

2.1.9 Gerichtliche Zuständigkeit

Zuletzt stellt sich, gerade aus praktischer Sicht, die Frage, vor welchem Gericht der Betroffene Schadensersatzansprüche geltend machen kann. Allein Erwägungsgrund 118a sowie Art. 77 Abs. 6 der Ratsversion versuchen, eine Antwort hierauf zu geben. Nach Erwägungsgrund 118a sollten die allgemeinen Vorschriften über die Gerichtsbarkeit, wie sie etwa in der EU-Verordnung Nr. 1215/2012 enthalten sind, der Anwendung dieser spezifischen Vorschriften der DS-GVO nicht entgegenstehen. Im Ergebnis stellen die Vorschriften der DS-GVO also eine *lex specialis* dar, welche anderen europäischen Vorschriften zur Gerichtszuständigkeit vorgehen. Gemäß Art. 77 Abs. 6 DS-GVO des Rates sind für Schadensersatzansprüche die in Art. 75 Abs. 2 DS-GVO benannten Gerichte zuständig.

Nach Art. 75 Abs. 2 DS-GVO (in allen drei Versionen) sind die Gerichte des Mitgliedstaates zuständig, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Hinzuweisen ist darauf, dass hier allein von der „Niederlassung“ die Rede ist und nicht etwa der Hauptsitz des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters ausschlaggebend ist. Klagen auf Schadensersatz können also in jedem Mitgliedstaat angestrengt werden, in dem der Anspruchsgegner niedergelassen ist. Daneben kann ein Betroffener (wahlweise) auch Klage bei den Gerichten des Mitgliedstaates einreichen, an dem er seinen Aufenthaltsort hat.

3. Fazit

Die Neuregelung der eigenständigen Datenschutzhaftung in Art. 77 DS-GVO wird einige Verbesserungen für den Betroffenen bringen. Die Pflicht zur Erstattung immateriellen Schadens wird für alle verantwortlichen Stellen gelten. Auftragsverarbeiter und gemeinsam Verantwortliche werden in die Haftungsregelungen speziell einbezogen. Offen ist, ob auch eine Anknüpfung der Haftung an die Rechtswidrigkeit bloßer „Handlungen“ kommt.



Prof. Peter Gola

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



Dr. Carlo Piltz

ist in der Kanzlei JBB Rechtsanwälte, Berlin als Rechtsanwalt mit den Schwerpunkten Datenschutz- und IT-Recht tätig.

Prof. Dr. Volker Lüdemann/Daniel Wenzel, LL.M.

Zur Funktionsfähigkeit der Datenschutzaufsicht in Deutschland

Der aktuelle Tätigkeitsbericht der Bundesbeauftragten für den Datenschutz liest sich wie ein Hilferuf. Die Bundesbeauftragte sieht den Datenschutz in Deutschland „existentiell gefährdet“¹. In zentralen Bereichen wie der Kontrolle der Nachrichtendienste, Big Data und dem Internet der Dinge ist die Aufsicht nicht mehr in der Lage, das Grundrecht auf informationelle Selbstbestimmung angemessen zu schützen. Es fehlt an Personal, effektiven Kontrollmöglichkeiten und wirksamen Durchsetzungsbefugnissen. Dieser Befund ist be-

unruhigend. Datenschutz ist Grundrechtsschutz. Der Staat ist verpflichtet, ein angemessenes Schutzregime zu konstituieren, um der grundrechtlichen Werteordnung Geltung zu verschaffen. Hierzu gehört eine funktionsfähige staatliche Kontrolle. Der Beitrag analysiert die aktuelle Situation der Datenschutzaufsicht in Deutschland und gibt einen Ausblick auf die sich abzeichnenden Neuerungen durch die Datenschutzgrundverordnung.

I. Einleitung

Die existentielle Gefährdung des Datenschutzes, den die Bundesbeauftragte in ihrem Tätigkeitsbericht anspricht, findet ihren Grund vor allem in der rasanten technologischen Entwicklung. Die digitale Revolution verändert unseren Alltag. Wir sind umgeben von modernen Technologien,

die allgegenwärtig und oftmals unmerklich Daten erheben. Informationstechnische Systeme greifen tief in unser berufliches und privates Leben ein. Dies bietet Chancen für persönliche Entfaltung, Komfort, Gesundheit, Umwelt, Wirtschaft und Arbeit. Die Digitalisierung bringt aber auch

¹ BfDI, 25. Tätigkeitsbericht (2013-14), 18.

enorme Herausforderungen für die informationelle Selbstbestimmung mit sich. Der Einzelne ist kaum mehr in der Lage zu überschauen, wer was wann über ihn weiß. Aus dem Datenstrom, den wir täglich gewollt und ungewollt erzeugen, lassen sich hochdetaillierte Bewegungs-, Verhaltens-, und Persönlichkeitsprofile gewinnen. Intelligente Stromzähler kennen unsere Haushaltsgewohnheiten², moderne Autos wissen alles über uns³ und vielfältige Smart Services erhalten im Gegenzug für Ihre Dienste Einblick in alle möglichen persönlichen Daten⁴. Zugleich stehen immer mehr Methoden, Technologien und Softwarelösungen zur Verfügung, um die Daten nutzbar zu machen. Erstmals in der Geschichte der Menschheit ist die Gefahr des gläsernen Bürgers wirklich real. Die Frage nach dem Umgang mit personenbezogenen Daten gehört damit zu den zentralen gesellschaftlichen Herausforderungen des 21. Jahrhunderts. Wenn sich die Datenschutzaufsicht in diesem Umfeld nicht mehr in der Lage sieht, die Einhaltung der datenschutzrechtlichen Bestimmungen wirksam zu kontrollieren und den Grundrechtsschutz zu gewährleisten, gibt dies Anlass zur Sorge. Der vorliegende Beitrag beleuchtet vor diesem Hintergrund die Funktionsfähigkeit der Datenschutzaufsicht in Deutschland. Der Schwerpunkt der Betrachtung liegt auf der Ausstattung mit Personal und den für die Aufgabenwahrnehmung erforderlichen Befugnissen. Zudem wird sich mit dem Selbstverständnis der Aufsichtsbehörden kritisch auseinandergesetzt.

II. Grundrechtlicher Schutzauftrag

Datenschutz ist Grundrechtsschutz. Schutzgut ist das Recht auf informationelle Selbstbestimmung⁵. Grundrechte sind zwar primär Abwehrrechte gegen den Staat⁶. Dem Staat erwächst aus den Grundrechten jedoch ein verfassungsrechtlicher Schutzauftrag. Dieser verpflichtet den Gesetzgeber, ein angemessenes Schutzregime zu konstituieren, um der grundrechtlichen Werteordnung im öffentlichen Recht und im Privatrecht Geltung zu verschaffen⁷. Er muss die erforderlichen gesetzlichen, verfahrensrechtlichen und organisatorischen Schutzvorkehrungen schaffen, um den einzelnen Bürger wirksam vor unerwünschten Persönlichkeitsgefährdungen Dritter zu schützen⁸. Hinsichtlich der Ausgestaltung hat der Gesetzgeber einen weiten Gestaltungsspielraum. Erforderlich ist aber in jedem Fall eine effektive staatliche Aufsicht⁹. Dieser kommt umso größere Bedeutung zu, je weniger der Bürger seine Rechte selbst wahrnehmen kann¹⁰. Heute ist der Einzelne aufgrund der allumfassenden, allgegenwärtigen und unmerklichen Datenerhebung kaum mehr in der Lage zu übersehen, welche persönlichen Daten, wann und wo erhoben und verarbeitet werden. Dementsprechend hat er nur eingeschränkte Möglichkeiten, um sich gegen Rechtsverletzungen zu wehren. Der Individualschutz ist daher in hohem Maße auf die Ergänzung durch die staatliche Datenschutzkontrolle angewiesen¹¹. Nur diese ist in der Lage, die fehlende Informationstransparenz der automatisierten Datenverarbeitung zu kompensieren.

