Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen



24. Datenschutz- und Informationsfreiheitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

www.ldi.nrw.de

24. Datenschutz- und Informationsfreiheitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Helga Block

für die Zeit vom 1. Januar 2017

bis zum 31. Dezember 2018

Herausgeber:

Landesbeauftragte für Datenschutz und Informationsfreiheit

Nordrhein-Westfalen

Helga Block

Kavalleriestraße 2–4

40213 Düsseldorf

Tel.: 0211 / 384 24 - 0

Fax: 0211 / 384 24 - 10

E-Mail: poststelle@ldi.nrw.de

Diese Broschüre kann unter www.ldi.nrw.de abgerufen werden.

Zitiervorschlag: 24. DIB LDI NRW

ISSN: 0179–2431

Düsseldorf 2019

Titelbild © psdesign1 – Fotolia.com

Gedruckt auf chlorfreiem Recyclingpapier

Inhaltsverzeichnis

Vorwort **7**

1. Teil: Datenschutzbericht **9**

Überblick **10**

1. Europäische Datenschutzreform **15**

1.1. Die Datenschutz-Grundverordnung 15

1.2 Anpassung auf Bundesebene 17

1.3 Anpassung auf Landesebene 19

1.4 Zusammenarbeit der deutschen Aufsichtsbehörden und auf europäischer Ebene 24

1.5 Datenschutzbeauftragte: Stellung und Aufgaben nach neuem Recht 26

1.6 Neue Verfahren nach der DS-GVO: Akkreditierung und Zertifizierung 29

1.7 Neue Sanktionsmöglichkeiten nach der DS-GVO: Praxis in NRW . 31

2. Internet und Medien **32**

2.1 Die ePrivacy-Verordnung – Aktueller Stand und Ausblick 32

2.2 Facebook-Fanpages – Gemeinsame Verantwortlichkeit von Facebook und Fanpage-Betreiberinnen und -Betreibern 35

2.3 Einbindung von Social Plugins auf Websites 38

3. Weiterhin Unsicherheiten im internationalen Datenverkehr **40**

4. Datenschutz und Kraftfahrzeuge **43**

4.1 Fahrerbewertungsportale – Bewertung von Privatpersonen im Internet (Fortsetzung aus dem 23. Bericht). 43

4.2 Automobilwerkstätten und -hersteller 44

4.3 Trotz Zulassung als Beweismittel im Einzelfall: Dauerhafter Einsatz von Dashcams weiterhin unzulässig! 48

5. Wirtschaft 49

5.1 Verhaltensregeln der deutschen Wirtschaftsauskunfteien zu Prüf- und Löschfristen 49

5.2 Prüfung von Inkassounternehmen 51

5.3 Identitätsprüfung beim Online-Banking 54

6. Datenschutz im Verein und Ehrenamt nach der DS-GVO 57

7. Datenschutz am Arbeitsplatz 59

7.1 Digitalisierte Personalakten in der Landesverwaltung 59

7.2 Beschwerdemanagement im öffentlichen Personennahverkehr (ÖPNV) – Recht auf Auskunft der beschäftigten Fahrerinnen und Fahrer 61

7.3 Kopien von Personalausweisen und Pässen zum Nachweis der Einhaltung des Arbeitnehmerüberlassungsgesetzes nicht erforderlich 63

7.4 Satellitengestützte Ortung zur Positionsbestimmung von Firmenfahrzeugen – kein zulässiges Mittel für eine Überwachung von Beschäftigten 65

7.5 Videoüberwachung im Beschäftigtenverhältnis 67

8. Beratung öffentlicher Stellen in Fragen des Datenschutzes 70

9. Innere Sicherheit und Justiz 71

9.1 Änderungen bereichsspezifischer Gesetze im Sicherheits- und Justizbereich 71

9.2 Entschließungen der Datenschutzkonferenz zum Datenschutz im Sicherheitsbereich 74

9.3 Ausweitung der Videoüberwachung durch die Polizei 76

9.4 Überprüfung von Datenspeicherungen im Zusammenhang mit dem G-20-Gipfel im Juli 2017 in Hamburg 78

10. Gesundheit und Soziales 79

10.1 Informationen der Heilberufskammern zur Anwendung der DS-GVO in der ambulanten Versorgung 79

10.2 Verfahren der Gutachterkommission bei den Ärztekammern und der Haftpflichtversicherer 80

10.3 Gültigkeitsdauer einer Einverständniserklärung zur Rechnungserstellung durch eine Abrechnungsgesellschaft 81

10.4 Rezeptbestellungen mittels WhatsApp 82

11. Datensicherheit 84

11.1 Meldungen von Datenschutzverstößen nach Art. 33 DS-GVO 84

11.2 Sicherheitslücken in Onlineshop-Software 86

11.3 Digitale Erpressung – jetzt auch analog 87

2. Teil: Informationsfreiheitsbericht 89

Überblick 90

1. Bundesverfassungsgericht (BVerfG): Informationsfreiheit hat Verfassungsrang! 92

2. Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) 93

3. Informationsfreiheitsrechtliche Beratung und Schulung durch die LDI NRW 94
4. Die Grenzen der Informationsfreiheit 95
5. Zivilrechtlich geschlossene Verträge unterfallen dem Informationsfreiheitsgesetz NRW (IFG NRW) 97
6. Auslagenerhebung ohne gesetzliche Grundlage 98
7. Befugnisse der Informationsfreiheitsbeauftragten durch Gesetzesreform beschnitten 99
8. Reformbedarf des Informationsfreiheitsgesetzes NRW (IFG NRW). 100

Anhang zum Datenschutzbericht 102

Presseinformation der LDI NRW vom 29. März 2018 – Datenschutz-Grundverordnung im Verein 103

Entschließungen der Datenschutzkonferenz 2017/2018 107

Entschließungen zwischen den Konferenzen 2017/2018 118

Beschlüsse der Datenschutzkonferenz 125

Pressemitteilung der Vorsitzenden der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder 135

Anhang zum Informationsfreiheitsbericht 137

Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland 138

Entschließungen der Informationsfreiheitsbeauftragten der Länder 140

Vorwort

Der Berichtszeitraum des 24. Datenschutz- und Informationsfreiheitsberichtes für die Jahre 2017 und 2018 war wesentlich vom Reformprozess auf der EU-Ebene geprägt: Bis zum 25. Mai 2018 galt es, den Übergangszeitraum für die Anpassung des nationalen Rechts an die Datenschutz-Grundverordnung (DS-GVO) zu nutzen. Daneben gibt seit Mai 2018 die Datenschutzrichtlinie im Bereich Justiz und Inneres (JI-RL) Mindeststandards für Polizei und Justiz vor, die alle Mitgliedsstaaten in ihrem nationalen Recht einhalten müssen. Die DS-GVO und die JI-RL bilden somit seit Mai 2018 den gemeinsamen neuen Datenschutzrahmen in der Europäischen Union.

Neben der Anpassung der landesrechtlichen Vorschriften, bei der wir Landesregierung und Landtag beraten haben, waren auch Behörden, Unternehmen und Vereine sowie die betroffenen Personen auf die neuen Regeln vorzubereiten. Nicht zuletzt mussten auch wir uns als Aufsichtsbehörde auf die neue Situation einrichten und die Zusammenarbeit mit deutschen und europäischen Aufsichtsbehörden neu regeln.

Die letzten sieben Monate des Berichtszeitraumes standen dann im Zeichen der ersten Erfahrungen mit dem neuen Recht.

Der Anspruch des EU-Datenschutzrechts ist hoch: Es geht einerseits um stärkere Datenschutzrechte der Bürgerinnen und Bürger in der Europäischen Union. Auf der anderen Seite soll der freie Verkehr personenbezogener Daten in einer der größten Volkswirtschaften der Welt weder eingeschränkt noch verboten werden.

Es ist noch zu früh, um zu beurteilen, wie sich das neue Recht in diesem Spannungsverhältnis bewährt. Offenkundig hat die Reform jedenfalls eine breite Debatte über das Thema Datenschutz entfacht, im öffentlichen Raum aber auch im privaten Umfeld, wie beim Arztbesuch, in Kindergärten und Schulen und nicht zuletzt in Vereinen.

So erfreulich es auch ist, dass dieses wichtige grundrechtsrelevante Thema im Fokus steht, so unerfreulich ist es, dass der Datenschutz dabei in Misskredit geraten ist. Sein Image hat gelitten, auch durch eine gewisse Polemik und Panikmache in der öffentlichen Debatte. Die Komplexität der Verordnung, die Sorge vor hohen Sanktionen sowie vereinzelt auch Nachholbedarf in Sachen Datenschutz, hat viele verunsichert, die beim Umgang mit persönlichen Daten Dritter Verantwortung tragen.

Auch wenn manches kompliziert und überreguliert erscheinen mag: Datenschutz ist wichtig und schützt davor, ungewollt zum Gegenstand von Ausforschungen und Manipulationen zu werden. Im Fokus des Datenschutzes stehen vor allem diejenigen, bei denen die Datenverarbeitung mit großen Risiken verbunden ist. Zwar müssen die neuen Regelungen von allen eingehalten werden, aber bei kleinen und mittleren Unternehmen sowie Vereinen sind die Verarbeitungsrisiken viel geringer als

etwa bei internationalen Konzernen. Daran orientiert sich auch die Datenschutzaufsicht.

Die Digitalisierung ist ein wichtiger technischer und vor allem auch gesellschaftlicher Prozess, bei dessen Verwirklichung die Nutzung personenbezogener Daten eine zentrale Rolle spielt. Ein hoher Standard beim Datenschutz sollte deshalb gesellschaftlicher Konsens sein, und zwar auch unabhängig von vorübergehenden Empörungen über Datenskandale wie zuletzt Facebook und Cambridge Analytica.

Der erste Berichtsteil beleuchtet datenschutzrechtliche Entwicklungen im Berichtszeitraum und stellt an Hand von Beispielen die Praxis unserer Tätigkeit dar. Wir wurden von einer großen Fülle von Beratungsanfragen und Beschwerden geradezu überrollt. Eine zeitnahe Bearbeitung war unter den gegebenen Umständen kaum möglich und anlasslose Schwerpunktprüfungen mussten zurückstehen.

Der zweite Berichtsteil nimmt den Umgang mit dem Recht auf Informationszugang und den Handlungsbedarf für eine Fortentwicklung des Informationsfreiheitsgesetzes in den Blick.

Der vorliegende Bericht ist der letzte, der in dieser Form einen Zeitraum von zwei Jahren abdeckt, da die DS-GVO die Aufsichtsbehörden verpflichtet, in Zukunft jährlich über ihre Tätigkeit zu berichten. Für den Bericht zur Informationsfreiheit wird es dagegen beim zweijährigen Zyklus bleiben.

Mein Dank gilt den Abgeordneten des Landtages, die meiner Behörde eine angemessene Ausstattung ermöglicht haben.

Besonders danke ich meinen Mitarbeiterinnen und Mitarbeitern für ihren Einsatz trotz schwieriger Rahmenbedingungen und für ihre Bereitschaft, sich den neuen Herausforderungen zu stellen. Dies gilt in besonderem Maße für die Bewältigung der vielen Beratungsanfragen und die Unterstützung beim NRW-Vorsitz der Datenschutzkonferenz im Jahr 2018.

Helga Block

Frühjahr 2019

1. Teil: Datenschutzbericht

Überblick

- **EU-Datenschutzreform**

Ab dem 25. Mai 2018 waren die Datenschutz-Grundverordnung (DS-GVO) sowie das neue Bundesdatenschutzgesetz und zahlreiche neue Ländergesetze als unmittelbar geltendes Recht anzuwenden. Vorausgegangen waren umfassende **Beratungen** auf Landesebene und – gemeinsam mit den anderen Aufsichtsbehörden – auf der Ebene Europas und des Bundes.

Auf Bundesebene wurde das neue **Bundesdatenschutzgesetz** an die DS-GVO angepasst und die Datenschutz-Richtlinie im Bereich Justiz und Inneres (JI-RL) umgesetzt. Zum Regierungsentwurf haben wir konkrete Änderungen vorgeschlagen. Dessen ungeachtet wurde im Ergebnis das Datenschutzniveau gegenüber der bis zum Mai 2018 geltenden Rechtslage in einigen Bereichen herabgesetzt. Manche der neuen Regelungen erscheinen auch mit den europarechtlichen Vorgaben nicht vereinbar, so dass ihre Anwendbarkeit in der Praxis in Frage steht. Siehe hierzu unter 1.2.

Ein wichtiger Baustein im Reformprozess steht noch aus: die **ePrivacy-Verordnung**. Sie soll die ePrivacy-Richtlinie aus dem Jahr 2002 ersetzen und die DS-GVO im Hinblick auf die elektronische Kommunikation präzisieren und ergänzen. Sie wird jedoch voraussichtlich nicht vor 2020 in Kraft treten. Nach der Positionierung der Datenschutzkonferenz können die Datenschutzregelungen des Telemediengesetzes seit dem 25. Mai 2018 nicht mehr angewendet werden. Stattdessen gelten für die Verarbeitung personenbezogener Daten durch nicht-öffentliche Dienstanbieter vorrangig die Regelungen der DS-GVO. Damit ist ein hohes Schutzniveau für die personenbezogenen Daten der Nutzerinnen und Nutzer von Telemedien gewährleistet. Siehe hierzu unter 2.1.

Auch auf der Landesebene stellen die Anpassung des Rechts an die Vorgaben der DS-GVO und die Umsetzung der JI-RL eine umfangreiche Aufgabe für den Gesetzgeber dar. Das neue **Datenschutzgesetz NRW** enthält die allgemeinen Vorschriften für die öffentlichen Stellen des Landes. Wir haben hierzu umfangreich beraten, jedoch wurden nicht alle unsere Kritikpunkte ausgeräumt: Einige der getroffenen Regelungen sind nach unserer Einschätzung europarechtlich fragwürdig und werden dem postulierten Ziel des Gesetzgebers, das bisherige Datenschutzniveau zu erhalten, nicht immer gerecht. Dies betrifft insbesondere die Neuregelung der Videoüberwachung und das Schutzniveau im Bereich der Forschung. Siehe hierzu unter 1.3.

Auch zu weiteren Landesgesetzen haben wir umfangreich beraten. Siehe hierzu unter 1.3 sowie zu den bereichsspezifischen Gesetzen im Sicherheits- und Justizbereich unter 9.1. Dies betrifft das **Polizeigesetz NRW**, das **Verfassungsschutzgesetz NRW** sowie das neu geschaffene J**ustizvollzugsdatenschutzgesetz**. Im Zuge unserer Beteiligung im Gesetzgebungsverfahren konnten zwar Verbesserungen erreicht werden. Es sind jedoch Regelungen ver-

blieben, die wir kritisch sehen. Problematisch ist aus unserer Sicht unter anderem die Einführung der Quellen-Telekommunikationsüberwachung im Polzeigesetz NRW. Kritikwürdig ist auch die neu geschaffene Regelung im Verfassungsschutzgesetz, wonach die Kontrollmöglichkeit der LDI NRW nunmehr unter erleichterten Voraussetzungen von der Verfassungsschutzbehörde selbst eingeschränkt werden kann.

- **Beratung öffentlicher Stellen**

Die Beratung öffentlicher Stellen bei der Verarbeitung personenbezogener Daten ist uns ein wichtiges Anliegen. Auch hier war die Nachfrage angesichts der neuen EU-Datenschutzregeln groß. Neben unseren Handreichungen zum neuen Recht wurden auch unsere Informationsveranstaltungen in Kooperation mit den Kommunalen Spitzenverbänden positiv aufgenommen. Siehe hierzu unter 8.

- **Datenschutz und Wirtschaft**

Die bisher für Unternehmen einschlägigen Regelungen des deutschen Datenschutzrechts wurden weitgehend durch die DS-GVO ersetzt, ergänzt durch nationale Regelungen des Bundesdatenschutzgesetzes. Der Beratungsbedarf für die Auslegung und Anwendung in der Praxis ist und bleibt hoch, abhängig von Branche und Unternehmensgröße bei Grundsatzfragen, aber auch bei sehr komplexen datenschutzrechtlichen Detail- und Einzelfragen.

Neben unserer täglichen Beratungspraxis haben wir zu häufig angefragten Themen aus dem Bereich der Wirtschaft auf unserer Homepage informiert. Veröffentlichungen gibt es etwa zu folgenden Themen:

- Informationspflichten nach der Datenschutz-Grundverordnung
- Datenverarbeitung in Inkassounternehmen
- Fotografien außerhalb des Journalismus

Daneben finden sich zahlreiche weitere Hinweise auf unserer Homepage, die zum Teil mit den anderen Aufsichtsbehörden innerhalb der Datenschutzkonferenz abgestimmt wurden und somit in diesem Rahmen eine einheitliche Handhabung gewährleisten. Zudem haben wir auf zahlreichen Veranstaltungen für Multiplikatoren sowie mit Fachvorträgen zur Anwendung der DS-GVO informiert.

- **Verhaltensregeln / „Codes of Conduct“ nach Art 40 DS-GVO**

Pünktlich zum Start der DS-GVO hat die LDI NRW am 25. Mai 2018 die **Verhaltensregeln des Verbandes „Die Wirtschaftsauskunfteien e.V.“ zum Thema Prüf- und Löschfristen von personenbezogenen Daten** genehmigt.

Solche „Codes of Conduct“ (CoC) sind ein wichtiges Instrument der Selbstregulierung der Wirtschaft bei der Konkretisierung allgemein gehaltener Normen. Der CoC der Wirtschaftsauskunfteien, dem sich alle großen deutschen Wirtschaftsauskunfteien unterworfen haben, wird zu einer höheren Rechtssicherheit sowohl für Verbraucherinnen und Verbraucher als auch für Auskunfteien beitragen. Siehe hierzu unter 5.1.

- **Datenschutz und Kraftfahrzeug**

Moderne Kraftfahrzeuge generieren eine große Anzahl von personenbezogenen Daten. Eine **Prüfung** der LDI NRW kam zu dem Ergebnis, dass die datenschutzrechtliche Verantwortlichkeit zwischen Automobilwerkstätten und Automobilherstellern noch nicht abschließend geklärt ist. Abzusehen ist schon jetzt: Mit verstärkter Elektromobilität wird auch die Datensammlung steigen. Siehe hierzu unter 4.2.

- **Verein und Ehrenamt**

Die Berichterstattung zur DS-GVO veranlasste viele Vereine, sich mit Anfragen an die LDI NRW zu wenden. Obwohl die DS-GVO gegenüber der bisherigen Rechtslage nur wenige wesentliche Änderungen für die Vereine mit sich brachte, war die Verunsicherung groß. Dies führte zu einem enormen Anstieg der Beratungsanfragen von Vereinen. Neben der Beratung im Einzelfall haben wir auf Veranstaltungen und mit Vorträgen informiert. Zudem haben wir den praxisorientierten **Ratgeber „Datenschutz im Verein nach der DS-GVO“** veröffentlicht. Siehe hierzu unter 6.

- **Innere Sicherheit**

Im Sicherheitsbereich waren auf Bundes- und Europaebene einige für die Balance zwischen Sicherheit und Freiheit bedenkliche Entwicklungen festzustellen. Die Datenschutzkonferenz hat sich dazu in mehreren Entschließungen positioniert. Ein wiederholt kritisierter Punkt waren dabei neuartige Eingriffe durch die Sicherheitsbehörden ohne darauf zugeschnittene spezielle Ermächtigungsgrundlagen. Siehe hierzu unter 9.2.

Neben Beratungen bei **Änderungen bereichsspezifischer Gesetze im Sicherheits- und Justizbereich in NRW** (siehe hierzu unter 9.1) haben wir die Ausweitung der polizeilichen Videoüberwachung überprüft. Wir sehen die Ausweitung der Videoüberwachung durch die Polizei zwar weiterhin grundsätzlich kritisch. In der praktischen Umsetzung zeigten sich die Polizeibehörden jedoch aufgeschlossen gegenüber unseren Hinweisen. Siehe hierzu unter 9.3.

- **Datenschutz am Arbeitsplatz**

Videotechnik wird immer günstiger, verfügbarer und technisch ausgefeilter. Auch die Nutzung moderner Ortungssysteme zur Positionsbestimmung etwa von Fahrzeugen nimmt zu. Gerade im Arbeitsverhältnis sind dem Einsatz jedoch Grenzen gesetzt, die wir regelmäßig aufzeigen müssen. Siehe hierzu unter 7.4 und 7.5.

- **Zahlen und Fakten**

Eingaben

Im Jahr 2018 hat uns – wie auch andere Aufsichtsbehörden – mit der Geltung der DS-GVO eine bislang nie dagewesene Flut von Eingaben erreicht. Nachdem die Zahl der Eingaben in den Jahren 2016 und 2017 konstant bei etwa 4.400 lagen, haben sich die Eingaben im Jahr 2018 fast verdreifacht: Mit etwa **12.000** schriftlichen Eingaben sind wir dabei an unsere Grenzen gestoßen. In dieser Zählung sind die zahlreichen telefonischen Anfragen nicht enthalten, die wir zusätzlich zu bewältigen hatten. An manchen Tagen waren die Kolleginnen und Kollegen fast ausschließlich mit telefonischen Beratungen beschäftigt.

Wir bemühen uns, jedes Anliegen im Rahmen der vorhandenen Kapazitäten zu bearbeiten, eine zeitnahe Erledigung ist dabei aber oft nicht mehr leistbar. Wir sind gezwungen, nach der Schwere der geltend gemachten Verstöße und dem Risiko der Datenverarbeitung Prioritäten zu setzen. Bei unvermeidbaren längeren Bearbeitungszeiten müssen wir auf das Verständnis und die Geduld der Anfragenden setzen.

