahmen normiert Art. 32 Abs. 1 Lit. d) DS-GVO darüber hinaus eine eigenständige Prüfvorgabe für das Unternehmen.

Die Einhaltungskontrolle beschränkt sich nicht nur auf die zulässige Datenverarbeitung, sondern auch auf die unzulässige. Deshalb empfiehlt es sich, die Kontrolltätigkeiten so zu konzipieren, dass Regelübertretungen erkannt werden. Die Kontrollhandlungen und -ergebnisse sollten als Nachweis dokumentiert werden.

Auf zwei Aspekte sei besonders hingewiesen:

- Eine besondere Herausforderung sind Softwareanwendungen und Geräte, die mehr Daten verarbeiten als erforderlich. Diese sind regelmäßig nicht konform mit der DS-GVO einsetzbar[34], so dass die Nutzung gegen Art. 25 Abs. 2 verstößt. Werden Daten, die nicht erforderlich sind, verarbeitet, liegt regelmäßig keine Rechtsgrundlage nach Art. 6-10 DS-GVO vor. Damit wird u.U. in der Folge zusätzlich gegen Art. 14 DS-GVO verstoßen. Bereits durch die Nutzung verstößt das Unternehmen gegen die DS-GVO, sodass die Frage, ob die Daten auch ausgewertet oder angeschaut werden, zurücktreten kann. Deaktivierte Funktionen sind hingegen unkritisch, da sie nicht ausgeführt werden, d.h. keine Wirkung zeigen. Es gilt deshalb, Softwareanwendungen und Geräte anhand ihrer Doku-

29 Art. 33 Abs. 2 DS-GVO.

30 Art. 28 Abs. 1 und 4 DS-GVO.

31 Art. 28 Abs. 2 DS-GVO.

32 Art. 28 Abs. 3 Lit. a) DS-GVO verlangt „dokumentierte" Weisungen und Art. 29 DS-GVO bindet den Auftragsverarbeiter an diese Weisungen; im Rahmen der gesamtschuldnerischen Haftung können dokumentierte Weisungen zu einer Freistellung führen (Art. 82 Abs. 2 DS-GVO).

33 Art. 39 Abs. 1 Lit. b) DS-GVO und Jaspers, A.; Reif, Y., Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung: Bestellpflicht, Rechtsstellung und Aufgaben. In: RDV, 2/2016, S. 66.

34 Lepperhoff/Müthlein, Neue Vorschriften auch für den CISO. In: KES, 2/2016, 19.

mentation und durch Funktionstest zu überprüfen. Diese Kontrolle erfolgt idealerweise vor der Beschaffung. Diese Kontrolle sollte auch Software as a service und andere Clouddienste umfassen, da für die Rechtmäßigkeit (auch) der Auftraggeber verantwortlich ist.[35] Ob es sich um eine Auftragsverarbeitung i.S.v. Art. 28 DS-GVO handelt, ist unerheblich. Da Updates den Funktionsumfang verändern können, sollte nach einem Update die betroffene Anwendung oder das Gerät erneut auf unerlaubte Datenverarbeitung überprüft werden.
- Die Datenschutz-Folgenabschätzung umfasst auch eine gesonderte Prüfpflicht, „ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird".[36]

4. Phase Mängelbeseitigung

Der Unternehmensführung obliegt es, zusammen mit den Fachbereichen die festgestellten Mängel zu beheben. Sofern sich Änderungen bspw. in Software, Prozessen oder Konzepten ergeben, sind die jeweiligen Dokumente zu aktualisieren. Explizite Aktualisierungspflichten nennt die DS-GVO u.a. in Art. 24 Abs. 1 für die allgemeinen Maßnahmen, in Art. 32 Abs. 1 Lit. d) für die Sicherheitsmaßnahmen und in Art. 35 Abs. 11 für die Datenschutz-Folgenabschätzung.

IV. Das Verzeichnis von Verarbeitungstätigkeiten

Auch wenn das „Verzeichnis von Verarbeitungstätigkeiten" nach Art. 30 DS-GVO auf dem ersten Blick als eine zusätzliche Dokumentationspflicht angesehen werden kann, stellt es bei näherer Betrachtung eine besondere Zusammenstellung vorhandener Angaben dar. Tabelle 1 stellt den Inhalten dieses Verzeichnisses von Verarbeitungstätigkeiten die Vorschriften gegenüber, nach denen die jeweilige Information unabhängig von diesem Verzeichnis vorhanden sein muss.

Die Pflicht zur Führung des Verzeichnisses entfällt, wenn jedes der folgenden Kriterien erfüllt ist:[38]
- weniger als 250 Mitarbeiter werden beschäftigt,
- die Verarbeitung birgt kein Risiko für die Rechte und Freiheiten der betroffenen Personen,
- die Verarbeitung erfolgt nur gelegentlich und
- es werden keine besonderen Datenkategorien nach Art. 9 Abs. 1 DS-GVO und keine Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten nach Art 10 DS-GVO verarbeitet.

Die Ausnahmen sind bei Licht betrachtet tatsächlich Ausnahmen. Regelmäßige Verarbeitungen scheitern an der Hürde „gelegentlich". Weiterhin birgt die Verarbeitung personenbezogener Daten grundsätzlich ein Risiko für die Rechte und Freiheiten der betroffenen Personen, da in deren Persönlichkeitsrechte eingegriffen wird.[39] Es müssen deshalb grundsätzlich alle Verarbeitungen im Rahmen von definierten Prozessen in dem Verzeichnis aufgeführt werden, auch wenn das Unternehmen weniger als 250 Mitarbeiter beschäftigt.

V. Fazit

Die Einhaltung der DS-GVO nachweisen zu können sowie zahlreiche Vorgaben machen eine umfassende Dokumentation erforderlich. Die Herausforderung für eine praktische Umsetzung liegt in dem Erschließen und systematischen

35 Müthlein, ADV 5.0 – Neugestaltung der Auftragsdatenverarbeitung in Deutschland, RDV, 2016, 74-87.

36 Art. 35 Abs. 11 DS-GVO.

37 Art. 30 Abs. 1 DS-GVO.

38 Art. 30 Abs. 5 DS-GVO formuliert die Ausnahmen in negierter Form mit „oder" verknüpft. Negiert man „Nicht A oder Nicht B" ergibt sich „A und B". Nach diesem Schema wurden die Kriterien in eine besser verständliche Form transformiert.

39 Vgl. 1. Erwägungsgrund der DS-GVO.

Angaben in der Verarbeitungsübersicht für Verantwortliche [37]	Bereits vorhanden wegen (Beispiel)
Kontaktdaten des Datenschutzbeauftragten	Art. 37 DS-GVO
Zwecke der Verarbeitung	Art. 5 Abs. 1 Lit. b) DS-GVO
Kategorien betroffener Personen	Art. 6 DS-GVO
Kategorien personenbezogener Daten	Art. 6 DS-GVO
Kategorien von Empfängern	Art. 6 DS-GVO
Drittstaatentransfer: Empfängerland oder internationale Organisation	Art. 44-46 DS-GVO
Drittstaatentransfer: Garantien	Art. 45-47 DS-GVO
Löschfristen	Art. 5 Abs. 1 Lit. e) DS-GVO
allgemeine Beschreibung der technischen und organisatorischen Maßnahmen	Art. 32 DS-GVO

Tabelle: Das Verzeichnis von Verarbeitungstätigkeiten kombiniert vorhandene Informationen

Zugänglichmachen bereits vorhandener Dokumente, die typischerweise in einzelnen Unternehmensbereichen mehr oder weniger als Insellösung vorhanden sind. Beispiele sind: Qualitätsmanagementsystem, IT-Betriebsdokumente, Protokolle von Anwendungen und Servern, Workflowdokumentation, Richtlinien, Prozessbeschreibungen, Checklisten und Arbeitsanweisungen.

Ein solches Dokumentationssystem wurde im BDSG nicht gefordert und stellt deshalb eine einschneidende Neuerung für Unternehmen dar.

Dr. Niels Lepperhoff
ist Geschäftsführer der Xamit Bewertungsgesellschaft mbH und der DSZ Datenschutz Zertifizierungsgesellschaft mbH (einem Gemeinschaftsunternehmen des BvD und der GDD). Er verfügt über langjährige Berufserfahrung als externer Datenschutzbeauftragter und berät sowohl deutsche als auch internationale Unternehmen. Daneben ist er Inhaber eines Lehrauftrages des Masterstudienganges „Medienrecht und Medienwirtschaft“ an der Technischen Hochschule Köln.

Kurzbeiträge

Aus den aktuellen Berichten der Aufsichtsbehörden (26): Nochmals: Datenerhebung mit Hilfe von Personalausweisen

Ausgewählt und kommentiert von Prof. Peter Gola, Königswinter*

Die Frage, ob Personalausweise zur Identifikation eines Antragstellers, Kunden oder Besuchers kopiert, eingescannt oder zur Sicherheit als Pfand einbehalten werden dürfen, ist seit Inkrafttreten des nunmehrigen Personalausweisgesetzes im Jahre 2009 immer wieder Gegenstand der Erörterung in Berichten der Aufsichtsbehörden (vgl. Gola, Bericht RDV 2013, 193). Inzwischen liegt auch ein Urteil vor, in dem das VG Hannover (v. 28.11 2013 – 10 A 5342/11 –, RDV 2014, 219) das Scannen des Personalausweises sowie die anschließende Speicherung des eingescannten Bildes als unzulässig bewertete. Das Verbot sah das Gericht in § 14 i.V.m. § 20 Abs. 2 PAusWG, wonach der Ausweis weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden darf.

Den Betroffenen wird auch eine diesbezügliche Verfügungsbefugnis abgesprochen, d.h. das Einscannen und Speichern soll auch nicht per Einwilligung möglich sein. Das ergebe sich daraus (so LfD Baden-Württemberg, 32. TB, 2014/15, Ziff. 10.10.1), „dass der Personalausweis ebenso wie der Reisepass Bundeseigentum ist und die Bundesrepublik Deutschland über die Verwendung (mit)entscheidet.“ Hinsichtlich des Kopierens des Ausweises liegt jedoch eine Entscheidung der Bundesrepublik vor. Nach Ansicht des Bundesinnenministeriums steht auch ohne spezielle Ermächtigungsnorm einem Kopieren des Ausweises nicht generell etwas entgegen (vgl. LfD B.-W, 32. TB, 2014/2015, Ziff. 10.10.1)

Allerdings werden hohe Anforderungen an die Zulässigkeit des Kopierens von Personalausweisen gestellt:

- Die Erstellung einer Kopie muss erforderlich sein.
- Dabei ist insbesondere zu prüfen, ob nicht die Vorlage des Personalausweises und ggf. die Anfertigung eines entsprechenden Vermerks (z.B.: ,,Personalausweis hat vorgelegen.“) ausreichend ist.
- Die Kopie darf ausschließlich zu Identifizierungszwecken verwendet werden.
- Die Kopie muss als solche erkennbar sein.
- Daten, die nicht zur Identifizierung benötigt werden, können und sollen von den Betroffenen auf der Kopie geschwärzt werden. Dies gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangs- und Seriennummer.

* Der Autor ist Ehrenvorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn.

Die Betroffenen sind auf die Möglichkeit und Notwendigkeit der Schwärzung hinzuweisen.
- Die Kopie ist vom Empfänger unverzüglich zu vernichten, sobald der mit der Kopie verfolgte Zweck erreicht ist.
- Eine automatisierte Speicherung der Ausweisdaten ist nach dem Personalausweisgesetz stets unzulässig.

Diese Auffassung vertreten auch der LDI NRW und der hambBfDI. Auch sie lassen das Kopieren des Ausweises durch den Ausweisinhaber bzw. mit dessen Einwilligung durch einen Verkäufer etc. zu, sofern keine automatisierte Speicherung erfolgt, was auch eine sofortige Löschung im Speicher des Kopiergeräts erfordert. Ein Kopieren zum Zwecke der Identifizierung unter Anwesenden ist jedoch regelmäßig unzulässig, weil Kenntnisnahme und ggf. das Abschreiben der benötigten Daten genügt.

Die für das Fertigen von Kopien aufgezeigten Voraussetzungen sah der LfD Baden-Württemberg sodann bei einem in einer unsicheren Bahnhofsgegend gelegenen Hotel mit sog. „Stundengästen", die die Zimmer gelegentlich in einem verwüsteten Zustand oder ohne zu bezahlen hinterließen, jedoch nicht als gegeben an. Das Hotel hatte bei Übernachtungen ohne Reservierung, die nicht per Vorkasse bezahlt werden, für die Dauer des Aufenthalts regelmäßig eine Kopie eines Ausweisdokumentes angefertigt. Damit sollten die Meldedaten überprüft, Schadensfälle leichter polizeilich verfolgt und potentielle Zechpreller im Idealfall von vornherein abgeschreckt werden. Nach der schadensfreien Abreise der Gäste wurden die Kopien unverzüglich vernichtet.

Die Erforderlichkeit der Speicherung der Kopie wurde verneint, wenngleich der Effekt der Abschreckung von Zechprellern bejaht wurde. Aus datenschutzrechtlicher Sicht wurde diese Verwendung personenbezogener Daten aber nicht als erforderlich angesehen, um die vertrauenswürdigen Gäste „auszusieben"; beispielsweise könnte auch ein Pfand oder eine Kaution verlangt werden. Zudem sei das Verfahren insoweit nicht hinnehmbar, als hier die personenbezogenen Daten nicht ihres Inhalts wegen, sondern nur für eine Drohkulisse erhoben und (nichtautomatisiert) gespeichert werden. Auch für die Verfolgung von Zechprellern durch die Polizei wurde in den Kopien im Vergleich zu Personalien, die beim Einchecken – auch unter Vorlage des Personalausweises (Sichtausweis) – aufgezeichnet werden, kein zusätzlicher Nutzen gesehen.

Andere Aufsichtsbehörden (vgl. die nachfolgenden Beispiele aus dem jüngsten Tätigkeitsbericht des LfDI Thüringen) sehen aber auch die Anfertigung von Kopien als durch das PAuswG untersagt an.

Abgelehnt hat der Thüringer LfDI (2. TB für den nichtöffentlichen Bereich, 2014/15, S. 61) demgemäß die Anfertigung von Kopien auch in Fällen, in denen eine gesetzliche Pflicht zur Datenerhebung besteht. Betroffen war ein Käufer eines Desinfektionsmittels, dessen Identitätsfeststellung in § 3 Abs. 1 S. 4 der Chemikalien-Verbotsverordnung dem Verkäufer vorgeschrieben ist. Der LfDI leitete auch das Kopierverbot aus § 20 Abs. 2 PAuswG ab. Aber auch ohne die fragwürdige Anwendung der Norm wäre die Erforderlichkeit der Kopieanfertigung zu verneinen gewesen, da das Ablesen der Identifikationsdaten des Ausweises genügt hätte, um die gesetzlichen Anforderungen zu erfüllen. Gleich problematisch war das Vorgehen eines Schrotthändlers, der das Ablichten des Personalausweises für erforderlich hielt, um seiner Nachweis- und Dokumentationspflicht gegenüber den Finanzbehörden nach § 160 und § 143 Abs. 3 Nr. 2 AO nachzukommen. Auch hier genügte die Verwendung eines die erforderlichen Daten des Verkäufers aufnehmenden Erfassungsformulars, dessen Angaben an Hand des Ausweisen überprüft werden konnten (ThürLfDI, 2. TB nicht-öffentlicher Bereich, 2014/15, S. 62). Gleiches gilt für den Identitätsnachweis eines Mietbewerbers (ThürLfDI, a.a.O., S. 32). Regelmäßig als nicht erforderlich wurde auch die Identitätsfeststellung eines Neupatienten eines Arztes per Ausweiskontrolle oder gar die Aufnahme einer Kopie des Ausweises in die Patientenakte angesehen (BlnBDI, JB 2013, Ziff 8.7).

Einen Fall der zulässigen Vorlage von Ausweiskopien sehen die Aufsichtsbehörden ggf. bei der Einholung von Eigenauskünften gegenüber Auskunfteien (BayLDA, TB 2013/14, Ziff. 11.1). Die Begründung wird neben der Identitätsprüfung bei namensgleichen oder namensähnlichen Personen in dem Erschweren bzw. Verhindern des Erschleichens von Bonitätsauskünften durch Unberechtigte gesehen (z.B. durch im Haushalt, in einer Wohngemeinschaft mitlebende Personen etc.), was in der Praxis – sei es aus Neugier, in Trennungsfällen, bei Streitigkeiten – immer wieder vorkomme. Für die Identifikation nicht notwendige Daten (wie z.B. Größe, Augenfarbe, Ausweisnummer, Bild, Unterschrift) können in der Ausweiskopie geschwärzt bzw. beim Kopieren abgedeckt werden, worauf der Auskunftssuchende hinzuweisen ist.

Keine Zulässigkeitsfrage stellt sich schließlich, wenn Unternehmen sich auf eine spezielle gesetzliche Regelung berufen können (vgl. LDI NW, 22. Datenschutzbericht 2015, Ziff. 5.7 sowie die Hinweise "Personalausweis und Datenschutz", WWW.ldi. NRW.de). So müssen Kredit- und Finanzdienstleistungsinstitute nach dem Geldwäschegesetz unter anderem bei Begründung einer Geschäftsbeziehung ihre Vertragspartner identifizieren. Hierfür ist bei einer natürlichen Person ein bestimmter Katalog von Angaben zu erheben und aufzuzeichnen. Das Institut hat dabei die Wahlmöglichkeit, ob eine Kopie des Personalausweises gefertigt wird oder die erforderlichen Daten aus dem Ausweis notiert werden, wobei im erstgenannten Fall die Daten, die für die Identifizierung nicht erforderlich sind, geschwärzt werden müssen.

Letztendlich ist festzuhalten, dass einem Verlangen zur Hinterlegung des Personalausweises als Pfand während des Besuches eines Unternehmens, Z.B. um die Rückmeldung des Besuchers oder die Rückgabe eines Schließfachschlüssels sicherzustellen, das insoweit eindeutige Verbot der Personalausweisvorschriften entgegensteht.

Und noch etwas Vorratsspeicherung … –

EU-Richtlinie über die Verwendung von Fluggastdaten beschlossen

RAin Yvette Reif, LL.M., Bonn*

Zeitgleich mit der Datenschutz-Grundverordnung wurde die EU-Richtlinie über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (Richtlinie (EU) 2016/681) verabschiedet. Durch das Sammeln, den Austausch und die Analyse der PNR-Daten sollen u.a. die Geheimdienste Muster verdächtigen Verhaltens erkennen und weiterverfolgen können.

PNR (Passenger Name Records) sind Fluggastdatensätze, die für jeden Passagierflug angelegt werden und in den Buchungs- und Abfertigungssystemen der Fluggesellschaften gespeichert werden. Anzahl und Inhalt der Felder in einem PNR-Datensatz variieren je nach Fluggesellschaft und Fluggast. Zu den Daten gehören etwa Informationen wie der Name des Fluggasts, Reisedaten, Reiserouten, Sitznummern, Gepäckangaben, Kontaktangaben und Zahlungsarten.

Durch die EU-Richtlinie sollen die Luftfahrtgesellschaften dazu verpflichtet werden, für Flüge von der EU in Drittländer und andersherum den zuständigen Behörden näher konkretisierte Informationen (vgl. Anhang I der Richtlinie) aus dem PNR-Datensatz zur Verfügung zu stellen. Die Richtlinie gilt verpflichtend nur für Flüge in Drittländer bzw. aus Drittländern, jedoch können die Mitgliedstaaten sie auch auf Flüge innerhalb der EU anwenden, wenn sie die EU-Kommission davon in Kenntnis setzen.

Die Fluggastdaten sollen von den Fluggesellschaften an eine entsprechend einzurichtende einzige, genau bezeichnete Stelle („PNR-Zentralstelle“) des jeweiligen Mitgliedstaates übermittelt werden. Die PNR-Zentralstelle wird für die Erhebung, Speicherung und Verarbeitung der PNR-Daten sowie für deren Übermittlung an die zuständigen Behörden und für deren Austausch mit den PNR-Zentralstellen der anderen Mitgliedstaaten und Europol verantwortlich sein.

Die Fluggastdaten werden bei der PNR-Zentralstelle für einen Zeitraum von 5 Jahren vorgehalten, wobei diese nach sechs Monaten die Daten so depersonalisieren muss, dass die Identität der Betroffenen nicht mehr unmittelbar festgestellt werden kann. Nach Ablauf der 6-Monats-Frist ist eine Offenlegung der vollständigen PNR-Daten nur zulässig, wenn berechtigter Grund zu der Annahme besteht, dass dies zur Erreichung der Zwecke der Richtlinie erforderlich ist und zusätzlich eine Genehmigung erfolgt durch

- eine Justizbehörde oder
- eine andere nationale Behörde, die nach nationalem Recht dafür zuständig ist zu überprüfen, ob die Bedingungen für die Offenlegung erfüllt sind, vorbehaltlich der Unterrichtung des Datenschutzbeauftragten der PNR-Zentralstelle und einer Ex-Post-Überprüfung durch diesen Datenschutzbeauftragten.

Die Richtlinie enthält eine Reihe von Vorkehrungen mit dem Ziel, die Grundrechte auf Schutz personenbezogener Daten, auf Privatsphäre und Nichtdiskriminierung zu schützen. Neben der bereits angesprochenen Pflicht zur Depersonalisierung der Datensätze nach einer Speicherfrist von 6 Monaten sind dies u.a.:

- Die Übermittlung sensibler Daten wie z.B. rassische oder ethnische Herkunft, religiöse Überzeugungen oder Gesundheitszustand an die PNR-Zentralstellen ist untersagt.
- Es ist sicherzustellen, dass die Fluggäste über die Erhebung der PNR-Daten, deren Übermittlung an die PNR-Zentralstelle und über ihre Rechte als betroffene Personen korrekt und auf leicht zugängliche und verständliche Weise informiert werden.
- Jegliche Verarbeitung von PNR-Daten ist zu dokumentieren.
- Die automatisierte Verarbeitung von PNR-Daten darf nicht einzige Grundlage für Entscheidungen sein, aus denen sich für die betreffende Person nachteilige Rechtsfolgen oder sonstige schwerwiegende Nachteile ergeben.
- Die Übermittlung von PNR-Daten an Drittländer darf nur unter ganz bestimmten Bedingungen und in Einzelfällen erfolgen.
- Der PNR-Zentralstelle muss ein Datenschutzbeauftragter angehören.
- Im Hinblick auf die Verarbeitung der PNR-Daten erfolgt eine Beratung und Kontrolle durch unabhängige nationale Kontrollstellen.

Die Richtlinie (EU) 2016/681 über die Verwendung von Fluggastdatensätzen bindet die betroffenen Fluggesellschaften nicht unmittelbar. Sie richtet sich an die Mitgliedstaaten, die die Regelungen bis zum 25. Mai 2018 in nationales Recht umzusetzen haben.