III. Mindestanforderungen an die Ausgestaltung der Aufsicht

Das Unions- und das Verfassungsrecht fordern aber nicht nur das Vorhandensein einer staatlichen Datenschutzaufsicht. Es enthält auch drei Mindestanforderungen an deren Ausgestaltung: Die Aufsicht muss einen vorgezogenen Rechtsschutz ermöglichen, unabhängig sein und über diejenigen Ressourcen und Befugnisse verfügen, die für einen wirksamen Grundrechtsschutz erforderlich sind¹². Die erste Voraussetzung ist unproblematisch gegeben. Das BDSG und die Landesdatenschutzgesetze sehen vor, dass sich jedermann, der sich durch die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten in seinen Rechten verletzt sieht, außerhalb des Rechtsweges an die zuständige Aufsichtsbehörde wenden und dort seine Belange vortragen kann¹³. Der vorgezogene Rechtsschutz ist damit gewährleistet. Auch die zweite Voraussetzung, die Unabhängigkeit der Datenschutzaufsicht, steht heute im Grundsatz nicht mehr in Rede. Im Anschluss an die Judikatur des EuGH, dass die Unabhängigkeit der Datenschutzaufsicht nicht funktional, sondern institutionell zu verstehen ist¹⁴, haben die Bundesländer Regelungen getroffen, die eine Aufsicht über die Landesdatenschutzbeauftragten ausschließen¹⁵. Die BfDI wird zum 1.1.2016 in eine eigenständige oberste Bundesbehörde umgewandelt¹⁶. Kritisch scheint mit Blick auf den Tätigkeitsbericht der BfDI allerdings die dritte Mindestanforderung: Die Ausstattung der Datenschutzkontrolle mit den für ihre Aufgabenerfüllung erforderlichen Ressourcen

2 Lüdemann/Scheerhorn/Sengstacken/Brettschneider, DUD 2015, 93 ff.; Lüdemann/Jürgens/Sengstacken, ZNER 2012, 325 ff.

3 Schwartmann/Ohr, RDV 2015, 59 ff.; Jaspers/Franck, RDV 2015, 69 ff.; Lüdemann, ZD 2015, 247 ff.

4 Becker/Schwab, ZD 2015, 151 ff.; Brandenburg/Leuthner, ZD 2015, 111 ff.; Raabe/Weis, RDV 2014, 231 ff.; Rüdiger, RDV 2014, 253 ff.; Lüdemann/Sengstacken, RDV 2014, 177 ff.; Lüdemann/Sengstacken/Vogelpohl, RDV 2014, 302 ff.

5 BVerfGE 65, 1 ff., ergänzt durch das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, vgl. BVerfG NJW 2008, 822.

6 BVerfGE 7, 198, 204 f.; von Münch, in: von Münch/Kunig (Hrsg.), GG, 6. Aufl. 2012, Band 1, Vorb. Art. 1-19 Rn. 16; Poscher, Grundrechte als Abwehrrechte, 2003.

7 Jarass, in: Jarass/Pieroth, GG, 13. Aufl. 2014, Vorb. vor Art. 1 Rn. 5 ff.; Simitis, in: Simitis (Hrsg.), BDSG, 8. Aufl. 2014, Einleitung, Rn. 109; Papier, Entwicklungen des Rechts auf informationelle Selbstbestimmung, in: Bitburger Gespräche in München, Tübingen 2012, 28 f.

8 BVerfG NJW 1999, 1322, 1323; Di Fabio, in: Maunz/Dürig (Hrsg.), GG-Kommentar, 72. EL 2014, Art. 2, Rn. 135; Jarass, in: Jarass/Pieroth (o. Fußn. 7), Vorb. vor Art. 1 Rn. 2.

9 BVerfG, Urt. v. 24.04.2013 – 1 BvR 1215/07, Rn. 215; BVerfGE 65, 1, 44, 46; Art. 28 Richtlinie 95/46/EG v. 24.10.1995 (DS-RL).

10 BVerfG, Urt. v. 24.04.2013 – 1 BvR 1215/07, Rn. 207 a.E.

11 BVerfG, Urt. v. 24.04.2013 – 1 BvR 1215/07, Rn. 217.

12 BVerfG, Urt. v. 24.04.2013 – 1 BvR 1215/07, Rn. 215; BVerfGE 65, 1, 46; Art. 28 Richtlinie 95/46/EG v. 24.10.1995 (DS-RL); EuGH, Urt. v. 9.3.2010 – C-518/07.

13 Vgl. nur § 21 BDSG und § 19 NDSG.

14 EuGH, Urt. v. 09.03.2010 – C-518/07.

15 Gola/Schomerus, BDSG, 12. Aufl. 2015, § 38 Rn. 31 f.; Thomé, Reform der Datenschutzaufsicht, 2015, 99 ff.; Schild, DuD 2010, 549 ff.

16 Ausführlich Roßnagel, ZD 2015, 106 ff.

und Befugnissen. Die Aufsichtsbehörden müssen über die für die Aufgabenerfüllung erforderlichen personellen und sachlichen Mittel sowie die notwendigen Befugnissen verfügen¹⁷. Den Maßstab für die Erforderlichkeit hat das Bundesverfassungsgericht operationalisiert: Die Datenschutzkontrolle muss so ausgestattet sein, dass sie in der Lage ist, den Gefährdungen durch eine sich ständig fortentwickelnde Datenverarbeitungswelt wirksam entgegenzuwirken¹⁸. Ist die Datenschutzaufsicht nicht in der Lage, einen angemessenen Grundrechtsschutz zu gewährleisten, stellt dies einen unverhältnismäßigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar, der verfassungsgerichtlich gerügt werden kann¹⁹.

IV. Ressourcen und Befugnisse der Aufsichtsbehörden

Die Ressourcen und Befugnisse der Aufsichtsbehörden werden im Folgenden vor der Folie dieser Anforderungen analysiert.

1. Personalsituation

Auf Ebene des Bundes und der Länder stehen derzeit ca. 440 Vollzeitstellen für die Datenschutzkontrolle zur Verfügung. Die Verteilung auf die einzelnen Datenschutzbehörden ist in der Tabelle dargestellt. Diese spiegelt die aktuelle Situation (Stand September 2015) wider und beruht auf einer von den Verfassern durchgeführten Abfrage bei den Datenschutzbehörden. Bei den ausgewiesenen Vollzeitstellen handelt es sich um Stellen, die der Behördenleitung für die effektive Überwachung zur Verfügung stehen²⁰.

Aufsichtsbehörden	Vollzeitstellen (Datenschutz)
Bund	61
Baden-Württemberg	18,5
Bayern (LDA)	16
Bayern (LfD)	17,8
Berlin	37
Brandenburg	24
Bremen	13,1
Hamburg	12,35
Hessen	32
Mecklenburg-Vorpommern	11,25
Niedersachsen	35,6
Nordrhein-Westfalen	35,5
Rheinland-Pfalz	18
Saarland	12,5
Sachsen	19
Sachsen-Anhalt	12,5
Schleswig-Holstein	15
Thüringen	13,5

Mit Ausnahme der Datenschutzaufsicht in Baden-Württemberg, Bayern, Bremen und Sachsen-Anhalt weisen die Aufsichtsbehörden in ihren Tätigkeitsberichten oder Stellungnahmen in unterschiedlichen Abstufungen auf eine unzureichende personelle Ausstattung hin.

a) Bund

Der deutlichste Hinweis auf eine unzureichende personelle Ausstattung findet sich bei der BfDI. Sie sieht sich mit dem derzeitigen Personalstand angesichts des Aufgabenzuwachses nicht in der Lage, einen sachgerechten Grundrechtsschutz zu gewährleisten²¹ – eine Einschätzung, die von der Konferenz der Datenschutzbeauftragten des Bundes der Länder geteilt wird²². Folge ist ein Rückgang der Prüfungstätigkeit, vor allem im Bereich der anlassunabhängigen Kontrollen²³. So müssen etwa die von der BfDI kontrollierten Telekommunikationsunternehmen im Durchschnitt nur alle 350 Jahre mit einer unangemeldeten aufsichtsbehördlichen Kontrolle rechnen²⁴. Unter den Auswirkungen des Personalmangels leiden zudem Prüfungen, denen das Bundesverfassungsgericht eine „herausragende Bedeutung“ zuspricht, wie bei heimlichen Eingriffen der Sicherheitsbehörden²⁵. Mit der Aufwertung der BfDI zur obersten Bundesbehörde verbessert sich die Personalsituation zunächst nicht. Die BfDI erhält sechs zusätzliche Vollzeitstellen²⁶. Diese sind aber zur Deckung des mit der Umwandlung einhergehenden Vollzugs- und Administrationsaufwands bestimmt. Für die eigentliche Datenschutzaufsicht stehen diese nicht zur Verfügung.