Meldung der Datenschutzbeauftragten

Nach Art. 37 Abs. 7 DS-GVO müssen Verantwortliche und Auftragsverarbeiter die Kontaktdaten ihres Datenschutzbeauftragten den Aufsichtsbehörden mitteilen. Bei der LDI NRW kann diese Meldung online auf einem dafür eingerichteten Meldeportal erfolgen. Verantwortliche und Auftragsverarbeiter haben uns bis zum 31. Dezember 2018 etwa **22.000** Kontaktdaten online gemeldet. Siehe hierzu unter 1.5.

Meldungen von Datenpannen

Die Meldepflicht des § 42a Bundesdatenschutzgesetzes alte Fassung wurde durch Art. 33 DS-GVO ersetzt. Verletzungen des Schutzes personenbezogener Daten sind uns danach unverzüglich, möglichst binnen 72 Stunden, zu melden. Von Mai bis Dezember 2018 wurden uns mehr als **1.200** Datenpannen nach Art. 33 DS-GVO über das auf unserer Website dafür bereitgestellte Formular gemeldet. Im Vergleich zu den Vorjahren ein enormer Anstieg: Im Jahr 2017 erhielten wir **60**, im Zeitraum von Januar bis Mai 2018 erhielten wir **61** Meldungen nach § 42a Bundesdatenschutzgesetz – alte Fassung. Siehe hierzu unter 11.1.

Bußgeldverfahren

In den Jahren 2017 und 2018 haben wir **182** Bußgeldverfahren durchgeführt.

- **Informationen und Öffentlichkeitsarbeit**

Der Informationsbedarf zu Fragen des Datenschutzes war noch nie so groß. Auf unserer Internetseite www.ldi.nrw haben wir über aktuelle Entwicklungen informiert und zahlreiche Broschüren, Orientierungshilfen und Muster veröffentlicht.

Die europaweit wirkende Datenschutzreform verlangt auch in einer föderal strukturierten Datenschutzaufsicht bundeseinheitliche Informationen. Um eine einheitliche Auslegung und Anwendung der neuen Regelungen in der Praxis zu erreichen, erarbeitete die Datenschutzkonferenz 20 sogenannter **Kurzpapiere**. Sie dienen den Verantwortlichen insbesondere im nicht-öffentlichen Bereich als Orientierung. Siehe hierzu unter 1.1.

Wie alle weiteren Informationen stehen diese Auffassungen dabei unter dem Vorbehalt einer zukünftigen, möglicherweise abweichenden Auslegung des Europäischen Datenschutzausschusses.

Zudem ist die Datenschutzkonferenz im Jahr des Vorsitzes von NRW mit einem **gemeinsamen Webauftritt** online gegangen www.datenschutzkonferenz-online.de. Neben den Kurzpapieren sind auf dieser zentralen Informationsplattform auch aktuelle Entschließungen und Orientierungshilfen der Datenschutzkonferenz sowie Dokumente des Europäischen Datenschutzausschusses abrufbar. Über Links sind zudem die Aufsichtsbehörden und die Datenschutzge-

setze des Bundes und der Länder zu finden.

Wir beteiligen uns weiter am **Virtuellen Datenschutzbüro** www.datenschutz.de, das Bürgerinnen und Bürgern als erste zentrale Informations- und Anlaufstelle dient.

Insbesondere um Jugendliche zu erreichen beteiligen wir uns zudem weiterhin an der Webseite **www.youngdata.de**.

Die große Resonanz auf das neue Datenschutzrecht hat sich auch in der stark angestiegenen Zahl von **Medienanfragen** manifestiert. Uns war es dabei wichtig zu informieren und damit auch der Verunsicherung und einer gewissen Panikmache entgegenzuwirken.

- **Datenschutzkonferenz und Expertengruppen des Europäischen Datenschutzausschusses**

Im Jahr 2018 haben wir turnusgemäß den **Vorsitz der Datenschutzkonferenz** übernommen, dem Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder. Neben zwei regulären Hauptkonferenzen und sechs weiteren Sonderkonferenzen waren viele Abstimmungen und Umlaufverfahren zu organisieren und die Konferenz nach außen zu vertreten. Im Jahr der „Zeitenwende“ bot dies besondere Herausforderungen, aber auch Gestaltungsmöglichkeiten, die wir gern angenommen haben.

Am 28. Januar 2019 fand unser Vorsitz mit der von uns ausgerichteten zentralen Veranstaltung der Datenschutzkonferenz zum 13. Europäischen Datenschutztag in Berlin seinen Abschluss.

Auch im Jahr 2019 werden wir wie bisher die Arbeitskreise Wirtschaft (vormals Düsseldorfer Kreis), Statistik, Kreditwirtschaft und gemeinsam mit Hessen den Arbeitskreis Auskunfteien leiten.

Auf europäischer Ebene sind wir in der Key Provisions Expert Subgroup und Financial Matters Expert Subgroup des Europäischen Datenschutzausschusses aktiv.

- **Ausblick**

Die Arbeit der Datenschutz-Aufsichtsbehörden hat sich stark verändert.

Zum einen steigen die Beratungsanfragen, Beschwerden sowie die Meldungen von Datenpannen. Zum anderen ist eine verstärkte Zusammenarbeit und Abstimmung auf deutscher und europäischer Ebene erforderlich. Dies alles steht unter dem Vorzeichen komplexer neuer Regelungen, deren Auslegung der Gesetzgeber vielfach den Aufsichtsbehörden überlassen hat. Hinzu kommen Kontrollen und wenn nötig auch die Durchsetzung mit Sanktionen. Das Interesse am Thema Datenschutz ist gewachsen und hat somit auch die Aufsichtsbehörden verstärkt in den Mittelpunkt gerückt.

Es versteht sich von selbst, dass dies nur mit einer gut ausgestatteten Behörde effektiv bewältigt werden kann.

1. Europäische Datenschutzreform

1.1. Die Datenschutz-Grundverordnung

Seit dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DS-GVO) als unmittelbar geltendes Recht anwendbar. Sie greift bekannte Themen auf und regelt neue Aspekte.

Weiterhin gilt für das neue Datenschutzrecht: Vorsicht, aber keine Panik!

Der Anspruch der DS-GVO ist hoch: stärkere Datenschutzrechte der etwa 510 Million Bürgerinnen und Bürger auf der einen Seite. Auf der anderen Seite soll der freie Verkehr personenbezogener Daten in einer der größten Volkswirtschaften der Welt aus Gründen des Datenschutzes weder eingeschränkt noch verboten werden. Gleichzeitig erfolgte die Reform des Datenschutzrechts auch mit Blick auf die drängenden aktuellen Themen und Fragen wie etwa Digitalisierung und künstliche Intelligenz.

Wir stehen weiterhin zu Beginn der Entwicklung, diese neuen Rahmenbedingungen zum Gewohnten zu machen.

Nicht alles ist neu in der DS-GVO, viele Aspekte existierten bereits im alten Recht. Der europäische Gesetzgeber behielt sie bei und passte sie – teils umfangreich – an. Beispiele sind die Informationspflichten des Verantwortlichen gegenüber der betroffenen Person und die Datenschutz-Folgenabschätzung, deren „Vorgänger“ die sogenannte Vorabkontrolle war.

Das Informationsbedürfnis ist groß: Auf der einen Seite nehmen die Bürgerinnen und Bürger vermehrt ihre Rechte war. Es kommt auf der anderen Seite zu Verunsicherung und Missverständnissen bei denjenigen, die mit den Daten anderer umgehen, aus wohl unterschiedlichen Gründen. Der abstrakte Wortlaut der DS-GVO ist an vielen Stellen noch nicht mit Leben gefüllt, anders als wir es von den alten Regelungen, allen voran dem Bundesdatenschutzgesetz (BDSG) und dem Datenschutzgesetz NRW (DSG NRW), gewohnt waren. Auch mussten und müssen viele datenverarbeitende Stellen in Sachen Datenschutz einiges nachholen. Daneben tragen die scharfen Sanktionsmöglichkeiten der DS-GVO zur Verunsicherung bei. Eine gewisse Panikmache, die bei manchen auch zum Geschäftsmodell zu gehören scheint, hat ein Übriges getan. Eine Geldbuße ist eine von vielen Handlungsoptionen, die Beratung spielt aber weiterhin eine wichtige Rolle in unserer Tätigkeit. Wo erforderlich, werden wir auf sämtliche Möglichkeiten zurückgreifen. Ebenso stellt das Ineinandergreifen von DS-GVO, BDSG, DSG NRW und bereichsspezifischen Regelungen datenverarbeitende Stellen vor Herausforderungen. Siehe hierzu unter 1. 2 und 1.3. Die DS-GVO spricht außerdem viele Themen an, ohne sie explizit zu regeln. Insbesondere im Hinblick auf die elektronische Kommunikation muss die ePrivacy-Verordnung die DS-GVO präzisieren und ergänzen. Siehe hierzu unter 2.1.

Wir wurden gerade zu Beginn der Geltung der DS-GVO von Anfragen geradezu überflutet, sowohl mit Bitten um Bera-

tung, also auch mit Beschwerden. Siehe hierzu im Überblick unter Zahlen und Fakten.

Neben der individuellen Beratung haben wir gleichwohl Informationen zur DS-GVO fortgeführt und erweitert, um die Rechtsanwendung zu erleichtern. Darunter sind die insgesamt 20 Kurzpapiere der Datenschutzkonferenz, die praxisrelevante Themen der DS-GVO aufgreifen:

- Verzeichnis von Verarbeitungstätigkeiten
- Aufsichtsbefugnisse/Sanktionen
- Verarbeitung personenbezogener Daten für Werbung
- Datenübermittlung in Drittländer
- Datenschutz-Folgenabschätzung
- Auskunftsrecht
- Marktortprinzip
- Maßnahmenplan „DS-GVO“ für Unternehmen
- Zertifizierung nach Art. 42 DS-GVO
- Informationspflichten bei Dritt- und Direkterhebung
- Recht auf Löschung / “Recht auf Vergessenwerden“
- Datenschutzbeauftragte
- Auftragsverarbeitung
- Beschäftigtendatenschutz
- Videoüberwachung
- Gemeinsam Verantwortliche
- Besondere Kategorien personenbezogener Daten
- Risiko für Rechte und Freiheiten natürlicher Personen
- Unterrichtung und Verpflichtung von Beschäftigten.
- Einwilligung nach der DS-GVO.

Inzwischen gibt es daneben zahlreiche vertiefende Hinweise zu einzelnen Aspekten der DS-GVO und Informationen für besondere Adressaten, zum Beispiel für Vereine oder für kleine und mittlere Unternehmen.

Alle Informationen sind auf unserer Internetseite www.ldi.nrw.de abrufbar. Die Dokumente der DSK finden Sie außerdem auf www.datenschutzkonferenz-online.de.

Wir ergänzen unsere Informationen zu Themen der DS-GVO kontinuierlich. Unsere Beratung von Politik, Wirtschaft, Verwaltung und nicht zuletzt Bürgerinnen und Bürgern in NRW zu Fragen zum neuen europäischen Datenschutzrecht führen wir fort.

1.2 Anpassung auf Bundesebene

Für die Anpassung des nationalen Rechts an die Datenschutz-Grundverordnung (DS-GVO) standen dem nationalen Gesetzgeber bis zum 25. Mai 2018 zwei Jahre zur Verfügung. Die Umsetzungsfrist für die Richtlinie (EU) 2016/680 (JI-RL) lief am 6. Mai 2018 ab. Einige Bundesgesetze wurden rechtzeitig zum Mai 2018 geändert. Der Reformprozess war aber insgesamt zu umfangreich, um fristgerecht abgeschlossen zu werden. Zum Zeitpunkt der Berichtserstellung war auf Bundesebene noch ein Artikelgesetz mit Änderungen an weiteren 154 Fachgesetzen in Arbeit.

Das erste große gesetzgeberische Projekt im Rahmen der europäischen Datenschutzreform war die Novellierung des Bundesdatenschutzgesetzes (BDSG). Sie wurde bereits im Jahre 2016 mit ersten Referentenentwürfen in Angriff genommen und mündete im neuen BDSG, das am 30. Juni 2017 beschlossen wurde und am 25. Mai 2018 in Kraft trat.

Die Umsetzung der europäischen Vorgaben und Ausgestaltung der neuen Regelungen im BDSG wurde, wie bei einer derart tiefgreifenden Rechtsreform nicht anders zu erwarten, von Beginn an kontrovers diskutiert. Obwohl es sich um eine Angelegenheit handelt, die in der Gesetzgebungskompetenz des Bundes liegt, hatten auch die Länder an der Gesetzesreform von Anfang an großes Interesse (siehe 23. Bericht unter 3.3), da das Bundesdatenschutzgesetz

- Vorgaben für Unternehmen, Vereine und andere nicht-öffentliche Stellen festlegt, für deren datenschutzrechtliche Kontrolle ganz überwiegend die Aufsichtsbehörden der Länder zuständig sind, und
- zu erwarten war, dass es als Vorbild für die Landesgesetzgebung im öffentlichen Bereich herangezogen werden würde.

Daher legte die LDI NRW, ebenso wie die Aufsichtsbehörden der anderen Länder, Stellungnahmen zu den verschiedenen Entwurfsfassungen vor. Zum Regierungsentwurf vom 2. Februar 2017 (BR-Drs. 110/17) verständigten wir uns mit den anderen Landesbeauftragten auf gemeinsame Änderungsvorschläge zu den folgenden dreizehn wichtigsten Kritikpunkten an dem Gesetzentwurf:

- Unangemessene Rollenverteilung zwischen Bund und Ländern bei der Vertretung im Europäischen Datenschutzausschuss
- Zu weitgehende nationale Einschränkungen der Betroffenenrechte
- Defizite bei den Verarbeitungsbefugnissen für besondere Kategorien personenbezogener Daten, wie zum Beispiel Gesundheitsdaten
- Einschränkung der Aufsichtsbefugnisse gegenüber Berufsgeheimnisträgern
- Zu enge Voraussetzungen der Klagemöglichkeiten für die Aufsichtsbehörden gegen bestimmte Beschlüsse der Europäischen Kommission
- Fehlende Vollstreckungsbefugnisse gegenüber öffentlichen Stellen

- Zu schwache Schutzmechanismen für Verbraucherinnen und Verbraucher bei den Regelungen zu Scoring und Auskunfteien
- Unzulängliche Regelung des Beschäftigtendatenschutzes
- Überdehnung der Ausnahmemöglichkeiten für Zweckänderungen
- Mangelnde Umsetzung der Anforderungen der DS-GVO im Bereich der Forschung
- Nicht mit der DS-GVO zu vereinbarende und unsachgemäße Regelung zur Erlaubnis privater Videoüberwachungen
- Fehlende Festschreibung des Direkterhebungsgrundsatzes
- Vergleichbare und weitere Defizite (etwa der Regelung zur Einwilligung) bei der Umsetzung der JI-RL in das nationale Recht.

Die Änderungsanträge zu diesen Kritikpunkten übermittelten wir dem Innenministerium NRW im Februar 2017, verbunden mit der Bitte, sich im Bundesrat hierfür einzusetzen. Abgesehen von einigen wenigen Verbesserungen im Hinblick auf Betroffenenrechte und erlaubte Zweckänderungen wurden die gewünschten Änderungen nicht in die Endfassung des Gesetzes übernommen.

Im neuen BDSG wurde das Datenschutzniveau gegenüber der bis zum Mai 2018 geltenden Rechtslage ohne Not in einigen Bereichen deutlich herabgesetzt. Manche der neuen Regelungen erscheinen auch mit den europarechtlichen Vorgaben nicht vereinbar, so dass ihre Anwendbarkeit in der Praxis in Frage steht.

1.3 Anpassung auf Landesebene

Die europäische Datenschutzreform bringt gerade im öffentlichen Bereich zahlreiche Regelungsaufträge und -spielräume für den nationalen Gesetzgeber mit sich. Diese betreffen zu einem großen Teil die Gesetzgebungskompetenz der Länder. Auch in Nordrhein-Westfalen entstand hierdurch großer Anpassungsbedarf.

Aufgrund der Datenschutz-Grundverordnung (DS-GVO) und der Richtlinie (EU) 2016/680 (JI-RL) war der Landesgesetzgeber gefordert, das gesamte Datenschutzrecht des Landes bis zum Mai 2018 neu zu gestalten. Die notwendigen Änderungen betreffen neben dem allgemeinen Datenschutzgesetz alle bereichsspezifischen Datenschutzregeln in einer Vielzahl von Landesgesetzen (siehe 23. Bericht unter 3.4). Hierzu haben wir der Landesregierung in unserem Eckpunktepapier vom April 2017 umfangreiche Hinweise zukommen lassen.

Ein wichtiger Schwerpunkt der Änderungen im Landesrecht war das „Nordrhein-Westfälische Datenschutz-Anpassungs- und Umsetzungsgesetz EU“ (NRWDSAnpUG-EU), das am 25. Mai 2018 in Kraft trat. Mit diesem Gesetz wurden das Datenschutzgesetz NRW (DSG NRW) und elf weitere Landesgesetze aus dem Geschäftsbereich des Innenministeriums infolge der europäischen Normen geändert.

Daneben wurden in weiteren Änderungsgesetzen fachspezifische Anpassungen durchgeführt.

Auch mehr als ein halbes Jahr nach Ablauf der Frist sind zum Zeitpunkt der Berichtserstellung noch weitere Änderungsvorhaben in Arbeit, und es dürfte im Hinblick auf die Vielzahl bereichsspezifischer Datenschutzregelungen in NRW auch darüber hinaus noch weiterer Anpassungsbedarf bestehen.

Wichtig für die Rechtsanwendung ist, dass im Anwendungsbereich der DS-GVO das DSG NRW und die Datenschutzbestimmungen der anderen Landesgesetze nun immer zusammen mit der DS-GVO gelesen werden müssen.

Das neue Landesdatenschutzgesetz

Das neue DSG NRW enthält die allgemeinen Vorschriften für die öffentlichen Stellen des Landes. Hierzu gehören nicht nur die Durchführungsbestimmungen zur DS-GVO, sondern auch die Vorschriften zur Umsetzung der JI-RL für den Bereich der Gefahrenabwehr, Strafverfolgung und Strafvollstreckung in Teil 3 des Gesetzes. Siehe hierzu unter 9.1.

In Beratungen und Stellungnahmen gegenüber dem Innenministerium und der Landesregierung konnte die LDI NRW bereits im Vorfeld der Landtagsbefassung einige Änderungen der Entwürfe zum DSG NRW initiieren. Ziel war dabei, das bisherige Datenschutzniveau zumindest zu erhalten, wenn nicht im Sinne der DS-GVO anzuheben. Auch wenn dieses Ziel nach der Entwurfsbegründung von der Landesregierung geteilt wurde, so enthielt doch insbesondere der Ende April in den Landtag eingebrachte Regierungsentwurf (LT-Drs. 17/11981) einige in dieser Hinsicht problematische Regelungen (siehe hierzu

unsere Stellungnahme an den Landtag vom 12. April 2018 (Landtag-Stellungnahme 17/508).

Besondere Bedeutung hatten dabei die folgenden Kritikpunkte, die auch nach Abschluss der Beratung nicht ausgeräumt wurden:

- Die Neuregelung der Videoüberwachung (§ 20 DSG NRW) erweitert – entgegen der ausdrücklichen Empfehlung der LDI NRW – die erlaubten Zwecke der Videoüberwachung um den „Schutz des Lebens, der Gesundheit, des Eigentums oder Besitzes“. Hierdurch könnte möglicherweise der Eindruck entstehen, dass die Befugnisse zur Videoüberwachung im Ergebnis stark ausgeweitet wurden. Dies ist jedoch nicht der Fall. Vielmehr muss die Videoüberwachung nach § 20 Abs. 1 DSG NRW zu einem der genannten Zwecke „erforderlich“ sein, und es dürfen zudem „keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen“. Diesen beiden maßgeblichen Einschränkungen des Einsatzes von Videokameras kommt bei der Prüfung der Rechtmäßigkeit der Maßnahme hohe Bedeutung zu. Im Ergebnis ist damit sicherzustellen, dass das bisherige hohe Datenschutzniveau erhalten bleibt.

- Eine deutliche Minderung des bisherigen Schutzniveaus ist im Bereich der Forschung zu verzeichnen (siehe § 17 DSG NRW). Insbesondere wird die Forschung auch im Hinblick auf die Verarbeitung von personenbezogenen Daten besonderer Kategorien im Sinne des Art. 9 DS-GVO – zum Beispiel von Gesundheitsdaten – deutlich erleichtert. Sogar eine Veröffentlichung derartiger Daten soll künftig nach Abwägung des öffentlichen Interesses mit den Belangen der Betroffenen auch ohne oder gar gegen deren Willen zulässig sein. Außerdem werden in dieser Vorschrift, die auch für den Bereich der Statistik gilt, die Rechte der Betroffenen auf Auskunft, Berichtigung und Einschränkung der Verarbeitung ihrer Daten sowie ihr Widerspruchsrecht (Art. 15, 16, 18 und 21 DS-GVO) ohne Not eingeschränkt. Bisher sind in der aufsichtsbehördlichen Praxis keine Fälle bekannt geworden, die solche Ausnahmeregelungen rechtfertigen könnten. Im Gegenteil: Auskunftsrechte können etwa die Akzeptanz bei den Betroffenen erhöhen und Berichtigungsansprüche können die Datenqualität durch korrekte statistische Angaben sichern.