Die Richtlinie enthält in Art. 19 eine Überprüfungsklausel. Anhand von Informationen der Mitgliedstaaten hat danach die Kommission bis zum 25. Mai 2020 eine Überprüfung aller Elemente der Richtlinie vorzunehmen und dem Europäischen Parlament (EP) und Rat entsprechend Bericht zu erstatten. Bei der Vornahme ihrer Überprüfung hat die Kommission insbesondere folgende Aspekte zu beachten:

- die Einhaltung des einschlägigen Schutzstandards bezüglich personenbezogener Daten;
- die Erforderlichkeit und Verhältnismäßigkeit der Erhebung und Verarbeitung von PNR-Daten für jeden der in der Richtlinie genannten Zwecke;
- die Datenspeicherungsfristen;

* Die Autorin ist stellvertretende Geschäftsführerin der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn.

– die Effektivität des Informationsaustauschs zwischen den Mitgliedstaaten und
– die Qualität der Prüfungen.

Kritiker sehen in der Richtlinie über die Verwendung von Fluggastdatensätzen die nächste anlasslose Vorratsdatenspeicherung. Die Kritikpunkte entsprechen im Wesentlichen denjenigen, die auch schon im Hinblick auf die Vorratsdatenspeicherung von Telekommunikationsdaten (Richtlinie 2006/24/EG) und die Fluggastdatenabkommen mit den USA (Ratsdokument 17434/11), Australien (Ratsdokument 10093/11) und Kanada (Ratsdokument 12657/1/13) vorgebracht wurden. Zwar dient die Richtlinie mit der effektiven Bekämpfung von Terrorismus und schwerer Kriminalität (ErwG 6) unzweifelhaft einem legitimen Zweck. Es bleibt aber die Frage, ob die anlasslose Speicherung von Reisedaten eines undifferenzierten Personenkreises über eine Dauer von 5 Jahren einen zur Erreichung dieses Zwecks geeigneten und verhältnismäßigen Grundrechtseingriff darstellt.

Im Hinblick auf das ausgehandelte Fluggastdatenabkommen mit Kanada ist aktuell ein Verfahren beim EuGH anhängig. Das EP hatte den Entwurf des Abkommens im November 2014 an den EuGH überwiesen, um die Vereinbarkeit mit EU-Recht prüfen zu lassen. Anlass für die Vorlage war u.a. die Erwägung, dass der Gerichtshof im April 2014 die bereits erwähnte Richtlinie 2006/24/EG über die Vorratsdatenspeicherung von TK-Daten für ungültig erklärt hatte (verbundene Rechtssachen C-293/12 und C-594/12). Auf Drängen des Ministerrats hat die Mehrheit der EP-Abgeordneten allerdings nunmehr der Einrichtung eines europäischen Fluggastdatensystems zugestimmt, ohne das Gutachten des EuGH zu dem Abkommen mit Kanada abzuwarten. Das Gutachten des EuGH wird in den nächsten Wochen erwartet. Der berichterstattende Richter Thomas von Danwitz hatte im Anhörungstermin am 5.4.2016 zahlreiche kritische Fragen und Anmerkungen im Hinblick das geplante Abkommen mit Kanada aufgeworfen. Diese bezogen sich u.a. auf die Frage, ob und wie Fluggastdatenüberwachung tatsächlich zur Aufklärung von Verbrechen beiträgt, die lange Speicherdauer der Daten, die Fraglichkeit der Gewährleistung eines effektiven Rechtsschutzes der Betroffenen sowie die fehlende Limitierung des Ausmaßes, in dem die PNR-Daten mit kanadischen Datenbanken abgeglichen werden könnten.

Rechtsprechung

Unzulässige Anordnung einer molekulargenetischen Untersuchung nach § 81g Abs. 1 StPO

(**Bundesverfassungsgericht**, Beschluss vom 3. Mai 2016 – 2 BvR 2349/15 –)

Die Feststellung, Speicherung und (künftige) Verwendung eines DNA-Identifizierungsmuster greift in das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verbürgte Grundrecht auf informationelle Selbstbestimmung ein. Bei der Auslegung und Anwendung des § 81g StPO sind die Gerichte gehalten, die Bedeutung und Tragweite dieses Grundrechts angemessen zu berücksichtigen. Notwendig für die Anordnung einer molekulargenetischen Untersuchung ist, dass aufgrund einer auf einer zureichenden Sachverhaltsaufklärung beruhenden Prognoseentscheidung wegen der Art der abgeurteilten Straftat, der Persönlichkeit des Verurteilten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn erneut Strafverfahren wegen Straftaten mit erheblicher Bedeutung zu führen sein werden.

(Nicht amtliche Leitsätze)

Sachverhalt:

1. Das Amtsgericht Augsburg verurteilte den nicht vorbestraften Beschwerdeführer am 25. November 2014 wegen gefährlicher Körperverletzung zu einer Freiheitsstrafe von sechs Monaten, deren Vollstreckung zur Bewährung ausgesetzt wurde. Nach den Feststellungen schlug der Beschwerdeführer am 30. Mai 2013 im Rahmen einer längeren Auseinandersetzung in bewusstem und gewolltem Zusammenwirken mit einem Mitangeklagten auf den Nebenkläger ein, wodurch dieser diverse Prellungen im Gesicht und an den Rippen, Schwellungen sowie andauernde Übelkeit und Schmerzen am Schultergelenk erlitt. Das Urteil ist rechtskräftig.

2. Auf Grund dieses Urteils ordnete das Amtsgericht Augsburg auf Antrag der Staatsanwaltschaft mit Beschluss vom 6. Oktober 2015 die molekulargenetische Untersuchung der durch eine körperliche Untersuchung zu erlangenden Körperzellen des Beschwerdeführers zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren an (vgl. § 81g Abs. 1 Satz 1 und Abs. 4 StPO). Zur Begründung führte es aus, dass es sich bei der am 25. November 2014 abgeurteilten Straftat um eine solche von erheblicher Bedeutung im Sinne von § 81g Abs. 1 Satz 1 StPO handle, denn sie zeuge „von einem hohen Maß an Brutalität und Gewaltbereitschaft des Betroffenen“. Wegen dieser erheblichen Gewaltbereitschaft bestehe zudem Grund zu der Annahme, dass gegen den Beschwerdeführer auch künftig Strafverfahren wegen Straftaten von erheblicher Bedeutung zu führen sein werden.

3. Die hiergegen eingelegte Beschwerde des Beschwerdeführers wurde vom Landgericht Augsburg mit Beschluss vom 6. November

2015 als unbegründet zurückgewiesen. Zur Begründung führte das Landgericht lediglich aus, es teile die Auffassung des Erstgerichts und trete den Gründen der angefochtenen Entscheidung, die durch das Beschwerdevorbringen nicht entkräftet würden, bei.

4. Den vom Beschwerdeführer gestellten Antrag, das Verfahren in die Lage vor Erlass der Entscheidung vom 6. November 2015 zurückzuversetzen, lehnte das Landgericht Augsburg mit Beschluss vom 26. November 2015 ab.

Mit seiner Verfassungsbeschwerde macht der Beschwerdeführer geltend, die Begründung der angefochtenen Beschlüsse sei unzureichend und verletze ihn in seinem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Soweit die Fachgerichte von einem hohen Maß an Brutalität und Gewaltbereitschaft ausgingen, stünde dies nicht in Einklang mit den im Urteil vom 25. November 2014 getroffenen Feststellungen. Zudem genüge die Begründung der Negativprognose nicht den verfassungsrechtlichen Anforderungen. Die angegriffenen Entscheidungen ließen weder den Prognosemaßstab noch eine konkrete, auf den Einzelfall bezogene Begründung der Wiederholungsgefahr erkennen.

Aus den Gründen:

Die Verfassungsbeschwerde wird zur Entscheidung angenommen, da dies zur Durchsetzung der in § 90 Abs. 1 BVerfGG genannten Rechte angezeigt erscheint (§ 93b i.V.m. § 93a Abs. 2 Buchst. b BVerfGG). Die Voraussetzungen des § 93c Abs. 1 Satz 1 BVerfGG für eine der Verfassungsbeschwerde stattgebende Entscheidung der Kammer sind gegeben. Die maßgeblichen verfassungsrechtlichen Fragen sind in der Rechtsprechung des Bundesverfassungsgerichts bereits geklärt. Danach ist die zulässige Verfassungsbeschwerde in einem die Entscheidungskompetenz der Kammer eröffnenden Sinn offensichtlich begründet.

1. Die Feststellung, Speicherung und (künftige) Verwendung eines DNA-Identifizierungsmusters greift in das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG verbürgte Grundrecht auf informationelle Selbstbestimmung ein. Dieses Recht gewährleistet die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden (BVerfGE 65, 1 <41 ff.>; 78, 77 <84>). Diese Verbürgung darf nur im überwiegenden Interesse der Allgemeinheit und unter Beachtung des Grundsatzes der Verhältnismäßigkeit aufgrund eines Gesetzes eingeschränkt werden; die Einschränkung darf nicht weiter gehen, als es zum Schutz des öffentlichen Interesses unerlässlich ist (vgl. BVerfGE 103, 21 <32 f.>).

Die Gerichte sind bei der Auslegung und Anwendung des § 81g StPO gehalten, die Bedeutung und Tragweite dieses Grundrechts angemessen zu berücksichtigen (vgl. nur BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 29. September 2013 – 2 BvR 939/13 –, NStZ-RR 2014, S. 48 m.w.N.). Notwendig für die Anordnung einer Maßnahme nach § 81g StPO ist, dass wegen der Art oder Ausführung der bereits abgeurteilten Straftat, der Persönlichkeit des Verurteilten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn erneut Strafverfahren wegen Straftaten von erheblicher Bedeutung zu führen sind. Die Prognoseentscheidung setzt voraus, dass ihr eine zureichende Sachaufklärung vorausgegangen ist und die für sie bedeutsamen Umstände nachvollziehbar dargestellt und abgewogen werden. Dabei ist stets eine auf den Einzelfall bezogene Entscheidung erforderlich; die bloße Wiedergabe des Gesetzeswortlauts reicht nicht aus (vgl. BVerfGE 103, 21 <36 f.> sowie BVerfG, Beschlüsse der 3. Kammer des Zweiten Senats vom 2. Juli 2013 – 2 BvR 2392/12 –, StV 2014, S. 578 <579> und 29. September 2013 – 2 BvR 939/13 –, NStZ-RR 2014, S. 48 f., beide m.w.N.).

2. Diesen, durch die Vorschrift des § 81g Abs. 3 Satz 5 StPO auch in das einfache Recht umgesetzten (vgl. BTDrucks 15/350, S. 23 zu § 81g Abs. 3 Satz 2 StPO a.F.), Begründungsanforderungen werden die angegriffenen Beschlüsse nicht gerecht. Es fehlt an der gebotenen einzelfallbezogenen Abwägung der für die Entscheidung bedeutsamen Umstände.

Dabei kann dahinstehen, ob der vom Amtsgericht nicht näher erläuterte Schluss vom festgestellten Tatgeschehen auf eine erhebliche Gewaltbereitschaft des Beschwerdeführers tragfähig ist. Denn das Amtsgericht stützt sich bei seiner Entscheidung allein auf diese pauschale Wertung, ohne auf die Umstände einzugehen, die das Vorliegen einer Negativprognose in Frage stellen könnten. Insbesondere setzt sich das Amtsgericht nicht damit auseinander, dass der geständige Beschwerdeführer nicht vorbestraft war, ausweislich der Urteilsgründe ein hohes Maß an Einsicht zeigte und dem Geschädigten bereits im Vorfeld der Hauptverhandlung Schmerzensgeldzahlungen angeboten hat. Zudem lag die Tat zum Zeitpunkt der Prognoseentscheidung mehr als zwei Jahre zurück, ohne dass der Beschwerdeführer zwischenzeitlich erneut auffällig geworden wäre. Schließlich hat das Amtsgericht nicht erkennbar bedacht, dass die verhängte Freiheitsstrafe zur Bewährung ausgesetzt worden war. Eine rechtliche Bindung an eine von einem anderen Gericht zur Frage der Strafaussetzung zur Bewährung getroffene Sozialprognose besteht zwar nicht, doch entsteht in Fällen gegenläufiger Prognosen verschiedener Gerichte regelmäßig ein erhöhter Begründungsbedarf für die nachfolgende gerichtliche Entscheidung, mit der eine Maßnahme nach § 81g StPO angeordnet wird (vgl. BVerfGE 103, 21 <36 f.> sowie BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 29. September 2013 – 2 BvR 939/13 –, NStZ-RR 2014, S. 48 <49> m.w.N.). Das Amtsgericht hätte sich daher mit den Gründen, die im Rahmen der Bewährungsentscheidung zu einer positiven Sozialprognose geführt haben, inhaltlich auseinandersetzen müssen. Dies betrifft insbesondere die in beruflicher Hinsicht geordneten Lebensverhältnisse des Beschwerdeführers.

Der Beschluss des Landgerichts vom 6. November 2015 verweist lediglich auf die Gründe der amtsgerichtlichen Entscheidung und begegnet daher denselben verfassungsrechtlichen Bedenken.

VI. Nach alledem waren die angegriffenen Beschlüsse aufzuheben und die Sache an das Amtsgericht Augsburg zurückzuverweisen (§ 93c Abs. 2 i.V.m. § 95 Abs. 2 BVerfGG).

Persönlichkeitsrechtsverletzung eines verurteilten Straftäters

(**Oberlandesgericht Frankfurt/M.**, Urteil vom 25. Mai 2016, – 16 U 198/15 –)

Die identifizierende Schilderung des Werdegangs eines wegen seiner Vorgehensweise bereits bestraften Dschihadisten, der die Strafe weitgehend verbüßt hat und

wegen des Strafrestes unter Bewährung steht, ist wegen der Gefährdung einer möglichen Resozialisierung nicht zulässig und zu unterlassen.

Aus den Gründen:

Wie das BVerfG in der ersten Lebach-Entscheidung ausgeführt hat, stellt eine öffentliche Berichterstattung über eine Straftat unter Namensnennung, Abbildung oder Darstellung des Täters zwangsläufig eine erhebliche Beeinträchtigung seines Persönlichkeitsrechts dar, weil das Fehlverhalten des Täters öffentlich bekannt gemacht und seine Person in den Augen der Adressaten von vornherein negativ qualifiziert wird. Für die Intensität der Beeinträchtigung kommt es auf die Art und Weise der Darstellung an, etwa ob es sich um eine um Objektivität und Sachlichkeit bemühte Berichterstattung handelt und in welchem Medium (Fernsehen oder Printmedium) berichtet wird. Insoweit ist auch der Grad der Verbreitung des Mediums von Bedeutung (BVerfG NJW 1973, 1226 (1229) [BVerfG 05.06.1973 – 1 BvR 536/72]).

Andererseits sprechen, wie das BVerfG ebenfalls betont, erhebliche Erwägungen für eine auch die Person des Täters einbeziehende vollständige Information der Öffentlichkeit über vorgefallene Straftaten, ihre Entstehungsursachen und Hintergründe. Straftaten gehören zum Zeitgeschehen, dessen Vermittlung Aufgabe der Medien ist. Darüber hinaus begründet die Verletzung der allgemeinen Rechtsordnung und die Beeinträchtigung individueller Rechtsgüter, die Sympathie mit den Opfern und Angehörigen, die Furcht vor Wiederholungen solcher Straftaten und das Bestreben, dem vorzubeugen, grds. ein anzuerkennendes Interesse der Öffentlichkeit an näherer Information über Tat und Täter. Dieses wird umso stärker sein, je mehr sich die Straftat in Begehungsweise und Schwere von der gewöhnlichen Kriminalität abhebt (BVerfG a.a.O., S. 1230).

Demnach ist bei der hier dargestellten Straftat einer mitgliedschaftlichen Beteiligung an einer international aktiven terroristischen Vereinigung im Ausland (D), welche viele Anschläge und Kampfhandlungen mit einer Vielzahl von Toten und Verletzungen begangen hat, ein über bloße Neugier und Sensationslust hinausgehendes Interesse an näherer Information über die Tat und ihren Hergang sowie über die Person des Klägers und sein persönliches Leben anzuerkennen, soweit es in unmittelbarer Beziehung zur Tat steht, Aufschlüsse über seine Motive gibt und für die Bewertung seiner Schuld als wesentlich erscheint.

Bei der Abwägung des Informationsinteresses an einer entsprechenden den Täter nennenden Berichterstattung mit der damit zwangsläufig verbundenen Beeinträchtigung seines Persönlichkeitsrechts kommt im Rahmen der aktuellen Berichterstattung über Straftaten dem Informationsinteresse genereller Vorrang zu. Denn wer den Rechtsfrieden bricht und durch diese Tat und ihre Folgen Mitmenschen oder Rechtsgüter der Gemeinschaft angreift oder verletzt, muss sich nicht nur den hierfür verhängten strafrechtlichen Sanktionen beugen, sondern auch dulden, dass das von ihm selbst durch seine Tat erregte Informationsinteresse der Öffentlichkeit in einer nach dem Prinzip freier Kommunikation lebenden Gemeinschaft auf den dafür üblichen Wegen befriedigt wird [BVerfG a.a.O.].

Auch wenn die dem Kläger zur Last gelegte Straftat gemäß § 129 a und b StGB bei ihrem Bekanntwerden beträchtliche Aufmerksamkeit in der Öffentlichkeit erregt hat und – wie die Beklagte meint – „zur deutschen Kriminalgeschichte“ geworden ist, lässt die Ausstrahlungswirkung des verfassungsrechtlichen Schutzes der Persönlichkeit es freilich nicht zu, dass die Kommunikationsmedien sich über die aktuelle Berichterstattung hinaus zeitlich unbeschränkt mit der Person des Klägers befassen (vgl. OLG Ffm. Beschl. vom 13.8.2001 – 11 W 20/01 – Rn. 11, 14; OLG Hamburg NJW-RR 1991, 990 (991) [OLG Hamburg 22.11.1990 – 3 U 170/90]; Prinz/Peters, Medienrecht, 1999, 3. Kap. Rn. 109).

Nach Befriedigung des aktuellen Informationsinteresses tritt mit fortschreitender zeitlichen Distanz zur Straftat und zum Strafverfahren das Interesse und Informationsbedürfnis der Öffentlichkeit, über diesen Fall unter namentlicher Erwähnung unterrichtet zu werden, immer weiter zurück, während das Recht des Täters darauf, „allein gelassen zu werden“, – auch bei schweren Straftaten – zunehmend an Bedeutung gewinnt und dem Wunsch der Massenmedien und einem Bedürfnis des Publikums, seinen individuellen Lebensbereich zum Gegenstand der Erörterung oder gar der Unterhaltung zu machen, Grenzen setzt. Auch der Täter, der durch eine schwere Straftat in das Blickfeld der Öffentlichkeit getreten ist und die allgemeine Missachtung erweckt hat, bleibt dennoch ein Glied dieser Gemeinschaft mit dem verfassungsrechtlichen Anspruch auf Schutz seiner Individualität. Hat die das öffentliche Interesse veranlassende Tat mit der Strafverfolgung und strafgerichtlichen Verurteilung die im Interesse des öffentlichen Wohls gebotene gerechte Reaktion der Gemeinschaft erfahren und ist die Öffentlichkeit hierüber hinreichend informiert worden, so lassen sich darüber hinausgehende fortgesetzte oder wiederholte Eingriffe in den Persönlichkeitsbereich des Täters im Hinblick auf sein Interesse an der Wiedereingliederung in die Gemeinschaft nicht ohne weiteres rechtfertigen (BVerfG a.a.O., S. 1231).

Die zeitliche Grenze zwischen der grds. zulässigen aktuellen Berichterstattung und einer unzulässigen späteren Darstellung oder Erörterung hat das BVerfG nicht mit einer fest umrissenen Frist fixiert. Das entscheidende Kriterium sieht es darin, ob die betreffende Berichterstattung gegenüber der aktuellen Information eine erhebliche neue oder zusätzliche Beeinträchtigung des Täters zu bewirken geeignet ist. Insoweit nennt das BVerfG als maßgeblichen Orientierungspunkt für die nähere Bestimmung der zeitlichen Grenze das Interesse an der Wiedereingliederung des Straftäters in die Gesellschaft, d.h. an seiner Resozialisierung, deren entscheidendes Stadium mit der Entlassung beginnt.

Hiermit ist allerdings keine vollständige Immunisierung vor der ungewollten Darstellung persönlichkeitsrelevanter Geschehnisse gemeint. Zutreffend führt die Berufung aus, dass das allgemeine Persönlichkeitsrecht dem Straftäter keinen Anspruch darauf vermittelt, nach Ablauf einer bestimmten Zeitspanne in der Öffentlichkeit überhaupt nicht mehr mit der Tat konfrontiert zu werden. Selbst die Verbüßung der Strafhaft führt nicht dazu, dass ein Täter den uneingeschränkten Anspruch erwirbt, vor einer Reaktualisierung seiner Verfehlung verschont zu bleiben, da mit der Verbüßung der Strafe lediglich dem Strafanspruch des Staates Genüge getan, nicht aber das Verhältnis des Täters zu Dritten, insbesondere den Medien, berührt wird. Wie das BVerfG in seiner zweiten Lebach-Entscheidung ausgeführt hat, ist maßgeblich vielmehr stets, in welchem Ausmaß das Persönlichkeitsrecht des Straftäters, insbesondere sein Interesse an der Wiedereingliederung in die Gesellschaft, welche zugleich im öffentlichen Interesse liegt, unter den konkreten Um-

ständen des Einzelfalls von der Berichterstattung beeinträchtigt wird (BVerfG NJW 2000, 1859 (1860) [BVerfG 25.11.1999 – 1 BvR 348/98]).

Unter Berücksichtigung dieser Grundsätze ist dem Landgericht darin beizupflichten, dass eine Identifizierbarkeit des Klägers im Zusammenhang mit der Berichterstattung über seine früheren Straftaten in dem streitgegenständlichen Buch nicht gerechtfertigt ist, auch wenn es sich aufgrund der Art und Schwere der Straftat nach § 129 a und b StGB und der Begleitumstände durchaus um einen aus dem durchschnittlichen Geschehen herausgehobenen gravierenden Kriminalfall gehandelt hat. Bei der gebotenen Güter- und Interessenabwägung hat die durch Art. 5 Abs. 1 Satz 2 GG gewährleistete Berichterstattungsfreiheit der Beklagten und das von ihr verfolgte Informationsinteresse der Öffentlichkeit vorliegend hinter dem Interesse des Klägers am Schutz seiner Persönlichkeit und an der Achtung seines Privatlebens zurückzutreten, insbesondere im Hinblick auf sein Resozialisierungsinteresse.