b) Berlin

Der BlnBDI weist angesichts der beständig steigenden Zahl von Eingaben, anlassabhängigen Kontrollen, Ordnungswidrigkeitsverfahren und der Beratung von Bürgern, Abgeordneten

17 EuGH ZD 2012, 563, Rn. 58; BVerfGE 133, 277, 370 f.

18 BVerfGE 65, 1, 46.

19 BVerfG, Urt. v. 24.04.2013 – 1 BvR 1215/07, Rn. 207.

20 Schreiben BfDI v. 28.05.2015, Schreiben LfD BW v. 11.05.2015, Schreiben BayLDA v. 05.05.2015, Schreiben BayLFD v. 29.04.2015 u. 07.09.2015, Schreiben BlnBDI v. 06.05.2015, Schreiben LDA Brandenburg v. 13.05.2015, Schreiben LfDI Bremen v. 27.04.2015 (und 03.09.2015 telefonisch), Schreiben HmbBfDI v. 23.07.2015, HDSB v. 05.05. und 28.07.2015, Schreiben LfDI MV v. 08.05.2015, Schreiben LfD Niedersachsen v. 28.07.2015 mit Verweis auf Einzelplan 17, Haushaltsplan 2015, Schreiben LDI NRW v. 08.05.2015, LfD RP v. 22.07.2015 (telefonische Auskunft), Schreiben LfDI Saarland v. 23.07.2015, Schreiben SächsDSB v. 27.04. und 23.07.2015, Schreiben LfD SA v. 11.05.2015, Schreiben ULD SH v. 22.07. und 09.09.2015, Schreiben TLfDI v. 28.07.2015.

21 BfDI (o. Fn. 1), 49. Die BfDI verfügt derzeit über 61 Vollzeitstellen für den Bereich Datenschutz. 9 Stellen betreuen den nicht öffentlichen Bereich und 52 Stellen den öffentlichen Bereich, vgl. Schreiben BfDI v. 28.05.2015.

22 Vgl. Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 08. und 09.10.2014.

23 In den Jahren 2013 und 2014 konnten insgesamt nur 93 anlassunabhängige Kontrollen durchgeführt werden.

24 <http://www.golem.de/news/datenschutzbeauftragte-vosshoff-will-keine-fehlbesetzung-mehr-sein-1506-114723.html>.

25 BfDI (o. Fn. 1), 36.

26 BT-Drs. 18/2848, 14.

und Datenverarbeitern auf eine personelle Unterdeckung hin und hält eine Personalaufstockung für unabdingbar²⁷.

c) Brandenburg

Gleiches gilt für die LDA Brandenburg. In den letzten Jahren sind der Aufgabenzuwachs und die steigende Zahl von Eingaben und Beratungersuchen nur teilweise personell unterlegt worden²⁸. Negative Auswirkungen ergeben sich vor allem im Hinblick auf die Begleitung öffentlicher Projekte und die Durchführung anlassunabhängiger Prüfungen²⁹. In den Doppelhaushalten 2013/2014 und 2015/2016 hat sich die personelle Situation zwar durch die Zuweisung jeweils einer Vollzeitstelle verbessert. Sie wird aber weiter für unzureichend gehalten³⁰.

d) Hamburg

Die personelle Ausstattung des HmbBfDI ist ungeachtet des erheblichen Aufgabenzuwachses sogar seit 2002 rückläufig³¹. Der HmbBfDI hält dies angesichts des Umstandes, dass in seinem Aufsichtsbereich die deutschen Dependancen von Alphabet (vormals Google), Facebook und XING und viele Start-Ups aus der Digitalwirtschaft beheimatet sind, für kritisch und mahnt eine Aufstockung an³². Für den Haushalt 2017/18 wird ein erhöhter Personalbedarf angemeldet. Ob dieser bewilligt wird, ist derzeit nicht absehbar³³.

e) Hessen

Auch der HDSB hält die Personaldecke zur Bewältigung der Aufgaben für eher knapp bemessen³⁴. So standen im Berichtszeitraum, der durch innerbehördliche Umstrukturierungs- und Konsolidierungsarbeiten zusätzlich belastet gewesen ist, kaum Kapazität für die präventive Datenschutzkontrolle zur Verfügung. Die aufsichtsbehördliche Tätigkeit beschränkte sich in dieser Zeit nahezu ausschließlich auf das Bearbeiten von Eingaben, die Beratung und die Durchführung anlassbezogener Kontrollen³⁵.

f) Mecklenburg-Vorpommern

Auch der LfDI MV macht Personalknappheit geltend³⁶. Auswirkungen ergeben sich vor allem in der Verfolgung von Datenschutzverstößen. Ordnungswidrigkeitsverfahren dauern mittlerweile bis zu 3 Jahre³⁷.

g) Niedersachsen

Die Personalausstattung der LfD Niedersachsen ist in den letzten beiden Jahren deutlich angehoben worden³⁸. Im Hinblick auf technische Themen wird jedoch eine weitere personelle Verstärkung im Technikbereich für erforderlich gehalten³⁹.

h) Nordrhein-Westfalen

Der LDI NRW hält eine massive personelle Aufstockung für die Verbesserung der Kontrolle und Durchsetzung des Datenschutzes sowie im Hinblick auf die absehbaren Änderun-

gen durch die DS-GVO für notwendig⁴⁰. Eine Aufstockung um weitere 16 Stellen ist zum nächstmöglichen Zeitpunkt beantragt⁴¹.

i) Rheinland-Pfalz

Auch der LfD RP verweist auf eine deutliche personelle Unterdeckung. Mangels ausreichender Kapazitäten können nicht alle Aufgaben in dem gewünschten Umfang durchgeführt werden⁴². In absehbarer Zeit wird mit keinem Zuwachs gerechnet⁴³.

j) Saarland

Die LfDI Saarland sieht sich aktuell gerüstet, geht aber von zusätzlichem Personalbedarf mit Inkrafttreten der DS-GVO aus⁴⁴.

27 BlnBDI, Jahresbericht 2014, 185. Aktuell sind 37 Vollzeitkräfte mit der Aufsicht über den öffentlichen und nicht-öffentlichen Bereich beschäftigt, vgl. Schreiben BlnBDI v. 06.05.2015.

28 LDA Brandenburg, 17. Tätigkeitsbericht (2012/2013), 156. Mit der im Jahr 2010 erfolgten Zusammenführung der Datenschutzaufsicht im öffentlichen und nicht öffentlichen Bereich wurden die Stellen des Innenministeriums, das zuvor für die Datenschutzaufsicht im nicht-öffentlichen Bereich zuständig war, auf die LDA übertragen. Für die Prüfung und Durchführung der arbeitsintensiven Ordnungswidrigkeitsverfahren wurde jedoch kein zusätzliches Personal bereitgestellt.

29 LDA Brandenburg (o. Fn. 28), 157.

30 Schreiben LDA Brandenburg v. 22.07.2015.

31 HmbBfDI, 24. Tätigkeitsbericht (2012/2013), S. 20 ff. Aktuell stehen 12,35 Vollzeitstellen für die effektive Datenschutzaufsicht zur Verfügung. Davon sind 1,5 Stellen befristet zum Jahresende, 1,1 Stellen ergeben sich aus der vorübergehenden Abordnung von anderen Behörden.