- Eine weitere gravierende Verschlechterung stellt die Beschränkung unserer Untersuchungsbefugnisse gegenüber sogenannten Berufsgeheimnisträgern (zum Beispiel Ärzten, Rechtsanwälten, Psychologen, Sozialarbeitern) dar (§ 27 Abs. 3 DSG NRW). Das gilt auch für Teil 3 des Gesetzes, für den die Regelung über § 60 Abs. 1 Satz 2 DSG NRW entsprechend anwendbar ist. Eine Kontrolle in diesen Bereichen ist danach nur noch sehr eingeschränkt möglich, obwohl hier ein besonders hoher Schutzbedarf besteht: Sogar bei Anhaltspunkten für gravierende Verstöße können wir

nicht mehr effektiv von Amts wegen ermitteln. Auch bei einem Untersuchungsbegehren uns namentlich bekannter Betroffener kann unserem Zugangsrecht die Geheimhaltungspflicht gegenüber anderen, namentlich nicht bekannten Betroffenen entgegengehalten werden. Ein sachlicher Grund für diese Einschränkung besteht nicht: Die Geheimhaltungsinteressen der Betroffenen sind bereits hinreichend gewahrt durch die Verschwiegenheitspflicht der Mitglieder der Aufsichtsbehörden nach Art. 54 Abs. 2 DS-GVO. Zudem ist es unsere Aufgabe, gerade die Einhaltung der Verschwiegenheitspflichten und des rechtmäßigen Umgangs mit sensiblen Daten zu überprüfen.

- Mit der neuen Einführung eines „Kunst- und Literaturprivilegs“ für öffentliche Stellen (§ 19 DSG NRW) wurde ein sehr weitreichender Ausnahmetatbestand mit einem unklaren Anwendungsbereich geschaffen. Der Bedarf für eine derartige, dem Medienprivileg nachgebildete Ausnahme für öffentliche Stellen wurde nicht deutlich gemacht. Ausnahmeregelungen für künstlerische und literarische Zwecke wären nach Art. 85 DS-GVO aber nur zulässig, wenn und soweit sie erforderlich wären, um den Schutz personenbezogener Daten mit dem Recht auf freie Meinungsäußerung in Einklang zu bringen.

Außerdem liegt dem DSG NRW ein von unserer Einschätzung teilweise abweichendes Verständnis über die Regelungsspielräume und Regelungsaufträge der DS-GVO für den nationalen Gesetzgeber zugrunde. So genügt es an den Stellen, an denen die DS-GVO nationale Maßnahmen für bestimmte Zwecke erlaubt – wie Art. 23 für die Einschränkung der Betroffenenrechte – nicht, wenn der Landesgesetzgeber Regelungen trifft, die lediglich die erlaubten Zwecke wiederholen. Ähnlich unzureichend sind aus unserer Sicht die Regelungen, die im Bereich der zulässigen Zweckänderungen und der Ausnahmeerlaubnisse für die Verarbeitung besonderer Kategorien personenbezogener Daten getroffen wurden.

Auch hat der Landesgesetzgeber keine ausreichenden Maßnahmen getroffen, um die Pflicht zur wirksamen nationalen Durchsetzung des europäischen Rechts zu erfüllen:

- Beispielsweise fehlt es entgegen Art. 58 Abs. 5 DS-GVO und Art. 47 Abs. 5 JI-RL bisher an einer Befugnis der LDI NRW, gerichtliche Verfahren einleiten zu können, um überprüfen zu lassen, ob das Verhalten von Verantwortlichen und Auftragsverarbeitern datenschutzgerecht war oder ist. Dies betrifft insbesondere Fälle, in denen wir von unseren Anordnungsbefugnissen Gebrauch gemacht haben, die jeweilige Behörde dieser Anordnung jedoch nicht nachkommt. Mangels wirksamer Mittel der Verwaltungsvollstreckung sollten wir jedenfalls die Möglichkeit haben, die Rechtmäßigkeit der eigenen Anordnung gerichtlich bestätigen zu lassen. Eine entsprechende Regelung ist beispielsweise im Datenschutzgesetz Hessen enthalten.

- Zum 3. Teil des DSG NRW (Umsetzung der JI-RL) ist grundsätzlich anzumerken, dass die Umsetzung der Richtlinie, soweit konkrete Anforderungen an die Datenverarbeitung gestellt werden, in einer bereichsspezifischen Norm sinnvoller wäre. Vorzugswürdig wäre daher ein Verfahren gewesen, in dem im ersten Schritt bereichsspezifische Normen geändert werden, um dann im zweiten Schritt verbliebene allgemeine Auffangregelungen im DSG NRW zu verorten. Dies gilt insbesondere für Ermächtigungsgrundlagen zur Datenverarbeitung und für Regelungen zu Zweckänderungen (beispielsweise §§ 3, 39 und 45 DSG NRW).

- Die in Umsetzung der JI-RL geschaffenen Untersuchungs- und Abhilfebefugnisse der LDI NRW entsprechen den Vorgaben der JI-RL bisher nicht. Zwar enthält Teil 3 des DSG NRW die Befugnisse, die in Art. 47 Abs. 2 JI-RL namentlich genannt sind. Art. 47 JI-RL enthält jedoch ausdrücklich nur eine beispielhafte und keinesfalls eine abschließende Aufzählung. Tatsächlich gibt Art. 47 JI-RL vor, dass in den Mitgliedstaaten wirksame Untersuchungs- und Abhilfebefugnisse zu schaffen sind. Das bedeutet, dass den Aufsichtsbehörden sämtliche Befugnisse an die Hand zu geben sind, die für einen wirksamen und effizienten Schutz der Rechte der betroffenen Personen erforderlich sind. Hierzu gehören weitere Anordnungsrechte, wie beispielsweise das Recht, den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen zu benachrichtigen. Auch fehlt das Recht der Beanstandung für den Justiz- und Polizeibereich, das noch im DSG NRW – alte Fassung enthalten war. Dies würde uns eine im Vergleich zur Anordnung mildere und dennoch deutliche Handlungsmöglichkeit gegenüber den Polizei- und Justizbehörden geben, bevor wir eine für die verantwortliche Stelle eingriffsintensivere Anordnung erlassen müssen. Diese Flexibilität der LDI NRW hinsichtlich der Handlungsmöglichkeiten käme somit auch den betroffenen Stellen zu Gute.

Weitere Landesgesetze

Nach altem wie neuem Recht (§ 27 Abs. 5 Satz 2 DSG NRW in Verbindung mit Art. 57 Abs. 1 Buchstabe c) DS-GVO) hat eine frühzeitige Unterrichtung der LDI NRW in den dort genannten Fällen zu erfolgen. Diesem Postulat entsprechend wurde die LDI NRW nicht nur zu den besonderen Gesetzgebungsvorhaben im Bereich von Justiz und innerer Sicherheit beteiligt (siehe hierzu unter 9.1), sondern auch hinsichtlich der Anpassung des Meldegesetzes NRW, des E-Governmentgesetzes NRW, des Abschiebungshaftvollzugsgesetzes NRW und des Hochschulgesetzes NRW. Viele Anregungen der LDI NRW wurden dabei berücksichtigt.

Auch im Bereich von Rundfunk und Medien waren umfangreiche gesetzgeberische Aktivitäten zu verzeichnen, die wir intensiv begleiteten (siehe unsere Stellungnahme an den Landtag vom 1. März 2018 zum 16. Rundfunkänderungsgesetz, LT-Drs. 17/1565 (Landtag-Stellungnahme 17/400). Diese betrafen

den Rundfunkstaatsvertrag sowie Landespresse-, Landesmedien- und WDR-Gesetz. Die dabei getroffenen ausdrücklichen Regelungen des Medienprivilegs erscheinen inhaltlich zu weit und beachten nicht die Anforderungen des Art. 85 DS-GVO, die die Datenschutzbeauftragten des Bundes und der Länder formuliert haben (siehe Entschließung der Datenschutzkonferenz „Umsetzung der DS-GVO im Medienrecht“ vom 9. November 2017, Abdruck im Anhang). Neu ist zum Beispiel, dass dieses Medienprivileg nun auch „sonstigen Anbietern von Telemedien“ zustehen soll, die weder zum Bereich des Rundfunks noch zu dem der Presseunternehmen zu zählen sind. Die Kontrollzuständigkeit wurde für die Bereiche des öffentlichen und des privaten Rundfunks und der journalistisch-redaktionellen Telemedien jeweils einer neuen, speziellen Aufsichtsbehörde zugewiesen. Für den WDR und seine Beteiligungsunternehmen ist dies „die oder der WDR-Rundfunkdatenschutzbeauftragte“. Für die Landesanstalt für Medien (LfM) sowie für die privaten Rundfunkveranstalter einschließlich ihrer Beteiligungsunternehmen und für die journalistisch-redaktionellen Telemedien ist „die oder der Datenschutzbeauftragte der LfM“ zuständig. Die von der DS-GVO geforderte unabhängige Stellung dieser neuen Aufsichtsbehörden ist zumindest fraglich.

Im Rahmen der weiteren laufenden Vorhaben zur Anpassung des Landesrechts waren wir zum Zeitpunkt der Berichtserstellung unter anderem an den Arbeiten zum Landeskrebsregistergesetz, zum Landesheilberufegesetz und zum Landesstatistikgesetz beteiligt.

Die Anpassung des Landesrechts an die Vorgaben der DS-GVO und die Umsetzung der JI-RL stellen eine umfangreiche Aufgabe für den Gesetzgeber dar, die eigentlich schon im Mai 2018 hätte abgeschlossen sein müssen. Manche der getroffenen Regelungen sind europarechtlich fragwürdig und werden dem postulierten Ziel des Gesetzgebers, das bisherige Datenschutzniveau zu erhalten, leider nicht immer gerecht.

1.4 Zusammenarbeit der deutschen Aufsichtsbehörden und auf europäischer Ebene

Die Datenschutz-Grundverordnung (DS-GVO) bestimmt Verfahren für eine europäische Meinungsbildung und Entscheidungsfindung der Datenschutzaufsichtsbehörden. Das Bundesdatenschutzgesetz (BDSG) enthält ergänzende Rahmenbedingungen für die Abstimmungen innerhalb Deutschlands.

Die DS-GVO hat das Ziel, dass das einheitliche europäische Recht in den Mitgliedstaaten auch einheitlich angewendet wird. Da die Regelungen der DS-GVO oft allgemein gehalten und die Rechtstraditionen der Mitgliedstaaten unterschiedlich sind, haben nun die Aufsichtsbehörden die Aufgabe, das neue Recht in der Interpretation und in der Praxis zu harmonisieren. Dazu müssen sich die Aufsichtsbehörden der Mitgliedstaaten abstimmen und – teils verbindliche – Rechtsauffassungen entwickeln.

Die Meinungsbildung der europäischen Aufsichtsbehörden findet in Abstimmungsverfahren der betroffenen Behörden untereinander und im Europäischen Datenschutzausschuss (EDSA) statt. Der EDSA löste die Artikel-29-Gruppe als Arbeitsgremium der europäischen Aufsichtsbehörden ab. In der Vollversammlung des EDSA (Plenum) werden die deutschen Aufsichtsbehörden durch den gemeinsamen Vertreter, den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), vertreten. Im Plenum werden beispielsweise Leitlinien oder Stellungnahmen des EDSA verabschiedet und verbindliche Beschlüsse in streitigen grenzüberschreitenden Fällen gefasst. Stellvertreter des gemeinsamen Vertreters ist eine Leiterin oder ein Leiter der Aufsichtsbehörde eines Landes.

In § 17 Abs. 1 BDSG ist geregelt, dass dieser vom Bundesrat für die Dauer von 5 Jahren gewählt wird und eine Wiederwahl zulässig ist. Diese Regelung wurde von der Datenschutzkonferenz kritisch begleitet, da sie es als ihre Aufgabe ansieht, den Stellvertreter im EDSA selbst zu bestimmen. Abgesehen davon ist bei der praktischen Handhabung dieser kritikwürdigen Regelung sehr bedauerlich, dass es dem Bundesrat bisher – jedenfalls bis zum Redaktionsschluss dieses Berichtes – noch nicht gelungen ist, diese Wahl zu vollziehen. Das BDSG ist immerhin – wie die DS-GVO – seit dem 25. Mai 2018 anzuwenden.

Der EDSA, der am 25. Mai 2018 seine Arbeit aufgenommen hat, bereitet seine Entscheidungen in Arbeitsgruppen (Expert Subgroups) vor, an denen Deutschland, jeweils durch den BfDI und durch Ländervertreter, beteiligt ist. Wie schon bei den nach der Datenschutzrichtlinie bestehenden Subgroups der Art.-29-Gruppe beteiligt sich die LDI NRW auch intensiv an den neu eingerichteten Expert Subgroups des EDSA.

Besonders wichtig für die gemeinsame Arbeit der europäischen Aufsichtsbehörden bei grenzüberschreitenden Fällen ist

das Verfahren der Zusammenarbeit. Hier tauschen sich die jeweils betroffenen Aufsichtsbehörden aus und stimmen Entscheidungen ab. Wir sind daran beteiligt, wenn es um Betroffene oder um datenverarbeitende Stellen in NRW geht oder wenn Betroffene sich bei uns beschwert haben.

Zusätzlich enthält das BDSG neue komplexe Regelungen für die Zuständigkeit und die Zusammenarbeit der deutschen Aufsichtsbehörden untereinander. Entsprechende Rahmenbedingungen sind wichtig, damit die deutschen Aufsichtsbehörden möglichst effektiv an der Meinungsbildung auf europäischer Ebene teilnehmen können. So sieht das BDSG vor, dass die Aufsichtsbehörden des Bundes und der Länder in strittigen Fragen zu EU-Angelegenheiten gemeinsame Standpunkte festlegen. Sofern sie betroffen sind, müssen dabei auch sogenannte spezifische Aufsichtsbehörden beteiligt werden, die zum Beispiel für den Bereich der Medien oder für Kirchen die Datenschutzaufsicht wahrnehmen.

Die Zentrale Anlaufstelle (ZASt) bei dem BfDI unterstützt die deutschen Aufsichtsbehörden bei der Kommunikation mit den europäischen Partnern.

Auf europäischer und auf deutscher Ebene mussten für diese Meinungsbildungen erst aufwändig Verfahren und Vereinbarungen geschaffen werden, die eine praktikable und schnelle Bearbeitung ermöglichen.

Die praktische Umsetzung dieser Regelungen wirft sehr viele neue Fragen auf. Solche Fragen zeigen sich sowohl bei der Entwicklung des europäisch einheitlichen Rechtsverständnisses als auch bei der Bearbeitung von einzelnen Beschwerden.

Die Entschließungen und Beschlüsse des EDSA sind im Internetangebot des EDSA unter der Adresse: www.edpb.europa.eu abrufbar

Die Mechanismen für eine EU-einheitliche Anwendung der DS-GVO ermöglichen eine umfassendere Meinungsbildung innerhalb der EU als bisher. Die Umsetzung dieser Prozesse ist zeitaufwändig und komplex. Die LDI NRW arbeitet daran intensiv mit. Dabei bleibt ein hoher, einheitlicher und praxisgerechter Datenschutzstandard unser Ziel.

1.5 Datenschutzbeauftragte: Stellung und Aufgaben nach neuem Recht

Die Datenschutz-Grundverordnung (DS-GVO) bringt einige Änderungen hinsichtlich der Stellung und der Aufgaben von Datenschutzbeauftragten (DSB) mit sich. Sie nehmen für viele Behörden, Unternehmen und Vereine weiterhin eine zentrale Rolle ein. Sie unterstützen dabei, die Einhaltung der neuen Regelungen zu gewährleisten und tragen erheblich dazu bei, ein effizientes Datenschutz-Managementsystem zu implementieren. Sie sind darüber hinaus wichtige Vermittler zwischen den Beteiligten, wie zum Beispiel Datenschutzaufsichtsbehörden, Betroffenen und den Verantwortlichen oder Auftragsverarbeitern.

Die Pflicht zur Benennung von DSB kann sich sowohl aus der DS-GVO unmittelbar als auch aus dem Bundesdatenschutzgesetz (BDSG) ergeben. Grundsätzlich gilt: Wer bereits nach altem Recht eine oder einen DSB benennen musste, ist dazu in der Regel auch weiterhin verpflichtet.

▪ Pflicht zur Benennung

In Deutschland kann sich die Pflicht zur Benennung von DSB aus einem der folgenden fünf Umstände ergeben:

- Mindestens zehn Personen sind regelmäßig ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (§ 38 Abs. 1 Satz 1 BDSG).
- Die datenverarbeitende Stelle ist eine öffentliche Stelle oder Behörde (Art. 37 Abs. 1 Buchstabe a) DS-GVO).
- Die Kerntätigkeit umfasst die umfangreiche Verarbeitung besonderer Kategorien von Daten oder strafrechtlicher Verurteilungen (Art. 37 Abs. 1 Buchstabe c) DS-GVO).
- Es ist eine Datenschutz-Folgenabschätzung durchzuführen (§ 38 Abs. 1 Satz 2 BDSG).
- Kerntätigkeit ist die umfangreiche oder systematische Überwachung von betroffenen Personen (Art. 37 Abs. 1 Buchstabe b) DS-GVO).

Bei Vorliegen eines der fünf Umstände sind nach neuem Recht auch Auftragsverarbeiter verpflichtet, einen DSB zu benennen.

Soweit keine Pflicht zur Benennung von DSB vorliegt, kann trotzdem eine freiwillige Benennung empfehlenswert sein (Art. 37 Abs. 4 S. 1 DS-GVO).

▪ Gemeinsame Datenschutzbeauftragte

Es besteht die Möglichkeit, für mehrere Behörden oder nicht-öffentliche Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe gemeinsame DSB zu benennen (Art. 37 Abs. 2 und 3 DS-GVO). Mit der Bezugnahme auf die Organisationsstruktur und Größe wird deutlich, dass der Verantwortliche sicherstellen muss, dass gemeinsame DSB in der Lage sind, die Aufgaben zu erfüllen, welche ihnen übertragen wurden. Voraussetzung ist außerdem, dass DSB von jeder Niederlassung aus leicht erreichbar sind.

- **Erreichbarkeit**

Die leichte Erreichbarkeit der DSB soll gleichermaßen sowohl für Betroffene, als auch für Aufsichtsbehörden sowie Beschäftigte innerhalb des Unternehmens gewährleistet sein. Es sind Vorkehrungen zu treffen, die es den betroffenen Personen oder anderen Stellen ermöglichen, einfach und problemlos Kontakt zu dem DSB herzustellen (etwa durch Einrichten einer Hotline oder eines Kontaktformulars auf der Homepage). Dem DSB muss eine Kommunikation in der Sprache möglich sein, welche für die Korrespondenz mit Aufsichtsbehörden und betroffenen Personen notwendig ist.

- **Aufgaben**

DSB haben nach Art. 39 Abs. 1 Buchstaben a) bis e) DS-GVO folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen bzw. Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Datenschutz-Pflichten;
- Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung;
- Zusammenarbeit mit der Aufsichtsbehörde und
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde.

Hinzu kommt die Beratung der betroffenen Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der DS-GVO im Zusammenhang stehenden Fragen (Art. 38 Abs. 4 DS-GVO).

- **Risikoorientierte Aufgabenerfüllung**

DSB nehmen ihre Aufgaben risikoorientiert wahr (Art. 39 Abs. 2 DS-GVO). Sie tragen bei der Erfüllung ihrer Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei sie Art, Umfang, Umstände und Zwecke der Verarbeitung berücksichtigen.

- **Keine Verantwortung für die Einhaltung der DS-GVO**

Die DS-GVO stellt ausdrücklich klar, dass es die Pflicht des Verantwortlichen bzw. des Auftragsverarbeiters – und nicht die der DSB – bleibt, sicherzustellen und nachzuweisen, dass die Datenverarbeitungen im Einklang mit den Regelungen der DS-GVO stehen (Art. 24 Abs. 1 DS-GVO). Gleichwohl sollten DSB ihre Tätigkeiten in angemessener Weise dokumentieren, um nachweisen zu können, dass sie ihren Aufgaben (insbesondere Unterrichtung und Beratung) ordnungsgemäß nachgekommen sind.

- **Stellung**

Verantwortliche oder Auftragsverarbeiter müssen die Weisungsfreiheit der DSB bei der Erfüllung ihrer Aufgaben sicherstellen. DSB dürfen wegen der Erfüllung ihrer Aufgaben nicht abberufen oder benachteiligt werden. Der besondere Abberufungs- und Kündigungsschutz für

DSB ist somit beibehalten worden (§ 6 Abs. 4, auch in Verbindung mit § 38 Abs. 2 BDSG). DSB berichten unmittelbar der höchsten Leitungsebene (Art. 38 Abs. 3 Satz 3 DS-GVO). Ferner muss nach Art. 38 DS-GVO sichergestellt werden, dass sie ordnungsgemäß und frühzeitig in alle Datenschutzfragen eingebunden und bei der Erfüllung ihrer Aufgaben unterstützt werden. Dazu gehören die Bereitstellung der für die Erfüllung der Aufgaben erforderlichen Ressourcen (einschließlich Personal), der Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung des Fachwissens erforderlichen Ressourcen.