(wird weiter ausgeführt)

Prozessuale Verwertung von Dashcam-Aufnahmen

(**Oberlandesgericht Stuttgart**, Beschluss vom 4. Mai 2016 – 4Ss 543/15 –)

1. **Aus einem Verstoß eines Verkehrsteilnehmers beim Betrieb einer dashcam (On-Board-Kamera) gegen das datenschutzrechtliche Verbot gem. § 6b BDSG, nach dem die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nur in engen Grenzen zulässig ist, folgt nicht zwingend ein Beweisverwertungsverbot im Bußgeldverfahren.**
2. **§ 6b BDSG, insbesondere dessen Abs. 3 Satz 2, enthält kein gesetzlich angeordnetes Beweisverwertungsverbot für das Straf- und Bußgeldverfahren.**
3. **Ob ein (möglicherweise) unter Verstoß gegen § 6b BDSG erlangtes Beweismittel zulasten eines Betroffenen in einem Bußgeldverfahren verwertet werden darf, ist im Einzelfall insbesondere nach dem Gewicht des Eingriffs sowie der Bedeutung der betroffenen Rechtsgüter unter Abwägung der widerstreitenden Interessen zu entscheiden.**
4. **Der Tatrichter ist grundsätzlich nicht gehindert, eine Videoaufzeichnung, die keine Einblicke in die engere Privatsphäre gewährt, sondern lediglich Verkehrsvorgänge dokumentiert und eine mittelbare Identifizierung des Betroffenen über das Kennzeichen seines Fahrzeugs zulässt, zu verwerten, wenn dies zur Verfolgung einer besonders verkehrssicherheitsbeeinträchtigenden Ordnungswidrigkeit erforderlich ist.**

Sachverhalt:

Das Amtsgericht Reutlingen verhängte gegen den Betroffenen wegen einer fahrlässigen Ordnungswidrigkeit des Missachtens des Rotlichts einer Lichtzeichenanlage, wobei die Rotphase länger als eine Sekunde andauerte, eine Geldbuße von 200 Euro und verbot ihm für die Dauer von einem Monat, im öffentlichen Straßenverkehr Kraftfahrzeuge jeder Art zu führen, wobei ihm die Schonfrist nach § 25 Abs. 2a StVG eingeräumt wurde.

Hiergegen wendet sich der Betroffene mit der Rechtsbeschwerde. Er erhebt die Sachrüge und greift mit einer Verfahrensrüge insbesondere die Verwertung einer von einem Zeugen mittels „dashcam" – einer kleinen Videokamera, die meist auf dem Armaturenbrett oder an der Windschutzscheibe eines Fahrzeugs angebracht ist und während der Fahrt aufzeichnen kann – gefertigten Videoaufnahme an.

Aus den Gründen:

Die gemäß § 79 Abs. 1 Nr. 2 OWIG statthafte, form- und fristgemäß eingelegte und begründete Rechtsbeschwerde des Betroffenen hat in der Sache keinen Erfolg. Auch die Verfahrensrüge, mit der der Betroffene einen Verstoß gegen ein angenommenes Beweisverwertungsverbot geltend macht, bleibt ohne Erfolg.

1. Der Rüge liegen folgende Feststellungen und Wertungen zugrunde:

Nach den Feststellungen des Amtsgerichts fuhr der Betroffene mit einem Pkw innerorts bei ruhiger Verkehrslage über eine näher bezeichnete Kreuzung, obwohl die sich dort befindende Wechsellichtzeichenanlage bereits seit mindestens sechs Sekunden für die Fahrtrichtung des Betroffenen Rot zeigte. Der Betroffene hätte bei ihm möglicher und jederzeit zumutbarer Aufmerksamkeit die Lichtzeichenanlage uneingeschränkt wahrnehmen und rechtzeitig anhalten können. Zuvor hatte der Betroffene eine ebenfalls für ihn Rot zeigende Lichtzeichenanlage überfahren, was allerdings nicht Gegenstand des Bußgeldverfahrens ist.

Zur Überzeugungsbildung hat das Amtsgericht unter anderem Folgendes herangezogen: Der Betroffene, der sich ansonsten nicht zur Sache eingelassen hat, hat über seinen Verteidiger die Fahrereigenschaft eingeräumt. Die Feststellungen zur Sache beruhen auf der Inaugenscheinnahme einer Videoaufzeichnung, welche ein Zeuge mit einer „dashcam" gefertigt hat. Dabei lief die Kameraaufzeichnung, wie sie auch komplett in der Hauptverhandlung in Augenschein genommen wurde, bereits seit Fahrtbeginn des Zeugen und anlasslos über seine gesamte Fahrtstrecke weiter. Diese Videoaufzeichnung wurde von einem Sachverständigen in der Hauptverhandlung vorgespielt und ausgewertet. Die Dauer des Rotlichtverstoßes ergab sich dabei aus der in der Videoaufzeichnung mitlaufenden Uhr, wobei der Sachverständige unter anderem feststellen konnte, dass die Uhrzeit als solche zutreffend im Sekundentakt mitzählt. Aus dem in Augenschein genommenen Video ergaben sich für das Amtsgericht ferner die weiteren Umstände der Fahrt sowie die Sicht- und Verkehrsverhältnisse. Zudem legte das Amtsgericht dar, dass ohne die Videoaufzeichnung allein mit der Aussage des Zeugen eine für eine Verurteilung ausreichende Überzeugungsbildung nicht erfolgt wäre. Weiter hat der Tatrichter die Frage der Verwertbarkeit der Videoaufzeichnung samt einer Abwägung ausdrücklich erörtert.

2. Die Verfahrensrüge, die die Verwertung der Erkenntnisse aus der Videoaufzeichnung der „dashcam" zu Lasten des Betroffenen trotz des Bestehens eines Beweisverwertungsverbotes geltend macht, ist in zulässiger Weise erhoben. Die Rügebegründung genügt den nach § 79 Abs. 3 OWiG i.V.m. § 344 Abs. 2 Satz 2 StPO zu stellenden Anforderungen. Insbesondere

geht aus der Rügebegründung in Verbindung mit den Urteilsgründen, die der Senat aufgrund der zulässigen Sachrüge ergänzend heranzuziehen hat (BGH, Beschlüsse vom 20. Juli 1995 – 1 StR 338/95, juris Rn. 8; vom 18. Dezember 2012 – 3 StR 458/12, juris Rn. 6), hervor, dass der Betroffene der Verwertung der Videoaufnahmen in der Hauptverhandlung rechtzeitig widersprochen hat.

3. Die Rüge ist jedoch unbegründet. Das Amtsgericht ist zu Recht davon ausgegangen, dass die vom Zeugen mittels „dashcam" gefertigte Videoaufzeichnung der Fahrt des Betroffenen verwertbar war.

a) Die Fertigung der Bildaufzeichnung stellte einen Eingriff in das allgemeine Persönlichkeitsrecht des Betroffenen aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in seiner Ausprägung als Recht auf informationelle Selbstbestimmung dar. Dieses Recht umfasst die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, und daher grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen. Durch die Aufzeichnung des gewonnenen Bildmaterials wurden die beobachteten Lebensvorgänge technisch fixiert. Sie konnten später zu Beweiszwecken abgerufen, aufbereitet und ausgewertet werden. Eine Identifizierung des Fahrzeugs bzw. des Fahrers war beabsichtigt und technisch auch möglich (vgl. BVerfG, Kammerbeschluss vom 11. August 2009 – 2 BvR 941/08, NZV 2009, 618 Rn. 15). Ob und unter welchen Umständen ein solcher Eingriff – auch durch Private – zulässig sein kann, regelt u.a. § 6b BDSG.

Ob der Zeuge durch den Betrieb seiner On-Board-Kamera in der von ihm gewählten Betriebsform gegen das datenschutzrechtliche Verbot des § 6b BDSG, nach dem die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur unter bestimmten Umständen zulässig ist, verstoßen hat oder ob sich die Zulässigkeit aus § 6b Abs. 1 Nr. 3 BDSG ergab, kann der Senat nicht abschließend beurteilten, da das angefochtene Urteil hierzu nicht sämtliche prüfungsrelevanten Tatsachen mitteilt. Gem. § 6b Abs. 1 Nr. 3 BDSG ist die Videoüberwachung nur zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

aa) Bei den Straßen, die vom Zeugen und dem Betroffenen mit ihren Fahrzeugen befahren wurden, handelt es sich um öffentlich zugängliche Räume. Die „dashcam" des Zeugen stellt eine optisch-elektronische Einrichtung dar. Zwar wird teilweise vertreten, dass als optisch-elektronische Einrichtungen in § 6b BDSG nur Einrichtungen zu verstehen seien, die fest angebracht sind. Mobile Kameras habe der Gesetzgeber nicht regeln wollen (AG Nienburg, Urteil vom 20. Januar 2015 – 4 Ds 520 Js 39473/14, DAR 2015, 280 ff.; zweifelnd: LG Landshut, Beschluss vom 1. Dezember 2015 – 12 S 2603/15, juris; AG Nürnberg, Urteil vom 8. Mai 2015 – 18 C 8938/14, DAR 2015, 472 ff.). Ein solches Verständnis der Regelung findet im Wortlaut keine Stütze. Vielmehr handelt es sich bei der gewählten Formulierung „optisch-elektronische Einrichtungen" gerade um einen wertneutralen Begriff, der jegliche Form der Videoüberwachung erfassen soll. § 6b BDSG verfolgt den Zweck, die Beobachtung öffentlich zugänglicher Räume nur in sehr begrenzten Ausnahmefällen zu gestatten, um das informationelle Selbstbestimmungsrecht der Betroffenen zu wahren. Durch den Klammerzusatz in § 6b Abs. 1 BDSG („Videoüberwachung") hat der Gesetzgeber zum Ausdruck gebracht, dass jegliches technisches Gerät, das Videos aufzeichnen kann, grundsätzlich als optisch-elektronische Einrichtung im Sinne dieser Norm zu verstehen ist. (LG Memmingen, Urteil vom 14. Januar 2016 – 22 O 1983/13, juris; VG Ansbach, ZfSch 2014, 663 ff.; so auch: Scholz, in: Simitis, Bundesdatenschutzgesetz, 8. Aufl., § 6b Rn. 37; Becker, in: Plath, BDSG, 2013, § 6b Rn. 12; Brink, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, § 6b BDSG Rn. 25; Onstein, in: Auernhammer, BDSG, 4. Aufl., § 6b Rn. 22). Die Nutzung der Daten erfolgte hier auch nicht ausschließlich für persönliche oder familiäre Tätigkeiten (vgl. § 1 Abs. 2 Nr. 3 BDSG). Die personenbezogenen Daten wurden der Bußgeldbehörde vorgelegt, dadurch wurde der persönliche und familiäre Bereich verlassen.

bb) Allerdings verhält sich das Urteil des Amtsgerichts nicht zu den Zwecken, die der Zeuge mit seiner Videoaufzeichnung verfolgt hat. Es bleibt offen, ob er einen solchen Zweck vorher überhaupt festgelegt hat. Es ist denkbar, dass er die Kamera deshalb verwendet hat, um mögliche Beweismittel bei einem Verkehrsunfall vorlegen zu können und so auch zivilrechtliche Ansprüche zu sichern; möglicherweise war bestimmendes Motiv aber auch, bei einem anderen verkehrsrechtlichen Sachverhalt Verkehrsteilnehmer anzeigen zu können. Da der genaue Zweck offen bleibt, kann der Senat nicht abschließend entscheiden, ob er als berechtigtes Interesse i.S.v. § 6b Abs. 1 Nr. 3 BDSG anzuerkennen wäre. Ebenso finden sich keine Feststellungen zur Betriebsform, in der die Kamera genutzt wurde (wurden bei eingeschalteter Zündung permanent Filmaufnahmen gemacht und auf einer SD-Karte gespeichert, bis deren Kapazität erschöpft ist? Wurden die Aufzeichnungen permanent gespeichert? Wer entscheidet bei der verwendeten Kamera, wann und wie welche Sequenzen der Videoaufzeichnung gesichert bzw. längerfristig gespeichert werden, um eventuell ein Überschreiben der Daten zu verhindern?). Auch diese Umstände könnten eventuell für die datenschutzrechtliche Beurteilung relevant sein.

b) Gleichwohl ist das angefochtene Urteil aber nicht durch Rechtsfehler beeinflusst, weil selbst im Falle eines Verstoßes gegen § 6b BDSG dieser in dem hier vorliegenden Einzelfall kein Beweisverwertungsverbot nach sich ziehen würde.

aa) Aus § 6b BDSG, insbesondere dessen Abs. 3 Satz 2, folgt kein gesetzlich angeordnetes Beweisverwertungsverbot für das Bußgeldverfahren. Weder der Gesetzeswortlaut noch die Gesetzgebungsmaterialien geben Hinweise, dass der Gesetzgeber ein solches Beweisverwertungsverbot regeln wollte. Ein solches kennt das deutsche Strafprozessrecht – und über § 46 OWiG auch das Verfahrensrecht im Bußgeldverfahren (BVerfG, Kammerbeschluss vom 20. Mai 2011 – 2 BvR 2072/10, NJW 2011, 2783 Rn. 13; Seitz, in: Göhler, OWiG, 16. Aufl. § 46 Rn. 10c) – ohnehin nur in Ausnahmefällen. In § 6b Abs. 3 Satz 2 BDSG ging es dem Gesetzgeber um eine Ausnahme von der strikten Zweckbindung des § 6b Abs. 3 Satz 1 BDSG für die durch Videoüberwachung gewonnenen Daten (BT-Drs. 14/5793, S. 62). Zur weitergehenden Frage eines Beweisverwertungsverbots im Straf- oder Bußgeldverfahren äußerte er sich jedoch gerade nicht, so dass auf die allgemeinen Grundsätze zurückzugreifen ist (so i. E. wohl auch: Becker, a.a.O., Rn. 31; Scholz, a.a.O., Rn. 160; für das Zivilverfahren: LG Landshut, a.a.O.; AG Nürnberg, a.a.O.; Greger, NZV 2015, 114, 115; vgl. auch Empfehlung des 54. Deutschen Verkehrsgerichtstag 2016, Arbeitskreis VI „dashcam" Nr. 5).

bb) Ob ein (hier möglicherweise) auf rechtswidrige Weise erlangtes Beweismittel zulasten des Betroffenen verwertet werden darf, ist nach der herrschenden und vom Bundesverfassungsgericht gebilligten Rechtsprechung im Einzelfall insbesondere nach Art des Verbotes und Gewicht des Verfahrensverstoßes sowie der Bedeutung der betroffenen Rechtsgüter unter Abwägung der widerstreitenden Interessen zu entscheiden, wenn es – wie hier – an einer ausdrücklichen gesetzlichen Anordnung eines Verwertungsverbotes fehlt. Von Verfassungs wegen besteht kein Rechtssatz des Inhalts, dass im Fall einer rechtsfehlerhaften Beweiserhebung die Verwertung der gewonnenen Beweise stets unzulässig wäre (BVerfG, Kammerbeschluss vom 20. Mai 2011 – 2 BvR 2072/10, NJW 2011, 2783 Rn. 12). Auch wenn die Strafprozessordnung nicht auf die Wahrheitserforschung um „jeden Preis" gerichtet ist, schränkt die Annahme eines Verwertungsverbotes ein wesentliches Prinzip des Strafrechts ein, nämlich den Grundsatz, dass das Gericht die Wahrheit zu erforschen und dazu die Beweisaufnahme von Amts wegen auf alle Tatsachen und Beweismittel zu erstrecken hat, die von Bedeutung sind (vgl. BGH, Urteile vom 11. November 1998 – 3 StR 181/98, BGHSt 44, 243, 249; vom 18. April 2007 – 5 StR 546/06, BGHSt 51, 285 Rn. 20). Ein Beweisverwertungsverbot ist ohne ausdrückliche gesetzliche Anordnung daher nur ausnahmsweise aus übergeordneten wichtigen Gesichtspunkten im Einzelfall anzunehmen, wenn einzelne Rechtsgüter durch Eingriffe fern jeder Rechtsgrundlage so massiv beeinträchtigt werden, dass dadurch das Ermittlungsverfahren als ein nach rechtsstaatlichen Grundsätzen geordnetes Verfahren nachhaltig geschädigt wird (vgl. BGH, Urteil vom 18. April 2007 – 5 StR 546/06, BGHSt 51, 285 Rn. 20). Insoweit wird ein Beweisverwertungsverbot dann angenommen, wenn die zur Fehlerhaftigkeit der Ermittlungsmaßnahmen führenden Verfahrensverstöße derart schwerwiegend waren oder bewusst oder willkürlich begangen wurden bzw. die grundrechtlichen Sicherungen planmäßig außer Acht gelassen worden sind (vgl. BVerfG, Kammerbeschluss vom 20. Mai 2011 – 2 BvR 2072/10, NJW 2011, 2783 Rn. 14). Diese Grundsätze sind über § 46 OWiG auch im Bußgeldverfahren heranzuziehen (BVerfG, Kammerbeschluss vom 20. Mai 2011 – 2 BvR 2072/10, NJW 2011, 2783 Rn. 13; Seitz, a.a.O.; Lampe, in: Karlsruher Kommentar zum OWiG, 4. Aufl., § 46 Rn. 18a).

cc) Nach den vorgenannten Grundsätzen ist es aus Rechtsgründen nicht zu beanstanden, dass der Tatrichter im vorliegenden Fall kein Beweisverwertungsverbot angenommen hat. Der Tatrichter ist grundsätzlich nicht gehindert, eine Videoaufzeichnung, die keine Einblicke in die engere Privatsphäre gewährt, sondern lediglich Verkehrsvorgänge dokumentiert und eine mittelbare Identifizierung des Betroffenen über das Kennzeichen seines Fahrzeugs zulässt, zu verwerten, wenn dies zur Verfolgung einer besonders verkehrssicherheitsbeeinträchtigenden Ordnungswidrigkeit erforderlich ist. So überwiegt hier im Rahmen der gebotenen Gesamtschau bei wertender Betrachtung unter Berücksichtigung der schutzwürdigen Belange des Betroffenen das allgemeine Interesse an der Effektivität der Verfolgung von erheblichem Fehlverhalten im Straßenverkehr.

(1) Bei der Abwägung ist zunächst zu sehen, dass es hier lediglich um die Ahndung einer Ordnungswidrigkeit und keiner Straftat geht. Die Videoaufzeichnung durch den Zeugen war geeignet, auch in das informationelle Selbstbestimmungsrecht einer unbestimmten, letztlich vom Zufall abhängigen Vielzahl weiterer Verkehrsteilnehmer einzugreifen. Sie wurde vom Betroffenen und allen anderen zufällig aufgezeichneten Verkehrsteilnehmern nach aller Lebenserfahrung nicht wahrgenommen, sondern geschah für sie verdeckt. Eine verdeckte Datenerhebung führt regelmäßig zur Erhöhung der Eingriffsintensität.

(2) Andererseits sind die hohe Bedeutung der Verkehrsüberwachung für die Sicherheit des öffentlichen Straßenverkehrs und das Gewicht des Verstoßes im Einzelfall (Rotlichtverstoß sehr deutlich über einer Sekunde) zu berücksichtigen. Es handelt sich nicht nur um eine Ordnungswidrigkeit im Verwarnungs- bzw. Bagatellbereich, sondern um eine solche, die bereits der Verordnungsgeber der Bußgeldkatalog-Verordnung nicht nur mit deutlich erhöhter Geldbuße, sondern im Regelfall wegen des groben Fehlverhaltens auch mit einem Fahrverbot sanktioniert sehen möchte. Der Verstoß ist im Fahreignungs-Bewertungssystem als besonders verkehrssicherheitsbeeinträchtigende Ordnungswidrigkeit eingestuft, die mit zwei Punkten bewertet wird (vgl. § 4 Abs. 2 Satz 2 Nr. 2 StVG). Die vom Rotlichtverstoß des Betroffenen ausgehende erhebliche Gefahr für die Sicherheit des öffentlichen Straßenverkehrs verleiht dem öffentlichen Interesse an einer effektiven Verfolgung derartiger Ordnungswidrigkeiten hier eine besondere Bedeutung. Die Aufrechterhaltung der Sicherheit des Straßenverkehrs dient angesichts des hohen Verkehrsaufkommens und der erheblichen Zahl von Verkehrsverstößen dem Schutz von Rechtsgütern mit – auch verfassungsrechtlich – ausreichendem Gewicht. Das Interesse der Allgemeinheit an der Sicherheit des Straßenverkehrs steht auch im Zusammenhang mit dem aus Art. 2 Abs. 2 Satz 1 GG ableitbaren Auftrag zum Schutz vor erheblichen Gefahren für Leib und Leben (vgl. BVerfG, Kammerbeschluss vom 5. Juli 2010, NJW 2010, 2717 Rn. 14).

Die Videoaufzeichnung wurde weder durch den Staat veranlasst, um grundrechtliche Sicherungen planmäßig außer Acht zu lassen, noch wurde ein Privater gezielt mit der Fertigung beauftragt, um Beweise zu erlangen, deren sich der Staat durch die Verkehrsüberwachungsbehörden selbst nicht hätte bedienen dürfen. Das wäre allenfalls dann der Fall, wenn Privatpersonen wiederholt bzw. dauerhaft aus eigener Machtvollkommenheit zielgerichtet mittels „dashcam"-Aufzeichnungen Daten, insbesondere Beweismittel, für staatliche Bußgeldverfahren erheben, sich so zu selbsternannten „Hilfssheriffs" aufschwingen und die Datenschutz- und Bußgeldbehörden dies dulden bzw. sogar aktiv fördern. Derartiges ist hier allerdings nicht festgestellt. Sollten die Bußgeldbehörden bzw. deren Aufsichtsbehörden einen „Orwellschen Überwachungsstaat" durch Private befürchten (vgl. hierzu bzw. ähnlichen Überlegungen: LG Memmingen, Urteil vom 14. Januar 2016, 22 O 1983/13, juris; LG Heilbronn, Urteil vom 3. Februar 2015 – 3 S 19/14, NJW-RR 2015, 1019 ff.; AG München, Beschluss vom 13. August 2014 – 345 C 5551/14, ZfSch 2014, 692 ff.; Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, Düsseldorfer Kreis am 25./26. Februar 2014), stünde es ihnen zudem frei, im Rahmen des das Ordnungswidrigkeitenverfahren beherrschenden Opportunitätsgrundsatzes (§ 47 OWiG) ausschließlich auf der Ermittlungstätigkeit von Privaten mittels „dashcam" beruhende Verfahren nicht weiter zu verfolgen. Die Bußgeldbehörden werden ihrerseits bereits bei Einleitung von Verfahren die Verwertbarkeit derartiger Aufnahmen zu prüfen und dabei auch die erforderlichen Abwägungen im Hinblick auf Bedeutung und Gewicht der angezeigten Ordnungswidrigkeit vorzunehmen haben.

Im Übrigen besteht kein Rechtssatz dahin, dass es im Straf- und Bußgeldverfahren stets untersagt wäre, von Privaten erlangte Beweismittel zu verwerten, sofern diese unter Verstoß gegen Gesetze gewonnen wurden. Aus der rechtswidrigen Erlangung eines Beweismittels durch einen Dritten folgt nicht ohne Weiteres die Unverwertbarkeit dieses Beweismittels im Strafverfahren (BGH, Urteil vom 12. April 1986 – 3 StR 453/88, BGHSt 36, 167, 173). Selbst Beweismittel, die von Privaten in strafbewehrter Weise erlangt wurden, sind – verfassungsrechtlich unbedenklich – grundsätzlich verwertbar und unterliegen nicht zwingend per se einem Beweisverwertungsverbot (vgl. zum Thema „Steuer-CDs": BVerfG, Kammerbeschluss vom 9. November 2010 – 2 BvR 2101/09, NStZ 2011, 103 Rn. 58; Verfassungsgerichtshof Rheinland-Pfalz, NJW 2014, 1434 ff.).