32 HmbBfDI (o. Fn. 31), 21 f.

33 HmbBfDI, Schreiben v. 22.7.2015.

34 HDSB, 43. Tätigkeitsbericht (2014), 39; von den Mitarbeitern, die die Facharbeit leisten, befassen sich jeweils fünf schwerpunktmäßig mit den Aufgabenstellungen aus dem öffentlichen bzw. nicht öffentlichen Bereich. Fünf Mitarbeiter sind jeweils dem öffentlichen und dem nicht öffentlichen Bereich direkt zugewiesen. Im Übrigen sind die Schwerpunkte unterschiedlich, je nach Arbeitsanfall und Anforderung, Schreiben HDSB v. 05.05.2015.

35 HDSB (o. Fn. 34), 39 ff.

36 LfDI MV, 6. Tätigkeitsbericht (2012-2013), 122. Für die Beaufsichtigung des öffentlichen Bereichs stehen 5, 25 Vollzeitstellen zur Verfügung, darunter eine befristete Halbtagsstelle. Ein Teil der für den öffentlichen Bereich zuständigen Mitarbeiter ist zu einem Zeitanteil von ca. einem Drittel parallel mit Fragen der Informationsfreiheit befasst. Für den nicht öffentlichen Bereich stehen drei Vollzeitstellen zur Verfügung, wobei auch hier eine Halbtagsstelle befristet ist. Hinzu kommen drei Vollzeitstellen im technischen Bereich, die mit wechselnden Zeitanteilen den öffentlichen und nicht-öffentlichen Bereich unterstützen, vgl. Schreiben LfDI MV v. 08.05.2015.

37 LfDI MV (o. Fußn. 36), 10.

38 Land Niedersachsen, Haushaltsplan für das Haushaltsjahr 2015, Einzelplan 17, Übersicht über das Beschäftigungsvolumen, das Budget und die Stellen (BBS), LfD, 3; telef. Auskunft der LfD Niedersachsen v. 22.07.2015.

39 LfD Niedersachsen, 20. Tätigkeitsbericht (2009-2010), 76.

40 LDI NRW, 22. Datenschutzbericht 2015, 11. Von den 35,5 Vollzeitstellen werden derzeit 16 Stellen für die Datenschutzaufsicht im öffentlichen Bereich und 19,5 Stellen für den nicht-öffentlichen Bereich eingesetzt, vgl. Schreiben LDI NRW v. 08.05.2015.

41 Schriftl. Auskunft LDI NRW v. 04.08.2015.

42 LfD RP, Datenschutzbericht 2012/2013, 50, 57.

43 Telefonische Auskunft des LfD RP v. 22.07.2015.

44 Schreiben LfDI Saarland v. 23.07.2015.

k) Sachsen

Der SächsDSB sieht aufgrund des Personalmangels seine Behörde an der Grenze ihrer Leistungsfähigkeit und die Arbeitsfähigkeit akut gefährdet⁴⁵. Der Personalmangel macht sich vor allem im nicht-öffentlichen Bereich bemerkbar. Im Berichtszeitraum 2011-2013 hat sich die Personalausstattung hier trotz gestiegener Arbeitsbelastung rückläufig entwickelt⁴⁶. Für die Aufsicht über ca. 175.000 sächsische Unternehmen stand im Berichtszeitraum nur eine niedrige einstellige Zahl von Mitarbeitern zu Verfügung. Anlassfreie, präventive Kontrollen wurden vor diesem Hintergrund auf ein Minimum beschränkt, festgestellte Datenschutzverstöße nur zum Teil verfolgt. Folge ist ein erhebliches Vollzugsdefizit im nicht-öffentlichen Bereich⁴⁷. Durchgreifende personelle Änderungen sind nicht absehbar⁴⁸.

l) Schleswig-Holstein

Eine Sonderrolle nimmt das ULD SH ein, das neben den klassischen Aufsichtsaufgaben Audits und Zertifizierungen anbietet sowie wissenschaftliche Studien und projektbegleitende Beratung durchführt⁴⁹. Während der Personalbedarf insoweit über Drittmittel realisiert wird, ist der Aufgabenzuwachs im Kernbereich bereits seit Jahren nicht mehr von der Zuweisung zusätzlicher Ressourcen gedeckt⁵⁰. Das ULD mahnt vor diesem Hintergrund eine bessere Ausstattung an, um Anfragen und Beschwerden zeitnah beantworten und notwendige strategische Maßnahmen durchführen zu können⁵¹.

m) Thüringen

Auch der TlFDI weist auf eine Diskrepanz zwischen Aufgaben und vorhandenem Personal hin⁵². Kritisch ist vor allem die Situation im nicht-öffentlichen Bereich. Bis Ende 2011 stand für die gesamte Aufsicht im nicht-öffentlichen Bereich lediglich eine 0,85 Vollzeitstelle im Thüringer Landesverwaltungsamt zur Verfügung. Die Personalsituation hat sich seitdem verbessert⁵³. Die sich aus der Unterbesetzung ergebende jahrelange Vakanz aufsichtsbehördlicher Tätigkeit wirkt jedoch bis heute nachteilig fort. In den Unternehmen ist die Sensibilität in Datenschutzfragen insgesamt unzureichend ausgeprägt. Es besteht ein hoher Schulungs- und Beratungsbedarf⁵⁴. Gleichzeitig haben sich die Fallzahlen im nicht-öffentlichen Bereich vervielfacht. Insbesondere ist die Zahl der Ordnungswidrigkeitsverfahren stark angestiegen. Mit Blick hierauf und den Aufgabenzuwachs sieht die Behörde eine Anpassung der Personalstärke an die Arbeitsdichte als notwendig an⁵⁵.

2. Befugnisse

Die hinreichende personelle Ausstattung ist aber nur ein Baustein für eine funktionsfähige Aufsicht. Die Datenschutzbehörden müssen auch über die notwendigen Befugnisse verfügen, um die Einhaltung der Datenschutzbestimmungen wirksam kontrollieren, durchsetzen und sanktionieren zu können. Sieht man einmal vom Spezialproblem der Kon-

trolle der Nachrichtendienste ab⁵⁶, sind es derzeit vor allem lückenhafte Einwirkungs- und Sanktionsbefugnisse, die einer effektiven Aufgabenerfüllung der staatlichen Datenschutzaufsicht entgegenstehen.

b) Einwirkungsbefugnisse

Im Bereich der Einwirkungsbefugnisse gibt es die größten Defizite bei der Überwachung der Post und Telekommunikation⁵⁷. Obgleich die BfDI für die Aufsicht über etwa 3.000 Telekommunikationsunternehmen und 1.500 Postdienstleister zuständig ist⁵⁸, verfügt sie über keine eigenen Mittel zur Sicherstellung einer rechtskonformen Datenverarbeitung. Sie hat derzeit nur die Möglichkeit, Beanstandungen bei der BNetzA geltend zu machen⁵⁹. Dieser Zustand ist mit dem geltenden Unionsrecht nicht vereinbar. Die geforderte Unabhängigkeit der Datenschutzaufsicht schließt jedwede unmittelbare oder mittelbare Abhängigkeit von einer anderen Behörde bei der Aufgabenerfüllung aus⁶⁰. Aber auch außerhalb der Überwachung des Post- und Telekommunikationsbereichs gibt es Lücken⁶¹. Aufsichtsbehördliche Anordnungen

45 SächsDSB, 6. Tätigkeitsbericht (01/2011-03/2013) – Datenschutz im nicht öffentlichen Bereich, 14. Der Haushalt für 2014 sieht 21 und für 2015 insgesamt 22 Vollzeitstellen vor. Davon sind 4,5 für den nicht öffentlichen und 14,5 für den öffentlichen Bereich vorgesehen. In den 14,5 Stellen für den öffentlichen Bereich sind allerdings die Mitarbeiter des Technikreferates enthalten, das für beide Bereiche tätig ist, vgl. Schreiben SächsDSB v. 23.07.2015.

46 SächsDSB (o. Fn. 45), S. 12. Die Beratungsanliegen sind im Vergleich zum vorherigen Berichtszeitraum um 25% gestiegen. Die Beanstandungen haben sich sogar um fast 40% – von 648 auf 904 – erhöht.

47 SächsDSB (o. Fn. 45), 12f. vgl. bereits SächsDSB, 5. Tätigkeitsbericht (2009-2010) – Datenschutz im nicht-öffentlichen Bereich, S. 13 ff.