DSB sind bei der Erfüllung ihrer Aufgaben zur Wahrung der Geheimhaltung oder Vertraulichkeit verpflichtet. Das BDSG regelt für DSB ergänzend die Pflicht zur Verschwiegenheit über die Identität der betroffenen Person, die der DSB zu Rate zieht, sowie über die Umstände, die Rückschlüsse auf die betroffene Person zulassen. Dies wirkt sich auch auf ein Zeugnisverweigerungsrecht aus (§ 6 Abs. 6, auch in Verbindung mit § 38 Abs. 2 BDSG).

DSB können noch weitere Aufgaben übertragen werden, wobei sichergestellt sein muss, dass keine Interessenkonflikte auftreten. Diese sind insbesondere dann anzunehmen, wenn gleichzeitig Positionen des leitenden Managements wahrgenommen werden oder die Tätigkeitsfelder die Festlegung von Zwecken und Mitteln der Datenverarbeitung mit sich bringen.

Meldeportal der LDI NRW

Verantwortliche und Auftragsverarbeiter müssen die Kontaktdaten ihrer DSB bei der für sie zuständigen Aufsichtsbehörde melden (Art. 37 Abs. 7 DS-GVO). Bei der LDI NRW kann diese Meldung online auf unserem Meldeportal vorgenommen werden. Diese Form der Meldung hat mehrere Vorteile: Die Meldung wird sofort bestätigt und kann bei Bedarf im eigenen Account jederzeit selbst und unbürokratisch angepasst werden.

Bis zum 31.12.2018 haben wir bereits über 22.000 Online-Meldungen erhalten.

Die Rolle der DSB ist auch im Rahmen der DS-GVO weiterhin bedeutend. Einige Änderungen im Tätigkeitsfeld haben die Rolle der DSB weiter gestärkt. DSB sind ein wesentliches Element für die erfolgreiche Umsetzung der Datenschutzregeln. Die Benennungspflicht für DSB in § 38 BDSG sollten nicht abgeschafft oder verwässert werden. Betriebliche DSB sorgen durch hohe interne Beratungsqualität und Kontrolle mit dafür, dass in Deutschland ein hohes Datenschutzniveau herrscht. Die Regelung des § 38 BDSG hat sich seit vielen Jahren bewährt. Sie ist deshalb aus guten Gründen auch bei der Datenschutzreform im deutschen Recht beibehalten worden und sollte nicht verändert werden. Ein Wegfall der Benennungspflicht würde nicht zum Wegfall der datenschutzrechtlichen Pflichten der Verantwortlichen führen. Wenn die Beratung und interne Kontrolle durch einen DSB fehlt, würde der Aufwand der Verantwortlichen eher noch erhöht.

1.6 Neue Verfahren nach der DS-GVO: Akkreditierung und Zertifizierung

Mit den Artikeln 42 und 43 der Datenschutz-Grundverordnung (DS-GVO) legte der Gesetzgeber einen rechtlichen Grundstein für einheitliche Akkreditierungs- und Zertifizierungsverfahren innerhalb der EU. Die Verfahren dienen dazu, die Einhaltung der DS-GVO bei Verarbeitungsvorgängen nachzuweisen. Zwar entbindet eine erfolgreiche Zertifizierung nicht von der Verantwortung zur Einhaltung der DS-GVO. Eine Zertifizierung nach den Kriterien der DS-GVO kann jedoch bei aufsichtsrechtlichen Kontrollen von Vorteil sein und die Prüfung erleichtern. Das Interesse an den neuen Verfahren ist erfreulicherweise hoch: Viele Stellen möchten sich gerade in NRW akkreditieren lassen, um Zertifizierungen am Markt durchzuführen, und viele möchten sich in Sachen Datenschutz zertifizieren lassen.

▪ Akkreditierung und Zertifizierung im Überblick

Um als Zertifizierungsstelle gemäß Artikel 42, 43 DS-GVO am Markt tätig werden zu können, muss sich eine Stelle zunächst für diese Tätigkeit akkreditieren lassen.

Eine Akkreditierung bestätigt, dass eine Zertifizierungsstelle die Kompetenz besitzt, bestimmte Zertifizierungsverfahren durchzuführen.

Die deutschen Datenschutzaufsichtsbehörden haben sich auf einheitliche Standards und ein Verfahren für Akkreditierungen geeinigt, das gemeinsam mit der Deutschen Akkreditierungsstelle GmbH (DAkkS) durchgeführt wird. Damit wird eine einheitliche Bewertung im Sinne der Datenschutz-Grundverordnung (DS-GVO) ermöglicht.

Eine erfolgreiche Zertifizierung bestätigt, dass festgelegte Anforderungen bezogen auf ein Produkt, einen Prozess oder eine Dienstleistung erfüllt sind.

▪ Akkreditierung

Wer sich zertifizieren lassen möchte, muss sich an eine akkreditierte Zertifizierungsstelle wenden. In Deutschland nimmt die DAkkS zusammen mit den unabhängigen Datenschutzaufsichtsbehörden die Akkreditierung von Zertifizierungsstellen gemäß § 39 BDSG vor. Hierzu haben die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder in Abstimmung mit der DAkkS bundesweit einheitliche Kriterien für die Akkreditierung entwickelt. Einschlägige ISO-Normen wurden dabei berücksichtigt. Die wichtigsten Schritte zur Akkreditierung sind die folgenden:

- Antrag bei der DAkkS
- Begutachtung durch die zuständige Datenschutzaufsichtsbehörde
- Entscheidung des Akkreditierungsauschusses
- Erteilung der Befugnis zu zertifizieren durch die zuständige Datenschutzaufsichtsbehörde
- Im Anschluss daran kann die Zertifizierungsstelle tätig werden, darf die Antragsteller prüfen und bei erfolgreicher Prüfung zertifizieren. Die einzelnen Schritte des Verfahrens

können ausführlich der Darstellung im Anhang entnommen werden.

Die Akkreditierung einer Zertifizierungsstelle erfolgt befristet auf maximal fünf Jahre (Art. 43 Abs. 4 DS-GVO).

- **Zertifizierung**

Voraussetzungen für eine Zertifizierung

Eine Stelle, die zertifiziert werden möchte, muss alle erforderlichen Informationen zur Verfügung stellen und Zugang zu den betroffenen Verarbeitungstätigkeiten gewähren. Dafür bedarf es einer guten Dokumentation und Überprüfung der eigenen Datenverarbeitungsvorgänge zur fachgerechten Umsetzung der DS-GVO.

Rahmenbedingungen

Die Zertifizierung ist zeitlich begrenzt zu erteilen. Die Höchstdauer beträgt drei Jahre (Art. 42 Abs. 7 DS-GVO). Bei Erfüllung der einschlägigen Voraussetzungen kann die Zertifizierung verlängert werden. Werden die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt, können die zuständige Zertifizierungsstelle oder die Datenschutzaufsichtsbehörde die Zertifizierung widerrufen.

Vorteile einer Zertifizierung

Bereits in der DS-GVO werden explizit Anwendungsbereiche aufgeführt, bei denen eine Zertifizierung für den Nachweis mit herangezogen werden kann, dass die DS-GVO eingehalten wird. Das sind beispielsweise:

- Pflichten des Verantwortlichen (Art. 24 Abs. 3 DS-GVO)
- Anforderungen an Technikgestaltung und datenschutzfreundliche Voreinstellungen nach Art. 25 (Art. 25 Abs. 3 DS-GVO)
- Garantien des Auftragsverarbeiters nach Art. 28 (Art. 28 Abs. 5 und 6 DS-GVO)
- Sicherheit der Verarbeitung (Art. 32 Abs. 3 DS-GVO)
- Datenübermittlung an ein Drittland (Art. 46 Abs. 2 Buchstabe f) DS-GVO)
- Datenschutz-Folgenabschätzung (Erwägungsgrund 90 zur DS-GVO).

Daneben kann eine Zertifizierung auch für Marketingzwecke (gegebenenfalls sogar als Alleinstellungsmerkmal) genutzt werden, um die besondere Beachtung des Datenschutzrechts zu betonen.

Mit der Möglichkeit der Akkreditierung und Zertifizierung wurde ein neues Instrumentarium geschaffen, um den Datenschutz weiter voranzubringen und dadurch einen Wettbewerbsvorteil zu erlangen. Zertifizierungen nach der DS-GVO können Klarheit darüber verschaffen, ob die gesetzlichen Datenschutzanforderungen eingehalten werden. Das bietet auch allen, deren Daten verarbeitet werden, mehr Transparenz.

1.7 Neue Sanktionsmöglichkeiten nach der DS-GVO: Praxis in NRW

Bei Verstößen gegen Datenschutzvorschriften drohen seit der Geltung der DS-GVO deutlich verschärfte Sanktionen. Bislang gab es in NRW keinen Anlass, hohe Geldbußen zu verhängen.

Zusätzlich oder anstelle der in Art. 58 DS-GVO genannten Instrumente zur Herstellung oder Durchsetzung rechtmäßiger Datenverarbeitungen können Verstöße gegen die DS-GVO mit hohen Geldbußen geahndet werden (Art. 83 DS-GVO in Verbindung mit §§ 41 ff. BDSG).

Im Vergleich zur bisherigen Rechtslage wurde der Bußgeldrahmen mit der DS-GVO erheblich erweitert. Nach Art. 83 Abs. 1 DS-GVO hat die Aufsichtsbehörde sicher zu stellen, dass die Verhängung von Geldbußen in jedem Einzelfall „wirksam, verhältnismäßig und abschreckend“ ist. So beträgt der Rahmen für Geldbußen bei bestimmten gravierenden Verstößen bis zu 20.000.000 Euro. Gegenüber Unternehmen bzw. Konzernen können sogar Geldbußen von bis zu 4 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden.

Für die konkrete Bestimmung der Höhe der Geldbuße ist eine Vielzahl von Aspekten einzubeziehen. Dabei ist neben Art, Schwere und Dauer des Verstoßes unter anderem auch zu berücksichtigen, welche Art von Daten verarbeitet wurde, ob früher angeordnete Maßnahmen von der verantwortlichen Stelle eingehalten wurden sowie ob und welche Vorteile durch die Datenverarbeitung erlangt wurden.

Berücksichtigt wird auch, ob und wie die verantwortlichen Stellen mit den Aufsichtsbehörden zusammengearbeitet haben, um Verstößen abzuhelfen und ob sie die Verstöße eigenständig mitgeteilt haben.

Bei der LDI NRW waren auf der Grundlage der DS-GVO seit dem 25. Mai bis zum 31. Dezember 2018 52 Bußgeldverfahren anhängig. Davon wurden in 36 Fällen Bußgeldbescheide in einer Gesamtsumme von 15.600 € erlassen. Die Bußgeldtatbestände waren überwiegend nicht erteilte Auskünfte gegenüber der LDI NRW und der Einsatz von Dashcams im Straßenverkehr.

Die LDI NRW berücksichtigt bei der Verhängung von Geldbußen, dass die Regelungen der DS-GVO teilweise die bisherigen Datenschutzregeln erweitern und für die Beteiligten insoweit neu sind. Allerdings sind die meisten der im Berichtszeitraum geahndeten Datenschutzverstöße „Klassiker“. Entscheidungen bezüglich der Verhängung von Geldbußen werden durch die LDI NRW maßvoll getroffen. Die weitere Entwicklung der Bußgeldpraxis bleibt auch mit Blick auf die Gesamtsituation in Deutschland und in der Europäischen Union abzuwarten.

2. Internet und Medien

2.1 Die ePrivacy-Verordnung – Aktueller Stand und Ausblick

Die ePrivacy-Verordnung soll die ePrivacy-Richtlinie aus dem Jahr 2002 ersetzen und die Datenschutz-Grundverordnung (DS-GVO) im Hinblick auf die elektronische Kommunikation präzisieren und ergänzen. Sie sollte eigentlich gemeinsam mit der DS-GVO ab dem 25. Mai 2018 gelten. Das Gesetzgebungsverfahren zur ePrivacy-Verordnung verzögert sich jedoch erheblich. Sie wird voraussichtlich nicht vor 2020 in Kraft treten. Daher musste geklärt werden, welche Regelungen nun für Diensteanbieter von Telemedien gelten, auf die vor dem 25. Mai 2018 die Datenschutzbestimmungen des Telemediengesetzes (TMG) anwendbar waren.

Vor diesem Hintergrund hat die Datenschutzkonferenz am 26. April 2018 festgestellt, dass ab dem 25. Mai 2018 im Grundsatz die Regelungen der DS-GVO auf die Verarbeitungen personenbezogener Daten durch nicht-öffentliche Diensteanbieter von Telemedien anzuwenden sind. Für öffentliche Diensteanbieter wie Behörden waren die Beratungen der DSK zum Zeitpunkt der Berichterstellung noch nicht abgeschlossen.

Zwar enthält die DS-GVO in Art. 95 eine sogenannte Kollisionsregel zum Verhältnis zwischen DS-GVO und ePrivacy-Richtlinie. Danach bleiben unter bestimmten Umständen nationale Regelungen, welche die ePrivacy-Richtlinie umsetzen, auch neben der DS-GVO anwendbar. Nach Auffassung der DSK stellen die Datenschutzvorschriften des TMG vorrangig lediglich eine Umsetzung der Datenschutzrichtlinie, nicht aber der ePrivacy-Richtlinie dar. Die DSK hält somit die Vorschrift des Art. 95 DS-GVO auf das TMG für nicht anwendbar. Da die TMG-Regelungen zum Datenschutz zudem auch nicht auf der Grundlage von sogenannten Öffnungsklauseln in der DS-GVO beibehalten werden können, sind die Vorschriften der DS-GVO anzuwenden.

Unter dieser Prämisse ergeben sich für Diensteanbieter aus der DS-GVO folgende rechtliche Möglichkeiten:

Diensteanbieter können mit der Verarbeitung personenbezogener Daten im Zusammenhang mit einer Internetseite eine Vielzahl von Interessen verfolgen. Ob und inwieweit die Verarbeitung personenbezogener Daten zur Verfolgung dieser Interessen rechtmäßig sein kann, hängt unter obiger Prämisse davon ab, ob die Verarbeitungen auf eine der Rechtsgrundlagen des Art. 6 Abs. 1 oder auf Abs. 4 DS-GVO gestützt werden können. Dabei ist zu beachten, dass sämtliche Erlaubnistatbestände der DS-GVO als gleichrangig und gleichwertig zu betrachten sind.

1. Die Verarbeitung personenbezogener Daten auf vertraglicher Grundlage ist gemäß Art. 6 Abs. 1 Buchstabe b) DS-GVO nur möglich, wenn die Datenverarbeitung erforderlich

ist zur Erfüllung eines Vertrages oder im Rahmen vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen. Ein Beispiel hierfür ist das Setzen eines Session-Cookies für den virtuellen Warenkorb eines Onlineshops, sofern der Cookie zu einem Zeitpunkt gelöscht wird, der dem Zweck angemessen ist. Cookies, die zur Nachverfolgung der Nutzerinnen und Nutzer über mehrere Websites (unterschiedliche Dienste oftmals unterschiedlicher Verantwortlicher) gesetzt werden, gehören nicht zu solchen ausdrücklich nachgefragten Diensten.

2. Daneben kommt die Regelung des Art. 6 Abs. 1 Buchstabe f) DS-GVO als Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung eines Telemediendienstes in Betracht. Art. 6 Abs. 1 Buchstabe f) DS-GVO verlangt, dass ein berechtigtes Interesse der Verantwortlichen für die personenbezogene Datenverarbeitung vorliegt und darüber hinaus die Interessen, Rechte und Freiheiten der betroffenen Personen nicht überwiegen. Im Rahmen der Interessenabwägung sind folgende Kriterien zugrundezulegen:

   - Zu den möglichen berechtigten Interessen der Diensteanbieter zählen zum Beispiel die nutzerfreundliche Form und die Integrität einer Website. Ausdrücklich benennt die DS-GVO im Erwägungsgrund 47 die Verhinderung von Betrug und die Direktwerbung als mögliche berechtigte Interessen.
   - Zudem muss die jeweilige Datenverarbeitung erforderlich für die Wahrung des jeweiligen Interesses sein. Für die Messung der Reichweite des eigenen Angebots ist es etwa nicht erforderlich, dass ein Verantwortlicher Daten über das Nutzungsverhalten Betroffener an Dritte weitergibt (etwa an soziale Netzwerke oder externe Analysedienste, die Nutzungsdaten mit Daten von anderen Websites zusammenführen).
   - Demgegenüber können die Interessen sowie Grundrechte und Grundfreiheiten der Nutzerinnen und Nutzer stehen. Darunter fallen zum Beispiel das Recht auf Schutz personenbezogener Daten gemäß Art. 8 der Charta der Grundrechte der Europäischen Union (GRCh) oder das Recht auf Vertraulichkeit der Kommunikation gemäß Art. 7 GRCh.
   - Bei der Interessenabwägung im Einzelfall sind die Ausgestaltung und die konkreten Auswirkungen der Verarbeitung auf die betroffenen Personen zu berücksichtigen. Maßgeblich sind dabei vor allem Folgen, Dauer und Intensität der Verarbeitung, die begründeten Erwartungen der Nutzerinnen und Nutzer sowie das Vorhandensein geeigneter Maßnahmen, um die schutzwürdigen Interessen zu wahren oder Eingriffe zu kompensieren. Im Rahmen der Abwägung sind unter anderem

die folgenden Kriterien zu berücksichtigen: die vernünftigen Erwartungen der betroffenen Personen, die Vorhersehbarkeit bzw. Transparenz, die Interventionsmöglichkeiten der betroffenen Personen, die Dauer der Beobachtung und der Kreis der Betroffenen (beispielsweise besonders schutzbedürftige Personen wie etwa Kinder). Letztlich muss jeder Verantwortliche eigenständig prüfen, ob bzw. unter welchen Voraussetzungen die von ihm verwendeten Produkte genutzt werden können.

3. Sofern eine Einwilligung nach Art. 6 Abs. 1 Buchstabe a) DS-GVO eingeholt wird, muss diese freiwillig sein und für den konkreten Fall sowie in informierter Weise und unmissverständlich erteilt werden. Art. 7 DS-GVO geht von einer selbstbestimmten und informierten Einwilligung der betroffenen Person in die jeweilige Datenverarbeitung aus. Dies setzt voraus, dass jegliche Datenerhebungen und anderweitige Datenverarbeitungen transparent und nachvollziehbar gemacht werden.

Diese von der LDI NRW vertretene Auffassung steht im Einklang mit der Rechtslage in den meisten anderen EU-Mitgliedstaaten.

Die Anwendung der Regelungen der DS-GVO auf die Verarbeitung personenbezogener Daten durch nicht-öffentliche Diensteanbieter von Telemedien gewährleistet ein hohes Schutzniveau für die personenbezogenen Daten der Nutzerinnen und Nutzer.

2.2 Facebook-Fanpages – Gemeinsame Verantwortlichkeit von Facebook und Fanpage-Betreiberinnen und -Betreibern

Nach einem Urteil des Gerichtshofes der Europäischen Union (EuGH) sind das Unternehmen Facebook und die Fanpage-Betreiberinnen und -Betreiber datenschutzrechtlich gemeinsam für den Betrieb einer Fanpage verantwortlich (Art. 26 Datenschutz-Grundverordnung (DS-GVO)). Bei einer gemeinsamen Verantwortlichkeit fordert Art. 26 DS-GVO unter anderem eine Vereinbarung zwischen den Beteiligten, die klarstellt, wie die Pflichten aus der DS-GVO erfüllt werden.

Schon bislang hatten wir den nordrhein-westfälischen öffentlichen Stellen wie auch den Unternehmen, Vereinen und anderen Stellen von der Nutzung Sozialer Medien abgeraten, wenn sie weder feststellen noch beeinflussen können, was mit den personenbezogenen Daten der Nutzerinnen und Nutzer geschieht, gesetzlich aber zumindest dazu verpflichtet sind, über die Datenverarbeitungsprozesse umfassend zu informieren.

Zwischenzeitlich hat der EuGH mit Urteil vom 5. Juni 2018 (Aktenzeichen C-210/16) die Auffassung der LDI NRW bestätigt und entschieden, dass Facebook-Fanpage-Betreiberinnen und -Betreiber gemeinsam mit Facebook verantwortlich sind. Die Datenschutzkonferenz hat daraufhin deutlich gemacht, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen – insbesondere für die Betreiberinnen und Betreiber einer Fanpage – ergeben. Bei einer gemeinsamen Verantwortlichkeit fordert Art. 26 DS-GVO unter anderem eine Vereinbarung zwischen den Beteiligten, die klarstellt, wie die Pflichten aus der DS-GVO erfüllt werden. Zudem sind den betroffenen Personen (Besucherinnen und Besucher der Fanpage) die erforderlichen Informationen nach Art. 12, 13 und 14 DS-GVO bereitzustellen (Entschließung der Datenschutzkonferenz vom 6. Juni 2018 „Die Zeit der Verantwortungslosigkeit ist vorbei: EuGH bestätigt gemeinsame Verantwortung von Facebook und Fanpage-Betreibern“).

Daraufhin hat Facebook am 11. September 2018 im Zusammenhang mit den Fanpages zwei Dokumente – eine so genannte „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ sowie eine „Informationen zu Seiten-Insights“ – veröffentlicht. Für die Funktion „Facebook Insight“ werden von Facebook Cookies bei den Besucherinnen und Besuchern der jeweiligen Fanpage gespeichert. Fanpage-Betreiberinnen und -Betreiber können dadurch anonymisierte statistische Daten der Besucher der Fanpage einsehen, während Facebook selbst die Möglichkeit hat, die Besucher eindeutig zu identifizieren. Abstellen lässt sich Facebook Insights weder von den Betreiberinnen und Betreibern, noch von den Besuchern der Fanpage.