Der verfahrensgegenständliche Verstoß hätte ohne weiteres durch eine rechtmäßige, anlassbezogene Messung und Aufzeichnung festgestellt werden können. Sofern eine Polizeistreife mit geeignetem Aufnahmegerät auf das grobe Fehlverhalten des Betroffenen an der ersten Lichtzeichenanlage, das nicht Gegenstand der Verurteilung wurde, aufmerksam geworden wäre, hätte einer anlassbezogenen Nachfahrt und Aufzeichnung des Fahr- und Fehlverhaltens nichts entgegengestanden. Ebenso wäre der Rotlichtverstoß durch eine geeignete stationäre Überwachungsanlage nachweisbar gewesen. Das Amtsgericht hat nur den zweiten Rotlichtverstoß geahndet; diesen hätte der Zeuge auch als Privatperson mittels Videotechnik aufnehmen dürfen, da er durch das vorangegangene erste Fehlverhalten des Betroffenen nicht anlasslos aufgezeichnet hätte.

Sonstige Beweismittel, die für die Überzeugungsbildung des Amtsgerichts zum Nachweis der Ordnungswidrigkeit ausgereicht hätten, lagen nicht vor.

Die Intensität und Reichweite des Eingriffs in das Recht auf informationelle Selbstbestimmung durch die Videoaufzeichnung des fließenden Verkehrs ist hier zudem sehr gering. Die aufgezeichneten Daten betreffen insbesondere nicht den Kernbereich privater Lebensgestaltung des Betroffenen oder seine engere Privat- oder gar Intimsphäre. Vielmehr setzte sich der Betroffene durch die Teilnahme am öffentlichen Straßenverkehr selbst der Wahrnehmung und Beobachtung durch andere Verkehrsteilnehmer wie auch der Kontrolle seines Verhaltens im Straßenverkehr durch die Polizei- und die Ordnungsbehörden aus. Der Betroffene selbst ist auf dem Video nicht bzw. allenfalls in Umrissen von hinten, sondern im Wesentlichen nur sein Fahrzeug abgebildet. Die Verpflichtung, als Halter die im öffentlichen Straßenverkehr verwendeten Kraftfahrzeuge mit Kennzeichen zu versehen (§§ 8 und 10 FZV) und gegebenenfalls ein Fahrtenbuch zu führen, wenn bei Verstößen der Fahrer nicht feststellbar ist (§ 31a StVZO), zeigt, dass der Gesetz- und Verordnungsgeber eine Identifizierung von Regelverletzern zumindest grundsätzlich ermöglichen möchte und sich keiner auf eine anonyme Teilnahme am Straßenverkehr verlassen und berufen können soll. Durch das Abspielen des Videos in der Hauptverhandlung und die Auswertung durch einen Sachverständigen wurde der Eingriff auch nicht wesentlich vertieft, da auch dabei nur das Verhalten des Betroffenen im öffentlichen Straßenraum zu sehen war, ohne ihn als Person überhaupt identifizieren zu können.

Auch weitere zufällig aufgezeichnete Personen waren nicht intensiver, sondern sogar noch wesentlich weniger tief in ihrem informationellen Selbstbestimmungsrecht betroffen. Deren Aufzeichnungsdauer war wesentlich kürzer als beim Betroffenen und die Bilder konnten schon daher kaum zu einer Identifizierung dienen. Auch sie setzten sich durch die Teilnahme am öffentlichen Straßenverkehr bzw. durch den Aufenthalt außerhalb des besonders geschützten Privatraums grundsätzlich selbst der Wahrnehmung und Beobachtung durch Dritte aus.

Persönlichkeitsschutz im Internet

(**Oberlandesgericht Frankfurt/M.**, Urteil vom 21. April 2016 – 16 U 251/15 –)

In der Teilnahme an einer öffentlichen Veranstaltung liegt keine konkludente Einwilligung für die Veröffentlichung von herausgeschnittenen Einzelbildern einer Person.

Sachverhalt:

Bei dem auf dem Twitter-Account www.twitter.com/A des Beklagten veröffentlichten Bildnis handelte es sich um einen Bildausschnitt aus einem Foto, das bei Anlass einer politischen Demonstration gegen das Töten von Delfinen in Japan unter dem Kundgabemotto „Germany Stop Taji" am 15. Februar 2014 in Frankfurt gefertigt worden war. Es zeigte den Kläger, wie er – zusammen mit weiteren Personen – einer im Rahmen der Kundgebung aufgeführten szenischen Darbietung zuschaute und dies mit seinem Handy festhielt. Das Foto war seit 15. Februar 2014 auf dem Facebookaccount „B" zusammen mit 73 weiteren Fotos der Kundgebung – auf denen der Kläger nicht zu sehen ist – eingestellt und ist dort noch immer abrufbar. Zu der Kundgebung war unter anderem auch auf der Plattform „WikiLeaks" eingeladen und um Unterstützung gebeten worden.

Ferner war das beanstandete Foto auf unterschiedlichen Internetforen zu sehen:

Der Kläger hat behauptet, der Text unter den Bildern sei inhaltlich falsch. Er sei zwar Mitgründer des WikiLeaks-Forum.com, er habe dieses bereits im Februar 2013 an einen Dritten weitergegeben. Er hat die Ansicht vertreten, dem Fotoausschnitt komme keinerlei Informationswert zu, es sei auch kein öffentliches Interesse an der Nutzung seines Bildes erkennbar. Der Beklagte habe mit falschen Informationen ein Personenprofil von ihm erstellt, damit Dritte gegen ihn „hetzen" könnten, was auch geschehen sei. Er hat behauptet, sich stets bemüht zu haben, dass keinerlei persönlichen Fotos von ihm im Internet gezeigt würden. Das streitgegenständliche Foto sei nach wie vor das einzige dort verfügbare Foto. Es sei erkennbar nur im Zusammenhang mit der öffentlichen Kundgebung vom 15. Februar 2014 und auch nur auf Facebook eingestellt worden.

Der Beklagte hat behauptet, der Kläger habe in die Nutzung des Fotos eingewilligt. Er hat die Ansicht vertreten, die Einwilligung sei jedenfalls konkludent erteilt worden, da der Kläger selbst das Foto im Internet veröffentlicht habe. Er hat behauptet, die Seite www.D würde vom Kläger persönlich verantwortet und betrieben, wofür es zahlreiche Indizien gebe.

Das Landgericht Frankfurt am Main hat mit einem dem Beklagten am 9. November 2015 zugestellten Urteil vom 5. November 2015 der Klage – mit Ausnahme eines Teils der geltend gemachten vorgerichtlichen Rechtsanwaltskosten – stattgegeben. Es hat ausgeführt, der Kläger habe in die Veröffentlichung seines Bildnisses nicht ausdrücklich oder konkludent eingewilligt, da die Abbildung nur für eine Verwendung in dem engen zeitlichen und sachlichen

Kontext der Kundgebung beschränkt sei. Auch die Verwendung des Fotos durch den Kläger beschränke sich auf den engen sachlichen Zusammenhang des gegen den Beklagten erhobenen Vorwurfs des „Stalkings". Auch die vorzunehmende Interessenabwägung ergebe, dass eine Veröffentlichung nur im Zusammenhang mit der Teilnahme des Klägers an der Demonstration und über den Kläger als Tierschützer zulässig sei.

Aus den Gründen:

Der Kläger kann von dem Beklagten die Unterlassung der Verbreitung des Bildnisses aus Anlage K 1 und K 2, das den Kläger zeigt, wie vom Landgericht im Tenor festgelegt aus §§ 1004, 823 BGB, Art. 1 und 2 GG, §§ 22 ff. KUG verlangen.

1. Nicht zu beanstanden ist im Ergebnis die Auffassung des Landgerichts, eine konkludente Einwilligung des Klägers in die streitgegenständliche Bildveröffentlichung habe nicht vorgelegen (§ 22 Satz 1 KUG).

Für die Beantwortung dieser Frage, ist der Erklärungswert des als Einwilligung zu wertenden Verhaltens im Wege der Auslegung zu ermitteln (BVerfG vom 14.09.2010 – 1 BvR 2538/08 Rn 44; BGH vom 18.10.2011 „Die lange Nacht der GOLDKINDER" – VI ZR 5/10 Rn 6 – zitiert nach iuris). Heranzuziehen sind dabei alle erkennbaren Umstände, insbesondere das Verhalten des Betroffenen selbst.

a) Zu Recht hat die Kammer des Landgerichts das Argument des Beklagten zurückgewiesen, mit der Teilnahme an der Kundgebung „Germany Stop Taji" habe er zugleich der Nutzung von dort aufgenommenen Fotos zustimmt. Ein Bildnis wird nicht gleichsam dadurch zum allgemeinen Gebrauch freigegeben, weil der Abgebildete sich in einem öffentlichen Raum bewegt und weiß, dass dort Fotos gefertigt werden. Denn die Teilnahme an einer öffentlichen Demonstration ist zweckbestimmt. Sie dient der Kundgabe der Überzeugung, die Ziele der Veranstaltung zu teilen und zu unterstützen und dafür mit seiner Person offen einzutreten. Auf andere Zwecke kann dieser Wille nicht übertragen werden.

b) Andere Handlungen, aus denen auf eine solche Einwilligung des Klägers an der Nutzung seines Bildnisses in anderem Zusammenhang geschlossen werden könnte, sind nicht dargetan. Das Gesamtfoto aus der Kundgebung ist offensichtlich nicht außerhalb der Berichterstattung über die Demonstration gegen das Töten von Delfinen in Japan mit Willen des Klägers verwendet worden. Der Beklagte bezieht sich insoweit selbst nur auf die Einstellung des Gesamtbildes im Facebookaccount „B". Dort ist das Foto eines von über 70 bei der Demonstration gefertigten Fotos. Es handelt sich bei allen Fotos um eine reine Bildergalerie, die ausschließlich den Verlauf der Kundgebung bebildern. Ein weitergehenden Erklärungswert kommt dem nicht zu. Denn das Social Media Netzwerk Facebook ist kein allgemeiner, jedem ohne weiteres wie ein Marktplatz öffentlich zugänglicher Raum. Denn es haben dort, was gerichtsbekannt ist, nur Inhaber eines Facebook-Accounts Zugang. Wie die Unterstützerseite „B" zeigt, können dort Bildnisse mit einer begrenzten Erklärungswirkung eingestellt werden, ohne dass diese gleichsam im Allgemeingebrauch frei verfügbar werden.

c) Dass der Kläger aus Anlass der gezeigten szenischen Darbietung auf der Kundgebung – dies scheint augenscheinlich so zu sein – mit seinem Handy Fotos angefertigt haben mag, ist für die Bewertung dieses Verhaltens als Einwilligung ohne jeden Erklärungswert. Das Anfertigen eigener Fotos lässt keinen Schluss auf den eigenen Willen zu, wie mit solchen Fotos nach der Vorstellung des Fotografierenden zu verfahren ist. Denn geschützt ist nach der Konzeption des Bildnisschutzes nicht das Herstellen von Fotos, sondern nur deren unbefugte Nutzung.

d) Auch die weitergehenden Handlungen, die der Beklagte als Beleg für eine konkludente Einwilligung heranzieht, ergeben hierfür nichts. Denn auf den vom Beklagten insoweit herangezogenen Belegstellen ist nicht das Ausgangsfoto zu sehen, sondern nur der beanstandete Ausschnitt. Dabei benutzt der Kläger das Foto nur zum Beleg der von ihm beanstandeten „Stalking-Vorwürfen" gegen den Beklagten. Dabei geht es dem Kläger ersichtlich nur um den Vorwurf, gegen ihn werde mit Hilfe eines unautorisierten Bildausschnitts eine Hetzkampagne geführt. Das Bildnis ist nicht selbst Träger einer Information, sondern dient nur als Beleg für das beanstandete Verhalten. Zwar hat der Senat in anderem Zusammenhang bereits entschieden, dass eine Person keinen Anspruch darauf hat, von anderen so dargestellt zu werden, wie sie sich selbst sieht oder gesehen werden möchte (OLG Frankfurt Urteil vom 4. Juni 2009, 16 U 206/08 zitiert nach [...], Rn 52). Darum geht es hier aber nicht. Es ist vorliegend auch unerheblich, ob und in welchem Umfang die vom Beklagten benannten Quellen in Blogs, Homepages und Twitter-Accounts vom Kläger betrieben werden oder nicht. Denn jedenfalls ist der räumliche, zeitliche und inhaltliche Bezug der insoweit vorliegenden Einwilligung des Klägers auf einen ganz engen Lebenssachverhalt, die Beanstandung des von ihm als „Stalking" bewerteten Verhaltens, beschränkt.

2. Die Kammer des Landgerichts beurteilt die Zulässigkeit der Bildveröffentlichung im Ansatz auch zu Recht nach dem abgestuften und von der höchstrichterlichen Rechtsprechung ausgeprägten Schutzkonzept der §§ 22, 23 KUG, das sowohl mit verfassungsrechtlichen Vorgaben (BVerfG vom 14.09.2010 – 1 BvR 1842/08) als auch mit der Rechtsprechung des Europäischen Gerichtshofes für Menschenrecht in Einklang steht (BGH vom 13.04. 2010 – VI ZR 125/08 – „Charlotte im Himmel" Rn 12 ff m.w.N.; EGMR vom 7.02.2012 – 39954/08 – Axel Springer AG; BGH Urteil vom 21.04.2015 – VI ZR 245/14 zitiert nach iuris). Danach dürfen Bildnisse einer Person ohne deren Einwilligung nach § 23 Abs. 1 KUG ausnahmsweise verbreitet werden, wenn es sich um Bildnisse aus dem Bereich der Zeitgeschichte handelt und durch die Verbreitung die berechtigten Interessen des Abgebildeten nicht verletzt werden (§ 23 Ab. 2 KUG). Dabei erfordert schon die Beurteilung, ob Bildnisse aus dem Bereich der Zeitgeschichte vorliegen, eine Abwägung zwischen den Rechten des Abgebildeten aus Art. 1 Abs. 1, Art. 2 Abs. 1 GG, Art. 10 Abs. 1 EMRK einerseits und dem Recht der Presse und Informationsfreiheit aus Art. 5 Abs. 1 GG, Art. 10 Abs. 1 EMRK (BGH a.a.O. mit m.w.N.) anderseits. Vorliegend ist auf Seiten des Beklagten die Informations- und Meinungsäußerungsfreiheit, nicht aber die Pressefreiheit betroffen. Auch in diesem Zusammenhang ist der Begriff des Zeitgeschehens weit auszulegen. Er umfasst alle Fragen von allgemeinem gesellschaftlichen Interesse, nicht nur Vorgänge von historischer Bedeutung (BGH vom 13.04.2010 – VI ZR 125/08 – „Charlotte im Himmel" Rn 12 ff m.w.N.). Ausgehend vom Informationswert der Nachricht ist dabei für die Abwägung von maßgeblicher Bedeutung, ob der Berichtende eine Angelegenheit von öffentlichem Interesse ernsthaft und sachbezogen erörtert, damit den Informationsanspruch des Publikums erfüllt und zur öffentlichen Meinungsbildung beiträgt oder lediglich die Neugier der so Informierten oder andere Bedürfnisse befriedigt. Dabei ist der Informationsgehalt einer Bildberichterstattung im Gesamtkontext, in den

das Personenbildnis gestellt ist, zu ermitteln, insbesondere unter Berücksichtigung der zugehörigen Textberichterstattung (BGH a.a.O. „Charlotte im Himmel", Rn 14). Hierbei sind die kollidierenden Rechtspositionen in der Abwägung in einen möglichst schonenden Ausgleich zu bringen, insbesondere auch zu prüfen, ob und inwieweit die Abbildung der Person für die Nachricht erforderlich ist. Dabei ist von dem Informationswert der Wortbildberichtbestattung im Gesamtkontext auszugehen (zum Ganzen ferner: BGH vom 18.10.2011 – VI ZR 5/10 – Die lange Nacht der GOLDKINDER"; BVerfG Beschluss vom 14.09.2010 – 1 BvR 1842/08; BGH Urteil vom 21.04.2015 – VI ZR 245/14 Rn. 14 ff.). Bei der Abbildung von unbekannten Personen, die im Zusammenhang mit einem Ereignis von allgemeinem öffentlichen Interesse zufällig mit abgebildet werden, ist ebenfalls eine Interessenabwägung erforderlich, dabei ist aber den Persönlichkeitsrechten des Betroffenen besonders Rechnung zu tragen (BGH Urteil vom 21. April 2015 – VI ZR 245/14, Rn. 21).

Vorliegend handelte sich bereits nicht um eine Berichterstattung im Sinne des Presserechts, sondern um einen privaten Beitrag des Beklagten im Internet, dessen Informationswert für das Zeitgeschehen an den v.g. Grundsätzen zu messen ist. Nach der danach vorzunehmenden Gesamtabwägung bezog sich die beanstandete Meinungsäußerung des Beklagten nicht auf ein Ereignis des Zeitgeschehens (a)). Ferner erweist sich das Benutzen des Bildnisses für den intendierten Informationsgehalt nicht als erforderlich (b)).

a) Bei dem herauskopiertes Einzelbild des Klägers handelt es sich um einen Ausschnitt, der aus dem Bildzusammenhang genommen worden ist. Es hat für sich gesehen als solches keinen Informationswert für die öffentliche Meinungsbildung, da es lediglich die Identifizierung des Klägers als Person ermöglicht. Über den Kontext der Demonstration, in dem das Bild aufgenommen wurde, wird gerade nicht berichtet. Der Kläger wird in hockender Stellung gezeigt, wie er auf sein Mobiltelefon schaut und möglicherweise Fotos fertigt, wobei dies aus dem Ausschnitt heraus nicht erkennbar ist.

Nimmt man den Wortbeitrag hinzu, erhält man die Information, welches „Gesicht" dem Namen des im Internet aktiven Klägers zuzuordnen ist. Dies mag zwar für eine belegende Berichterstattung insoweit sprechen, als damit die Aussage verbunden ist „Z...". Welcher Beitrag damit aber zur öffentlichen Meinungsbildung in diesem konkreten Kontext geleistet wird, erschließt sich dem Betrachter und Leser der Nachricht nicht. Zwar macht der Beklagte geltend, es solle damit über den Bruch des Klägers mit der WikiLeaks -Bewegung und seine inzwischen offenbar kritische bis ablehnende Haltung zur Person D informiert und aufgezeigt werden, wer sich persönlich hinter dem Namen als Person verbirgt. Diese Information liegt aber nicht in für die öffentliche Meinungsbildung erforderlichem allgemeinen Interesse. Denn es handelt sich dabei nur um eine interne, eher dem privaten Bereich zuzurechnende persönliche Auseinandersetzung der Beteiligten selbst, der nicht der gleiche Rang für die öffentliche Meinungsbildung zuzumessen ist, wie den Debatten über die politischen Ziele der WikiLeaks-Bewegung selbst. Der Beklagte macht auch nicht geltend, seinen Beitrag in einem Amt oder einer Funktion für die WikiLeaks-Bewegung zu führen, sondern gibt nur seine persönliche Auffassung kund, wie er die Rolle des Klägers innerhalb der WikiLeaks-Bewegung persönlich bewertet. Der angegriffene Wortbildbeitrag des Beklagten befasst sich auch erkennbar nicht mit einer inhaltlichen Position, mit der der Beklagte für oder gegen die WikiLeaks Bewegung Stellung genommen haben mag, sondern bezieht sich ausschließlich auf die Person des Klägers. Seinem Namen wird ein Gesicht zugeordnet. Die Bebilderung derartiger rein persönlichen Meinungsäußerung liegt aber nicht im allgemeinen öffentlichen Interesse und sind von dem Abgebildeten nicht ohne weiteres hinzunehmen. Das Grundrecht der freien Meinungsäußerung hat gegenüber dem Persönlichkeitsrecht des Klägers an seinem Bildnis im Rahmen der vorzunehmenden Abwägung der Grundrechte gegeneinander hier zurückzutreten.

b) Im Übrigen erscheint die Nutzung des Bildnisses für die Berichterstattung nach Abwägung der Grundrechte des Klägers gegen den Informationswert der Nachricht vorliegend als nicht erforderlich. Denn wie der Kläger aussehen mag, ist keine Nachricht, die in diesem Zusammenhang von besonderem Informationswert für die Öffentlichkeit ist. Wenn die Berufung in diesem Zusammenhang anführt, die Bebilderung des Namens sei doch ohne weiteres z.B. in den Nachrichten oder anderen Medien bei Berichten über öffentliche Debatten üblich, überzeugt dies vorliegend nicht. Denn auch wenn beim Bildnisschutz nicht mehr zwischen den Kategorien der absoluten und relativen Person der Zeitgeschichte zu unterscheiden ist, spielt es bei Prüfung der Erforderlichkeit hier eine Rolle, ob das Hinzufügen eines Gesichts zum Namen für die Meinungsbildung bedeutsam für den Informationswert der Nachricht ist. Dies ist vorliegend für die angegriffenen Äußerungen nicht ersichtlich. Auf die persönliche Integrität des Klägers oder die Bewertung seiner persönlichen Verhältnisse kommt es bei der hier streitgegenständlichen Auseinandersetzung nicht an. Es ist auch nicht ersichtlich, dass der Kläger im Rahmen seiner Beiträge auf den hier benannten Foren und Internetseiten besonderes persönliches Vertrauen in Anspruch genommen oder diese sonst irgendwie mit seiner Person besonders wertschätzend geprägt hat.

Zwar trifft es zu, wie die Berufung geltend macht, dass es für die Abwägung auch darauf ankommt, wie der Abgebildete sonst mit seinem Bildnis in der Öffentlichkeit umgeht. Dies spricht aber hier für den Persönlichkeitsschutz des Klägers. Denn auch nach dem Vortrag des Beklagten gibt es offensichtlich keine anderen verfügbaren Bildnisse des Klägers sonst im Internet oder anderen elektronischen Kommunikationsmedien. Dies zeigt, dass jedenfalls der Kläger selbst keine persönlichen Bilder ins Internet gestellt oder sonst veröffentlicht hat. In diesem Zusammenhang ist auch ohne Bedeutung, dass das Bild die Sozialsphäre des Klägers betrifft. Denn auch die Nutzung von Bildnissen aus der Sozialsphäre sind an dem abgestuften Schutzkonzept der §§ 22, 23 KUG zu messen und sind nicht ohne weiteres gemeinfrei. Auch die weiteren Beiträge, bei denen der Kläger den Bildausschnitt öffentlich selbst benutzt hat, führen zu keiner anderen Beurteilung. Denn in allen diesen Beiträgen beanstandete der Kläger gerade die Nutzung des Bildes als Vorgang des „Stalkens". Sie dienten letztlich der Wahrung der Persönlichkeitssphäre des Klägers.

Schließlich verkennt der Senat nicht, dass die WikiLeaks-Bewegung als solche und die unter deren Forum unter ihrem Namen vertretenen Meinungen grundsätzlich Angelegenheiten von öffentlicher Bedeutung sind, weil – dies ist auch dem Gericht als offenkundiger Sachverhalt bekannt – die WikiLeaks-Bewegung gesellschaftliche Debatten von einigem Gewicht angestoßen hat. Dies gilt aber nicht ohne weiteres für jeden im Zusammenhang mit dieser Bewegung erörterten Sachver-

halt und auch nicht ohne weiteres für jeden an der Debatte beteiligten Teilnehmer. Das pauschale Argument, wer in diesem Rahmen meinungsführend hervortritt, müsse die Abbildung seines Gesichts jederzeit hinnehmen, verfängt nicht. Es bleibt bei der abgestuften Grundrechtsprüfung anhand der konkret vorliegenden Umstände, die hier zugunsten des Bildnisschutzes ausfällt.