48 Schreiben SächsDSB v. 23.07.2015.

49 ULD SH, 35. Tätigkeitsbericht 2015, 125.

50 Schreiben ULD SH v. 27.07.2015; ULD SH, 34. Tätigkeitsbericht 2013, 23. Die klassische Aufsichtstätigkeit wird von der Landesbeauftragten für Datenschutz (eine Stelle) und 9 Beschäftigten (4 Mitarbeiter im nicht-öffentlichen und 5 Mitarbeiter im öffentlichen Bereich, teilweise mit Stellenanteilen) unter rechtlichen Gesichtspunkten wahrgenommen. Hinzu kommen 8 Beschäftigte im Bereich Technik, die zu unterschiedlichen Zeitanteilen in beiden Bereichen tätig sind, und 4 Servicekräfte, die bei der Aufsichtstätigkeit unterstützen. Insgesamt unter Einberechnung der Beschäftigten im Bereich Technik und der Servicekräfte ergibt sich für die Aufsichtstätigkeit ein Umfang von etwa 5-6 Vollzeitäquivalenten im nicht-öffentlichen Bereich sowie von etwa 8-9 im öffentlichen Bereich, vgl. Schreiben ULD SH v. 09.09.2015.

51 ULD SH (o. Fn. 49), 12, 23.

52 TlFDI, 1. Tätigkeitsbericht zum Datenschutz: Nicht-öffentlicher Bereich 2012/13, S. 7 ff. Aktuell stehen 13,5 volle Stellen aus den vier Referaten für den gesamten öffentlichen und nicht öffentlichen Bereich zur Verfügung.

53 Derzeit sind beim TlFDI effektiv 4,8 Stellen referatsübergreifend mit der Beaufsichtigung beschäftigt, vgl. Schreiben TlFDI v. 28.07.2015.

54 TlFDI (o. Fn. 52), 7, 10; Schreiben TlFDI v. 28.07.2015.

55 TlFDI (o. Fn. 52), 8f.; Schreiben TlFDI v. 28.07.2015.

56 Hierzu BfDI (o. Fn. 1), 35 ff.

57 BfDI (o. Fn. 1), 49.

58 § 115 Abs. 4 TKG und § 42 Abs. 3 PostG; BT-Drs. 18/2848, 19.

59 § 25 BDSG, § 115 Abs. 4 TKG, § 42 Abs. 3 PostG.

60 EuGH, Urt. v. 09.03.2010 – C-518/07; EuGH ZD 2012, 563, Rn. 41 f., 51, Roßnagel, ZD 2015, 106 ff.

61 Gola/Schomerus (o. Fn. 15), § 38 Rn. 25.

können nicht ohne weiteres mit der Anordnung der sofortigen Vollziehung verbunden werden. Die Einwirkungsbefugnisse der Datenschutzaufsicht bleiben damit in einem zentralen Punkt hinter den üblichen Möglichkeiten der Gefahrenabwehr zurück⁶².

b) Sanktionsbefugnisse

Auch die Befugnisse zur Sanktionierung festgestellter Datenschutzverstöße sind unzureichend. Hier steht wiederum die Situation im Post- und im Telekommunikationssektor im Vordergrund. Die BfDI kann aufgrund mangelnder Zuständigkeit keine Bußgelder wegen Verstößen gegen das BDSG verhängen. Die BNetzA ist hierzu allerdings auch nicht berechtigt. Sie kann nur Verstöße gegen die datenschutzrechtlichen Bestimmungen des TMG und TKG mit einem Bußgeld ahnden. Die Sanktionierung von Verstößen gegen das BDSG bleibt daher oftmals folgenlos⁶³. Dieser Zustand ist mit dem verfassungsrechtlichen Gebot effektiven Grundrechtsschutzes unvereinbar. Die fehlende Sanktionsbefugnis der BfDI ist zudem europarechtswidrig. Artikel 8 Abs. 3 EU-Grundrechtecharta und Art. 28 Abs. 1 DS-RL sehen vor, dass die Sanktionierung datenschutzrechtlicher Bestimmungen institutionell unabhängigen Behörden zu übertragen ist⁶⁴. Die Bundesnetzagentur weist nicht die geforderte Unabhängigkeit auf. Sie ist als obere Bundesbehörde dem Bundesministerium für Wirtschaft und Energie nachgeordnet und untersteht im Telekommunikationsrecht der Fachaufsicht des Bundesministeriums für Verkehr und digitale Infrastruktur⁶⁵. Die strafrechtliche Sanktionierung kann die Aufsicht zwar über einen Strafantrag einleiten, ist dann aber von der Staatsanwaltschaft abhängig. Dies ist grundsätzlich zulässig. Die Datenschutzaufsicht ist keine Strafverfolgungsbehörde. Insoweit ist jedoch zu überlegen, der Aufsicht Akteneinsicht zu gewähren, sie vor staatsanwaltschaftlichen Einstellungsverfügungen anzuhören und bei Hauptverhandlungen zu laden⁶⁶.

V. Selbstverständnis der Aufsichtsbehörden

Problematisch für einen wirksamen Grundrechtsschutz ist neben der mangelnden Ausstattung und den fehlenden Befugnissen auch das Selbstverständnis der Datenschutzaufsicht. Viele Aufsichtsbehörden sehen ihren Aufgabenschwerpunkt eher in der Beratung und Unterstützung⁶⁷. Dies findet seinen Ausdruck unter anderem in der für Aufsichtsbehörden zurückhaltenden Bußgeld- und Strafantragspraxis, die durch Personalmangel allein nicht zu erklären ist.

1. Restriktive Bußgeldpraxis

Die Datenschutzaufsichtsbehörden in Deutschland haben im Jahr 2014 insgesamt ca. 1,9 Mio. € an Bußgeldern verhängt⁶⁸. Hiervon resultieren 1,3 Mio. € aus einem einzigen Fall: Dem einvernehmlichen Abschluss der Ordnungswidrigkeitsverfahren gegen die Debeka-Versicherung im sog. Tipp-

geber-Skandal in Rheinland-Pfalz⁶⁹. Neben Rheinland-Pfalz, auf das damit insgesamt ca. 1,4 Mio. € entfallen⁷⁰, hat lediglich die Aufsicht in Sachsen in größerem Umfang Bußgelder verhängt (195.832 €)⁷¹. Mit deutlichem Abstand folgen Nordrhein-Westfalen (89.000 €)⁷², Berlin (88.205 €)⁷³, Bayern (44.290 €)⁷⁴, Baden-Württemberg (21.550 €)⁷⁵, Bremen (16.500 €)⁷⁶, Hamburg (14.600 €)⁷⁷, Niedersachsen (10.700 €)⁷⁸, Thüringen (7.175 €)⁷⁹, Schleswig-Holstein (5.300 €)⁸⁰, Brandenburg (4.300 €)⁸¹, Hessen (2.500 €)⁸² und Sachsen-Anhalt (565,50 €)⁸³. In Mecklenburg-Vorpommern wurden 2014 keine Bußgelder verhängt⁸⁴. Für das Saarland liegen keine Angaben vor⁸⁵.

2. Zurückhaltender Gebrauch des Strafantragsrechts

Die zurückhaltende Bußgeldpraxis setzt sich im restriktiven Gebrauch des Strafantragsrechts fort. Im Jahr 2014 wurden in Berlin 17, in Nordrhein-Westfalen 10, in Rheinland-Pfalz drei, in Bayern und Thüringen jeweils zwei, sowie ein Strafantrag in Sachsen und Sachsen-Anhalt gestellt⁸⁶. Auf Bundesebene sowie in Hamburg, Bremen, Mecklenburg-Vorpommern, Baden-Württemberg, Schleswig-Holstein, Hessen und

62 Ebenso Petri, in: Simitis (o. Fn. 7), § 38 Rn. 6.

63 BfDI (o. Fn. 1), 87.

64 Hierzu ausführlich oben unter III.

65 Schreiben BNetzA v. 30.06.2015.

66 Vgl. auch Roßnagel, ZD 2015, 106, 111.

67 LfD Niedersachsen (o. Fn. 39), 64; LfD Baden-Württemberg, 31. Tätigkeitsbericht (2012/2013), 77 f.; LfD RP (o. Fn. 42), 50; LfDI MV, Tätigkeitsberichts 2012/2013, S. 2. Umfassend hierzu auch Ehmann, in: Simitis (o. Fn. 7), § 43 Rn. 79 ff.; Born, RDV 2015, 125 ff.; Holländer, RDV 2009, 215.