Allerdings sind die von Facebook veröffentlichten Informationen nicht hinreichend transparent und konkret in Bezug auf die Verarbeitungstätigkeiten, die im Zusammenhang mit Fanpages und insbesondere Seiten-Insights durchge-

führt werden und der gemeinsamen Verantwortlichkeit von Facebook und Fanpage-Betreiberinnen und -Betreibern unterfallen. Sie ermöglichen den Fanpage-Betreiberinnen und -Betreibern noch keinen rechtskonformen Betrieb ihrer Fanpages, da sie nicht den Vorgaben des Art. 26 und des Art. 5 Abs. 2 DS-GVO genügen.

Für die Durchsetzung der Datenschutzvorgaben im Zusammenhang mit einer Fanpage ist zum einen die für die jeweilige Fanpage-Betreiberin bzw. den jeweiligen Fanpage-Betreiber zuständige Aufsichtsbehörde verantwortlich. Für nordrhein-westfälische Fanpage-Betreiberinnen und -Betreiber ist dies die LDI NRW.

Im Verantwortungsbereich von Facebook selbst ist zum anderen in erster Linie die irische Datenschutzaufsicht für die Durchsetzung der Datenschutzvorgaben zuständig, weil sich die EU-Hauptniederlassung von Facebook in Irland befindet. Da Facebook seine (einzige) deutsche Niederlassung in Hamburg hat, ist der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit in Deutschland federführend zuständig für die europäische Zusammenarbeit mit der irischen Aufsichtsbehörde in Sachen Facebook. Auf europäischer Ebene wird das weitere Vorgehen gegenüber Facebook beraten. Bei Redaktionsschluss lagen dazu noch keine Ergebnisse vor.

Den Fanpage-Betreiberinnen und -Betreibern in Nordrhein-Westfalen empfiehlt die LDI NRW, zunächst zu prüfen, ob sie ihre Fanpages für erforderlich halten. Sofern sie auf die Fanpages nicht verzichten möchten, sollten sich die Betreiberinnen und Betreiber an Facebook wenden und den Abschluss einer Vereinbarung nach Art. 26 DS-GVO sowie die erforderlichen Informationen einfordern. Als Richtschnur für die zu klärenden Punkte kann der von der DSK entwickelte Fragenkatalog dienen, den Fanpage-Betreiberinnen und -Betreiber beantworten können müssen (siehe Beschluss der DSK zu Facebook Fanpages vom 5. September 2018, Abdruck im Anhang):

1. In welcher Art und Weise wird zwischen Ihnen und anderen gemeinsam Verantwortlichen festgelegt, wer von Ihnen welche Verpflichtung gemäß der DS-GVO erfüllt? (Art. 26 Abs. 1 DS-GVO)
2. Auf Grundlage welcher Vereinbarung haben Sie untereinander festgelegt, wer welchen Informationspflichten nach Art. 13 und 14 DS-GVO nachkommt?
3. Auf welche Weise werden die wesentlichen Aspekte dieser Vereinbarung den betroffenen Personen zur Verfügung gestellt?
4. Wie stellen Sie sicher, dass die Betroffenenrechte (Art. 12 ff. DS-GVO) erfüllt werden können, insbesondere die Rechte auf Löschung nach Art. 17 DS-GVO, auf Einschränkung der Verarbeitung nach Art. 18 DS-GVO, auf Widerspruch nach Art. 21 DS-GVO und auf Auskunft nach Art. 15 DS-GVO?
5. Zu welchen Zwecken und auf welcher Rechtsgrundlage verarbeiten Sie die personenbezogenen Daten der Besucherinnen und Besucher von Fanpages? Welche personenbezogenen Daten werden gespei-

chert? Inwieweit werden aufgrund der Besuche von Facebook-Fanpages Profile erstellt oder angereichert? Werden auch personenbezogene Daten von Nicht-Facebook-Mitgliedern zur Erstellung von Profilen verwendet? Welche Löschfristen sind vorgesehen?

6. Zu welchen Zwecken und auf welcher Rechtsgrundlage werden beim Erstaufruf einer Fanpage auch bei Nicht-Mitgliedern Einträge im sogenannten Local Storage erzeugt?
7. Zu welchen Zwecken und auf welcher Rechtsgrundlage werden nach Aufruf einer Unterseite innerhalb des Fanpage-Angebots ein Session-Cookie und drei Cookies mit Lebenszeiten zwischen vier Monaten und zwei Jahren gespeichert?
8. Welche Maßnahmen haben Sie ergriffen, um Ihren Verpflichtungen aus Art. 26 DS-GVO als gemeinsam für die Verarbeitung Verantwortlicher gerecht zu werden und eine entsprechende Vereinbarung abzuschließen?

Je nachdem, zu welchem Ergebnis die Prüfung bzw. Rückmeldung von Facebook führt, sollten die Fanpage-Betreiberinnen und -Betreiber eine Löschung, jedenfalls aber eine Deaktivierung der Fanpage in Betracht ziehen.

Das Unternehmen Facebook und die Fanpage-Betreiberinnen und -Betreiber sind datenschutzrechtlich gemeinsam für den Betrieb einer Fanpage verantwortlich (Art. 26 DS-GVO). Daher bedarf es einer Vereinbarung zwischen den Beteiligten, die klarstellt, wie die Pflichten aus der DS-GVO erfüllt werden, sowie der Bereitstellung der erforderlichen Informationen für die Besucherinnen und Besucher der Fanpage. Durch die beiden von Facebook im Zusammenhang mit den Fanpages veröffentlichten Dokumente werden die Anforderungen des Art. 26 und Art. 5 Abs. 2 DS-GVO nicht erfüllt.

Die LDI NRW bittet derzeit nordrhein-westfälische Fanpage-Betreiberinnen und -Betreiber zunächst um Auskunft zu den oben genannten Fragen. Sofern die Fanpage-Betreiberinnen und -Betreiber die Fragen nicht zufriedenstellend beantworten können, werden wir weitere mögliche Maßnahmen prüfen.

2.3 Einbindung von Social Plugins auf Websites

Sogenannte Social Plugins wie der Facebook-Like-Button sind ein beliebtes Mittel von Websitebetreibern, um die Wahrnehmung ihrer Website zu erhöhen und durch das „Liken" kostenlos und zielgerichtet für ihr Angebot zu werben. Bei diesem Vorgehen sind die Datenschutzrechte der Nutzerinnen und Nutzer zu wahren.

Social Plugins können in unterschiedlicher Weise auf Internetseiten integriert werden. Werden sie als IFrames eingebunden, werden beim Aufruf der Internetseite Daten an den Anbieter des Plugins übertragen. Dies geschieht, indem der Browser der Nutzerinnen und Nutzer automatisch und ohne ihr Wissen neben der Verbindung zum Server der Website zugleich eine Verbindung zum Server des Plugin-Anbieters aufbaut. So erhält dieser zugleich die Information über den Aufruf der Seite und die Möglichkeit, im Browser der Nutzerinnen oder Nutzer ein Cookie zu setzen. Dadurch sind diese bei späteren Aufrufen identifizierbar und der Plugin-Anbieter kann auf dieser Grundlage weitere zielgerichtete Auswertungen vornehmen (siehe auch 23. Bericht unter 12.5).

Da wir diese Vorgehensweise nicht für zulässig halten, raten wir den Verantwortlichen seit Jahren, die Einbindung derartiger Plugins, wenn überhaupt, nur auf datenschutzfreundlichem Weg vorzunehmen. Hierfür stehen das so genannte Doppelklickverfahren oder andere datenschutzgerechte Gestaltungen der Social Media Buttons zur Verfügung. In der Praxis greifen viele Verantwortliche diese Empfehlung auf.

Eine nordrhein-westfälische Online-Händlerin setzte die datenschutzgerechte Lösung nach Intervention der Verbraucherzentrale NRW zwar auch um. Sie strebte jedoch, mit Facebook als Streithelferin an ihrer Seite, eine grundsätzliche gerichtliche Klärung der Frage an, ob die Einbindung von Social Plugins als IFrame datenschutzrechtlich zulässig ist (siehe 23. Bericht unter 12.5). Über das Oberlandesgericht (OLG) Düsseldorf gelangte die Angelegenheit schließlich zum Europäischen Gerichtshof (EuGH), dem das OLG Düsseldorf verschiedene Fragen zur Auslegung maßgeblicher europäischer Rechtsvorschriften vorlegte:

Im Wesentlichen soll der EuGH darüber entscheiden, ob eine Website-Betreiberin, die ein derartiges Plugin in ihre Seite einbindet, für die Datenverarbeitung verantwortlich ist, die hierdurch ausgelöst wird. Außerdem geht es um die Frage, welche Informationspflichten sie treffen und ob sie gegebenenfalls sogar die Einwilligungen der betroffenen Personen einholen muss.

Das OLG Düsseldorf gab uns im Berufungsverfahren zwischen der Verbraucherzentrale NRW und dem betroffenen Unternehmen gemäß § 12 a des Unterlassungsklagegesetzes Gelegenheit zur Stellungnahme. Wir gaben sowohl gegenüber dem OLG Düsseldorf als auch später gegenüber dem EuGH umfangreiche schriftliche Stellungnahmen ab und nahmen an den jeweiligen mündli-

chen Verhandlungen teil. Dabei vertraten wir die Auffassung, die Website-Betreiberin sei datenschutzrechtlich verantwortlich für die Datenübertragung an Facebook und entscheide alleine über die Einbindung des Plugins. Außerdem müsse mangels einer Rechtsgrundlage für die Datenverarbeitungsvorgänge die Einwilligung der Nutzerinnen und Nutzer eingeholt werden. In ähnlicher Weise äußerten sich die Verbraucherzentrale als Klägerin und Berufungsbeklagte, die Europäische Kommission, die Bundesregierung und weitere Mitgliedstaaten im Verfahren.

Im Anschluss an die mündliche Verhandlung vom September 2018 stellte der Generalanwalt beim EuGH am 19. Dezember 2018 seine Schlussanträge. Auch wenn er an verschiedenen Stellen weitere Feststellungen durch das vorlegende Gericht fordert, stellt er darin fest, dass grundsätzlich eine Mitverantwortung der Websitebetreiberin an der durch das Plugin ausgelösten Datenverarbeitung besteht. Diese umfasse zwar nicht alle im weiteren Verlauf von Facebook durchgeführten Datenverarbeitungen. Soweit die Verantwortung der Websitebetreiberin aber gehe, sei sie auch zur Information der betroffenen Personen und zur Einholung der je nach den genauen Umständen erforderlichen Einwilligung verpflichtet.

Nachdem der Generalanwalt damit seinen Entscheidungsvorschlag vorgelegt hat, bleibt nun abzuwarten, ob der EuGH sich dem anschließen wird.

Die Schlussanträge des Generalanwalts bestärken uns in unserer Rechtsauffassung. Aus unserer Sicht ist zu vermuten, dass der EuGH in seinen grundsätzlichen Erwägungen in eine ähnliche Richtung tendieren wird. Bis zu einer endgültigen Entscheidung ist Website-Betreiberinnen und -Betreibern weiterhin anzuraten, Social Plugins, wenn überhaupt, nur in datenschutzgerechter Weise einzubinden.

3. Weiterhin Unsicherheiten im internationalen Datenverkehr

Zur Datenübermittlung in Länder außerhalb der EU (Drittländer) finden sich in der DS-GVO sowohl bereits aus der Datenschutzrichtlinie bekannte Ansätze und Instrumente als auch neue Instrumente. Themen aus den Vorjahren setzten sich fort, etwa der EU-US Privacy Shield.

Bereits die Datenschutzrichtlinie (95/46/EG) erwähnte die Standardvertragsklauseln der EU-Kommission (EU-Standardvertragsklauseln) und verbindliche unternehmensinterne Verhaltensregeln (Binding Corporate Rules, BCR) als mögliche geeignete Garantien bei Datenübermittlungen in Drittländer. Die DS-GVO führt sie fort und regelt zusätzlich eine Reihe neuer Übermittlungsinstrumente, wie Zertifizierungen und Verhaltensregeln (Codes of Conduct). Neben der EU-Kommission haben nun auch die Aufsichtsbehörden die Möglichkeit, Standarddatenschutzklauseln zu erstellen. Diese müssen in einem bestimmten Prüfverfahren von der EU-Kommission genehmigt werden. Es wird einige Zeit dauern, bis sich die notwendigen Prozesse in der Praxis eingespielt haben. Bei der Umsetzung tauchen immer wieder neue Fragen auf, die wir gemeinsam mit den anderen Aufsichtsbehörden und den betroffenen datenverarbeitenden Stellen lösen. Auf unserer Homepage informieren wir über die aktuellen Rahmenbedingungen für Datenübermittlungen in Drittländer nach der DS-GVO.

Ab Ende 2016 beteiligten wir uns mit neun weiteren deutschen Aufsichtsbehörden an einer koordinierten Prüfaktion zum internationalen Datenverkehr. Ganz überwiegend kamen die angeschriebenen Unternehmen ihrer Auskunftspflicht nach. Die hohe Rückmeldequote vollständiger Auskünfte war für uns sehr erfreulich und lässt auf eine grundsätzlich vorhandene Sensibilität zum Thema Datenschutz schließen. Wir mussten lediglich zwei Bußgeldbescheide wegen nicht erteilter Auskunft erlassen. Für uns stand der Aspekt der Sensibilisierung und Beratung im Vordergrund. In manchen Fällen fragten wir bei einzelnen angeschriebenen Unternehmen weiter nach. Bei Bedarf werden wir noch offene Punkte mit Blick auf die DS-GVO klären. Alle angeschriebenen Unternehmen erhalten abschließende Informationen von uns zu verschiedenen Themenkomplexen aus der Prüfung mit Blick auf die aktuellen Regelungen der DS-GVO.

Die Regelungen des EU-US Privacy Shield (Privacy Shield) unterliegen einer jährlichen Prüfung der EU-Kommission, an der die europäischen Aufsichtsbehörden teilnehmen. Im Jahr 2017 fand eine solche erste Prüfung unter der Teilnahme einer Delegation der Artikel-29-Gruppe statt. Die Aufsichtsbehörden der Artikel-29-Gruppe erkannten Fortschritte gegenüber der Vorgängerentscheidung der EU-Kommission („Safe Harbor“) an. Gleichzeitig identifizierten sie eine Reihe erheblicher Belange, die Fragen aufwarfen. Diese betrafen die Aufsicht durch die zuständigen US-Behörden hinsichtlich der Zertifizierungen der US-Unternehmen sowie den Anwendungsbereich bei Beschäftigten-

daten. Ein weiterer Schwerpunkt waren Themen im Zusammenhang mit Zugriffsmöglichkeiten durch öffentliche Stellen auf Daten, die unter dem Privacy Shield in die USA übermittelt werden. Die Artikel-29-Gruppe veröffentlichte ihren Prüfbericht als Arbeitsdokument WP 255. Das Dokument kann auf der Newsroom-Seite der EU-Kommission unter www.ec.europa.eu abgerufen werden. Es ist lediglich in englischer Sprachfassung verfügbar.

Im Jahr 2018 nahm der Europäische Datenausschuss (EDSA) – das Nachfolgegremium der Artikel-29-Gruppe – an der jährlichen Prüfung teil. Die bereits 2017 identifizierten Fragestellungen wurden erneut aufgegriffen. Viele der Feststellungen der Artikel-29-Gruppe aus der ersten jährlichen Überprüfung wurden von den US-Behörden berücksichtigt. So hat das US-Handelsministerium den erstmaligen Zertifizierungsprozess angepasst, um Widersprüche zwischen Angaben auf der Privacy-Shield-Liste und Angaben der selbstzertifizierten Unternehmen auf deren eigenen Webseiten zu vermeiden. Ebenso wurden drei neue Mitglieder des sogenannten Privacy and Civil Liberties Oversight Board (PCLOB) ernannt. Es bleiben weiterhin offene Punkte. Der EDSA begrüßt in seinem Bericht die unternommenen Schritte und äußert Besorgnis über die weiterhin offenen Punkte. Der Prüfbericht des EDSA ist unter www.edpb.europa.eu abrufbar. Das Dokument ist lediglich in englischer Sprachfassung verfügbar.

Ende 2016 wurden gegen die Angemessenheitsentscheidung der EU-Kommission zum Privacy Shield Klagen eingereicht. Klägerinnen waren die Bürgerrechtsorganisationen Digital Rights Ireland und La Quadrature du Net (gemeinsam mit French Data Network und der Fédération FDN). Die Klage von La Quadrature du Net ist mit Stand Oktober 2018 noch anhängig (Az. T-738/16); ihre Erfolgsaussichten sind nach unserer Einschätzung offen. Die Klage von Digital Rights Ireland wurde vom Gericht der Europäischen Union (EuG) als unzulässig abgewiesen (Az. T-670/16).

2016 brachte die irische Aufsichtsbehörde die Standardvertragsklauseln der EU-Kommission für Auftragsdatenverarbeiter vor das zuständige irische Gericht (High Court). Der High Court legte Mitte 2018 dem europäischen Gerichtshof (EuGH) Fragen zu den Standardvertragsklauseln vor (Az. C-311/18). Diese beziehen sich auf den Einsatz der Klauseln für Datenübermittlungen in die USA. Auch bei diesem Verfahren ist der Ausgang des Verfahrens aus unserer Sicht offen.

Datenübermittlungen in Drittländer sind weiterhin mit Risiken verbunden. Wir bleiben deshalb bei unseren Ratschlägen:

Datenverarbeitende Stellen sollten sorgfältig prüfen, ob sie Leistungen in Anspruch nehmen, bei denen Daten in Länder außerhalb der EU und des Europäischen Wirtschaftsraumes (Drittländer) übermittelt werden. Erfolgt ein Datentransfer in Drittstaaten, empfehlen wir den datenverarbeitenden Stellen dringend, für die technisch-organisatorischen Sicherungsmaßnahmen höchste Standards anzuwenden. Dazu ist zumindest eine starke Ver-

schlüsselung zu empfehlen. Nutzerinnen und Nutzer können sich in Nutzungsbedingungen und Datenschutzerklärungen über vorgesehene Datenverarbeitungen in Drittländern informieren. Sie können sich dann bewusst entscheiden, ob sie das entsprechende Angebot nutzen möchten. Bleibt ein Angebot insoweit intransparent, raten wir davon ab.

4. Datenschutz und Kraftfahrzeuge

4.1 Fahrerbewertungsportale – Bewertung von Privatpersonen im Internet (Fortsetzung aus dem 23. Bericht).

Nachdem das Verwaltungsgericht Köln unsere datenschutzrechtlichen Maßnahmen zur Anpassung des Bewertungsportals erstinstanzlich bestätigt hatte, hat im Berichtszeitraum auch das Oberverwaltungsgericht Nordrhein-Westfalen unsere Anordnungen bekräftigt. Danach musste das Fahrerbewertungsportal geändert werden.

In unserem 23. Bericht (siehe unter 15.2) hatten wir darüber informiert, dass wir die Betreiberin eines Fahrerbewertungsportals aufgefordert hatten, das Portal durch verschiedene Maßnahmen datenschutzgerecht anzupassen. Hiergegen hatte das Unternehmen den verwaltungsgerichtlichen Weg beschritten. Erste Instanz und Berufungsinstanz haben unsere Position bestätigt. Mit dem Urteil des OVG NRW vom 19. Oktober 2017, Az. 16 A 770/17 (VG Köln 13 K 6093/15) ist der Rechtsstreit zu Gunsten eines besseren Datenschutzes rechtskräftig entschieden. Das Bundesverwaltungsgericht hat eine Revision abgelehnt. Die Betreiberin hat anwaltlich bestätigt, dass sie ihr Portal angepasst hat.

Die Durchsetzung der datenschutzrechtlichen Belange hat in diesem Fall über drei Jahre in Anspruch genommen. Es würde wertvolle Personalressourcen schonen, wenn Unternehmen den datenschutzrechtlichen Empfehlungen der Aufsichtsbehörden frühzeitig mehr Akzeptanz entgegenbringen würden. Ein Erfolg dieses Falles ist es, dass nun das Urteil eines Oberverwaltungsgerichtes zur datenschutzrechtlichen Einordnung von Bewertungsportalen vorliegt. Der Einsatz hat sich damit gelohnt.

4.2 Automobilwerkstätten und -hersteller

Moderne Kraftfahrzeuge generieren eine große Anzahl von personenbezogenen Daten. In der Automobilwerkstatt werden diese Daten für Wartung, Service oder Reparatur verwendet. Wie gestaltet sich die Datenverarbeitung in den Automobilwerkstätten, wie sind die Automobilhersteller in die Datenverarbeitung eingebunden, wie können die personenbezogenen Daten zulässig verarbeitet werden?

Auch zunächst rein technische Daten eines Kraftfahrzeuges sind personenbezogene Daten, wenn sie über die Fahrzeugidentifikationsnummer mit den Halterdaten oder den Kundendaten verknüpft werden (können). Für diese weite Definition des Personenbezugs – und damit für die Anwendbarkeit des Datenschutzrechts – musste bei den Automobilherstellern erst einmal ein Problembewusstsein geschaffen werden. Dies ist offenbar noch nicht bei allen Herstellern vollständig gelungen.