Voraussetzungen für Grundbucheinsicht durch einen Pressevertreter (Ls)

(**Oberlandesgericht München**, Beschluss vom 20. April 2016 – 34 Wx 407/15 –)

Die Gestattung von Grundbucheinsicht an einen Pressevertreter setzt voraus, dass das Rechercheinteresse in tatsächlicher Sicht hinreichend konkret dargelegt wird und sich aus der Sachverhaltsdarstellung ergibt, dass die beantragte Grundbucheinsicht auf die Beschaffung journalistisch verwertbarer Informationen abzielt und daher als Teil der publizistischen Vorbereitungstätigkeit dem Schutzbereich der Pressefreiheit zuzuordnen ist (vgl. BVerfG vom 7.10.2000, 1 BvR 1521/00). – Im konkreten Fall verneint für Recherchen „u.a. in Belangen von öffentlichem Interesse aufgrund Gesundheits- und Umweltgefahren im Zusammenhang mit ehemaligen militärischen Liegenschaften" und „Begleitung" einer Person in einem Verfahren gegen die öffentliche Hand.

Recht auf Grundbucheinsicht eines Pressevertreters für Recherchen über eine „Wehrsportgruppe"

(**Oberlandesgericht München**, Beschluss vom 20. April 2016 – 34 Wx 127/16 –)

Zum Recht auf Grundbucheinsicht eines Pressevertreters nach Darlegung des Einsichtsinteresses (hier bejaht für Recherchen über Eigentums- und Vermögensverhältnisse von Personen im Umfeld einer „Wehrsportgruppe").

Sachverhalt:

Der Beteiligte ersuchte am 28.1.2016 beim Grundbuchamt unter Verweis auf einen Auskunftsanspruch als Vertreter der Presse um Auskunft über den derzeitigen im Grundbuch eingetragenen Eigentümer eines mit Orts-, Straßen- und Hausnummernangabe bezeichneten Grundstücks. Ihm seien Informationen über angebliche finanzielle Schwierigkeiten des Eigentümers zugegangen, weshalb er Klarheit über die Belastungen und Eigentumsverhältnisse benötige.

Die Urkundsbeamtin des Grundbuchamts wies zunächst darauf hin, dass ein berechtigtes Interesse nicht hinreichend dargelegt sei, und hat sodann mit Beschluss vom 2.3.2016 den Antrag auf Grundbucheinsicht zurückgewiesen.

Der Erinnerung vom 10.3.2016 hat der Rechtspfleger mit Beschluss vom 16.3.2016 nicht stattgegeben. Hiergegen richtet sich die Beschwerde vom 2.4.2016, die das Grundbuchamt, ohne abzuhelfen, dem Oberlandesgericht vorgelegt hat. Der Beteiligte hat daraufhin ergänzend vorgetragen, dass er bereits mehrfach, etwa in online-Medien, über die sogenannte Artgemeinschaft und ein dieser von einer namentlich bezeichneten Person zur Verfügung gestelltes Anwesen berichtet habe. Es gebe Berichte, dass die Person, die einer Wehrsportgruppe angehört habe, wie auch der Gründer dieser Wehrsportgruppe selbst Immobilien durch Zwangsversteigerung verloren hätten. Es gehe nun um die Frage, ob auch weitere Immobilien den zum Umfeld der Wehrsportgruppe gehörenden Eigentümern entglitten seien und nun versucht werde, diese durch Eigentümerwechsel innerhalb der Szene „zu retten".

Aus den Gründen:

Die Beschwerde ist begründet. Ihr ist durch die Anweisung an das Grundbuchamt stattzugeben, dem Antragsteller einen – vollständigen – Grundbuchauszug für das bezeichnete Grundbuchblatt in Form einer – einfachen – Abschrift zu erteilen (§ 12 Abs. 1 Satz 1, Abs. 2 Halbs. 1 GBO, § 46 Abs. 1 und 3 GBV).

a) Ein berechtigtes Interesse an der Einsicht des Grundbuchs i.S.v. § 12 Abs. 1 GBO ist gegeben, wenn ein verständiges, durch die Sachlage gerechtfertigtes Interesse des Antragstellers dargetan wird, das sich im Unterschied zum rechtlichen Interesse nicht auf ein bereits vorhandenes Recht oder konkretes Rechtsverhältnis stützen muss, sondern auch mit einem bloß tatsächlichen Interesse begründet werden kann (OLG Oldenburg RPfleger 2014, 131). Auch einem Journalisten oder Presseorgan kann im Rahmen journalistischer Recherche aufgrund der Wahrnehmung öffentlicher Interessen grundsätzlich ein Anspruch auf Grundbucheinsicht zustehen. Dabei ist es verfassungsrechtlich nicht zu beanstanden, wenn das Einsichtsrecht der Presse von der Darlegung des Einsichtsinteresses abhängig gemacht wird; denn das Grundrecht auf Pressefreiheit gemäß Art. 5 Abs. 1 Satz 2 GG ist mit dem Grundrechtsschutz der eingetragenen Personen aus Art. 2 Abs. 1 GG in einen angemessenen Ausgleich zu bringen (BVerfG NJW 2001, 503/505), zumal eine vorherige Anhörung des Eigentümers grundsätzlich nicht stattfindet (BVerfG a.a.O.). Deshalb hat das Grundbuchamt bei einem Einsichtsersuchen der Presse oder eines Journalisten zu Recherchezwecken außerdem zu prüfen, ob sich das Informationsinteresse auf Rechte der im Grundbuch Eingetragenen bezieht, für die Einsicht verlangt wird, also geeignet ist, dem Informationsanliegen Rechnung zu tragen, ferner ob sich die begehrte Einsichtnahme auf das zur Recherche Erforderliche begrenzt und ob die gewünschten Informationen in unproblematischer Weise unter geringerer Beeinträchtigung des Persönlichkeitsschutzes von Eingetragenen erlangt werden können (BVerfG NJW 2001, 503/506). Schließlich kann der beabsichtigte Verwertungszweck im Rahmen einer Angemessenheitsprüfung unter Abwägung mit den kollidierenden Persönlichkeitsinteressen von Bedeutung sein (BVerfG NJW 2001, 503/506). So kann die Presse unter Berufung auf die Pressefreiheit kein das informationelle Selbstbestimmungsrecht des eingetragenen Eigentümers überwiegendes Interesse an der Grundbucheinsicht, beispielsweise in Abteilung III mit den dort ersichtlichen Belastungen (vgl. § 11 GBV), geltend machen, wenn es lediglich um unterhaltende Berichterstattung und Befriedigung einer öffentlichen Neugier etwa dahin geht, etwas über die finanzielle Gesamtsituation des Betroffenen und seiner Familie zu erfahren (vgl. KG Rpfleger

2001, 539). Es müssen daher konkrete Umstände vorgetragen werden, die dem Grundbuchamt bzw. dem Beschwerdegericht die inhaltlich beschränkte Überprüfung des Informationsinteresses ermöglichen (BVerfG NJW 2001, 503; OLG Düsseldorf NJW 2016, 89).

b) Dass der Antragsteller im konkreten Fall ein solches presserechtliches Interesse hat, ergibt sich noch nicht zwingend und allein aus der Vorlage eines Presseausweises. Er hat aber im Beschwerdeverfahren seine auf das Einsichtsersuchen bezogene journalistische Tätigkeit konkretisiert und von ihm veröffentlichte Artikel zu dem Thema vorgelegt, über das er weiterhin recherchieren wolle. Dieser neue Vortrag ist vom Beschwerdegericht zu berücksichtigen, § 74 GBO. Aus ihm ergibt sich nunmehr hinreichend, dass die Person des Eigentümers und seine finanzielle Situation für die Allgemeinheit und nicht allein für den Antragsteller relevant sein können.

c) Die Einsichtnahme ist auch geeignet, dem Informationsanliegen Rechnung zu tragen. Eine Einsicht in das gesamte Grundbuchblatt kann die gewünschte Information geben, da es dem Beteiligten nach seinem präzisierten Vortrag neben den aus Abteilung I ersichtlichen (vgl. § 9 GBV) Eigentumsverhältnissen auch um Klarheit über etwaige Belastungen geht. Hinsichtlich der Belastungen hat der Beteiligte dargelegt, dass seine Recherche nicht nur mögliche finanzielle Schwierigkeiten, sondern auch einen drohenden Verlust des Grundstücks betrifft. Die Eintragung von Grundschulden oder Hypotheken lässt sich aus Abteilung III ersehen (§ 11 GBV). Soweit es auch um den drohenden Verlust des Grundstücks durch eine Zwangsversteigerung oder den Verdacht geht, dass durch Eigentümerwechsel innerhalb der „Szene" dieser Grundbesitz gerettet werden soll, wären entsprechende Informationen aus Abteilung II (vgl. § 10 GBV) zu entnehmen.

d) Ein anderer für die Informationsgewinnung ebenso zielführender Weg, der für den (die) von der Einsichtnahme Betroffenen aber weniger belastend wäre, ist nicht ersichtlich.

Datenübermittlung an eine Auskunftei durch Dritte (Ls)

(**Kammergericht Berlin**, Urteil vom 17. Februar 2016 – 26 U 197/12 –)

1. **Eine Übermittlung nach § 28a Abs. 1 S. 1 Nr. 1 BDSG kann auch durch jemanden – hier ein Inkassobüro – erfolgen, der nicht der Inhaber des Titels ist. Dies gilt in jedem Falle, wenn das Inkassounternehmen durch den tatsächlichen Gläubiger der Forderung und Inhaber des Titels bevollmächtigt wurde.**

2. **Allein wirtschaftliche Interessen des Betroffenen an der Erhaltung seiner Kreditwürdigkeit reichen nicht aus, um ein Widerspruchsrecht nach § 35 Abs. 5 BDSG zu begründen. Allein der Umstand, dass die bei der Schufa eingemeldete Forderung bereits aus den frühen 1990er Jahren stammt, genügt nicht für die Annahme einer besonderen persönlichen Situation i.S.d. § 35 Abs. 5 S. 1 BDSG.**

(Nicht amtliche Leitsätze)

Auskunftsrecht des Gefangenen nach dem Landesjustizvollzugsdatenschutzgesetz Rheinland-Pfalz

(**Oberlandesgericht Koblenz**, Beschluss vom 4. Februar 2016 – 2 Ws 689/15 Vollz –)

Das Auskunfts- und Akteneinsichtsrecht nach §§ 36 und 37 Landesjustizvollzugsdatenschutzgesetz (LJVollzDSG) gilt nicht nur für die Gefangenenpersonalakte, sondern auch für personenbezogene Daten der Gesundheitsakte. Über das Auskunfts- und Akteneinsichtsrecht hinaus gewährt § 37 Abs. 4 Satz 1 LJVollzDSG den Gefangenen einen Anspruch auf Ablichtungen einzelner Dokumente bzw. Ausdruck eines Teilbestands der Daten aus automatisierten Dateien, soweit die Akten der Einsicht unterliegen und ein nachvollziehbarer Grund vorliegt; ein solcher ist nach dem Gesetzeswortlaut insbesondere anzunehmen, wenn die Gefangenen zur Geltendmachung von Rechten gegenüber Gerichten und Behörden auf Ablichtungen oder Ausdrucke angewiesen sind (§ 37 Abs. 4 Satz 2 LJVollzDSG).

Sachverhalt:

Der Beschwerdeführer befindet in Strafhaft in der Justizvollzugs- und Sicherungsverwahrungsanstalt .... Er verbüßt mehrere Freiheitsstrafen wegen Totschlags, Meineids und Mordes.

Mit Schreiben vom 6. August 2015 beantragte er gegenüber der Anstaltsleitung die „Aushändigung von Kopien der beiden letzten Blutuntersuchungen". In einer ergänzenden Stellungnahme vom 30. Oktober 2015 führte der Beschwerdeführer aus, die Ergebnisse der aktuellen Blutuntersuchungen seien vom Anstaltsarzt mit ihm besprochen worden, nicht aber die Ergebnisse früherer Untersuchungen. Die Aushändigung von Kopien der Ergebnisse der beiden früheren Blutuntersuchungen lehnte die Antragsgegnerin durch von der Anstaltsärztin mündlich bekanntgegebenen Bescheid am 14. September 2015 ab.

In ihrer an die Strafvollstreckungskammer gerichteten und durch Bezugnahme in den angefochtenen Beschluss aufgenommenen Stellungnahme vom 14. Oktober 2015 führte die Antragsgegnerin unter anderem folgendes aus:

„Ein Anspruch des Gefangenen auf Ausfertigung von Kopien ist nicht gegeben. Weder ergibt sich ein solcher aus dem Strafvollzugsgesetz noch ist vorliegend ein solcher aus anderen Gründen gegeben. Unter Berücksichtigung des immensen Verwaltungsaufwandes, der die Anfertigung von Kopien für Inhaftierte nach sich zieht, ist in diesem Fall die beantragte Anfertigung von Kopien nicht angemessen."

Den auf Verpflichtung der Antragsgegnerin zur Neubescheidung seines Antrages vom 6. August 2015 abzielenden Antrag des Beschwerdeführers auf gerichtliche Entscheidung hat die Strafvollstreckungskammer mit Beschluss vom 5. November 2015 als unbegründet verworfen. Gegen die ihm am 9. November 2015 zugestellte Entscheidung hat der Beschwerdeführer am 23. November 2015 Rechtsbeschwerde zu Protokoll der Geschäftsstelle eingelegt, mit der er die Verletzung materiellen Rechts rügt.

Aus den Gründen:

1. Die form- und fristgerecht eingelegte Rechtsbeschwerde ist zulässig, weil es geboten ist, die Nachprüfung der Entscheidung

zur Sicherung einer einheitlichen Rechtsprechung zu ermöglichen (§ 116 Abs. 1 StVollzG). Die Strafvollstreckungskammer hat bei ihrer Entscheidung zwar das Landesgesetz zur Weiterentwicklung von Justizvollzug, Sicherungsverwahrung und Datenschutz vom 8. Mai 2013 gesehen, rechtsfehlerhaft jedoch den Prüfungsmaßstab der §§ 72 ff. (Gesundheitsfürsorge) des Landesjustizvollzugsgesetzes (LJVollzG) sowie Rechte aus „allgemeinen Informationsansprüchen" zugrunde gelegt. Die Überprüfung durch den Senat dient der Vermeidung künftiger gleichgelagerter Rechtsfehler (vgl. Senat 2 Ws 780/03 v. 6.1.2004; 2 Ws 606/06 v. 13.2.2009; 2 Ws 387/15 v. 20.10.2015).

2. Die Rechtsbeschwerde hat mit der Sachrüge einen zumindest vorläufigen Erfolg. Die angegriffene Entscheidung kann schon deswegen keinen Bestand haben, weil sie auf unzutreffender rechtlicher Grundlage ergangen und nicht auszuschließen ist, dass unter Heranziehung des zutreffenden Maßstabes ein Anspruch des Rechtsbeschwerdeführers auf Aushändigung von Ablichtungen der Untersuchungsergebnisse besteht.

Über den Antrag des Beschwerdeführers auf gerichtliche Entscheidung und auch über seinen ursprünglich bei der Antragsgegnerin gestellten Antrag hätte nach Maßgabe der §§ 36 und 37 des bereits am 1. Juni 2013 in Kraft getretenen Landesjustizvollzugsdatenschutzgesetzes Rheinland-Pfalz (LJVollzDSG) vom 8. Mai 2013 entschieden werden müssen. Gemäß Art. 4 des Landesgesetzes zur Weiterentwicklung von Justizvollzug, Sicherungsverwahrung und Datenschutz vom 8. Mai 2013 ersetzt dieses Gesetz nach Art. 125a Abs. 1 Satz 2 GG in seinem Geltungsbereich das Strafvollzugsgesetz des Bundes mit Ausnahme der Vorschriften über den Pfändungsschutz (§ 50 Abs. 2 Satz 5, § 51 Abs. 4 und 5 , § 75 Abs. 3), das Handeln auf Anordnung (§ 97), das gerichtliche Verfahren (§§ 109 bis 121), die Unterbringung in einem psychiatrischen Krankenhaus und einer Entziehungsanstalt (§§ 136 bis 138), den Vollzug von Ordnungs-, Sicherungs-, Zwangs- und Erzwingungshaft (§§ 171 bis 175) und den unmittelbaren Zwang in Justizvollzugsanstalten für andere Arten des Freiheitsentzugs (§ 178).

Die vorliegend heranzuziehenden §§ 36 und 37 LJVollzDSG sehen ein gestuftes System des Auskunfts- und Akteneinsichtsrechts vor (vgl. Senat, Beschluss 2 Ws 704/14 Vollz vom 19.02.2015, juris Rn. 10 f.), das nicht nur für die Gefangenenpersonalakte, sondern auch für personenbezogene Daten der Gesundheitsakte gilt. Nach § 36 Abs. 2 LJVollzDSG besteht zunächst ein Auskunftsrecht, wobei die Form der Auskunftserteilung im pflichtgemäßen Ermessen der Justizvollzugsbehörde steht (§ 36 Abs. 2 Satz 4 LJVollzDSG). § 36 Abs. 4 bis 6 LJVollzDSG enthält Einschränkungen des Auskunftsrechts nach Abs. 2 der Bestimmung.

Gemäß § 37 Abs. 1 Satz 1 LJVollzDSG besteht ein Anspruch der Gefangenen auf Akteneinsicht nur, soweit eine Auskunft nach § 36 LJVollzDSG für die Wahrnehmung ihrer rechtlichen Interessen nicht ausreicht und sie hierfür auf die Einsichtnahme angewiesen sind. Das Akteneinsichtsrecht setzt damit einen Auskunftsanspruch nach § 36 LJVollzDSG voraus und ist zusätzlich an die genannte weitere Voraussetzung geknüpft. Über das Akteneinsichtsrecht hinaus gewährt § 37 Abs. 4 Satz 1 LJVollzDSG den Gefangenen einen Anspruch auf Ablichtungen einzelner Dokumente bzw. Ausdruck eines Teilbestands der Daten aus automatisierten Dateien, soweit die Akten der Einsicht unterliegen und ein nachvollziehbarer Grund vorliegt; ein solcher ist nach dem Gesetzeswortlaut insbesondere anzunehmen, wenn die Gefangenen zur Geltendmachung von Rechten gegenüber Gerichten und Behörden auf Ablichtungen oder Ausdrucke angewiesen sind (§ 37 Abs. 4 Satz 2 LJVollzDSG). Gemäß § 37 Abs. 5 LJVollzDSG ist die Fertigung von Ablichtungen und Ausdrucken gebührenpflichtig; die zu erwartenden Kosten sind im Voraus zu entrichten.

Da die Antragsgegnerin in ihrer Stellungnahme vom 14. Oktober 2015 ausführte, ein Anspruch des Beschwerdeführers auf Anfertigung von Kopien sei weder aus dem Strafvollzugsgesetz noch aus anderen Gründen gegeben, hat sie – ebenso wie die Strafvollstreckungskammer in dem angefochtenen Beschluss – die Zurückweisung des Antrages ersichtlich nicht auf der zum Entscheidungszeitpunkt geltenden gesetzlichen Grundlage getroffen. Obwohl der Beschwerdeführer vorträgt, die Ergebnisse der früheren Blutwerte seien weder mit ihm besprochen worden noch habe man ihm antragsgemäß Kopien davon zur Verfügung gestellt, hat die Justizvollzugsanstalt keine Versagungsgründe nach § 36 Abs. 4 bis 6 LJVollzDSG geprüft und bejaht. Aufgrund der Gesetzessystematik war das Auskunftsbegehren als Minus dem gestellten Antrag auf Akteneinsicht in Form der Aushändigung von Kopien immanent und hätte deshalb bei Nichtgewährung von Akteneinsicht beschieden werden müssen (vgl. Senat, 2 Ws 387/15 -Vollz- v. 20.10.2015). Bei der erneuten Entscheidung der Antragsgegnerin sind die von dem Beschwerdeführer gegebenenfalls zur Begründung seines Antrags auf Erörterung der Untersuchungsergebnisse und Aushändigung von Kopien vorgebrachten Argumente nach §§ 36 Abs. 4 bis 6, 37 Abs. 4 LJVollzDSG zu bewerten, und zwar unter Beachtung seines verfassungsrechtlich geschützten Informationsinteresses (BVerfG, 2 BvR 443/02 v. 09.01.2006, NJW 2006, 1116). Eine bereits die Verpflichtung der Antragsgegnerin durch den Senat gebietende Ermessensreduzierung ist nach bisherigem Sachstand nicht eingetreten, da dem Antragsteller zunächst Gelegenheit einzuräumen ist, seinen Antrag auf der Grundlage des geltenden Rechts zu begründen.

Bei dieser Sach- und Rechtslage hätte die Strafvollstreckungskammer den Antrag auf gerichtliche Entscheidung mangels Spruchreife der Sache nicht zurückweisen dürfen.

3. Gemäß § 119 Abs. 4 Satz 1 ist die angefochtene Entscheidung aufzuheben. Nach § 119 Abs. 4 Satz 2 StVollzG kann der Senat an Stelle der Strafvollstreckungskammer die erforderliche Entscheidung ohne Zurückverweisung selbst treffen, da die Sache jedenfalls insoweit spruchreif ist.

Widerspruch gegen die automatisierte Speicherung von personenbezogenen Daten im Rahmen eines Gerichtsverfahrens

(**Verwaltungsgericht Stade**, Urteil vom 30. Mai 2016 – 1 A 1754/14 –)

Einem gegen die automatisierte Speicherung von personenbezogegen Daten bei einem Gericht gerichteten Widerspruch, der nicht mit einer besonderen Situation des Betroffenen, sondern mit prinzipiellen Bedenken gegenüber automatisierter Datenverarbeitung begründet

wird, steht das vorrangige Interesse der rechtsprechenden Gewalt an einer mit Hilfe automatisierter Datenverarbeitung erreichten effektiven Aufgabenerfüllung entgegen.

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Klägerin möchte den Beklagten dazu verpflichten, die Speicherung ihrer persönlichen Daten im Rahmen eines Klageverfahrens, welches sie bei dem Beklagten führt, zu unterlassen.

Die Klägerin führt vor dem erkennenden Verwaltungsgericht ein wasserrechtliches Klageverfahren unter dem Aktenzeichen D. Den dazugehörigen Antrag auf Erlass einer einstweiligen Anordnung unter dem Aktenzeichen E. hat das erkennende Verwaltungsgericht mit Beschluss vom 17. Dezember 2014 abgelehnt. Dieser Beschluss ist rechtskräftig.

Mit Schriftsatz vom 7. August 2014 widersprach die Klägerin im Verfahren D. der Speicherung ihrer persönlichen Daten im Rahmen des Verfahrens, insbesondere des Schriftverkehrs und der Terminplanung.

Mit Schreiben vom 13. August 2014 bestätigte der Beklagte den Eingang des Widerspruchs, wies auf die Regelungen des Niedersächsischen Datenschutzgesetzes hin und gab der Klägerin die Gelegenheit, schutzwürdige persönliche Gründe für ihren Widerspruch bis zum 5. September 2014 darzulegen.