68 Keine Bußgelder wurden von der BfDI verhängt, da ihr die Befugnis fehlt, Verstöße der von ihr direkt überwachten Post- und Telekommunikationsunternehmen zu sanktionieren, vgl. hierzu IV.2.

69 Vgl. hierzu die Pressemitteilung des LfD RP v. 29.12.2014, abrufbar unter <https://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2014122901>.

70 LfD RP v. 22.07.2015 (telefonische Auskunft).

71 Schreiben SächsDSB v. 24.07.2015.

72 Schreiben LDI NRW v. 08.05.2015.

73 Schreiben BlnBDI v. 06.05.2015.

74 Schreiben LDA Bayern v. 05.05.2015.

75 Schreiben LfD BW v. 11.05.2015.

76 Schreiben LfDI Bremen v. 05.05.2015.

77 Schreiben HmbBfDI v. 23.07.2015.

78 Schreiben LfD Niedersachsen v. 28.07.2015.

79 Schreiben TLfDI v. 20.05.2015.

80 Schreiben ULd SH v. 18.05.2015.

81 Schreiben LDA Brandenburg v. 13.05.2015.

82 Schreiben HDSB v. 05.05.2015.

83 Schreiben LfD Sachsen-Anhalt v. 11.05.2015.

84 Die eingeleiteten Ordnungswidrigkeitsverfahren wurden nach erteilter Auskunft sämtlich eingestellt, vgl. Schreiben LDA MV v. 08.05.2015.

85 Eine Statistik über verhängte Bußgelder wird im Saarland nicht geführt, vgl. Schreiben LfDI Saarland v. 23.07.2015.

86 Schreiben BlnBDI v. 06.05.2015; Schreiben LDI NRW v. 08.05.2015; LfDI RP v. 22.07.2015 (telefonisch); Schreiben BayLDA v. 05.05.2015; Schreiben TLfDI v. 20.05.2015; Schreiben SächsDSB v. 23.07.2015; Schreiben LfD Sachsen-Anhalt v. 11.05.2015.

Niedersachsen kam es im Betrachtungszeitraum zu keinen Anträgen⁸⁷. Für das Saarland liegen keine Angaben vor⁸⁸. Diese Zurückhaltung ist besonders problematisch, weil im Unterschied zu § 205 Abs. 1 StGB die Strafverfolgungsbehörde in der Regel nicht wegen eines besonderen öffentlichen Interesses an der Strafverfolgung von Amts wegen ermitteln kann. Eine strafrechtliche Ahndung scheidet damit bei Nichtantrag regelmäßig aus.

3. Gesetzliche Aufgabenzuweisung

Der Umstand, dass viele Aufsichtsbehörden ihren Tätigkeitsschwerpunkt eher in der Beratung und Unterstützung als in der Kontrolle und repressiven Aufsicht sehen, ist von der gesetzlichen Aufgabenzuweisung nur auf den ersten Blick gedeckt. § 38 Abs. 1 S. 2 BDSG sieht zwar vor, dass die Aufsichtsbehörden die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse beraten und unterstützen. Die Vorschrift, die im Zuge der Mittelstandsentlastung 2006 in das BDSG eingefügt wurde⁸⁹, hatte aber zu keinem Zeitpunkt das Ziel, den Charakter der Datenschutzaufsicht grundlegend zu ändern. Der gesetzgeberische Anlass war vielmehr zu gewährleisten, dass mit der gelebten Beratungspraxis kein Verstoß gegen das Rechtsberatungsgesetz begründet wird⁹⁰. Prägendes Merkmal der Datenschutzaufsicht ist im Grundsatz weiterhin die Kontrolle. Dies belegt auch die Binnensystematik der Norm. Die Kontrollfunktion der Aufsichtsbehörden wird an erster Stelle genannt (§ 38 Abs. 1 Satz 1 BDSG). Die datenverarbeitenden Stellen tragen grundsätzlich selbst die Verantwortung für den Datenumgang⁹¹. Präventiv-kooperative Tätigkeiten haben lediglich eine ergänzende Funktion. Die Entscheidung einiger Aufsichtsbehörden, wegen der angespannten Personalsituation anlassfreie Kontrollen zugunsten von Beratungs- und Unterstützungsleistungen zurückzufahren⁹², ist vor diesem Hintergrund nicht unproblematisch. Der Ressourceneinsatz liegt zwar im Ermessen der Aufsichtsbehörde. Er muss sich allerdings an der effektiven Aufgabewahrnehmung und der Gewährleistung eines wirksamen Grundrechtsschutzes messen lassen. Gleiches gilt für die restriktive Handhabung der Bußgeldpraxis. Wenn selbst bei festgestellten Verstößen einige Aufsichtsbehörden bewusst auf Sanktionen verzichten, sofern die verantwortlichen Stellen erklären, sich künftig an die Datenschutzvorschriften zu halten⁹³, lädt dies vor allem im nicht-öffentlichen Bereich zu kalkulierten Rechtsbrüchen ein. Ein wirksamer Grundrechtsschutz ist jedoch nicht möglich, solange sich Verstöße unternehmerisch rechnen⁹⁴. Dies wird durch Erfahrungen aus den Ländern bestätigt. Der HDSB berichtet, dass die Anzahl der Verfahren wegen Nichterfüllung der Auskunftspflicht zurückgegangen ist, seit vermehrt Zwangsgelder angedroht und durchgesetzt werden⁹⁵. Auch das BayLDA setzt aufgrund seiner Erfahrungen aus der Vergangenheit verstärkt auf Kontrollen und Sanktionen⁹⁶. Der LfD RP berichtet sogar, dass Mitbewerber zunehmend spürbare Sanktionen einfordern, wenn andere Unternehmen das Datenschutzrecht verletzen⁹⁷.

VI. Fazit und Ausblick auf die EU-Datenschutzreform

Grundrechtsschutz braucht wirksame Kontrolle. Dies gilt insbesondere für das Recht auf informationelle Selbstbestimmung und die verwandten Datenschutzgrundrechte. In der modernen Datenverarbeitungswelt ist der Einzelne immer weniger in der Lage zu überschauen, was mit seinen persönlichen Daten geschieht. Mangels Kenntnis kann er seine Rechte selbst nur eingeschränkt wahrnehmen. Der individuelle Schutz der informationellen Selbstbestimmung bedarf daher der Ergänzung durch eine effektive staatliche Aufsicht. Derzeit können die Datenschutzbehörden des Bundes und der Länder die Einhaltung der Datenschutzbestimmungen nur unzureichend gewährleisten. Es fehlt an Personal und den für die Aufgabenerfüllung notwendigen Befugnissen.

Die sich derzeit im Trilog-Verfahren befindliche Datenschutzgrundverordnung (DS-GVO-E)⁹⁸ bringt nach derzeitigem Stand allenfalls eine teilweise Entlastung⁹⁹. Verbesserungen zeichnen sich bei den Eingriffsbefugnissen ab. Künftig ist jede Aufsichtsbehörde in der Lage, selbstständig den Rechtsweg zu beschreiten, um die Einhaltung der

87 Schreiben BfDI v. 28.05.2014; HmbBfDI v. 22.07.2015 (telefonisch); Schreiben LfDI Bremen v. 05.05.105; Schreiben LfDI MV v. 08.05.2015; Schreiben LfD BW v. 11.05.2015; Schreiben ULD SH v. 18.05.2015; Schreiben HDSB v. 05.05.2015; Schreiben LfD Niedersachsen v. 28.07.2015.

88 Gestellte Strafanträge werden im Saarland statistisch nicht erfasst, vgl. Schreiben LfDI Saarland v. 23.07.2015.

89 Eingefügt durch das „Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft“ (Mittelstandsentsetzungsgesetz I) v. 22.08.2006, BGBl. I S. 1970.