Im Juni 2017 beteiligte sich die LDI NRW an einer gemeinsamen Prüfung von Automobilwerkstätten durch Datenschutzaufsichtsbehörden aus sechs Bundesländern, um die Verarbeitung von aus Fahrzeugen erhobenen Daten nachzuvollziehen und auf die Vereinbarkeit mit datenschutzrechtlichen Anforderungen zu untersuchen. Dabei wurden Anhaltspunkte für eine zentrale Rolle der Automobilhersteller bei der Verarbeitung von bei Werkstattbesuchen erhobenen personenbezogenen Daten festgestellt.

Wir haben zehn in NRW ansässige Vertragswerkstätten von Automobilherstellern mit deutschen und internationalen Unternehmenssitzen angeschrieben und sie zur Beantwortung eines umfangreichen Fragenkatalogs aufgefordert. Dabei wurden die Automobilwerkstätten unter anderem befragt, welche personenbezogenen Daten aus dem Fahrzeug bei einem Werkstattbesuch ausgelesen, in Datenverarbeitungssystemen gespeichert und übermittelt werden. Zentrale Themen waren die organisatorischen und technischen Abläufe sowie die Rechtsgrundlagen für die Datenverarbeitung, die Weitergabe der Daten an den Automobilhersteller oder an andere Dritte wie beispielsweise Versicherungen und die Information der Kundinnen und Kunden über die Datenverarbeitung.

Im folgenden Jahr 2018 wurden sieben Automobilhersteller und -importeure mit Unternehmenssitzen in NRW im schriftlichen Verfahren geprüft. Dabei wurden auch Besonderheiten der Datenverarbeitung bei Fahrzeugen mit Elektroantrieb betrachtet. Uns interessierte, welche personenbezogenen Daten auf welchen Wegen aus dem Fahrzeug bei einem Werkstattbesuch zu den Herstellern gelangen, wie die Daten in ihren Datenverarbeitungssystemen gespeichert und an wen diese Daten weiter übermittelt werden.

Die Auswertung zeigte, dass die Datenverarbeitung von zwingend für Reparatur, Service und Wartung erforderlichen Daten inklusive Datenübermittlung an den Hersteller bereits im Rahmen der

Vertragserfüllung über Art. 6 Abs. 1 Satz 1 Buchstabe b) der Datenschutz-Grundverordnung (DS-GVO) legitimiert ist. Für eine Einwilligung in die Datenverarbeitung besteht daher in diesen Fällen keine Notwendigkeit mehr.

Datenschutzrechtlich unzulässig ist es, wenn Automobilwerkstätten Einwilligungen für eine Datenverarbeitung vorlegen, die so weit gefasst sind, dass pauschal in jede Datenverarbeitung eingewilligt werden soll und diese Einwilligung mit der Auftragsannahme verknüpft wird.

Jede Einwilligung in eine Datenverarbeitung muss zweckgebunden sein. Es muss ersichtlich sein, welche Daten zu welchem Zweck erhoben werden und wie sie verarbeitet werden. Die Abgabe einer Einwilligung muss freiwillig sein, ihre Verweigerung darf nicht an nachteilige Folgen gekoppelt werden. Eine Reparaturannahme darf daher nicht davon abhängig gemacht werden, dass Kundinnen und Kunden auch die Einwilligung unterschreiben.

Die DS-GVO verlangt, dass die Kundinnen und Kunden in präziser, transparenter, verständlicher und leicht zugänglicher Art und Weise über die Verarbeitung informiert werden. Die Automobilwerkstätten gaben an, dass Informationen zur Datenverarbeitung entweder in den Betriebsanleitungen der Fahrzeuge oder in den Einwilligungserklärungen vorhanden seien oder die Kundinnen und Kunden durch Servicemitarbeiterinnen und -mitarbeiter aufgeklärt würden. Es ist den Automobilwerkstätten zu empfehlen, ein Informationsblatt zur Datenverarbeitung an die Kundschaft mit den Inhalten gemäß Art. 12, 13 DS-GVO zusammen mit dem Auftrag auszuhändigen, auf dem Auftragsdokument mit aufzudrucken oder zumindest an der Reparaturannahme leicht wahrnehmbar auszulegen.

Schwieriger ist zu beantworten, nach welchen rechtlichen Grundlagen die Verknüpfung der technischen Daten mit dem Namen der Kundinnen und Kunden oder mit der Fahrzeugidentifikationsnummer übermittelt werden darf. Viele der Übermittlungen an den jeweiligen Automobilhersteller erfolgen aufgrund einer Vertragserfüllung gemäß Art. 6 Absatz 1 Satz 1 Buchstabe b) der DS-GVO. Darunter fallen beispielsweise bei Garantie-, Gewährleistungs- und Kulanzfällen die Prüfung der Leistungserstattung durch die Automobilhersteller und bei konkreten Reparaturdurchführungen wie Fahrzeugdiagnosen die Kommunikation mit dem Automobilhersteller.

Aufgefallen ist bei Reparaturdurchführungen mit Fahrzeugdiagnosen, dass eine Kommunikation mit dem Automobilhersteller für die Automobilwerkstätten nur beschränkt steuerbar ist. Denn die Automobilhersteller setzen den informationstechnischen Rahmen durch die Bereitstellung der Diagnosehardware und -software sowie von zentralen, für manche Reparaturen, Wartungen und Serviceleistungen benötigten Datenbanken mit beispielsweise Spezifikationen und Fehleranalysen. Die Werkstätten sind insoweit eher in einer Mittlerrolle ohne hinreichende eigene Einwirkungsmöglichkeiten. Die Transparenz ist hier defizitär und daher zu optimieren.

Die datenschutzrechtliche Grundlage für die Verarbeitung der erforderlichen Fahrzeugdaten für die Produktüberwachung/Produktbeobachtung und für eventuelle Rückrufaktionen ist die Erfüllung einer rechtlichen Verpflichtung gemäß Art. 6 Abs. 1 Satz 1 Buchstabe c) der DS-GVO. Denn die Automobilhersteller haben Pflichten aus Produkthaftungs- und Produktsicherungsgesetzen. Da in diesen Fällen sowohl die Automobilwerkstatt als auch der Automobilhersteller die Daten der Kundinnen und Kunden für die erwähnten Zwecke verarbeiten, könnte hier eine gemeinsame Verantwortlichkeit gemäß Art. 26 DS-GVO vorliegen. Dann hätten die Automobilwerkstätten und die Automobilhersteller in einer gemeinsamen Vereinbarung festzulegen, wer welchen Informationspflichten nachzukommen hat. Eine solche Vereinbarung ist – soweit ersichtlich – bislang (noch) nicht existent.

Für eine Datenverarbeitung zu Zwecken von Produkt- und Qualitätsverbesserungen sowie von Produktfortentwicklungen kann die Wahrung berechtigter Interessen nach Art. 6 Abs.1 Satz 1 Buchstabe f) der DS-GVO einschlägig sein. Gleiches gilt für Datenverarbeitungen im Kontext von Marketingaktionen und Kundenzufriedenheitsbefragungen. Es ist stets zu Beginn zu prüfen, ob in diesen Fällen nicht auch eine anonymisierte Verarbeitung möglich ist, weil diese für das Persönlichkeitsrecht der Kundin oder des Kunden weniger einschneidend wäre.

Die zentrale Führung einer elektronischen Wartungs- und Reparaturhistorie beim Automobilhersteller (sogenannter Digitaler Servicenachweis) kann jedoch nur mit expliziter Einwilligung der Halterin oder des Halters durchgeführt werden. Gleiches gilt für die Teilnahme an Vergütungs- und Bonusprogrammen.

Den geprüften Werkstätten war nicht immer ausreichend bewusst, welche Daten sie für welche Zwecke erheben. Die Datenverarbeitung für eigene Zwecke (zum Beispiel Erfüllung eines Reparatur-, Wartungs- oder Servicevertrages) und für Zwecke, die dem Hersteller dienen (zum Beispiel Produktbeobachtung und -verbesserung), sind jedoch voneinander getrennt zu betrachten. Ohne eine solche Unterscheidung ist eine ordnungsgemäße Information der Kundinnen und Kunden und eine ordnungsgemäße Vereinbarung über die Aufteilung der Verantwortlichkeit zwischen Werkstätten und Herstellern nicht möglich.

Der Datenbestand bei den Automobilherstellern ist umfangreich. Sie verarbeiten eine Vielzahl personenbezogener Daten, zum Beispiel Namen, Adressen, Fahrzeugidentifikationsnummer, Kfz-Kennzeichen. Diese werden teilweise mit fahrzeugbezogenen Daten (etwa Kilometerstand, Fahrzeugzustand, einzelne Fahrwerte) verknüpft. Aus der Gesamtheit dieser Daten kann sich eine zentral beim Automobilhersteller angelegte Fahrzeughistorie ergeben, aus der sich Rückschlüsse auf den/die Fahrzeughalter/in bzw. Fahrzeugführer/in ziehen lassen.

Bei Fahrzeugen mit Elektromotor ist die Menge der Daten und Tiefe der Verarbeitung noch größer. Über Telematik-Boxen werden nämlich in regelmäßigen, kurzen Abständen verbrauchsrelevante

Werte der Batterien erhoben und bei bestimmten Ereignissen (zum Beispiel in Gewährleistungsfällen) ausgewertet. Die Datenübertragung ist also bei Elektrofahrzeugen sogar im laufenden Betrieb intensiver.

Bei Automobilherstellern mit Konzernzentralen außerhalb Deutschlands bzw. außerhalb der Europäischen Union erfolgt eine Übermittlung der Daten zu den Konzernzentralen. Über eine anschließende Datenverarbeitung bzw. -nutzung bestehen bisher wegen des grenzüberschreitenden Bezugs noch keine vollständigen Erkenntnisse.

Die datenschutzrechtliche Verantwortlichkeit zwischen Automobilwerkstätten und Automobilherstellern ist noch nicht abschließend geklärt. Möglicherweise sind Automobilwerkstätten und Automobilhersteller – anders als von den Automobilherstellern angenommen – gemeinsame Verantwortliche nach Art. 26 der DS-GVO. Teilweise wollen sich die Automobilhersteller nur als Auftragsverarbeiter für die Werkstätten verstehen. Allerdings wurde bereits deutlich, dass die Hersteller aufgrund ihrer Produkthoheit (Verpflichtung zum Datenschutz durch Technikgestaltung, Art. 25 DS-GVO) und über die Bereitstellung von Diagnosehardware und -software – insbesondere Datenbanken und technische Betreuung – eine zentrale Rolle in der Verarbeitung der in der Werkstatt aus den Fahrzeugen erhobenen Daten innehaben. Die Frage der Verteilung der Verantwortlichkeiten zwischen Hersteller und Werkstätten sollten die Aufsichtsbehörden als nächstes mit den Automobilherstellern klären und dabei Wert auf größtmögliche Transparenz für die Kundinnen und Kunden legen.

Beim Automobilhersteller und in der Automobilwerkstatt können auch zunächst rein technisch verstandene Datenverarbeitungen durch die Verknüpfung mit Kundendaten, Kfz-Kennzeichen oder Fahrzeugidentifikationsnummer einen Personenbezug erhalten. Daher sind auch die Anforderungen hinsichtlich Rechtsgrundlagen, Zweckbindung, Schaffung von Transparenz und Aufteilung der Verantwortlichkeit zu erfüllen. Viele Verarbeitungsvorgänge in den Automobilwerkstätten sind bereits von den Automobilherstellern durch Setzen eines informationstechnischen Rahmens vorbestimmt. Wir sehen diese daher vorrangig in der Situation, im Rahmen ihrer technischen Hoheit die Automobilwerkstätten auch in datenschutzrechtlicher Hinsicht zu unterstützen. Wir werden unseren Fokus daher zukünftig auf die Hersteller legen.

4.3 Trotz Zulassung als Beweismittel im Einzelfall: Dauerhafter Einsatz von Dashcams weiterhin unzulässig!

Die Rechtsprechung war bisher in der Frage, ob Dashcams vor Gericht als Beweismittel dienen können, noch uneinheitlich. Der Bundesgerichtshof hat nun für mehr Klarheit gesorgt.

Bereits im 23. Bericht (siehe unter 14.2) hatten wir über den zunehmenden Gebrauch von Dashcams in öffentlich zugänglichen Bereichen, vor allem im Straßenverkehr, berichtet. Wir hatten darauf hingewiesen, dass dies zumeist datenschutzrechtlich unzulässig ist, weil mit den Dashcams anlasslos und dauerhaft Daten anderer Verkehrsteilnehmer (Bilddaten, Autokennzeichen) aufgezeichnet werden.

Ob derartige Aufnahmen vor Gericht verwertet werden können, wurde in der Rechtsprechung seinerzeit noch uneinheitlich beantwortet.

Der Bundesgerichtshof hat in einem Urteil vom 15. Mai 2018 (Az. VI ZR 233/17) in einem Zivilprozess im Hinblick auf die bisherige Rechtslage klargestellt, dass das permanente und anlasslose Aufzeichnen mit einer Dashcam im Straßenverkehr mit den datenschutzrechtlichen Bestimmungen nicht vereinbar und daher unzulässig ist. Ein Gericht kann allerdings unabhängig davon, im Rahmen einer Interessen- und Güterabwägung im Einzelfall, entscheiden, ob auf unzulässige Weise entstandene Dashcam-Aufzeichnungen dennoch als Beweismittel verwertet werden können.

Daran hat sich auch mit der Geltung der Datenschutz-Grundverordnung (DS-GVO) zum 25. Mai 2018 nichts geändert. Nach Art. 6 Abs. 1 Satz 1 Buchstabe f) der DS-GVO, § 4 Abs. 1 und 3 Bundesdatenschutzgesetz ist die Nutzung einer Dashcam im öffentlichen Raum weiterhin regelmäßig unzulässig und nach Art. 83 Abs. 5 Buchstaben a) und b) der DS-GVO bußgeldbewehrt. Hinzu kommt die fehlende Möglichkeit, an einem fahrenden Fahrzeug transparent im Sinne der Art. 12 ff. DS-GVO auf die kameragestützte Verarbeitung personenbezogener Daten hinzuweisen.

Anlasslose Aufzeichnungen durch Dashcams sind auch weiterhin datenschutzrechtlich unzulässig. Verstöße können mit einem Bußgeld geahndet werden. Gleichwohl können derartige Aufnahmen vor Gericht im Einzelfall als Beweismittel dienen.

5. Wirtschaft

5.1 Verhaltensregeln der deutschen Wirtschaftsauskunfteien zu Prüf- und Löschfristen

Die Datenschutz-Grundverordnung fördert – wie schon das bisherige Recht auch – die Selbstregulierung der Wirtschaft bei der Konkretisierung allgemein gehaltener Normen durch Verhaltensregeln. Pünktlich zum Start der DS-GVO hat die LDI NRW die Verhaltensregeln des Verbands „Die Wirtschaftsauskunfteien e.V." zum Thema Prüf- und Löschfristen genehmigt.

Unter dem Regime des Bundesdatenschutzgesetzes – alte Fassung (BDSG a. F.) existierten in Deutschland bis zum 24. Mai 2018 mit den §§ 28a, 29 und 35 BDSG a. F. dezidierte Regelungen für den Umgang mit personenbezogenen Daten durch Wirtschaftsauskunfteien. Mit unmittelbarer Geltung der DS-GVO ab dem 25. Mai 2018 sowie des neuen, an die DS-GVO angepassten Bundesdatenschutzgesetzes traten allgemeiner formulierte Normen in Kraft, die für bestimmte Wirtschaftsbereiche einer spezifischen Ausgestaltung bedürfen. Ein wichtiges Instrument für eine solche Ausgestaltung stellen die Verhaltensregeln (englisch: Code of Coduct – CoC) gemäß Art. 40 der DS-GVO dar.

Der Verband „Die Wirtschaftsauskunfteien e.V." hat von dieser Ausgestaltungsmöglichkeit zum Thema Prüf- und Löschfristen Gebrauch gemacht und seinen Entwurf mit den Datenschutzaufsichtsbehörden des Bundes und der Länder in mehreren Gremien der Datenschutzkonferenz (DSK) über einen längeren Zeitraum hinweg verhandelt und erörtert.

Pünktlich zum Start der DS-GVO wurde der LDI NRW dann eine konsolidierte Fassung vorgelegt, die auch die Zustimmung der DSK fand. Zum 25. Mai 2018 wurde diese Fassung von der LDI NRW genehmigt.

Die nunmehr geltenden Verhaltensregelungen zum Thema Prüf- und Löschfristen, denen sich alle großen deutschen Wirtschaftsauskunfteien unterworfen haben, führen zunächst den hohen, vormals in Deutschland geltenden Standard weiter. Darüber hinaus bieten sie aber auch wichtige Verbesserungen für Verbraucherinnen und Verbraucher.

So wird zukünftig nicht mehr jeweils zum Ende eines Kalenderjahres gelöscht – was in der Vergangenheit in Einzelfällen zu längeren Löschfristen geführt hatte –, sondern taggenau nach Ablauf der Frist. Die regelmäßigen Prüffristen werden von ehemals vier auf nunmehr durchgängig drei Jahre verkürzt. Außerdem erhalten die betroffenen Personen die Möglichkeit, eingemeldete personenbezogene Daten zu Dauerschuldverhältnissen mit finanziellem Ausfallrisiko für die Unternehmen unmittelbar nach Erledigung auf Antrag löschen zu lassen. Die Auskunfteien bleiben jedoch trotz des Fristenregimes nach dem CoC verpflichtet, auf Antrag eine individuelle Prüfung vorzunehmen, ob die Speicherung der Daten noch notwendig im Sin-

ne des Art. 17 Abs. 1 Buchstabe a) der DS-GVO ist. Der CoC unterliegt einer regelmäßigen Evaluierung.

Gemäß Art. 40 Abs. 6 DS-GVO haben wir als Genehmigungsbehörde die Verhaltensregeln auf unserer Internetseite www.ldi.nrw.de veröffentlicht.

Das Instrument der Verhaltensregeln hat eine große Wirkung, wenn es darum geht, abstrakte Regelungen für spezielle Wirtschaftsbereiche zu konkretisieren. Der vorlegende Verband sollte jedoch genau abwägen, welche Themen einem solchen CoC zugänglich sind. Es bietet sich an, Themen zu wählen, die sich mit klar abgegrenzten Bereichen beschäftigen. Die Verhaltensregeln der Wirtschaftsauskunfteien zu Prüf- und Löschfristen werden in der Zukunft zu einer höheren Rechtssicherheit für Verbraucher und Wirtschaftsauskunfteien beitragen.

5.2 Prüfung von Inkassounternehmen

Die Durchsetzung von Geldforderungen durch private Unternehmen unter Zuhilfenahme von Inkassounternehmen ist im Alltag oft streitbefangen. Deshalb ist es sehr wichtig, dass die Inkassounternehmen auf der Grundlage korrekter Daten arbeiten und im Umgang mit diesen Daten den Datenschutz beachten. Wir haben daher diesen Wirtschaftszweig besonders überprüft und stellen hier die wichtigsten datenschutzrechtlichen Anforderungen zusammen.

Der Schwerpunkt der Prüfung zur Datenverarbeitung in Inkassounternehmen lag auf der elektronischen Datenerhebung, insbesondere unter Einschaltung von Adressermittlungsdienstleistern, der Zusammenarbeit mit Wirtschaftsauskunfteien und der Auskunfterteilung nach § 34 Bundesdatenschutzgesetz – alte Fassung (BDSG a. F.), Art. 15 der Datenschutz-Grundverordnung (DS-GVO).

Viele bei der LDI NRW eingehende Beschwerden über die Datenverarbeitung durch Inkassounternehmen haben eine Personenverwechslung zum Inhalt. Bei der Prüfung wurde daher besonderes Augenmerk auf die Adressermittlungen über eingeschaltete Dienstleister gelegt. Um Personenverwechslungen auszuschließen, muss das Inkassounternehmen bei Adressermittlungen sicherstellen, dass Name, Anschrift und Geburtsdatum der Schuldnerinnen und Schuldner entsprechend den Angaben der Gläubiger übermittelt und die zurückgelieferten Daten entsprechend abgeglichen werden. Sollte sich herausstellen, dass Datensätze bei einem Adressdienstleister falsch miteinander verknüpft wurden, legen wir Wert auf eine entsprechende Rückmeldung an den Dienstleister, um diesem eine Korrektur zu ermöglichen und Wiederholungsfälle für die Zukunft zu vermeiden. Darüber hinaus bietet es sich an, durch Speicherung der fälschlich ermittelten Adresse sicherzustellen, dass diese Person nicht erneut als vermeintliche Schuldnerin oder vermeintlicher Schuldner angeschrieben wird.

Inkassounternehmen dürfen Bonitätsdaten über Schuldnerinnen und Schuldner bei Wirtschaftsauskunfteien auf der Grundlage von Art. 6 Abs. 1 Satz 1 Buchstabe f) der DS-GVO abfragen, wenn ein berechtigtes Interesse an dieser Datenerhebung vorliegt. Gegenüber den Inkassounternehmen wurde deutlich gemacht, dass ein solches Interesse zum Beispiel dann zu bejahen ist, wenn eine Entscheidung über die Einleitung von weiteren Maßnahmen mit einem finanziellen Ausfallrisiko – auch in Bezug auf die entstehenden Beitreibungskosten – ansteht.