Mit Schreiben vom 5. September 2014 nahm die Klägerin Stellung: Das Landesgesetz, welches die Speicherung und Nutzung persönlicher Daten erlaube, sei verfassungswidrig. Zahlreiche Fälle von Datenmissbrauch bewiesen, dass ein Schutz der persönlichen Daten bei Speicherung nicht möglich sei. Die Negativfolgen seien nicht absehbar und überwögen den praktischen Nutzen für das Gericht. Die Behörde habe zudem einige für sie, die Klägerin, schädliche und nicht beweisbare Vorwürfe in den Raum gestellt. Wegen der mangelhaften Berücksichtigung sensibler persönlicher Daten durch die Behörde wünsche sie keine weiteren Experimente auf ihre Kosten. Dem Schreiben lagen zehn Adresskarten der Klägerin mit Aktenzeichen bei.

Mit Bescheid vom 18. September 2014 lehnte der Beklagte den Widerspruch der Klägerin auf Unterlassung der Speicherung ihrer persönlichen Daten ab. Die von der Klägerin geltend gemachten schutzwürdigen Interessen überwögen nicht die Interessen des Beklagten an der Speicherung ihrer Daten. Die Speicherung diene der ordnungsgemäßen Erfüllung der öffentlichen Aufgaben, etwa der Ladung der Klägerin zur mündlichen Verhandlung oder der Abwicklung des Schriftverkehres. Das öffentliche Interesse an einer sachgerechten Aufgabenbewältigung solle nur im Einzelfall hinter die Interessen der von der Datenspeicherung Betroffenen zurücktreten, etwa bei Gefahren für Leib, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen. Solche Interessen seien bei der Klägerin nicht erkennbar. Die von ihr genannten Negativfolgen seien nicht zu befürchten. Die personenbezogenen Daten würden ausschließlich zur Abwicklung des Gerichtsverfahrens in einem hochgradig gesicherten, nach außen abgeschlossenen System gespeichert; der Datenzugriff sei nur für die für das jeweilige Gerichtsverfahren zuständigen Mitarbeiterinnen und Mitarbeiter möglich.

Gegen diesen Bescheid hat die Klägerin am 20. Oktober 2014 Klage erhoben. Diese Klage begründet sie umfangreich in mehreren Schriftsätzen mit Datum vom 16. Oktober 2014, vom 11. Dezember 2014, vom 2. Januar 2015, vom 29. Januar 2015 und vom 24. April 2015. Sie bemängelt die Versendung von Schreiben durch das Gericht per einfachen Brief und wendet sich dagegen, dass Gerichtskosten erhoben werden. Es gebe keine Systeme, die nach außen hochgradig abgesichert werden könnten. Datensicherheit sei in ihrer Firma von höchster Bedeutung. Aus eigener Erfahrung sei ihr bekannt, dass Gerichte Daten missbräuchlich verwendeten. So habe sie einseitige Zeugenbefragungen und missbräuchliche Gesetzesinterpretation erfahren. Dem offensichtlichen Missbrauch folge ein verdeckter durch Überwachung und Kontrolle, da die Daten jederzeit im Zuge von Amtsanfragen durch andere Behörden und staatsnahe Institutionen eingesehen werden könnten. Die willkürliche Verbreitung und fehlerhafte Nutzung der Daten sei so möglich; Betroffene seien weitgehend schutzlos dagegen, sie könnten die Rechtmäßigkeit der Anfragen und Weitergabe nicht überprüfen. Wegen der nationalsozialistischen Vergangenheit und angesichts der heute bestehenden digitalen Möglichkeiten dürfe eine Speicherung ihrer Daten gegen ihren erklärten Willen nur bei einer Gefährdung der öffentlichen Sicherheit und Ordnung erfolgen. Diese sei nicht gegeben. Die Sachlage stelle eine ständige Bedrohung an Leib und Seele dar. Die Datenspeicherung habe negative Auswirkungen auf ihre Forschungsarbeit und stelle eine Rufschädigung dar. Die Speicherung verletze ihre Persönlichkeitsrechte und stelle eine Enteignung dar. Dass sie sich nur mit einer kostenpflichtigen Klage wehren könne, sei Diebstahl und Rechtsverhinderung; die Speicherung sei Rechtsbeugung. Die totalitäre Art der Durchführung verstoße gegen die freiheitlich-demokratische Grundordnung. Es existiere eine Papierakte, die zusätzliche Speicherung sei nicht notwendig und dürfe nicht aus Bequemlichkeit erfolgen. Es sei auch nicht zulässig, die datenschutzrechtlichen Fragen vom Gesamtfall auszugliedern. Sie, die Klägerin, werde in ein weiteres Gerichtsverfahren gezwungen und müsse weitere Kosten tragen.

Die Klägerin beantragt sinngemäß,

den Bescheid des Beklagten vom 18. September 2014 aufzuheben und den Beklagten zu verpflichten, die automatisierte Speicherung ihrer persönlichen Daten im Gerichtsverfahren D. zu unterlassen.

Der Beklagte beantragt, die Klage abzuweisen.

Er bezieht sich zur Begründung auf den angegriffenen Bescheid. Nach Aufforderung durch das erkennende Gericht hat er die getroffenen Sicherungsvorkehrungen zum Schutz gespeicherter Daten näher erläutert. Er weist weiter auf Ausführungsbestimmungen des Justizministeriums zur Aufbewahrung und Archivierung von Verfahren hin. Die automatisierte Löschung von Adressen sowie von Dokumenten weggelegter Verfahren erfolge über das Datenverarbeitungsprogramm EUREKA-Fach. Bei allen Kammern sei gerade die Datenrumpfung erfolgt. Diese beinhalte, dass Name und Vorname in der Adressdatenbank erhalten blieben einschließlich des Aktenzeichens zu dem von dieser Person geführten gerichtlichen Verfahren. Die Aufbewahrung dieser Daten sei als Teil der gerichtlichen Vorgangsverwaltung notwendig, um einen ordnungsgemäßen Dienstbetrieb zu gewährleisten. Die Aufgaben der Gerichte ergäben sich aus dem Niedersächsischen Justizgesetz und der Verwaltungsgerichtsordnung; nähere Regelungen zur Registrierung der Neueingänge in elektronischer Form enthalte § 18 Abs. 1 der Aktenordnung für die Geschäftsstellen der Gerichte der Verwaltungsgerichtsbarkeit. Schutzwürdige Interessen der Klägerin daran, dass ihre persönlichen Daten nicht elektronisch gespeichert werden dürfen, seien nicht erkennbar. Sie mache ihre personenbezogenen Daten im Internet auf einer von ihr betriebenen Webseite für jedermann sichtbar.

Aus den Gründen:

Die zulässige Klage, über die gemäß § 102 Abs. 2 Verwaltungsgerichtsordnung (VwGO) auch trotz Abwesenheit der Klägerin in

der mündlichen Verhandlung entscheiden werden konnte, ist unbegründet.

Statthafte Klageart ist die Verpflichtungsklage in Form der Versagungsgegenklage (vgl. Mallmann, in: Simitis, BDSG, 7. Aufl. 2011, § 20 Rn. 106; Gola/Schomerus, BDSG, 12. Aufl. 2015, § 20 Rn. 40). Das Begehren der Klägerin ist entsprechend zu formulieren. Sie wendet sich ausschließlich dagegen, dass der Beklagte ihre Daten elektronisch in seinem Datenverarbeitungssystem speichert. Es geht ihr allein um die automatisierte Datenverarbeitung i.S. des § 3 Abs. 5 Niedersächsisches Datenschutzgesetz (in der Fassung vom 29.1.2002, Nds. GVBl. S. 22, zuletzt geändert durch Gesetz vom 12.12.2012, Nds. GVBl. S. 589 – NDSG). Einverstanden ist sie dagegen damit, dass eine Papierakte über sie geführt wird.

Die Klage ist unbegründet, weil die Klägerin keinen Anspruch darauf hat, dass der Beklagte die automatisierte Speicherung ihrer persönlichen Daten in Gestalt von Namen und Anschrift im Zusammenhang mit dem gerichtlichen Verfahren, das sie bei dem Verwaltungsgericht Stade führt, unterlässt. Sie wird durch den insoweit ablehnenden Verwaltungsakt des Beklagten vom 18. September 2014 nicht in ihren Rechten verletzt (vgl. § 113 Abs. 5 Satz 1 VwGO).

Der geltend gemachte Anspruch richtet sich nach § 17a NDSG. Diese Vorschrift setzt das Widerspruchsrecht gemäß Art. 14 Satz 1 Buchst. a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz der natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Abl. Nr. L 281/31 vom 23.11.1995) in nationales Recht um (vgl. Mallmann, a.a.O., § 20 Rn. 80, 110; Wahlbrink, Das Niedersächsische Datenschutzgesetz, November 2014, zu § 17a).

Gemäß § 2 Abs. 1 Satz 1 Nr. 1 NDSG gilt dieses Gesetz für die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen des Landes. Bei dem Beklagten handelt es sich um eine sonstige öffentliche Stelle des Landes Niedersachsen, weil auch Gerichte die materiell-rechtlichen Anforderungen des Datenschutzrechts, insbesondere zur Datensicherung, zu erfüllen haben (Wahlbrink, Das Niedersächsische Datenschutzgesetz, November 2014, zu § 2 Abs. 1 und 2, Ziffer 3.2).

§ 17a Satz 1 NDSG sieht vor, dass Betroffene gegenüber der Daten verarbeitenden Stelle das Recht haben, der Verarbeitung der sie betreffenden Daten aus schutzwürdigen Gründen zu widersprechen. Nach § 17a Satz 2 NDSG ist die Verarbeitung der Daten unzulässig, soweit diese Gründe überwiegen. § 17a Satz 3 NDSG sieht vor, dass Satz 1 nicht gilt, wenn eine Rechtsvorschrift zur Verarbeitung verpflichtet.

Die Klägerin hat ein Widerspruchsrecht nach § 17a Satz 1 NDSG. Denn eine zur (automatisierten) Datenverarbeitung verpflichtende Vorschrift besteht für die Niedersächsische Verwaltungsgerichtsbarkeit nicht. § 18 Abs. 1 Satz 1 Aktenordnung für die Geschäftsstellen der Gerichte der Verwaltungsgerichtsbarkeit (vom 23.12.2015, Nds. Rpfl. S. 42 – AktO-VG) bestimmt zwar, dass die Registrierung der Neueingänge in elektronischer Form erfolgt, ist aber lediglich eine verwaltungsinterne Anweisung und keine zur Datenverarbeitung verpflichtende Rechtsvorschrift i.S. des § 17a Satz 1 NDSG. Die Klägerin hat von ihrem Widerspruchsrecht Gebrauch gemacht. Ihr Widerspruch ist indes nicht erfolgreich. Überwiegende schutzwürdige Gründe dafür, dass die automatisierte Speicherung zu unterbleiben hat, liegen nicht vor.

Bei der Prüfung, ob überwiegende schutzwürdige Gründe für eine Datenspeicherung vorliegen, ist eine Interessenabwägung vorzunehmen. Die konkreten Umstände des Einzelfalls, einschließlich der Art der Daten und der Konsequenzen einer Erhebung, Verarbeitung oder Nutzung, für den Betroffenen sind zu berücksichtigen und dem öffentlichen Interesse an der Datenverarbeitung gegenüberzustellen. Voraussetzung dafür, dass ein überwiegendes öffentliches Interesse überhaupt angenommen werden kann ist, dass die Datenverarbeitung und Nutzung rechtmäßig erfolgt (vgl. Mallmann, a.a.O., § 20 Rn. 88).

Eine rechtmäßige Speicherung von Namen und Adresse der Klägerin durch den Beklagten ist gegeben. Eine Verarbeitung personenbezogener Daten, zu denen das Speichern von Name und Adresse der Klägerin nach § 3 Abs. 1 und Abs. 2 Satz 1 NDSG gehört, ist nach § 4 Abs. 1 Nr. 1 NDSG zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift dies vorsieht. Nach § 10 Abs. 1 Satz 1 NDSG ist das Speichern, Verändern und Nutzen personenbezogener Daten zulässig, wenn es zur Erfüllung der Aufgabe der öffentlichen Stelle erforderlich ist und die Daten für diese Zwecke erhoben worden sind. Satz 2 bestimmt, dass die öffentliche Stelle, wenn sie Kenntnis von personenbezogenen Daten erlangt, ohne diese erhoben zu haben, diese Daten nur für Zwecke verarbeiten darf, für die sie diese Daten erstmals speichert. Bei den streitgegenständlichen Daten der Klägerin handelt es sich um erlangte Daten i.S. des § 10 Abs. 1 Satz 2 NDSG, weil sie mit Klageerhebung im Verfahren 1 A 1224/14 ihren Namen und ihre Adresse dem Beklagten ohne Aufforderung zugeleitet hat.

Die Speicherung dieser Daten ist für die Erfüllung der Aufgaben des Beklagten erforderlich. Anlass für die Speicherung der Daten der Klägerin sind die bei dem Beklagten geführten gerichtlichen Verfahren der Klägerin. Die Speicherung dient damit der verfassungsrechtlich aufgrund von Art. 92 Grundgesetz und Art. 51 Abs. 1 Niedersächsische Verfassung den Gerichten anvertrauten und durch sie ausgeübten rechtsprechenden Gewalt. Bei öffentlich-rechtlichen Streitigkeiten nichtverfassungsrechtlicher Art, zu denen die Verfahren der Klägerin vor dem Verwaltungsgericht Stade zählen, wird die Rechtsprechung gemäß § 40 Abs. 1 Satz 1 VwGO grundsätzlich durch die Verwaltungsgerichte ausgeübt. Zu diesen zählt gemäß § 73 Abs. 1 NJG der Beklagte, also das Verwaltungsgericht mit Sitz in Stade. Dieses ist auch sachlich und örtlich zuständig für die Verfahren der Klägerin. Die Verwaltungsgerichtsordnung trifft Regelungen zur Gerichtsverwaltung, siehe §§ 38, 39 VwGO. Eine ordnungsgemäße Aufgabenerfüllung durch den Beklagten setzt eine Vorgangsverwaltung in dem Sinne voraus, dass Klageeingänge nachgewiesen, Klagen bearbeitet sowie Schreiben, Urteile und Beschlüsse an die Beteiligten versendet werden können (zur Vorgangsverwaltung vgl. nur Nds. OVG, Beschluss vom 8.8.2008 – 11 LA 194/08 –, juris; Urteil vom 30.1.2013 – 11 LC 470/10 –). Schon wegen § 82 Abs. 1 Satz 1 VwGO ist es unerlässlich, dass Name und Anschrift der Klägerin dem Beklagten zur Kenntnis gelangen und von ihm im weiteren Verfahren verwendet werden dürfen, weil es zur ordnungsgemäßen Klageerhebung gehört, dass der Kläger bzw. die Klägerin mit ladungsfähiger Anschrift eindeutig bezeichnet ist (Kopp/Schenke, VwGO, 20. Aufl. 2014, § 82 Rn. 3).

Zur Erfüllung seiner Aufgaben darf sich der Beklagte – wie es mittlerweile allgemein üblich ist und in der Aktenordnung für die Geschäftsstellen der Gerichte der Verwaltungsgerichtsbarkeit vorausgesetzt wird – automatisierter Abläufe bedienen und

eine automatisierte Verarbeitung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen i.S. von § 3 Abs. 5 NDSG vornehmen. Denn zur ordnungsgemäßen Aufgabenerfüllung gehört auch eine effiziente und zeitgemäße Arbeitsorganisation. In diesem Zusammenhang erfolgt die von der Klägerin beanstandete Speicherung ihres Namens und ihrer Anschrift in der Datenverarbeitungsanlage des Beklagten. Dass dieser dabei die nach § 7 Abs. 1 Satz 1 NDSG erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Verarbeitung personenbezogener Daten sicherzustellen, steht nach den ausführlichen und anschaulichen Erläuterungen im Schriftsatz vom 13. Mai 2016 für die Kammer fest.

§ 7 Abs. 2 NDSG stellt einen Katalog von Kontrollmaßnahmen auf, die bei der automatisierten Datenverarbeitung zu beachten sind. Es sind die Kontrolle des Zugangs zu den Verarbeitungsanlagen, des Datenträgers, des Datenspeichers, des Benutzerkreises, des Zugriffs auf die Daten und ihrer Übermittlung, der Eingabe und des Verlustes bzw. der Zerstörung der Daten, ggf. des Auftrags (bei der Auftragsverarbeitung) und des Transports der Daten sowie der Organisation der datenverarbeitenden Stelle sicherzustellen. § 7 Abs. 3 Satz 1 NDSG stellt sicher, dass ein automatisiertes Verfahren nur eingesetzt werden darf, soweit Gefahren für die Rechte Betroffener, die wegen der Art der zu verarbeitenden Daten oder Verwendung neuer Technologien entstehen können, durch Maßnahmen nach § 7 Abs. 1 NDSG wirksam beherrscht werden können. Nach § 7 Abs. 1 Satz 2 NDSG muss der Aufwand für die Maßnahmen unter Berücksichtigung des Standes der Technik in einem angemessenen Verhältnis zu dem angestrebten Zweck stehen.

Diesen Anforderungen genügt die automatisierte Datenverarbeitung durch den Beklagten, wie er sie im Schriftsatz vom 13. Mai 2016 darlegt. Der Beklagte bedient sich einer eigens für den Zweck der Datenverarbeitung in gerichtlichen Verfahren erstellten Software, für die eine Verfahrensbeschreibung i.S. des § 8 NDSG besteht. Der Zugriff auf diese Software ist auf den Personenkreis beschränkt, der für die ordnungsgemäße Führung eines gerichtlichen Verfahrens notwendig ist. Die automatisierte Datenverarbeitung findet in Räumen ohne Publikumsverkehr statt und ist passwortgeschützt. Die Daten werden nicht an Dritte übermittelt. Das Betriebssystem ist nur einem kleinen Kreis von Administratoren zugänglich. Die Datenspeicherung erfolgt auf einem lokalen Server, dieser ist mit Zugangsschutz ausgestattet. Es gibt eine Dienstanweisung zum Datenschutz. Die Landesverwaltung hat keinen Zugriff auf Daten aus dem Justiznetz, dieses ist vom Landesdatennetz getrennt. Das Internet ist wiederum von den genannten Netzen getrennt und durch eine zentrale Landesfirewall abgesichert. Damit nicht versehentlich Schadstoffsoftware heruntergeladen wird, gibt es technische Beschränkungen, die jede Art von ausführbaren Programmen auf den Rechnern der Justiz unterbindet. Der Beklagte bedient sich also umfangreicher technischer und organisatorischer Kontrollmaßnahmen zum Schutz der bei ihm automatisiert verarbeiteter Daten von Verfahrensbeteiligten. Es bestehen keine Zweifel, dass der Aufwand der Maßnahmen in einem angemessenen Verhältnis zum angestrebten Zweck steht. Dabei fällt auch ins Gewicht, dass es sich bei den verarbeiteten Daten der Verfahrensbeteiligten (Name und Anschrift) in vielen Fällen – so auch im Fall der Klägerin wegen ihres Internetauftritts – um allgemein zugängliche Daten handelt, welche im Zuge der Klageerhebung erlangt und nicht erhoben werden. Es handelt sich also regelmäßig nicht um Informationen, die zum Schutz des Privatlebens oder der Intimsphäre besonders zu sichern sind. Weiter werden diese Daten in Einklang mit den Vorgaben von § 10 Abs. 1 Satz 2 NDSG nur für den Zweck, nämlich die Vorgangsverwaltung gerichtlicher Verfahren, verarbeitet, für den sie erstmals gespeichert worden sind. Eine Weitergabe an Dritte oder ein Zugriff durch Dritte, wie die Klägerin es offenbar befürchtet, findet gerade nicht statt.

Dem öffentlichen Interesse an der ordnungsgemäßen Aufgabenerfüllung der rechtsprechenden Gewalt stehen überwiegende schutzwürdige Belange der Klägerin daran, dass der Beklagte ihren Namen und ihre Anschrift nicht in seiner Datenverarbeitungsanlage speichern dürfe, nicht entgegen. Hierfür müsste die Klägerin darlegen, dass die Speicherung ihrer Daten sie in ihrer besonderen persönlichen, gesellschaftlichen, sozialen, wirtschaftlichen, rechtlichen oder familiären Situation nachteilig treffe oder berühre (Gola/Schomerus, a.a.O., § 20 Rn. 23). Eine solche Situation hat die Klägerin nicht konkret dargelegt. Soweit die Klägerin ihr prinzipielles Missfallen an der Datenspeicherung äußert und dabei grundsätzliche historische, gesellschaftspolitische sowie rechtliche Erwägungen anstellt, fehlt es bereits an der Besonderheit ihrer Situation. Soweit die Klägerin geltend macht, dass ihr aus eigener Erfahrung bekannt sei, dass Gerichte Daten missbräuchlich verwendeten, bleibt ihr Einwand unkonkret und allgemein. Soweit die Klägerin schließlich darauf hinweist, dass eine hochgradige Absicherung von Datensystemen nach außen nicht gewährleistet werden könne, bleibt ihre Aussage allgemein und spekulativ.

Das vollständige Fehlen einer konkreten und individuellen Sondersituation der Klägerin führt dazu, dass der Beklagte seine Arbeitsabläufe nicht dem Wunsch der Klägerin, der darauf gerichtet ist, dass ihre Daten lediglich „auf Papier" verwendet werden dürfen, anzupassen braucht. Vielmehr darf er im Interesse einer effektiven Aufgabenerfüllung der rechtsprechenden Gewalt ihre Daten automatisiert verarbeiten, indem er sie in seinem Datenverarbeitungssystem speichert.

Kündigungsschutz eines stellvertretenden Datenschutzbeauftragten

(**Arbeitsgericht Hamburg**, Urteil vom 13. April 2016 – 27-Ca 486/15 –)

1. **Ist eine Stelle zur Bestellung eines Datenschutzbeauftragten nach § 4f Abs. 1 BDSG verpflichtet, genießt ein stellvertretender Datenschutzbeauftragter Kündigungsschutz nach § 4f Abs. 3 BDSG nach denselben Grundsätzen wie ein Ersatzmitglied des Betriebsrats.**

2. **Der stellvertretende Datenschutzbeauftragte unterfällt für die Dauer der Vertretung dem Kündigungsschutz nach § 4f Abs. 3 S. 5 BDSG. Unabhängig von der Frage, ob eine Verpflichtung besteht, einen stellvertretenden Datenschutzbeauftragten zu bestellen, handelt es sich während des Vertretungsfalles jedenfalls nicht um einen freiwillig bestellten Datenschutzbeauftragten, für den der Kündigungsschutz nach § 4f Abs. 3 S. 5 BDSG nicht gilt.**

3. Der nachwirkende Kündigungsschutz nach § 4f Abs. 3 S. 6 BDSG greift nur ein, wenn nicht nur der Vertretungsfall eingetreten ist, sondern der stellvertretende Datenschutzbeauftragte auch tatsächlich Aufgaben als Datenschutzbeauftragter wahrgenommen hat.

Sachverhalt:

Die Parteien streiten über die Beendigung des Arbeitsverhältnisses und um Weiterbeschäftigung.

Bei der Beklagten handelt es sich um eine Betriebskrankenkasse in der Rechtsform einer Körperschaft des öffentlichen Rechts mit ca. 400 Mitarbeitern. Es besteht ein Personalrat. Der am ... geborene Kläger ist seit dem 01.04.2014 als Referent Risikomanagement bei der Beklagten beschäftigt. Die Stelle des Klägers als Referent Risikomanagement wurde im Rahmen eines Pilotprojektes neu geschaffen. Inhalt seiner Tätigkeit war u.a. der Auf- und Ausbau von Risikosteuerungsprozessen. Die Aufgaben des Risikomanagements wurden zwischenzeitlich auf den Vorstand übertragen, der im Bedarfsfalle von einem externen Dienstleister unterstützt wird.