90 Petri, in: Simitis (o. Fn. 7), § 38, Rn. 37; a.A. Brink, in: Wolff/Brink (Hrsg.), Datenschutzrecht 2013, München 2013, § 38 Rn. 30-32.

91 Ebenso Nguyen, ZD 2015, S. 265, 269.

92 In diese Richtung vgl. nur ULD SH, Stellungnahme gegenüber dem Landesrechnungshof Schleswig-Holstein v. 23.01.2006, abrufbar unter: <https://www.datenschutzzentrum.de/allgemein/20060519-rechnungshof.htm>.

93 Vgl. etwa LfD Niedersachsen (o. Fn. 39), 64, wonach grundsätzlich keine Bußgelder verhängt werden, wenn sich die verantwortliche Stelle einsichtig zeigt und erklärt, derartige Verstöße für die Zukunft zu vermeiden. Auch der LfDI MV hat im Jahr 2014 mehrere Ordnungswidrigkeitsverfahren eingeleitet und nach erhaltener Auskunft bußgeldfrei wieder eingestellt, vgl. Schreiben LfDI MV v. 08.05.2015.

94 Vgl. auch LfDI MV (o. Fn. 36), 10.

95 HDSB (o. Fn. 34), Kapitel 4.1.1.1.

96 „Bayerische Datenschutzaufsicht setzt verstärkt auf Bußgeldverfahren“, abrufbar unter www.haufe.de/marketing-vertrieb/recht/datenschutzaufsicht-setzt-staerker-auf-bussgeldverfahren_128_287594.html.

97 LfD RP (o. Fn. 42), 98.

98 Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) KOM (2012) 11 endgültig, 2012/0011 (COD).

99 Am 24.06.2015 haben das EU-Parlament, der Rat und die EU-Kommission Mitentscheidungsverhandlungen über die DS-GVO aufgenommen. Grundlage des Trilogs sind der Vorschlag der Kommission vom Januar 2012, die legislative Entschließung des Parlaments vom 12.03.2014 und die Allgemeine Ausrichtung des Rates vom 15.06.2015.

Datenschutzbestimmungen durchzusetzen (Art. 76 Abs. 2 DS-GVO-E). Dies führt vor allem im öffentlichen Bereich zu deutlich verbesserten Einwirkungsmöglichkeiten. Datenschutzbehörden können damit bei nicht-kooperativem Verhalten von Behörden das Verwaltungsgericht anrufen. Die Datenschutzaufsicht erhält auch die Befugnis, ihre Anordnungen für sofort vollziehbar zu erklären¹⁰⁰. Den Aufsichtsbehörden steht damit künftig auch dieses zentrale Instrument der Gefahrenabwehr zur Verfügung. Auch die Regelungslücken im Post- und Telekommunikationsbereich werden geschlossen¹⁰¹. Welche Auswirkung die EU-Datenschutzreform auf Art und Umfang der Sanktionsmöglichkeiten hat, lässt sich derzeit noch nicht abschließend beurteilen. Viele Rahmenregelungen stehen noch aus. Die Positionen der Trilog-Verhandlungspartner unterscheiden sich noch zum Teil deutlich, insbesondere hinsichtlich der Frage, was durch die DS-GVO zentralisiert wird und was auf Ebene der Mitgliedstaaten zu regeln ist¹⁰². Einigkeit besteht allerdings darin, dass die Sanktionen „wirksam, verhältnismäßig und abschreckend“ sein sollen¹⁰³. Der Bußgeldrahmen wird dementsprechend gegenüber dem geltenden Recht erhöht, wenngleich um die Details noch gerungen wird¹⁰⁴. Es zeichnet sich zudem ab, dass die Datenschutzaufsicht in bußgeldrechtlichen Verfahren selbst Vertreter des öffentlichen Interesses wird und ihre Bußgeldentscheidungen unabhängig von anderen exekutiven Stellen trifft. Möglicherweise ist sie künftig auch befugt, Bußgelder gegen öffentliche Stellen zu verhängen¹⁰⁵. Während im Bereich der Eingriffs- und Sanktionsmöglichkeiten mit hin durchgreifende Verbesserungen zu erwarten sind, wird sich durch die EU-Datenschutzreform an der Personalsituation voraussichtlich nichts ändern. Die derzeit diskutierten Entwürfe sehen zwar übereinstimmend vor, dass die Aufsichtsbehörde mit angemessenen personellen, technischen, und finanziellen Ressourcen sowie mit Räumlichkeiten und der erforderlichen Infrastruktur ausgestattet wird¹⁰⁶. Diese Regelung geht aber über das geltende Recht im Grundsatz nicht hinaus¹⁰⁷. Sie vermittelt auch keine Ansprüche gegen den Haushaltsgesetzgeber. Dies wäre mit dem Demokratieprinzip (Art. 20 Abs. 2 Satz 1 GG) nicht vereinbar. Die Vorschrift hat daher in erster Linie appellativen Charakter. Sie zielt vor allem darauf, den zusätzlichen bürokratischen Aufwand personell zu unterlegen, der durch die vorgesehene Amtshilfe und Zusammenarbeit mit anderen Aufsichtsbehörden in der gesamten Union entsteht¹⁰⁸. Dieses Personal steht aber nicht für die Vertiefung der eigentlich operativen Aufsichtstätigkeit im eigenen Zuständigkeitsbereich zur Verfügung. Um die Effektivität der Aufsichtsbehörden und ihre zukünftig hinzukommende Kooperationsstruktur gewährleisten zu können, bedarf es weiterer Anstrengungen zu einer deutlichen Aufstockung des Personals. Insoweit bleiben die Haushaltsgesetzgeber auf Bundes- und Landesebene in der Verantwortung. Sie sind verfassungsrechtlich verpflichtet, die Aufsicht in die Lage zu

versetzen, regelmäßige Kontrollen durchzuführen, und die erforderlichen Ressourcen zur Verfügung zu stellen¹⁰⁹. Auch in Zeiten angespannter Haushaltslage darf der Schutz der Grundrechte nicht zur Disposition stehen.

Um eine durchgreifende Verbesserung der Funktionsfähigkeit der Aufsicht zu erreichen, greift allerdings der Ruf nach dem Gesetzgeber zu kurz. Auch die Aufsichtsbehörden selbst stehen in der Pflicht. Angesichts knapper Ressourcen müssen sich die Datenschutzbehörden stärker auf ihre hoheitliche Aufsichtsfunktion besinnen. Hierzu gehört die konsequente Aufdeckung, Verfolgung und Sanktionierung von Datenschutzverstößen. Präventiv-kooperative Tätigkeiten haben lediglich eine ergänzende Funktion. Sie müssen im Zweifel zurückgestellt werden. Dies gilt insbesondere mit Blick auf die Beratung und Unterstützung nicht-öffentlicher Unternehmen. Die datenverarbeitenden Stellen tragen grundsätzlich selbst die Verantwortung für den rechtskonformen Datenumgang. Ihnen ist durchaus zuzumuten, sich das notwendige Wissen auf anderem Wege als durch die Aufsichtsbehörden anzueignen. Die Rolle der Aufsichtsbehörde als „Freund und Helfer“ mag wünschenswert sein, bei begrenzten Ressourcen ist sie aber nicht ohne Vernachlässigung der klassischen Aufsicht zu leisten. Angesichts der aktuellen Gefahren für das Recht auf informationelle Selbstbestimmung sollten die Kräfte auf den aufsichtsbehördlichen Kernbereich konzentriert werden, um einen wirksamen Grundrechtsschutz zu gewährleisten. Diese Schwerpunktsetzung steht im Übrigen in Einklang mit der EU-Datenschutzreform. Aufsichtsbehörden sind ausweislich der Binnensystematik des Aufgabenkatalogs in Art. 52 Abs. 1 DS-GVO vor allem für die Überwachung und Gewährleistung der Datenschutzbestimmungen zuständig. In allen Entwürfen steht dies an erster Stelle¹¹⁰.