Die Datenschutzkonferenz weist in ihrem Beschluss vom 23. März 2018 darauf hin, dass die Einmeldung offener und unbestrittener Forderungen in eine Wirtschaftsauskunftei nach Art. 6 Abs. 1 Satz 1 Buchstabe f) der DS-GVO nur bei Vorliegen von bestimmten, strengen Voraussetzungen möglich ist, die sich am bisherigen Rechtsverständnis orientieren.

Den Beschwerden war häufig zu entnehmen, dass ein Bestreiten der Forderung durch die Schuldnerin oder den Schuldner entweder gar nicht oder erst verspätet – auf nochmaligen Hinweis – berücksichtigt wurde. Ein einfaches Bestreiten ist dabei ausreichend, ein qualifizierter Vortrag der Schuldnerin oder des Schuldners ist nicht zwingend erforderlich. Das Bestreiten der Forderung muss im Datenbestand, zum Beispiel über ein bestimmtes Merkmal, erfasst und damit sichergestellt werden, dass eine Einmeldung bei einer Auskunftei dann nicht mehr möglich ist. Durch technisch-organisatorische Maßnahmen muss das Inkassounternehmen zudem vor einer Übermittlung an eine Auskunftei dafür Sorge tragen, dass nicht zuvor ein Bestreiten gegenüber der Gläubigerin oder dem Gläubiger erfolgt ist; ggf. ist eine Nachberichtigung an die Auskunftei erforderlich.

Offene Forderungen, die den Auskunfteien gemeldet worden sind, aber deren Einziehung nicht mehr weiter betrieben wird, sollen jährlich überprüft und der Abbruch der Weiterverfolgung den Auskunfteien mitgeteilt werden, denen diese bereits zuvor als Negativmerkmal übermittelt wurden. Auch bei Eintritt der Löschfristen sollte eine entsprechende Meldung an die jeweilige Auskunftei erfolgen.

In der Inkassopraxis ist die Erteilung einer Auskunft über die zu einer Person gespeicherten Daten (§ 34 BDSG a.F., Art. 15 DS-GVO) sowie die Berichtigung, Löschung und Sperrung (§ 35 BDSG a.F., Art. 16, 17, 18 DS-GVO) von großer Bedeutung. In diesen Bereichen kann bereits der faire Umgang zwischen den Inkassounternehmen und den Schuldnerinnen und Schuldnern viele Konflikte vermeiden. Deshalb legen wir Wert darauf, dass die Inkassounternehmen die Rechte der betroffenen Personen datenschutzrechtlich einwandfrei gewährleisten. Hierzu geben wir die nachfolgenden Empfehlungen:

Auskunftsbegehren, Lösch- und Sperrersuchen sowie weitere Rechte der Betroffenen sollten in einem Unternehmen von speziellen Teams im Datenschutzbereich bearbeitet werden.

Die Einführung eines Prozesses, durch den schnell festgestellt wird, welche Rechte die Anfragenden geltend machen, um die Bearbeitung zielsicher zu steuern, halten wir für unerlässlich. Hierzu eignen sich zum Beispiel das Vier-Augen-Prinzip bei der Sichtung der Eingänge, Schlüsselwortlisten bei der manuellen Bearbeitung des Posteingangs oder Texterkennungssoftware, die datenschutzrelevante Schlagwörter erkennt.

Wenn sich die Bearbeitung eines Antrags zur Geltendmachung eines Betroffenenrechts – zum Beispiel ein Auskunftsverlangen – verzögert, hat das Unternehmen, eine kurze Zwischeninformation mit Erläuterung zur Verspätung zu senden (siehe auch Art. 12 Abs. 3 der DS-GVO).

Da es sich um höchstpersönliche Daten handelt, dürfen diese auch nur an die anfragende Person selbst beauskunftet werden. Hierauf ist insbesondere bei mündlicher oder elektronischer Auskunftserteilung zu achten. Hat der Verantwortliche begründete Zweifel an der

Identität eines Antragstellers auf Datenauskunft, so kann er nach Art. 12 Abs. 6 der DS-GVO zusätzliche Informationen zur Bestätigung der Identität nachfordern. Erwägungsgrund Nr. 64 der DS-GVO sieht vor, dass in diesen Fällen „alle vertretbaren Mittel“ genutzt werden sollen, um die Identität einer Auskunft ersuchenden Person zu überprüfen. Dem Verantwortlichen steht ein Ermessensspielraum hinsichtlich der Beurteilung des Vorliegens begründeter Zweifel zu. Eine Personalausweiskopie ist aber nur ausnahmsweise zu fordern, wenn ernstliche Zweifel an einer sicheren Identifikation bestehen. Dabei ist seitens der Unternehmen darauf hinzuweisen, dass auf der Kopie alle bis auf die für die Identifikation erforderlichen Datenfelder (Name, Anschrift und Geburtsdatum) durch die betroffene Person geschwärzt werden können.

Auskunftsersuchen und ihre Erledigung sind nicht so lange aufzubewahren wie Unterlagen für steuerliche oder handelsrechtliche Zwecke. Die Aufbewahrungsfrist richtet sich vielmehr nach der Überprüfungsmöglichkeit durch die Datenschutzaufsichtsbehörden. Da die Verfolgungsverjährung drei Jahre beträgt, wäre eine gleichlaufende Aufbewahrungsfrist angemessen. Eine Aufbewahrungspflicht bei Negativauskünften – das heißt die Auskunft, dass zu einer Person keine Daten vorliegen – ist nicht gegeben. Es besteht aber eine Berechtigung zur Aufbewahrung, um im Falle der Kontrolle durch die Datenschutzaufsicht die Pflichterfüllung nachweisen zu können. Drei Jahre dürften auch in diesen Fällen die Höchstgrenze bilden.

Unsere Prüfung hat gezeigt, dass die Geschäftsprozesse zur Umsetzung der datenschutzrechtlichen Anforderungen bei den Inkassounternehmen insgesamt bereits gut verankert sind. Die LDI NRW achtet verstärkt darauf, dass auch den Mitarbeiterinnen und Mitarbeitern mit direktem Kontakt zur Schuldnerin oder zum Schuldner diese Prozesse und Anforderungen laufend vermittelt werden.

Der zügigen und vollständigen Beachtung von Betroffenenrechten misst die DS-GVO große Bedeutung zu. Sie ist ein Indiz für den fairen Umgang miteinander. Ihre Nichterfüllung kann daher hohe Sanktionen nach sich ziehen.

Bei vielen Unternehmen besteht im Zusammenhang mit Personenverwechslungen noch Handlungsbedarf, insbesondere in Bezug auf ein Rückmeldesystem an den Adressdienstleister und bei der Sicherstellung, dass es nicht infolge einer weiteren Schuldnerermittlung zu einer erneuten Personenverwechslung kommt.

5.3 Identitätsprüfung beim Online-Banking

Für die Kontoeröffnung beim Online-Banking nutzen Kundinnen und Kunden das POSTIDENT-Verfahren der Deutschen Post AG. Kurze Zeit später erhalten sie an ihre E-Mail-Adresse und über ihr Handy den Hinweis, sich im POSTID-Portal registrieren zu lassen. Entspricht dieses Verfahren den Grundsätzen des Datenschutzes?

Seit 2017 erreichten die LDI NRW vermehrt Anfragen besorgter Bürgerinnen und Bürger zu POSTIDENT und POSTID: Zwei Dienstleistungsangebote der Deutschen Post AG zur Identifizierung von Personen mit ähnlicher Bezeichnung, aber unterschiedlicher Zielsetzung, führten zu Verwirrung.

Was ist POSTIDENT?

Bei den POSTIDENT-Verfahren handelt es sich um ein Dienstleistungsangebot der Deutschen Post AG zur Identitätsprüfung, das die Deutsche Post AG für ihre verschiedenen Geschäftskundinnen und -kunden durchführt, wie zum Beispiel Banken. Nach § 11 Geldwäschegesetz (GwG) müssen Banken ihre Vertragspartner, für diese auftretende Personen und wirtschaftlich Berechtigte identifizieren und die Identifizierung dokumentieren. Im Zuge der auf die 4. EU-Geldwäscherichtlinie zurückgehenden Änderungen des GwG sind Banken nach § 8 Abs. 2 GwG nunmehr sogar verpflichtet, vollständige Kopien der Ausweisdokumente anzufertigen oder sie vollständig optisch digitalisiert zu erfassen (scannen). Eine Schwärzung muss und darf die Bank daher nicht mehr vornehmen.

Die Identitätsprüfung dient der Geldwäscheprävention und damit der Bekämpfung organisierter Kriminalität. Sie ist auch in datenschutzrechtlicher Hinsicht nach Art. 6 Abs. 1 Satz 1 Buchstabe c) der Datenschutz-Grundverordnung (DS-GVO) rechtmäßig. Die Daten zum Nachweis der Identifizierung erhebt die Deutsche Post AG als datenschutzrechtlich Verantwortlicher (Art. 4 Nr. 7 DS-GVO) nur temporär und löscht sie nach der Übermittlung an die Bank. Bei der Bank als weitere verantwortliche Stelle kann die Kundschaft Auskunft über ihre dort gespeicherten Daten und deren zweckgebundene Speicherdauer erfragen. Die Erhebung der Daten für die geldwäscherechtliche Identitätsprüfung erfolgt immer nur für den Einzelfall. Für weitere Identifizierungsanlässe gemäß GwG bedarf es der Durchführung eines erneuten POSTIDENT-Verfahrens.

Und warum dann zusätzlich eine POSTID?

Von dem POSTIDENT-Verfahren zu unterscheiden ist das POSTID-Portal, einem weiteren Dienstleistungsangebot der Deutschen Post AG. Die POSTID kann für Identifizierungsanlässe genutzt werden, die keine Konformität nach dem GwG erfordern. Die Deutsche Post AG bietet diesen Service als „Ausweis für das digitale Leben“ an, um den Zugang zu Online-Portalen und in Communities mit Identitäts- und Altersnachweis zu vereinfachen, wie zum Beispiel beim Carsharing und der Autovermietung, bei Handyverträgen oder zum Freischalten der Inhalte bei digitalen Entertainment-Anbietern. Im Auftrag des Kunden wer-

den dann ausgewählte Identitätsdaten im POSTID-Portal des Kunden archiviert und für eine Wiederverwendung zur Verfügung gestellt, ohne eine erneute Identifizierung durchführen zu müssen, sofern das entsprechende Angebot nicht dem GwG unterliegt.

Bei einzelnen Geschäftskunden der Deutschen Post AG kann das POSTIDENT-Verfahren bislang nicht ohne Weiterleitung auf das POSTID-Portal, das weitere Dienstleistungsangebot der Deutschen Post AG, genutzt werden.

Geschäftskunden der Deutschen Post AG, insbesondere Telekommunikationsunternehmen und Banken, haben die Möglichkeit, ihre Kundinnen und Kunden mit dem POSTID-Portal zu verlinken und verschiedene Identifizierungsverfahren zur Auswahl zu stellen. Diese Unternehmen leiten die auf ihrer Webseite im Rahmen der Erstregistrierung erhobenen Daten ihrer Kundschaft (inklusive E-Mail-Adresse und Mobilfunknummer) an die Deutsche Post AG weiter.

Die Weiterleitung der Daten erfolgt aber erst, nachdem die Kundinnen und Kunden den Allgemeinen Geschäftsbedingungen der Deutschen Post AG für die Nutzung des POSTID-Portals und den dazugehörigen Datenschutzhinweisen zugestimmt haben. Wählen sie zum Beispiel zur geldwäscherechtlichen Identitätsprüfung die Identifizierung durch die Postfiliale, stimmen sie durch Klicken des Buttons „Coupon herunterladen“ den Allgemeinen Geschäftsbedingungen für die Nutzung des POSTID-Portals und den Datenschutzhinweisen zu.

Mit der Zustimmung kommt ein Vertrag zwischen der zu identifizierenden Person und der Deutschen Post AG zustande. Dieser ist Grundlage für die Vorhaltung und Verwendung der in den Datenschutzhinweisen aufgeführten Identitätsdaten bei der Deutschen Post AG (Art. 6 Abs. 1 Satz 1 Buchstabe b) der DS-GVO). Über die so der Deutschen Post AG übermittelte E-Mail-Adresse übersendet die Deutsche Post AG den Aktivierungslink für die POSTID (Double-Opt-In). Durch Registrierung auf dem POSTID-Portal kann die Kundin oder der Kunde die POSTID aktivieren und so für weitere einfache digitale Identifizierungsanlässe nutzen, sofern diese keine Konformität nach dem GwG erfordern. Sofern jedoch die Registrierung auf dem POSTID-Portal nicht abschließend vorgenommen wurde, wird die Deutsche Post AG die ihr übermittelten Daten nach 90 Tagen löschen.

Schaffung von Transparenz als Problemlöser!

Der Unterschied zwischen POSTIDENT und POSTID wurde nicht erkannt. Dies betraf insbesondere den verwendeten Hinweistext zur Zustimmung zu den Allgemeinen Geschäftsbedingungen und die Datenschutzhinweise zum POSTID-Portal.

Infolge unserer mit der Deutschen Post AG geführten Gespräche konnte die LDI NRW die Überarbeitung sowohl des Hinweistextes als auch der Datenschutzhinweise zum POSTID-Portal erreichen. Eine vereinfachte Darstellung, insbesondere die Vereinheitlichung verwendeter Begriffe und eine klare Übersicht über die Löschpflichten in den Datenschutzhinweisen, tragen zur bes-

seren Verständlichkeit der beiden Angebote bei.

Das Beschwerdeaufkommen hierzu bei der LDI NRW hat sich im Anschluss entsprechend deutlich reduziert.

Unsere weitere Forderung nach einer Trennung des POSTIDENT-Verfahrens vom POSTID-Portal bei allen Geschäftspartnern bedarf noch der Umsetzung. Diese würde die erforderliche Transparenz in der Abgrenzung der beiden Dienstleistungsangebote der Deutschen Post AG zum POSTIDENT-Verfahren einerseits und zum POSTID-Portal andererseits erhöhen.

Unternehmen müssen stets darauf achten, dass sie ihre Dienstleistungsangebote mit ihrer Markteinführung nachvollziehbar erläutern. Denn mehr Transparenz in der Datenverarbeitung schafft mehr Akzeptanz bei den Bürgerinnen und Bürgern.

6. Datenschutz im Verein und Ehrenamt nach der DS-GVO

Bei der Umsetzung der DS-GVO durch Vereine und im Ehrenamt ist der Beratungsbedarf sehr hoch. Die Verunsicherung erklärt sich zum Teil mit der Furcht vor Sanktionen, und teilweise besteht auch Nachholbedarf im praktischen Vollzug.

Die Berichterstattung zur DS-GVO veranlasste viele Vereine, sich mit Anfragen an die LDI NRW zu wenden. Obwohl die DS-GVO gegenüber der bisherigen Rechtslage nur wenige wesentliche Änderungen für die Vereine mit sich brachte, war die Verunsicherung bei den Vereinen groß.

So hat sich bereits vor, aber vor allem nach Geltung der DS-GVO zum 25. Mai 2018 die Zahl der schriftlichen Anfragen gegenüber dem Vorjahr verdreifacht; hinzu kommt eine große Anzahl telefonischer Anfragen. Hauptsächlich geht es darum, wie die DS-GVO in der Vereinspraxis umzusetzen ist.

Dabei ist festzustellen, dass sich die zumeist ehrenamtlichen Vereinsfunktionäre – vor allem in kleinen Vereinen – mit dem Regelwerk teilweise überfordert fühlen. Dies nicht zuletzt, weil die DS-GVO sowohl von (rechtsfähigen und nicht rechtsfähigen) Vereinen und Stiftungen als auch von Unternehmen und Behörden zu beachten ist – unabhängig von ihrer Größe und Organisation. Erwähnt sei, dass die DS-GVO auch für selbstorganisierte Gruppen gilt, wenn sie personenbezogene Daten verarbeiten.

Viele der Regelungen in der DS-GVO, die unmittelbar auch für Vereine gelten, stellen keine gravierenden Änderungen gegenüber der bisherigen Rechtslage dar. In der Beratungspraxis hat sich aber gezeigt, dass bei vielen Vereinen auch schon in Bezug auf das bislang geltende Datenschutzrecht Nachholbedarf besteht.

Die meisten Anfragen beziehen sich auf die datenschutzgerechte Erhebung, Speicherung und Nutzung von Mitgliederdaten und die damit verbundene Gestaltung von Formularen, die Gestaltung von Webseiten, die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten sowie die Benennung von Datenschutzbeauftragten. Weitere Anfrageschwerpunkte sind die Einhaltung der Informationspflichten und die Möglichkeit Einwilligungserklärungen einzuholen.

Das ehrenamtliche Engagement in und außerhalb von Vereinen ist eine wichtige gesellschaftliche Aufgabe. Es geht nicht darum Vereine zu sanktionieren, sondern den Datenschutz auch mit Hilfe der neuen EU-Regeln zu stärken. Dabei stehen wir den Vereinen in erster Linie mit adressatengerechter Beratung zur Seite. Hauptziel ist es, in den Vereinen einen guten Schutz der ihnen anvertrauten Daten zu erreichen.

Die Verhängung einer Geldbuße ist dabei nur eine von vielen Möglichkeiten, die uns als Aufsichtsbehörde zur Verfügung stehen, wie etwa die Erteilung von

Hinweisen, Warnungen und Verwarnungen.

Gerade in den zumeist ehrenamtlich geführten kleineren Vereinen fehlt es häufig an Zeit und Mitteln für eine umfangreiche Prüfung und Umsetzung der datenschutzrechtlichen Regularien.

Es gibt zwar einige Hilfestellungen – etwa im Internet – aber häufig bleibt unklar, was dies für die Arbeit im Verein konkret bedeutet.

Um diese Lücke zu schließen, haben wir die Broschüre „Datenschutz im Verein nach der Datenschutz-Grundverordnung“ vorgelegt. Sie ist ein praxisorientierter Ratgeber mit konkreten Beispielen und Mustertexten.

Im März 2018 haben wir auf der Grundlage der regelmäßig gestellten Fragen in einer umfangreichen Presseinformation über die Auswirkungen der DS-GVO in Vereinen und Ehrenamt informiert (Abdruck im Anhang).

Auch in Vereinen und im Ehrenamt ist Datenschutz wichtig und richtet sich nach der DS-GVO. Bei der Umsetzung steht für die LDI NRW Beratung und Unterstützung der Vereine im Vordergrund. Auf unserer Homepage www.ldi.nrw haben wir unseren praxisorientierten Ratgeber „Datenschutz im Verein nach der Datenschutz-Grundverordnung“ mit Fallbeispielen und Mustertexten eingestellt.

7. Datenschutz am Arbeitsplatz

7.1 Digitalisierte Personalakten in der Landesverwaltung

Die Einführung digitalisierter Personalakten in der Landesverwaltung wird intensiv vorbereitet. Bereits bei der Planung des Umstellungsverfahrens sind datenschutzrechtliche Vorgaben zur automatisierten Verarbeitung der Daten der Betroffenen in die Projektgestaltung einzubeziehen.

Das Innenministerium hat der LDI NRW eine Entwurfsfassung der Richtlinien über die Personalaktenführung zur Kenntnis gegeben. Diese Regelungen sollen dazu beitragen, dass die Landesbehörden ihrer Pflicht gemäß § 9 Abs. 3 des Gesetzes zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen nachkommen können, ihre Akten spätestens ab dem 1. Januar 2022 ausschließlich elektronisch zu führen. Um eine gesetzeskonforme Überführung der bisherigen in digitalisierte Personalakten zu gewährleisten, muss mit den dazu erforderlichen Maßnahmen zügig begonnen werden.

Hierzu haben wir in einer ausführlichen Stellungnahme Hinweise gegeben und Vorschläge unterbreitet, wie den Datenschutzanforderungen genügt werden kann. Personalakten von Beamtinnen und Beamten sowie von Tarifbeschäftigten enthalten eine Vielzahl sensibler, dem Personalaktengeheimnis unterliegender Daten, deren Schutz vom Recht der Betroffenen auf informationelle Selbstbestimmung umfasst ist. Besonders wichtig sind Maßnahmen, die gewährleisten, dass die Daten bei der Digitalisierung der Personalakten vollständig und inhaltlich richtig elektronisch erfasst und gespeichert werden. Demnach müssen hohe technische und organisatorische Anforderungen erfüllt werden, damit Beeinträchtigungen der Rechte Betroffener ausgeschlossen sind. Insoweit ist insbesondere Folgendes zu beachten:

- Das manipulationssichere Scannen muss gewährleistet sein. In der elektronischen Personalakte gespeicherte Dokumente müssen mit den Originaldokumenten bildlich und inhaltlich übereinstimmen.

- Ein gescanntes Dokument ist beweissicher mit einer qualifizierten elektronischen Signatur zu versehen. Geprüft werden muss, ob und gegebenenfalls bei welchen Dokumenten eine Vernichtung aufgrund einer gesetzlich vorgeschriebenen Schriftform bzw. einer Pflicht zur Aufbewahrung von Originaldokumenten ausgeschlossen ist.

- Für den Ablauf des Scanverfahrens sollte geregelt werden,

  • welche Maßnahmen zu treffen sind, falls während des Scannens Originale der Personalakten beschädigt oder zerstört werden oder ein Originaldokument verloren geht,

  • wie die Dokumentation zur Nachvollziehbarkeit von Fehlerfällen beim Einscannen erfolgt und

• in welcher Form eine vollständige Sichtprüfung durchgeführt wird.