Die Beklagte bestellte eine Mitarbeiterin zur Beauftragten für den Datenschutz. Da diese für längere Zeit krankheitsbedingt ausgefallen war, wandte sich der Vorstand der Beklagten im Juli 2014 an den Kläger und fragte bei diesem an, ob er bereit sei, aufgrund des langfristigen Ausfalls der Datenschutzbeauftragten diese Position auszufüllen. Mit Schreiben vom 01.08.2014 wurde der Kläger mit seiner Zustimmung zum stellvertretenden Datenschutzbeauftragten für einen Zeitraum von sechs Monaten vom 01.08.2014 bis 01.02.2015 bestellt. Während der krankheitsbedingten Abwesenheit der Beauftragten für den Datenschutz nahm der Kläger ihre Aufgaben war.

Mit Schreiben vom 01.10.2015 erklärte die Beklagte die ordentliche Kündigung des Arbeitsverhältnisses. Gegen diese Kündigung hat der Kläger am 13.10.2015 Kündigungsschutzklage erhoben und die Unwirksamkeit der Kündigung geltend gemacht. Die Klage ist der Beklagten am 22.10.2015 zugestellt worden.

Der Kläger ist der Ansicht, dass die Kündigung nicht durch dringende betriebliche Erfordernisse gerechtfertigt sei. Insbesondere sei der Beschäftigungsbedarf für ihn nicht entfallen.

Der Kläger genieße auch besonderen Kündigungsschutz nach § 4f Abs. 3 BDSG. Nachdem er sogar über das Befristungsende hinaus bis zur Übernahme durch den externen Datenschutzbeauftragten ab dem 11.04.2015 Aufgaben der erkrankten Datenschutzbeauftragten wahrgenommen habe, deren Bestellung nicht freiwillig erfolgt sei, gelte für ihn der nachwirkende Kündigungsschutz. Seine Bestellung sei im Übrigen auch nicht freiwillig gewesen, da die Beklagte ihre Pflicht nach dem BDSG habe erfüllen müssen. Einer analogen Anwendung des § 4f Abs. 3 BDSG bedürfe es insofern nicht.

Die Beklagte trägt vor, dass der Beschäftigungsbedarf für den Kläger entfallen sei. Der Vorstand habe am 18.08.2015 einen Beschluss gefasst, die Aufgaben des Referenten Risikomanagement auf den Vorstand zu übertragen und im Bedarfsfall einen externen Dienstleister zur Unterstützung heranzuziehen. Eine Beschäftigungsmöglichkeit bestehe für den Kläger nicht mehr. Der Kläger könne nicht die Stelle des Innenrevisors ausfüllen, da es ihm u.a. an dem erforderlichen BWL-Studium fehle.

Der Kläger habe keinen besonderen Kündigungsschutz als stellvertretender Datenschutzbeauftragter. Das BDSG sehe in § 4f Abs. 3 lediglich für den verpflichtend zu bestellenden Datenschutzbeauftragten nach § 4f Abs. 1 BDSG einen Sonderkündigungsschutz vor. Anders als im SGB IX sei jedoch kein Kündigungsschutz für einen Stellvertreter vorgesehen. Der stellvertretende Datenschutzbeauftragte sei lediglich freiwillig zu bestellen, sodass § 4f Abs. 3 BDSG nicht einschlägig sei. Eine Analogie verbiete sich im Hinblick darauf, dass die Problematik dem Gesetzgeber durch § 96 Abs. 3 SGB IX bewusst gewesen sei, er jedoch auf eine entsprechende Regelung im BDSG verzichtet habe.

Aus den Gründen:

Der Kläger genießt als ehemaliger Datenschutzbeauftragter besonderen Kündigungsschutz nach § 4f Abs. 3 BDSG. Da der Kläger die Aufgaben eines Datenschutzbeauftragten tatsächlich wahrgenommen hat, kommt es nicht auf die Frage an, in welchem Umfang der stellvertretende Datenschutzbeauftragte allein aufgrund seiner Bestellung Kündigungsschutz hat.

Nach § 4f Abs. 3 S. 5 BDSG kann ein Beauftragter für den Datenschutz, der nach § 4f Abs. 1 BDSG zu bestellen ist, nur dann gekündigt werden, wenn Tatsachen vorliegen, welche die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Damit ist das Recht zur ordentlichen Kündigung vorübergehend ausgeschlossen (vgl. Greiner, in: Ascheid/Preis/Schmidt, Kündigungsrecht, 4. Aufl. 2012, BDSG, § 4f Rn. 16). Nach der Abberufung als Beauftragter für den Datenschutz ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist (§ 4f Abs. 3 S. 6 BDSG). Damit hat der Gesetzgeber den Kündigungsschutz für den Beauftragten für Datenschutz u.a. an den der Betriebsratsmitglieder nach § 15 Abs. 1 S. 1, 2 KSchG angelehnt (BT-Drucks. 16/12011, S. 30). Dieser Schutz gilt nach dem Wortlaut des § 4f Abs. 3 S. 5 BDSG nur für solche Datenschutzbeauftragte, deren Bestellung nicht freiwillig erfolgt (so auch die Gesetzesbegründung BT-Drucks. 16/12011, S. 30).

a. Unstreitig ist die Beklagte nach § 4f Abs. 1 BDSG verpflichtet, einen Beauftragten für den Datenschutz zu bestellen. Dies hat die Beklagte getan, indem sie eine Mitarbeiterin zur Datenschutzbeauftragten bestellt hat. Die verpflichtete Stelle kann auch einen Vertreter bestellen. Die Bestellung eines Stellvertreters wird im BDSG nicht ausgeschlossen. Auch wenn es im Gesetz keine ausdrückliche Regelung gibt, besteht gleichwohl ein Bedürfnis, eine kontrollfreie Situation zu vermeiden, wenn der Beauftragte für den Datenschutz an einer Amtsausübung gehindert ist (Däubler, in: Däubler/Klebe/Wedde/Weichert, BDSG, 5. Aufl. 2016, § 4f Rn. 25a; ebenso Simitis, in: ders., BDSG, 8. Aufl. 2014, § 4f Rn. 145; Gola/Wronka, Handbuch Arbeitnehmerdatenschutz, 6. Aufl. 2013, Rn. 1478; Lembke, in: Henssler/Willemsen/Kalb, Arbeitsrecht Kommentar, 7. Aufl. 2016, BDSG, §§ 4f/4g Rn. 3). Insofern ist die Bestellung eines Stellvertreters zur Sicherstellung geeignet, dass die Aufgaben nach dem BDSG durchgehend wahrgenommen werden, auch wenn der Beauftragte für den Datenschutz vorübergehend verhindert ist. Hierdurch entsteht kein Kompetenzkonflikt, da nicht zeitgleich zwei Beauftragte für den Datenschutz tätig werden (vgl. zur Problematik der Kompetenzabgrenzung bei mehreren Datenschutzbeauftragten Franck/Reif, ZD 2015, 405, 406). Der Stellvertreter rückt nur für die Dauer des Vertretungsfalls nach und ersetzt den eigentlichen Datenschutzbeauftragten vollumfänglich (Franck/Reif, ZD 2015, 405, 407). Insofern handelt es sich für den Vertreter, der den Beauftragten auch bei einer kurzfristigen Verhinderung ersetzt, nicht um eine Verlagerung gesetzlich gewährleisteter Kompetenzen des Beauftragten (vgl. Simitis, in: ders., BDSG, 8. Aufl. 2014, § 4f Rn. 145). Damit ist die Bestellung eines Stellvertreters nicht vergleichbar

mit der Problematik der Bestellung mehrerer Datenschutzbeauftragter.

Ob und in welchen Fällen eine Stellvertretung nach dem BDSG geboten ist, kann vorliegend offen bleiben. Auf die Pflicht zur Bestellung eines Stellvertreters kommt es nicht an. Wird jedenfalls ein stellvertretender Datenschutzbeauftragter bestellt und nimmt dieser im Verhinderungsfall die Aufgaben eines Datenschutzbeauftragten iSd § 4f Abs. 1 BDSG wahr, bedeutet dies, dass ebenfalls die Schutzvorschriften nach § 4f Abs. 3 BDSG einschlägig sind (vgl. Däubler, in: Däubler/Klebe/Wedde/Weichert, BDSG, 5. Aufl. 2016, § 4f Rn. 25a; Franck/Reif, ZD 2015, 405, 407; so wohl im Ergebnis auch Lembke, in: Henssler/Willemsen/Kalb, Arbeitsrecht Kommentar, 7. Aufl. 2016, BDSG, §§ 4f/4g Rn. 24). Ist die Stelle nach § 4f Abs. 1 BDSG zur Bestellung eines Beauftragten für den Datenschutz verpflichtet, ist die Rechtsstellung auch auf den Stellvertreter zu übertragen, soweit der Vertretungsfall eingetreten ist. Auch wenn der Stellvertreter freiwillig bestellt wurde und grundsätzlich kein Kündigungsschutz besteht, gilt dies für den Vertretungsfall nicht. Der Vertreter, der vollumfänglich die Aufgaben des Vertretenen wahrnimmt, ist kein Datenschutzbeauftragter „2. Klasse". Vielmehr bedarf er im Vertretungsfall des Schutzes vor etwaigen Nachteilen aufgrund seiner Amtsführung.

Der Anwendung des Kündigungsschutzes nach § 4f Abs. 3 BDSG auf den stellvertretenden Beauftragten für den Datenschutz steht nicht entgegen, dass das SGB IX in § 96 Abs. 3 SGB IX einen besonderen Kündigungsschutz für das stellvertretende Mitglied der Schwerbehindertenvertretung regelt, der Gesetzgeber bei der Einführung des BDSG hierauf jedoch verzichtet hat. Die Aufgaben des stellvertretenden Mitglieds der Schwerbehindertenvertretung sind gesondert ausgestaltet. Insbesondere können die Vertrauensperson und der Stellvertreter nach § 95 Abs. 1 S. 4 SGB IX nach Absprache parallel tätig werden, mithin gleichzeitig ihre Aufgaben wahrnehmen. Insofern lässt sich aus dem Schweigen des BDSG zu einer Stellvertretung – die Gesetzesbegründung enthält hierzu keinen Hinweis – nicht entnehmen, dass der Gesetzgeber eine solche ausschließen wollte. Im Übrigen enthält auch § 15 Abs. 1 KSchG keinen eigenen Kündigungsschutz zugunsten der Ersatzmitglieder des Betriebsrats. Gleichwohl genießen Ersatzmitglieder im Vertretungsfall den Kündigungsschutz der Betriebsratsmitglieder. Weder in § 15 Abs. 1 KSchG noch in § 4f Abs. 3 BDSG geht es um einen originären Kündigungsschutz der Ersatzmitglieder bzw. Stellvertreter, sondern lediglich um den Schutz während und nach Eintritt des Vertretungsfalls. Aus diesem Grund bedarf es keiner analogen Anwendung der Kündigungsschutzvorschriften, sodass auch die Voraussetzungen der Analogie – insbesondere das Vorliegen einer ungewollten Regelungslücke – nicht gegeben sein müssen.

Da der Kündigungsschutz des Beauftragten für Datenschutz an denjenigen des Betriebsrats nach § 15 Abs. 1 KSchG angelehnt ist, sind auch die Rechtsgrundsätze zu übertragen (vgl. BT-Drucks. 16/12011, S. 30; Däubler, in: Däubler/Klebe/Wedde/Weichert, BDSG, 5. Aufl. 2016, § 4f Rn. 73b; ErfK-Franzen, 16. Aufl. 2016, § 4f BDSG Rn. 9). Während der Dauer des Vertretungsfalls gilt der Kündigungsschutz nach § 4f Abs. 3 S. 5 BDSG (Deeg/Müller, ArbRAktuell 2010, 365, 366). Ein nachwirkender Kündigungsschutz greift hingegen nur dann ein, wenn auch tatsächlich die Aufgaben eines Datenschutzbeauftragten wahrgenommen wurden. Bei einem Ersatzmitglied des Betriebsrats reicht es nicht aus, dass ein Vertretungsfall eingetreten ist, um einen nachwirkenden Kündigungsschutz zu erlangen. Vielmehr muss das Ersatzmitglied auch konkrete Betriebsratsaufgaben tatsächlich wahrgenommen haben (BAG v. 19.04.2012 – 2 AZR 233/11 –, Rn. 41, juris; KR-Etzel/Kreft, 11. Aufl. 2016, § 15 KSchG Rn. 90). Entsprechendes gilt auch für den Beauftragten für Datenschutz. Auch für diesen ist im Gesetz nach Ende der Amtszeit eine „Abkühlungsphase" vorgesehen, während derer sich eine mögliche Verärgerung des Arbeitgebers über die Amtsführung legen soll. Dies rechtfertigt es, eine solche „Abkühlungsphase" nur dann anzunehmen, wenn eine Amtstätigkeit erfolgt ist, aufgrund derer überhaupt eine negative Reaktion des Arbeitgebers in Betracht kommen kann.

b. Unter Anwendung der vorstehenden Rechtsgrundsätze konnte die Beklagte den Kläger nach § 4f Abs. 3 S. 6 BDSG im Zeitpunkt des Zugangs der Kündigung am 01.10.2015 nur außerordentlich kündigen, jedoch nicht ordentlich aus betriebsbedingten Gründen. Zwar war der Kläger zu diesem Zeitpunkt wohl nicht mehr Beauftragter für den Datenschutz, da sowohl seine befristete Bestellung abgelaufen als auch der Vertretungsfall mit der Bestellung eines externen Datenschutzbeauftragten abgelaufen war. Jedoch kann sich der Kläger aufgrund seiner Tätigkeit als Datenschutzbeauftragter auf den nachwirkenden Kündigungsschutz berufen.

Der Kläger wurde von der Beklagten mit Schreiben vom 01.08.2014 zum stellvertretenden Datenschutzbeauftragten bestellt, da die Datenschutzbeauftragte aus krankheitsbedingten Gründen absehbar für einen längeren Zeitraum verhindert war. Auf dieser Grundlage ist der Kläger tätig geworden. Der Kläger hat damit das Amt des Beauftragten für Datenschutz wahrgenommen, sodass es nicht maßgeblich ist, ob die Bestellung eines Stellvertreters freiwillig erfolgt ist. Aus diesem Grund war die Kündigungsmöglichkeit innerhalb eines Jahres gem. § 4f Abs. 3 S. 6 BDSG eingeschränkt. Da die Beklagte innerhalb eines Jahres nach Amtsbeendigung eine ordentliche Kündigung ausgesprochen hat und diese nicht auf einen wichtigen Grund zur Kündigung ohne Einhaltung einer Kündigungsfrist stützen kann, ist diese nach § 4f Abs. 3 S. 6 BDSG i.V.m. § 134 BGB nichtig.

Berichte, Informationen, Sonstiges

BfDI: 5. Tätigkeitsbericht zur Informationsfreiheit vorgelegt

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Andrea Voßhoff hat am 21. Juni ihren 5. Tätigkeitsbericht zur Informationsfreiheit für die Jahre 2014 und 2015 vorgelegt. Nach ihren Resumee wurde das Recht auf Informationszugang auch in den letzten beiden Jahren wiederum verstärkt genutzt. Mit 10 Jahren sei das IFG zwar immer noch vergleichsweise jung, aber es habe sich bereits behauptet und sich seinen Platz erobert.

Bei den Bundesbehörden gingen im Berichtszeitraum 18.049 IFG-Anträge ein. Dies ist eine deutliche Steigerung gegenüber den Jahren 2012/2013. Auch die Zahl der Eingaben, mit denen sich Antragsteller nach dem IFG mit der Bitte um Unterstützung oder mit allgemeinen Anfragen an die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wenden, ist weiter gestiegen.

Auch die Rechtsprechung hat in den letzten zwei Jahren erneut wichtige Beiträge für eine breitere Anwendung des Informationsfreiheitsgesetzes geleistet. So ist die Zahl der Anträge auf Zugang zu Ausarbeitungen der Wissenschaftlichen Dienste des Deutschen Bundestages signifikant gestiegen, nachdem das Bundesverwaltungsgericht am 25. Juni 2015 entschieden hatte, dass auch diese mandatsunterstützende Funktion als „Verwaltungstätigkeit“ im Sinne des IFG dem Informationszugang unterliegt.

Als ausgewählte Fälle aus dem 5. Tätigkeitsbericht werden aufgezeigt:

– *Das Ende einer langen Diskussion? Der Deutsche Bundestag muss Zugang zu Ausarbeitungen der Wissenschaftlichen Dienste gewähren (Nr. 2.1.1)*

Das Bundesverwaltungsgericht hat in letzter Instanz die Verwaltung des Deutschen Bundestages verpflichtet, Ausarbeitungen der Wissenschaftlichen Dienste zugänglich zu machen. Das IFG sei auf die Tätigkeit der Wissenschaftlichen Dienste anwendbar, das Urheberrecht stehe einem Informationszugang nicht entgegen.

– *Keine personalisierten Informationen zur Anschaffung von Büromaterial für Abgeordnete (Nr. 2.1.2)*

Das Bundesverwaltungsgericht sieht eine Verpflichtung des Bundestages, Zugang zu nicht-personalisierten Informationen zum sog. Sachmittelkonsum der Abgeordneten zu gewähren. Eine parallele Klage auf Zugang zu personalisierten Informationen zur Beschaffung von Büroausstattung blieb dagegen auch in der dritten Instanz erfolglos. Bei der Beschaffung von Büromaterial für Abgeordnete und ihre Mitarbeiter handelt es sich zwar um eine Verwaltungsaufgabe, so dass das IFG grundsätzlich anwendbar ist. Der Zugang zu den personalisierten Informationen ist jedoch ausgeschlossen, da es sich hierbei um solche handelt, die mit dem Mandat der Abgeordneten in Zusammenhang stehen. Insoweit ist der Informationszugang durch § 5 Abs. 2 IFG ausgeschlossen.

– *Recht auf Aktualitätsvorsprung beim Informationszugang von Journalisten? (Nr. 2.1.8)*

Die Neutralitätspflicht des Staates gebietet es nicht, bei mehreren Anträgen auf Informationszugang zu einem bestimmten Themenkomplex dem ersten Antragsteller einen Aktualitätsvorsprung gegenüber späteren Antragstellern einzuräumen. Das Verwaltungsgericht Berlin hatte über die Klage eines Journalisten zu entscheiden, ob sein inhaltlich ähnlicher, jedoch zeitlich früherer IFG-Antrag vor dem eines Kollegen zu bescheiden gewesen wäre, um ihm einen Vorsprung bei der Veröffentlichung seines Beitrags zu gewähren. Dies hat das VG verneint.

– *Informationszugang zu den Telefonlisten von Jobcentern? (Nr. 2.1.15)*

Die Frage, ob Jobcenter die Telefonverzeichnisse ihrer Beschäftigten öffentlich machen müssen, ist auch in der Rechtsprechung umstritten. Nachdem mehrere Verwaltungsgerichte den Anspruch auf Zugang zu den kompletten Telefonlisten von Jobcentern bejaht hatten, haben nun die zwei Oberverwaltungsgerichte Berlin Brandenburg und Nordrhein-Westfalen sowie der Bayerische VGH anders entschieden und einen Anspruch aus unterschiedlichen Gründen verneint. Die Revisionsentscheidung des Bundesverwaltungsgerichts steht noch aus.

– *Informationsfreiheit gegen Steuer- und Zollgeheimnis (Nr. 4.3.1): In Zolllagern können Waren zollfrei gelagert werden*

Zollrechtlich sind diese damit gewissermaßen „Ausland“. Ein Bürger stellte unter Berufung auf das IFG beim Hauptzollamt Hamburg-Hafen Fragen zu einem für das Bundesamt für Seeschifffahrt und Hydrographie eingerichteten Zolllager. Der IFG-Antrag wurde von der damaligen Bundesfinanzdirektion Nord sehr kurz und ohne weitere Begründung zurückgewiesen, „da einer Auskunft die Regelung des § 3 Nummer 4 IFG entgegensteht.“

Hier war weder für den Antragsteller noch für meine Mitarbeiter erkennbar, durch welche steuer- oder zollrechtliche Regelung eines Amtsgeheimnisses hier i.V.m. § 3 Nr. 4 IFG der Informationszugang ausgeschlossen sein sollte. Der Bescheid wies damit ein deutliches Begründungsdefizit auf, das nicht allgemeine Praxis werden sollte. Erst in ihrer Stellungnahme mir gegenüber berief sich die Behörde mit knappen Worten auf das Steuergeheimnis (§ 30 Abs. 2 Nr. 1 Buchst. a Abgabenordnung). Die „Beantragung eines Zolllagers bei der Bundeszollverwaltung“ sei „zweifellos ein (...) Verwaltungsverfahren, das dem Steuergeheimnis un-

terliegt." Auch das war m.E. noch keine überzeugende Begründung. Weshalb hier „zweifellos" das Steuergeheimnis und nicht das gemeinschaftsrechtlich begründete, in Art. 15 des so genannten Zollkodex geregelte Zollgeheimnis i.V.m § 3 Nummer 4 IFG den Informationszugang ausschließen sollte, wurde im Bescheid nicht angesprochen, obwohl die Abgrenzung der Anwendungs- und Schutzbereiche der beiden Vorschriften auch Fachleuten nicht schon auf den ersten Blick klar sein dürfte.

– *BVS verliert Klageverfahren (Nr. 4.3.4)*

Mit bemerkenswerter juristischer Phantasie, aber letztlich erfolglos versuchte die Bundesanstalt für vereinigungsbedingte Sonderaufgaben (BVS) einen IFG-Antrag abzuwehren. In einem verwaltungsgerichtlichen Verfahren wegen des Zugangs zu Unterlagen nach dem IFG war die BVS u.a. der Auffassung, sie könne diesen wegen der anwaltlichen Schweigepflicht ihrer eigenen Anwälte nicht gewähren. Das Verwaltungsgericht teilte hier meine Bedenken und hat die BVS zur Zugangsgewährung verpflichtet.

– *Gebühren – noch immer ein Thema (Nr. 4.3.6)*

Ein Petent beantragte Einsicht in die Aufsichtsakten der BaFin. Nach Vorbereitung, aber noch vor Gewährung der Einsicht in die umfangreichen Unterlagen machte die BaFin eine Gebühr von 60 Euro für die Bereitstellung der Informationen und die Unkenntlichmachung schutzwürdiger Aktenbestandteile geltend. Hier war zu prüfen, ob ein Vorschuss i.S.d. § 15 BGebG für eine noch zu erbringende antragsgebundene Leistung von der BaFingefordert werden durfte oder – jedenfalls die bereits durchgeführten – Vorbereitungsmaßnahmen als „individuell zurechenbare öffentliche Leistung(en)" i.S.d. § 10 Abs. 1 IFG bereits vor der Akteneinsicht in Rechnung gestellt werden konnten. Anhaltspunkte für eine Gefährdung des Haushaltsinteresses wie z.B. offene Gebührenforderungen aus anderen IFG-Verfahren oder Anzeichen für eine Zahlungsunfähigkeit konnte ich in diesem Fall nicht erkennen; die Voraussetzungen für einen Vorschuss waren hier also nicht gegeben. Solange der Informationszugang noch nicht gewährt und diese Leistung lediglich vorbereitet war, durften deshalb noch keine Gebühren festgesetzt und erhoben werden.