100 Art. 53 Abs. 1 lit. g DS-GVO-E; Art. 53 Abs. 1b lit. e DS-GVO-Rat.

101 Art. 53 Abs. 1 DS-GVO-E weist der Datenschutzbehörde umfassende Anordnungs- und Untersuchungsbefugnisse gegenüber sämtlichen verantwortlichen Stellen der Privatwirtschaft zu.

102 Zuletzt hierzu Roßnagel/Nebel/Richter, ZD 2015, 455, 460.

103 Art. 78 Abs. 1 S. 2 DS-GVO Rat; Art. 78 Abs. 1 S. 2 DS-GVO-EP; Art. 79 Abs. 1 DS-GVO-Rat.

104 Kommission und Rat treten für Geldbußen bis zu 2 Prozent des weltweiten Jahresumsatzes oder eine Million Euro ein (Art. 79 Abs. 6 DS-GVO-E, Art. 79a Abs. 3 DS-GVO-Rat). Die legislative Entschließung des EU-Parlaments sieht sogar Bußgelder bis zu fünf Prozent des weltweiten Jahresumsatzes von Unternehmen oder 100 Millionen Euro vor (Art. 79 Abs. 2a lit. c DS-GVO-EP).

105 Hiergegen gibt es allerdings noch erhebliche Widerstände im Rat, darunter auch von deutscher Seite, vgl. Art. 79 Abs. 3b DS-GVO-Rat; Roßnagel/Nebel/Richter, ZD 2015, 455, 460.

106 Art. 47 Abs. 5 DS-GVO-E; Art. 47 Abs. 5; DS-GVO-EP; Art. 47 Abs. 5 DS-GVO-Rat.

107 § 22 Abs. 5 BDSG. Mit der Novellierung des BDSG zum 1.1.2016 entfällt die Regelung. Aus der künftigen Stellung der BfDI als oberste Bundesbehörde ergibt sich dies selbst, da sie einen eigenen Haushaltsplan beim Bundesministerium der Finanzen anmeldet.

108 Vgl. jeweils Erwägungsgrund 94 in DS-GVO-E, DS-GVO-EP und DS-GVO-Rat.

109 BVerfG, Urt. v. 24.04.2013 – 1 BvR 1215/07, Rn. 207.

110 Art. 52 DS-GVO-E; Art. 52 DS-GVO-EP, Art. 52 DS-GVO-Rat.

Die DS-GVO wird ihre Wirkungen, auch wenn sich die Triolog-Parteien wie vorgesehen bis Ende des Jahres einigen, frühestens 2017 entfalten. In der Verordnung ist für den Beginn ihrer Anwendbarkeit eine zweijährige Übergangsphase nach Veröffentlichung im Amtsblatt der Europäischen Union vorgesehen. Es bleibt zu hoffen, dass die Zeit bis dahin nicht ungenutzt verstreicht und der Gesetzgeber sich zu einer funktionierenden Datenschutzaufsicht bekennt. Die Verbesserung der personellen Ausstattung ist die vordringlichste Aufgabe. Auch das Schließen der Lücken in der Aufsicht über die Post- und Telekommunikation kann schnell erfolgen. Hier nachzusteuern kollidiert nicht mit den Reformbemühungen auf europäischer Ebene. Für die Verbesserung der Funktionsfähigkeit ebenso wichtig ist allerdings ein Wandel im Selbstverständnis der Aufsichtsbehörden. In Zeiten knapper Ressourcen muss der Schwerpunkt auf der klassischen hoheitlichen Aufsichtstätigkeit liegen.



Prof. Dr. Lüdemann

ist Professor für Wirtschafts- und Wettbewerbsrecht an der Hochschule Osnabrück und wissenschaftlicher Leiter des Niedersächsischen Datenschutzzentrums (NDZ).



Daniel Wenzel, LL.M.

ist Promotionsstipendiat der VW-Stiftung und beschäftigt sich am Niedersächsischen Datenschutzzentrum (NDZ) mit aktuellen Fragen des Datenschutzrechts.

Dr. Christoph Schnabel, LL.M.

Aktuelle Rechtsprechung zum Datenschutz bei Auskunftsansprüchen

Der Datenschutz leidet trotz allem öffentlichen Interesse an einem Mangel an abschließender Klärung auslegungsbedürftiger Begriffe durch die Rechtsprechung. Dies führt zu einem Mangel an Sicherheit für dem Datenschutz unterliegende Stellen und die Aufsichtsbehörden. Abhilfe bietet eine Orientierung an Rechtsprechung, die datenschutzrechtliche Problem-

kreise berührt, auch wenn sie nicht unmittelbar zum BDSG oder einem LDSG ergangen ist. Dieser Beitrag wertet aktuelle Rechtsprechung aus, die datenschutzrechtliche Fragen im Rahmen von Auskunftsansprüchen gegen den Staat nach IFG, UIG und Presserecht beantwortet und macht sie für die Anwendung im allgemeinen Datenschutzrecht nutzbar.

A. Einleitung

In der Jugendzeit der Informationsfreiheit wurde vielfach davon ausgegangen, dass es sich bei den IFGs um „Schnüffelgesetze“ handeln würde¹, die insbesondere den Datenschutz aushebeln würden. In der Literatur wurden „massive Konflikte“ befürchtet². Diese Befürchtungen haben sich zwar als unbegründet erwiesen, allerdings ist das Verhältnis beider Rechte auch nicht „völlig unproblematisch“³. Da im Datenschutzrecht der Grundsatz des Verbots mit Erlaubnisvorbehalt gilt, also jede Verarbeitung personenbezogener Daten einer Rechtsgrundlage oder einer Einwilligung des Betroffenen bedarf und die Ansprüche nach dem Informationsfreiheitsgesetz gleichzeitig auf alle vorhandenen Informationen gerichtet sind, sind Konflikte zwischen beiden Rechten nicht zu vermeiden⁴. Dabei entsteht der Eindruck, dass die Konflikte zunehmen und personenbezogene Daten nicht mehr nur reiner Beifang sind, der ruhig entfernt werden kann, sondern vielmehr Anträge stärker konkret auf personenbezogene Daten gerichtet sind. Dies mag an der Kombination einer verstärkten Nutzung des IFG durch Jour-

nalisten⁵ bei gleichzeitiger Personalisierung der Berichterstattung liegen.

Zu den Auskunftsansprüchen ergeht eine erhebliche Menge an Rechtsprechung⁶, wohingegen im Datenschutz ein Mangel an Rechtsprechung durch die Fachgerichte besteht, der in einem diametralen Widerspruch zur gesellschaftlichen und wissenschaftlichen Bedeutung des Datenschutzes steht.

1 So die Gegner eines hessischen IFG, zitiert nach Frankfurter Rundschau v. 23.3.2010, abrufbar unter <http://www.fr-online.de/rhein-main/kein-freier-zugang-zu-informationen-in-hessen-bleiben-behorden-verschwiegen,1472796,3113780.html>.

2 So Roßnagel, MMR 2007, 16.

3 So noch Schaar/Schultze, in: Dix u.a. (Hrsg.) Jahrbuch Informationsfreiheit und Informationsrecht – Jahrbuch 2008, 1, 10.

4 Schnabel, DuD 2012, 520 m.w.N.

5 Das IFG ist neben dem presserechtlichen Auskunftsanspruch anwendbar: Schnabel, NVwZ 2012, 854, 857 ff.; BVerwG, NVwZ 2013, 431, 434; OVG NRW, DVBl. 2014, 243, 246; Schoch, NVwZ 2013, 434, 435.

6 Siehe dazu nur Schoch, NVwZ 2013, 1033 ff.; ders., VBIBW 2010, 333 ff.; ders., NJW 2009, 2987 ff.; Rossi, DVBl. 2010, 554 ff.; Schnabel, ZD 2012, 67 ff.; sowie die jährlichen Veröffentlichungen in: Dix et al. (Hrsg.), Jahrbuch Informationsfreiheit und Informationsrecht: Schiller/Wolf, Jahrbuch 2011, 305 ff.; Blatt/Franßen, Jahrbuch 2012, 59 ff.; Blatt, Jahrbuch 2013, 301 ff.; ders., Jahrbuch 2014, 73 ff.