– *Die Protokolle der Bundesstiftung zur Aufarbeitung der SED-Diktatur (Nr. 4.13.1)*

Auch das OVG Berlin-Brandenburg bestätigt den Informationszugang zu den Protokollen des Stiftungsrates und Vorstandes der Bundesstiftung. Die Stiftung berief sich u.a. darauf, dass nach ihrer Satzung die Teilnahme an den Sitzungen nur einem ausdrücklich genannten Kreis von Personen gestattet sei, und hat daher den Zugang zu den Protokollen wegen Vertraulichkeit abgelehnt. Auch das OVG hat im Rahmen der Entscheidung über die Zulassung der Berufung diese Rechtsauffassung abgelehnt.

Literaturhinweise

Buchbesprechungen

Stiftung Datenschutz (Hrsg.), **Zukunft der informationellen Selbstbestimmung,** Erich Schmidt Verlag, Berlin 2016, 173 S., 38,– €.

Die gesellschaftliche Reflektion über den Datenschutz – woher er kommt, in welchem Stadium er sich befindet und wohin er will – findet an vielen Orten und in vielen Formen statt. Ein Ort soll künftig die mit Steuergeldern errichtete „Stiftung Datenschutz" sein, die als Form eine „Schriftenreihe der Stiftung Datenschutz" mit dem Untertitel „DatenDebatten" gewählt hat, wozu nun Band 1 vorliegt. Das generell bestehende Interesse an dem Büchlein wird durch eine Passage im Vorwort des Stiftungsvorstands Frederick Richter verstärkt: „Texte zur Geschichte gibt es viele. Zustandsbeschreibungen zu seiner Gegenwart sind Legion. Mutmaßungen und Visionen zur Datenschutzzukunft dagegen sind rar." Und diese Lücke solle das Büchlein schließen helfen.

Der Rezensent teilt zwar nicht die Analyse, es fehle an Visionen zum Datenschutz, besser zum digitalen Grundrechtsschutz, in einer globalisierten technisierten Gesellschaft. Literarische, zumeist eher düstere Visionen gibt es von George Orwell, Aldous Huxley bis hin zu Marc Elsberg, Dave Eggers oder Juli Zeh. Es gibt Visionen als Roman, als Film, auch als wissenschaftliche Abhandlung. Die dessen ungeachtet im Vorwort geweckte Neugierde verwandelte sich im Lauf der Lektüre immer mehr in Enttäuschung, fehlt es doch dem Sammelband nicht nur an Visionen, sondern hält sich auch dessen Wert für Neuerkenntnisse in Grenzen. Umso wichtiger ist die „Datendebatte" darüber:

In den ersten Beiträgen lassen sich zwei ehemalige Datenschutzbeauftragte, Hans Peter Bull und Thomas Giesen, mit folgenden Titeln aus: „Hat die ‚informationelle Selbstbestimmung' eine Zukunft?" und „Euphorie ist kein Prinzip des Rechtsstaats". Bulls Antwort am Ende seines Beitrages: „Niemand weiß, wie es weitergeht. Die Welt steht nicht still". Zwischen seiner Frage und dieser Antwort steht das, was Herr Bull seit Jahren verbreitet, nämlich dass das Datenschutzrecht insbesondere im privaten Bereich hypertrophiert sei; das „Verbot mit Erlaubnisvorbehalt", das nun durch die Datenschutz-Grundverordnung (DSGVO) europaweit bekräftigt und modernisiert wurde, gehöre abgeschafft. Mit dem bestehenden Zivilrecht und dem Strafgesetzbuch könne digitalem Fehlverhalten ausreichend Einhalt geboten werden. Herr Giesen fährt noch gewaltigere Geschütze auf und endet mit ähnlichen Botschaften, etwa zur DSGVO: „Sie wird scheitern." Vom „Zeitgeist" „euphorisierte" „gute Mitmenschen" würden bei ihrem Kampf gegen Geheimdienste und die „(natürlich ‚bösen') Konzerne" vergessen, dass Datenschutz in unsere rechtsstaatliche Ordnung integriert werden müsse: „Dann aber muss Datenverarbeitung auch endlich als Freiheitsrecht begriffen werden." Weitere Überschriften bei Giesen sind „Informationelle Selbstbestimmung ist unmöglich", „Freiheit für die Daten", „Alle sind zugleich Opfer und Täter" und schließlich „Exekutivischer Kontrollwahn", in dem er totalitäre Tendenzen bei den Datenschützern entlarvt. Originell ist die abschließende Aussage, dass die EU zum Erlass der DSGVO gar keine rechtliche Kompetenz habe.

Als genüge dies nicht an Defaitismus zum Datenschutz, kommen zwei – intelligenter argumentierende – Post-Privacy-Protagonisten zu Wort: Julia Schramm und Michael Seemann. Doch auch deren Texte wiederholen nur das in aktualisiertem Gewand, was die beiden schon vor zehn Jahren vertreten haben: Für den Kontrollwahn der Datenschützer gebe es keinen Grund; die insbesondere von US-Anbietern vorangetriebene Digitalisierung beinhalte mit ihrem Informations- und Verarbeitungsangebot kaum eine Gefahr, sondern eröffne ein Reich der Freiheit und der Selbstverwirklichung.

Wer nun hofft, dass in dem Büchlein diesen Positionen auch widersprochen werde, wird – fast – nicht fündig. Peter Schaar versucht unter dem Titel „Datenschutz ohne Zukunft?" etwas Optimismus zu verbreiten. Und Sabine Leutheusser-Schnarrenberger fordert die „Verantwortung der Internet-Giganten – Algorithmen und Selbstbestimmung" ein und am Ende ihres Beitrages, mit guten Gründen, dass „die Politik diese Herausforderungen und Handlungsnotwendigkeit erkennen" müsse. Auch nicht visionär, dafür aber handfest und qualifiziert belegt, kommt der Text von Christiane Schulzki-Haddouti daher, in dem sie eine gewaltig verbesserte Ausstattung der Datenschutzbehörden in Europa fordert.

Die weiteren Texte, z.B. von Jürgen Kühling, Kai von Lewinski, Indra Spieker oder Sabine Trepe, sind fachlich interessant, etwa im Hinblick auf Fragen zu Rechtssystematik oder Psychologie. Visionen enthalten sie nicht. So stellt sich die Frage, was diese Publikation über die „Zukunft der informationellen Selbstbestimmung" soll. Man könnte den Eindruck haben, dass hier das Bundesinnenministerium, das den Vorsitz im Verwaltungsrat der Stiftung Datenschutz innehat, publizistisch nochmals eine Breitseite gegen die DSGVO abfeuern wollte, zu der es seine Bedenkenträgerpositionen politisch nicht durchsetzen konnte. Doch diese Lesart würde einigen der Autorinnen und Autoren nicht gerecht.

Jedenfalls ist das Büchlein Ausdruck für den Umstand, dass die Stiftung Datenschutz immer noch nicht ihre Bestimmung gefunden hat. Ihre ursprüngliche Funktion, analog zur Stiftung Warentest eine Test- und Zertifizierungsumgebung für digitalen Grundrechts- und Verbraucherschutz zu schaffen, hat sie bisher verspielt.

Dass hierfür die DSGVO fast ideale rechtliche Rahmenbedingungen schafft, hat die Stiftung womöglich noch nicht erkannt; plausibler ist, dass ihr Verwaltungsrat dies einfach nicht wünscht, was sehr zu bedauern ist.

Positive Visionen zum digitalen Grundrechtsschutz – insofern ist dem Vorwort zuzustimmen – gibt es bisher noch nicht im Übermaß. Diese sollten aber von dem in dem Büchlein verbreiteten Eindruck befreit sein, dass Datenschutz auf hergekommenen Privatsphärenschutz reduziert werden kann und nichts mit „Verarbeitungsfreiheit" zu tun hat. Genau ein solches Konzept verfolgen von Anfang an das deutsche Bundesverfassungsgericht mit der „informationellen Selbstbestimmung" und der Nestor des deutschen Datenschutzes Spiros Simitis mit seinem Credo, Datenschutz als gesellschaftliches Kommunikationsrecht zu verstehen und zu leben.

Datenschutz hat sowohl eine individuelle wie auch eine demokratisch gesellschaftliche und rechtsstaatliche Dimension. Er steht sowohl in einem Spannungs- wie auch in einem Ergänzungsverhältnis zur Meinungs- und Informationsfreiheit und ist ein zentraler Baustein eines umfassenderen digitalen Grundrechtsschutzes. Der in dem Büchlein mehrfach geäußerte Totalitarismusvorwurf gegen „den Datenschutz" zeugt von einer eindimensionalen Sichtweise und ignoriert, dass von Anfang an bis zur DSGVO der Abwägungsaspekt im Vordergrund stand und steht. Zu den Dimensionen des Datenschutzes gehören das Diskriminierungsverbot und der Anspruch auf solidarischen Umgang in einer sich entsolidarisierenden Informationsgesellschaft (vgl. Art. 9 DSGVO). Er begründet Teilhaberechte und einen staatlichen Schutzauftrag. Damit wird durch einen modernen Datenschutz eine Zukunftsvorstellung für unser Leben und Arbeiten beschrieben, die sich nicht, wie viele Autoren des vorliegenden Stiftungsbüchleins, an einem unkontrollierten, weil angeblich unkontrollierbaren Silicon-Valley-Kapitalismus orientiert, sondern an einer auf humanistischen Grundlagen beruhenden demokratisch gestalteten Informationsgesellschaft. Ein solcher Blick in die Zukunft muss sich des derzeit global in der Informationstechnik ausgetragenen zentralen Konflikts bewusst sein, nämlich dem einer werteorientierten modernen Gesellschaftsordnung mit Kräften, die eine weitgehend ungezügelte Technikentfaltung propagieren und praktizieren. Diese Kräfte sind außerhalb von Europa (noch) dominant, nicht nur in Südostasien und insbesondere in China, sondern auch in den USA. Es ist erschreckend, dass sich die steuerfinanzierte Stiftung Datenschutz – möglicherweise nicht vollständig bewusst – mit seinem Büchlein zum Sprachrohr dieser Kräfte macht.

(Thilo Weichert, Kiel)

Peter Wedde (Hrsg.), **Handbuch Datenschutz und Mitbestimmung,** Bund Verlag, Frankfurt a.M., 2016, 417 S., 49,– €.

Im Bund-Verlag ist ein von Peter Wedde herausgegebenes „Handbuch zum Datenschutz und Mitbestimmung" erschienen. Konkret geht es, wie die im Titel gleichrangig genannte Thematik der Mitbestimmung deutlich macht, um eine Darstellung des Arbeitnehmerdatenschutzes in allen seinen Aspekten, d.h. um

- die rechtlichen Grundlagen des Beschäftigtendatenschutzes,
- die Ausgestaltung des Datenschutzes am Arbeitsplatz,
- die Sicherung des Beschäftigtendatenschutzes durch die Interessenvertretungen,
- die Aufgaben und Arbeitsmöglichkeiten der betrieblichen Datenschutzbeauftragten,
- neue Techniken und neue datenschutz-Anforderungen.

Neben dem Herausgeber haben zu dem Buch Kapitel beigetragen: Stefan Brink, Isabel Eder, Nadia Häfner-Beil, Heinz-Peter Höller, Silvia Mittländer, Marc-Oliver Schulze, Regina Steiner.

Dargestellt wird die derzeit noch geltende Rechtslage. Die EU-DS-GVO findet im Hinblick auf die derzeit noch offenen Umsetzungsmaßnahmen des nationalen Gesetzgebers Erwähnung im Wesentlichen nur in einem halbseitigen Hinweis. Wahrscheinlich hätte mancher Leser hier aber etwas mehr Vorausschau erwartet, da mit einem die Regelungen der DS-GVO ersetzenden nationalen Beschäftigtendatenschutzgesetz bis zur Ingeltungtretung der DS-GVO im Mai 2018 zweifelsohne nicht zu rechnen ist.

Eindeutig handelt es sich aber um eine umfassende Darstellung der geltenden Situation des Datenschutzes im Arbeitsverhältnis, wobei wohl alle aktuellen Problemstellungen und auch sich abzeichnende Entwicklungen der Verarbeitungen von Arbeitnehmerdaten durch Beispiele belegt deutlich und auch für Praktiker verständlich dargestellt werden. Ein Blick in das ausführliche Stichwortverzeichnis zeigt auf, dass der Leser wohl zu jedem ihn beschäftigtenden Problem des Arbeitnehmerdatenschutzes Aussagen vorfindet. Eine Auswahl aktueller Stichworte reicht von App, Assessment Center, Background-Checks, cloud, dashboard, Graph, Industrie 4.0, Netzrecherche, OLAP, soziale Netzwerke bis Whistleblower.

Das Buch hat eine „betriebsratfreundliche" Tendenz. Aufgabenbezogene betriebsinterne „Datenübermittlungen" an den Betriebsrat sollen generell per § 80 BetrVG gestattet sein (Rn. 260 ff; anders und zutreffend aber in Rn. 86). Datenschutzrechtliche Grenzen – wie sie insbesondere das BVerwG kennt – werden nicht aufgezeigt, wobei das Personalvertretungsrecht und die datenschutzrechtlichen Regelungen für Beamte insgesamt nur randweise Beachtung finden (vgl. z.B. zum beamtenrechtlichen Personalakteneinsichtsrecht Rn.58 ff). Die fehlende Kontrolle der Mitarbeitervertretung durch den DSB wird nicht in Frage gestellt (Rn. 256 ff), wenngleich eine Kooperation als sinnvoll empfohlen wird (Rn. 45).

Insgesamt aber für jeden, insbesonders wenn er sich praxisbezogen mit Fragen des Arbeitnehmerdatenschutzes zu beschäftigen hat, eine auf dem aktuellen Stand befindliche, hilfreiche Lektüre.

(Peter Gola, Königswinter)

Neuerscheinungen

Aufsätze

Die RDV weist regelmäßig auch auf in anderen Zeitschriften erschienene Beiträge zum Recht der Datenverarbeitung hin, um Recherchen zu relevanten Themen zu erleichtern. Einreichungen von Beiträgen zur Aufnahme eines Hinweises werden gerne entgegengenommen.

Dammann, Ullrich, **Erfolge und Defizite der EU-Datenschutzgrundverordnung**, ZD 2016, 307 ff.

Der Beitrag erörtert die Erfolge, Defizite und Perspektiven der Grundverordnung. Positiv bewertet werden bessere Regelungen zur Technik, Organisation und Verfahren sowie Funktion der Aufsicht. Partieller Rückschritt wird bei der Zweckbindung gesehen. Viele von den Mitgliedsstaaten zu füllende Leerflächen werden aufgezeigt. Insgesamt wird in der Verordnung ein bedeutsamer Meilenstein in der Entwicklung des Datenschutzes auf nationaler, europäischer und internationaler Ebene gesehen.

Dietrich, Thomas, **Rechtsdurchsetzungsmöglichkeiten der DS-GVO**, ZD 2016, 260 ff.

Fazit des Beitrags ist, dass ein einheitlicher Rechtsrahmen nicht zwangsläufig zur einheitlichen Rechtsanwendung führt. Es komme auf eine hinreichende Ausstattung der Aufsichtsbehörden, eine angemessene und einheitliche Bußgeldpraxis und effektive Verbraucherverbände an.

Franck, Lorenz, **Verlust und Fund von Datenspeichern**, ZD 2016, 324 ff.

Der Beitrag beleuchtet die zivil- und datenschutzrechtlichen Pflichten für Verlierer, Finder und Fundbüros hinsichtlich Verwahr-, Benachrichtigungs- und Löschpflichten der jeweils Beteiligten.

Fuhlrott, Michael/Oltmanns, Sönke, **Social Media im Arbeitsverhältnis – Der schmale Grat zwischen Meinungsfreiheit und Pflichtverletzung**, NZA 2016, 785 ff.

Der Beitrag untersucht die arbeitgeberseitigen Reaktionsmöglichkeiten auf nicht akzeptable Äußerungen von Arbeitnehmern in sozialen Medien und zeigt präventive Gestaltungsmöglichkeiten auf.

Klug, Christoph, **Der Datenschutzbeauftragte in der EU**, ZD 2016, 315 ff.

Die EU-DS-GVO etabliert den Datenschutzbeauftragten europaweit, wenn auch gegenüber der bisherigen deutschen Regelung in „reduzierter" Form. Der Beitrag skizziert die Bestellvoraussetzungen, die Rechtsstellung und Aufgaben nach dem neuen Recht.

Mittländer, Sylvia, **Betriebsrat contra Arbeitnehmerdaten**, CuA 7-8/2016, 8 ff.

Der Betriebsrat hat hinsichtlich der ihm vom Arbeitgeber zur Verfügung gestellten Personaldaten die Einhaltung der datenschutzrechtlichen Regelungen einschließlich der Datensicherheit eigenständig zu verantworten.

Möhrke-Sobolewski, Christine/Klas, Benedikt, **Zur Gestaltung des Minderjährigendatenschutzes in digitalen Informationsdiensten**, K&R 2016, 373 ff.

Der Beitrag befasst sich mit Fragen des Minderjährigendatenschutzes im Internet vor dem Hintergrund der in zwei Jahren anzuwendenden EU-DS-GVO. Ausgehend von der gestiegenen Relevanz für Unternehmen, Minderjährige gezielt als zukünftige Kunden anzusprechen, werden im Beitrag die aktuelle Rechtslage und deren Auswirkungen auf die unternehmerische Praxis dargestellt.

Wilmer, Stefan, **Wearables und Datenschutz - Gesetze von gestern für die Technik von morgen**?, K&R 2016, 382 ff.

Der Autor befasst sich mit Fragen des Datenschutzes, bei Wearables und dem dabei bestehenden Spannungsfeld zwischen dem Interesse der Anbieter von Wearables an den Daten der Nutzer und den restriktiven Regelungen des Bundesdatenschutzgesetzes (BDSG) und des Telemediengesetzes (TM6).

Tod im Roboterauto

Autonome Autos fahren ohne menschliche Mitwirkung. Der menschliche Beitrag besteht darin, der Maschine alle Parameter für eine optimale Entscheidung an die Hand zu geben. Das Ziel ist das Optimum im Verhalten bis zur Grenze der Unfehlbarkeit. Das ist noch nicht optimal gelöst. Weil sie derzeit nicht alle Entscheidungsparameter kennen, verwechseln Maschinen Steckdosen mit Schweineschnauzen und ein Verkehrsschild mit einem weißen LKW. Beides sieht nämlich für Maschinenaugen ähnlich aus. Der Zeitpunkt wird kommen, dann werden Maschinen solche Fehler mit tödlichen Folgen nicht mehr machen. Ihnen werden Differenzierungsvermögen, Empathie, moralische Werte und die Verpflichtung zum Wohlverhalten einprogrammiert sein. Sie werden im Vergleich zum Menschen die besseren und sichereren Entscheider sein. Nicht nur als Autofahrer, sondern auch als Ärzte, Pastoren, Therapeuten, Techniker und Richter; am Ende für jede menschliche Tätigkeit.

Auch wenn Maschinen nach menschlichen Maßstäben optimal entscheiden werden, werden sie eines niemals besitzen können: Menschenmaß. Dafür bleibt der Mensch zuständig. Die Idee der künstlichen Intelligenz im Auto und überhaupt, macht aber nur dann Sinn, wenn der Mensch die optimale Entscheidung der Maschine akzeptiert. Menschenmaß muss nach dieser Logik Maschinenmaß nach menschlichen Maßstäben weichen. Mit dieser Erkenntnis kann man sich über mehr Sicherheit im Straßenverkehr und in vielen anderen Lebensbereichen freuen. Die Freude hat aber einen beängstigenden Beigeschmack.

Autonome Entscheidungen von Maschinen haben im Guten wie im Schlechten dieselben Auswirkungen, wie menschliche Entscheidungen. Sie sind aber seelenlos und deshalb im juristischen Sinne frei von Verantwortung. Ein selbstfahrendes Auto wird sich entscheiden müssen, ob es in einer unausweichlichen Situation in eine Gruppe Familienangehöriger, eine Gruppe fremder Kinder oder fremder Rentner fährt. Es wird diese Entscheidung nach vorher vom Menschen festgelegten optimalen Parametern treffen. Unser Recht lässt diese Abwägung von Menschenleben nicht zu. Sie verletzt die Menschenwürde.

Die Entscheidung, wie das autonome Fahren sich damit verträgt, führt den Gesetzgeber an seine Grenzen.

Einzigartig kommentiert.

Redeker (Hrsg.)
Handbuch der IT-Verträge
Loseblatt, z.Zt. 4.786 Seiten in 3 Ordnern, inkl. CD mit allen Mustern. Nur 159,– € bei einem Abonnement für mindestens zwei Jahre. Ergänzungslieferungen 1–3-mal im Jahr. ISBN 978-3-504-56008-9. Ohne Abonnement 299,– €. ISBN 978-3-504-560274

Das Handbuch für die IT-rechtliche Vertragsgestaltung: Es kommentiert und erläutert alle im EDV-Recht, IT-Recht und TK-Recht wesentlichen Verträge. Die Autoren stellen aktuelle Muster bereit, für Besonderheiten werden Ihnen alternative Formulierungen angeboten. Auf unzulässige Klauseln werden Sie hingewiesen. So durchschauen Sie in jedem Fall die komplizierten Sachverhalte der Materie und kommen beim Abschluss von Verträgen leichter zu besseren Ergebnissen. Sämtliche Vertragsmuster finden Sie auf der CD.

Aktuell in der Juni-Lieferung:

Vertragsmuster zu Kernthemen des IT-Rechts – vollständig überarbeitet, aktualisiert, kommentiert:
- Software as a Service
- Mediation

Neues Vertragsmuster:

- SEO-Vertrag

Handbuch der IT-Verträge. Am besten gleich Probe lesen und bestellen bei **www.otto-schmidt.de/riv**

ottoschmidt

15 JAHRE beck-online DIE DATENBANK

Datenschutzrecht PLUS

Datenschutzrecht PLUS

ZD – Zeitschrift für Datenschutz, Gola/Schomerus, BDSG und Simitis, BDSG, dazu der Beck'sche Online-Kommentar Datenschutzrecht: diese und weitere wichtigen Informationsquellen stehen Ihnen auch online zur Verfügung – übersichtlich, zitierfähig und zu günstigen Preisen. Dazu vieles, was die Arbeit im Datenschutzrecht erleichtert: Rechtsprechung in Hülle und Fülle, sorgfältig aktualisierte Gesetzestexte und konkrete Lösungen für die Unternehmenspraxis. Damit macht sich dieses umfassende Informationspaket schnell für Sie bezahlt.

▸ schon ab **€ 47,–/Monat**
(zzgl. MwSt., 6-Monats-Abo)

4 Wochen kostenlos testen
Infos: www.beck-shop.de/yqaxb

facebook.com/beckonline | twitter.com/beckonlinede

C.H.BECK

Verlag C.H.BECK oHG, Wilhelmstraße 9, 80801 München | 161053