- Die Integrität der elektronischen Akte muss insgesamt sichergestellt sein. Dies bedeutet, dass Dokumente nicht nachträglich entfernt oder hinzugefügt werden. Bei automatisierter Speicherung von Personalaktendaten müssen die entsprechenden Daten, soweit dies gesetzlich (etwa aus disziplinarrechtlichen Gründen) geboten ist, gelöscht werden, ohne Spuren zu hinterlassen.

- Zudem ist zu gewährleisten, dass elektronisch gespeicherte Personalaktendaten unverzüglich gelöscht werden, soweit sie für Zwecke der Personalverwaltung und Personalwirtschaft nicht mehr erforderlich und die gesetzlichen Aufbewahrungsfristen abgelaufen sind.

- Durch ein geeignetes Protokollierungsverfahren muss ferner gewährleistet werden, dass nachträglich überprüft werden kann, wer welche Beschäftigtendaten zu welchem Zeitpunkt eingegeben, verändert, übermittelt und abgerufen hat.

- Insgesamt müssen die Datensicherungsmaßnahmen der deutlich längeren, regelmäßig mehrere Jahrzehnte dauernden Aufbewahrung von Personalakten gerecht werden. Dies bedeutet, dass eine Verfügbarkeit der Daten auch bei Veränderung von technischen Standards während der Gesamtaufbewahrungsdauer der elektronischen Personalakte gewährleistet sein muss.

- Sichergestellt werden muss zudem, dass nach einer Umstellung auf die elektronische Personalaktenführung die Einsichts- und Auskunftsrechte der Beschäftigten, die zu ihren grundlegenden Datenschutzrechten gehören, nicht eingeschränkt werden.

Nur wenn die aufgezeigten Maßnahmen konsequent umgesetzt werden, kann eine auch datenschutzrechtlich reibungslose Umstellung der Personalaktenführung gelingen.

7.2 Beschwerdemanagement im öffentlichen Personennahverkehr (ÖPNV) – Recht auf Auskunft der beschäftigten Fahrerinnen und Fahrer

Der Auskunftsanspruch von Beschäftigten gegenüber ihrem Arbeitgeber ist sicher zu stellen und darf nicht am Beschwerdemanagement des Auftragsgebers scheitern, der im Verhältnis zu den Beschäftigten Dritter ist.

Im ÖPNV können private Verkehrsunternehmen, zum Beispiel Mitgliedsunternehmen von Verkehrsverbünden, als sogenannte „Linienkonzessionäre“ in einer bestimmten Region eingesetzt werden. Sie haben die Genehmigung für die Errichtung und den Betrieb eines Linienverkehrs mit Kraftfahrzeugen gemäß § 42 Personenbeförderungsgesetz (PBefG). Diese beinhaltet die Pflicht zur Beförderung gemäß § 22 PBefG sowie die Pflicht zur Aufrechterhaltung des Betriebs gemäß § 21 PBefG.

Linienkonzessionäre vergeben Aufträge an Leistungserbringer im Linienverkehr (Partnerunternehmen), die ganz oder zum Teil das Fahrpersonal für die vom Verkehrsunternehmen überlassenen Fahrzeuge stellen (zum Beispiel Busse). Zwischen dem Fahrgast und dem Partnerunternehmen kommt kein Beförderungsvertrag zustande, sondern allein zwischen dem Fahrgast und dem Linienkonzessionär.

In einem hier zu bewertenden Fall gingen Beschwerden gegen das Fahrpersonal ausschließlich beim Linienkonzessionär ein. Das Beschwerdemanagement war so eingerichtet, dass zwar der Inhalt der Beschwerde elektronisch an das Partnerunternehmen zur internen Prüfung und zum Bericht übermittelt wurde. Allerdings erhielten weder das Partnerunternehmen als Arbeitgeber noch das betroffene Fahrpersonal Kenntnis über die Identität des Beschwerdeführers oder der Beschwerdeführerin. Umgekehrt wurden die personenbezogenen Daten des Fahrpersonals in der Regel nicht an den Linienkonzessionär weitergegeben.

Im konkreten Beschwerdefall ermittelte das Partnerunternehmen anhand der vom Linienkonzessionär mitgeteilten Beschwerde den kritisierten Fahrer.

Dem Auskunftsbegehren des betroffenen Fahrers gegenüber seinem Arbeitgeber konnte dieser nicht entsprechen, da er keine Kenntnis über die Identität des Beschwerdeführers hatte.

Aufgrund dieser Konstellation haben Fahrerinnen und Fahrer, über die sich jemand beschwert hat, nur die Möglichkeit, den Linienkonzessionär (Auftraggeber) um Auskunft zu bitten. Zu diesem Zweck hätte er allerdings seine personenbezogenen Daten übermitteln müssen, was mit dem Schutz der Fahrerdaten nicht zu vereinbaren gewesen wäre.

Unsere Prüfung ergab, dass die genannte Praxis des Beschwerdemanagements mit den Anforderungen des Beschäftigtendatenschutzes nicht zu vereinbaren ist. Verantwortliche Stelle für die Prüfung von Beschwerden gegen

Fahrerinnen und Fahrer sind die jeweiligen Partnerunternehmen als Arbeitgeber. Ihnen obliegt gem. § 26 Abs. 1 Bundesdatenschutzgesetz (BDSG) die Verhaltens- und Leistungskontrolle ihrer Beschäftigten (§ 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz – alte Fassung – BDSG a. F.). Sie sind gegenüber ihren Beschäftigten gem. Art. 15 DS-GVO (§ 34 Abs. 1 BDSG a. F.) zur Auskunft verpflichtet – auch über die Herkunft ihrer Daten. Soweit der Linienkonzessionär die Identität der Beschwerde führenden Person nicht an das Partnerunternehmen weitergibt, kann dieses seiner Verpflichtung zur Auskunftserteilung gegenüber der betroffenen Fahrerin bzw. dem betroffenen Fahrer nicht nachkommen.

Nach umfassender Erörterung der datenschutzrechtlichen Aspekte hat der Linienkonzessionär sein Beschwerdemanagement neu aufgestellt.

Er gibt die personenbezogenen Daten der Beschwerde führenden Person nunmehr nach Prüfung und sorgfältiger Abwägung der Belange der betroffenen Personen im Einzelfall gemäß Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO (§ 28 Abs. 1 Satz 1 Nr. 1 und 2; Abs. 2 Nr. 2 Buchstabe a) BDSG a. F.) an das Partnerunternehmen weiter. Damit ist die Auskunftserteilung hinsichtlich der Beschwerde führenden Person gegenüber dem oder der Beschäftigten jetzt möglich.

Arbeitgeber müssen betroffene Beschäftigte in einem Beschwerdefall gemäß Art. 15 DS-GVO (§ 34 Abs. 1 BDSG a. F.) auch über die Herkunft der Daten unterrichten. Dazu bedürfen sie entsprechender Informationen durch die Stelle, bei der die Beschwerde eingegangen ist, zum Beispiel einem Auftraggeber. Dieser muss vor einer Datenweitergabe die berechtigten Interessen abwägen: Das Interesse der Beschwerde führenden Person an der vertraulichen Behandlung ihrer Mitteilung mit dem Interesse der Auftragnehmerin bzw. des Auftragnehmers und/oder der betroffenen Beschäftigten an der Datenverarbeitung. Eine pauschale Verweigerung der Datenübermittlung ist datenschutzrechtlich nicht zulässig.

7.3 Kopien von Personalausweisen und Pässen zum Nachweis der Einhaltung des Arbeitnehmerüberlassungsgesetzes nicht erforderlich

Unsicherheiten bestanden in der Frage, ob Zeitarbeitsfirmen zum Nachweis der Einhaltung des Arbeitnehmerüberlassungsgesetzes Kopien von Personalausweisen und Pässen von Bewerberinnen und Bewerbern bzw. der Beschäftigten anfertigen dürfen oder müssen. Nunmehr besteht darüber Klarheit.

Ein Unternehmen der Zeitarbeitsbranche verlangte von Bewerberinnen und Bewerbern sowie von Leiharbeitskräften die Kopie von Personalausweisen, um die Staatsangehörigkeit und damit die Einhaltung ausländerrechtlicher Vorschriften unter anderem gegenüber der Bundesagentur für Arbeit nachweisen zu können. Um den Nachweis führen zu können, dass die Beschäftigten tatsächlich keine Aufenthalts- und/oder Arbeitspapiere benötigen, wurden allerdings auch Ausweiskopien von Deutschen und EU-Bürgern angefertigt.

Nach der seit 2017 – nur für Deutsche geltenden – gesetzlichen Regelung in § 20 Abs. 2 Personalausweisgesetz (PauswG) darf der Ausweis nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Ausweisinhabers tun. Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt.

Datenschutzrechtlich muss die Kopie allerdings weiterhin erforderlich sein. Die Erforderlichkeit entfällt, wenn der Personalausweis ohne großen Aufwand vor Ort vorgezeigt und eingesehen werden kann.

Mit Unterstützung der LDI NRW konnte mit den beteiligten Behörden (Bundesministerium für Arbeit und Sozialordnung, Bundesministerium des Innern, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bundesagentur für Arbeit) geklärt werden, dass Erlaubnisinhaber nach dem Arbeitnehmerüberlassungsgesetz zwar in geeigneter Form nachweisen müssen, dass sie die Vorschriften über die Ausländerbeschäftigung einhalten. Dieser Nachweis kann insbesondere durch eine Fotokopie des Aufenthaltstitels betroffener Leiharbeitskräfte in der Personalakte geführt werden. Fotokopien von Personalausweisen und Pässen sind jedoch nicht erforderlich und werden seitens der Bundesanstalt für Arbeit auch nicht verlangt. Es reicht aus, wenn Erlaubnisinhaber den Personalausweis bzw. Reisepass im Original einsehen und relevante Daten (Staatsangehörigkeit) in der Personalakte dokumentieren. Das Unternehmen und der Petent wurden

durch die LDI NRW entsprechend unterrichtet.

Kopien von Personalausweisen und Pässen sind nicht erforderlich, um nachzuweisen, dass die Vorschriften über die Ausländerbeschäftigung eingehalten werden. Es reicht aus, wenn Leiharbeitsunternehmen eine Fotokopie des Aufenthaltstitels betroffener Leiharbeitskräfte in deren Personalakte aufnehmen bzw. den Personalausweis oder Reisepass von Deutschen und EU-Bürgern im Original einsehen und relevante Daten (Staatsangehörigkeit) in der Personalakte dokumentieren.

7.4 Satellitengestützte Ortung zur Positionsbestimmung von Firmenfahrzeugen – kein zulässiges Mittel für eine Überwachung von Beschäftigten

Die Nutzung moderner Ortungssysteme wie das Global Positioning System (GPS) zur Positionsbestimmung von Fahrzeugen darf nicht zur lückenlosen Verhaltens- und Leistungskontrolle von Beschäftigten genutzt werden. Eingesetzt werden dürfen Sie nur, wenn es zur Durchführung des Arbeitsverhältnisses oder Steuerung der betrieblichen Belange erforderlich ist. Einwilligungen Beschäftigter sind regelmäßig unwirksam.

Immer häufiger erreichen uns Anfragen von besorgten Beschäftigten zur Frage der datenschutzrechtlichen Zulässigkeit des Einsatzes von Ortungssystemen in Firmenfahrzeugen. Im Mittelpunkt steht dabei regelmäßig die Besorgnis, der Arbeitgeber könne die Daten zu einer Vollkontrolle der Beschäftigten nutzen, etwa indem er die Fahrstrecken- und die Standortdaten oder die Daten zur Aufenthaltszeit an einem bestimmten Ort kontinuierlich erhebt und auswertet (siehe 23. Bericht unter 9.2.1).

Die mittels GPS-Ortung erfolgende Verarbeitung personenbezogener Daten von Beschäftigten kann nach § 26 Abs. 1 BDSG (bis 25. Mai 2018: § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz – alte Fassung) zulässig sein, soweit sie für die Durchführung des Arbeitsverhältnisses erforderlich ist. Daneben kommt Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO als Rechtsgrundlage in Betracht. Danach ist die Datenverarbeitung zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, die den Schutz personenbezogener Daten erfordern.

So ist es datenschutzrechtlich unproblematisch, wenn die Ortung zur reinen Standortbestimmung erfolgt, um ggf. weitere Aufträge zu einer standortnahen Zieladresse vergeben zu können. Auch die Erfassung der Arbeitszeit kann mittels eines Ortungssystems zur Durchführung des Arbeitsverhältnisses erfolgen. Die Zulässigkeit der Spurverfolgung (Streckenverfolgung) zum Nachweis bzw. zur Rückverfolgung einer Auftragsanfahrt bemisst sich demgegenüber nach Art. 6 Abs. 1 Satz 1 Buchstabe f) DS-GVO. Erforderlich ist insoweit eine Abwägung mit den schutzwürdigen Interessen der betroffenen Beschäftigten. Es muss sichergestellt sein, dass die Daten nicht zur Verhaltens- und Leistungskontrolle herangezogen werden. Unabhängig davon, ob der Arbeitgeber beabsichtigt, die genannten technischen Einrichtungen zu Kontrollzwecken der Beschäftigten zu nutzen, handelt es sich bei deren Einsatz regelmäßig um eine Maßnahme, die zur Überwachung des Verhaltens und der Leistung der Beschäftigten objektiv geeignet ist (ständige Rechtsprechung des Bundesarbeitsgerichts, BAG Beschluss vom 6. Dezember 1983, 1 ABR 43/81). Daher ist gem. § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) der Betriebsrat zu beteiligen. In

einer Betriebsvereinbarung ist darauf hinzuwirken, dass der Katalog der Daten und die Auswertung in so engen Grenzen gehalten werden wie möglich.

Ist der Abschluss einer Betriebsvereinbarung mangels Existenz eines Betriebsrates nicht möglich, wäre an eine schriftliche Selbstbindungserklärung des Arbeitgebers oder aber an einen Annex zum individuellen Arbeitsvertrag zu denken.

In einem hier geprüften Fall setzte der Arbeitgeber die GPS-Ortung ein, um gegenüber seinen kommunalen Auftraggebern die Ordnungsmäßigkeit der zweimal jährlich erfolgenden Abwasser-Kanalreinigung dokumentieren zu können. Problematisch dabei war, dass die Ortung bereits ab einer Haltezeit von mehr als 60 Sekunden erfolgte und die Haltepunkte in einer Straßenkarte als rote Punkte abgebildet wurden. Damit war es ohne weiteres möglich, ein Bewegungsprofil der betroffenen Beschäftigten zu erstellen, unzulässige Privatfahrten zu identifizieren und die Betroffenen auf Umwegfahrten oder zu lange Aufenthalte anzusprechen. Nach dem festgestellten Sachverhalt machte der Arbeitgeber hiervon auch Gebrauch. Darüber hinaus wurden die per GPS-Technik erhobenen Daten für 30 Tage gespeichert. Die verantwortliche Stelle berief sich auf eine Einverständniserklärung der Beschäftigten in die GPS-Ortung.

Unsere Prüfung ergab, dass das Unternehmen durch die GPS-Ortung der Beschäftigten in unzulässiger Weise personenbezogene Daten erhob und verarbeitete. Hinzu kam im weiteren Verfahren die nicht richtige und nicht vollständige Erteilung einer Auskunft uns gegenüber, so dass wir beide Verstöße mit einem Bußgeld ahndeten. Das Unternehmen entfernte daraufhin die GPS-Tracker aus den Firmenfahrzeugen.

Bei der Fahrzeugortung mittels GPS-Technik ist insbesondere die Streckenverfolgung dazu geeignet, ein Bewegungsprofil der Fahrerinnen bzw. Fahrer zu erstellen. Der Arbeitgeber sollte zunächst nach alternativen Möglichkeiten der Kontrolle suchen, zum Beispiel könnte seinem Überwachungsinteresse durch die Führung eines manuellen Fahrtenbuchs entsprochen werden.

7.5 Videoüberwachung im Beschäftigtenverhältnis

Videotechnik wird immer günstiger, verfügbarer und technisch ausgefeilter. Die Übertragung der Videobilder mittels W-LAN oder im Videogerät eingebauter SIM-Karten auf Smartphone und Tablet begünstigen die Möglichkeit der jederzeitigen Überwachung am Arbeitsplatz. Vieles ist datenschutzrechtlich nicht zulässig.

Vielfach nutzen Arbeitgeber diese technischen Möglichkeiten, um im Betrieb, Ladenlokal oder in der Gaststätte immer „präsent“ sein zu können, ohne tatsächlich vor Ort sein zu müssen. Auf diese Weise ist eine intensive Kontrolle der Beschäftigten möglich. In Einzelfällen wurde uns berichtet, dass diese Kontrolle dazu genutzt wird, die Beschäftigten telefonisch auf ihr Verhalten aufmerksam zu machen oder ihr Verhalten zu kommentieren.

Unsere Beratungspraxis hat gezeigt, dass der Umfang von Videoüberwachung am Arbeitsplatz in den letzten Jahren kontinuierlich gestiegen ist.

Diese ist jedoch nur dann zulässig, wenn dadurch nicht in unzulässiger Weise in das Recht auf informationelle Selbstbestimmung der Beschäftigten eingegriffen wird.

Zentrale Vorschriften für eine Videoüberwachung im Beschäftigungsverhältnis zu einem privaten Arbeitgeber sind Art. 88 DS-GVO in Verbindung mit § 26 BDSG. Nach § 26 Abs. 1 S. 1 BDSG dürfen Beschäftigtendaten nach der Begründung eines Beschäftigungsverhältnisses nur verarbeitet werden, wenn dies für dessen Durchführung oder Beendigung erforderlich ist. Die Videoüberwachung ist eine Datenverarbeitung.

Schwerpunkt bei der Prüfung der Zulässigkeit einer Videoüberwachung nach § 26 Abs. 1 Satz 1 BDSG ist die Prüfung ihrer Erforderlichkeit. Dabei sind die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten gegeneinander abzuwägen.

Für die Mitarbeiterinnen und Mitarbeiter bedeutet die Installation von Kameras im Betrieb oftmals einen Stressfaktor, weil sie sich nicht sicher sein können, wieweit sie einer Überwachung unterliegen. Sie sehen sich im Verhältnis zu den Vorgesetzten in der schwächeren Position, vor allem wenn kein Betriebsrat vorhanden ist, der sich als Sprachrohr der Beschäftigten mit dem Arbeitgeber auseinander setzt. So wurde uns etwa mitgeteilt, dass Beschäftigte sich nicht direkt an die Vorgesetzten wenden – aus Angst, den Arbeitsplatz zu verlieren. In einem solchen Fall konnte der Abbau von unzulässiger Videotechnik erreicht und ein Beitrag dazu geleistet werden, dass die Kommunikation zwischen Arbeitgeber und Beschäftigten wieder aufgenommen wurde.

Die Erforderlichkeit einer Videoüberwachung kann sich daraus ergeben, dass Produktionsabläufe zur Sicherstellung eines ordnungsgemäßen Betriebs per Kamera beobachtet werden müssen. Auch zur Sicherung des Kassenbereichs können Videoaufzeichnungen erforderlich sein. Diese sollten allerdings be-

schränkt sein auf die Kasse und die Ladentheke, ohne eine Erfassung des Personals.

Auf eine Beschwerde hin haben wir den Inhaber eines Unternehmens, das hochwertige Waren verkauft, zu einer datenschutzgerechten Gestaltung der Videoüberwachung aufgefordert. Zunächst war der Raum, in dem sowohl die Ware gelagert wurde, als auch die Schreibtische der Mitarbeiterinnen und Mitarbeiter standen, vollständig videoüberwacht. Unsere Prüf- und Beratungstätigkeit hat dazu geführt, dass der Arbeitgeber die Videoaufzeichnungen so verpixelt hat, dass tatsächlich nur noch das Warenlager zu sehen war. Die übrigen Flächen, auf denen sich Mitarbeiter die Beschäftigten auch dauerhaft aufhielten, waren unkenntlich gemacht.

Das vorgenannte Beispiel zeigt nicht nur die Möglichkeiten des Einsatzes von Videoüberwachung im Beschäftigtenverhältnis auf, sondern deutet auch auf dessen Grenzen hin: Eine Videoüberwachung ist grundsätzlich als unzulässig zu bewerten, wenn Zweck der Datenverarbeitung eine Überwachung der Beschäftigten ist. In Ausnahmefällen kann sie zulässig sein, wenn Beschäftigte etwa einer gefahrengeneigten Tätigkeit nachgehen und die Videoüberwachung der Unfallverhütung dient. Eine Verhältnismäßigkeitsprüfung geht hier zu Gunsten der Zulässigkeit der Videoüberwachung aus.

Stets unverhältnismäßig und damit unzulässig ist eine Videoüberwachung im sogenannten „Kernbereich privater Lebensführung“ (etwa Umkleideräume). Gleiches gilt für reine Freizeitbereiche, wie Sozialräume für Beschäftigte.

Auch für eine Videoüberwachung im Beschäftigtenkontext gelten die umfangreichen Informations- und Hinweispflichten, die die DS-GVO vorgibt. Der Arbeitgeber hat also bei Beginn des Beschäftigungsverhältnisses bzw. bei Einführung der Videoüberwachung im Betrieb die Beschäftigten auf den Umstand der Videoüberwachung hinzuweisen und die weiteren Informationen nach Art. 13 DS-GVO den Betroffenen zugänglich zu machen. Mit den Informationspflichten korrespondieren die Auskunftsrechte der betroffenen Personen nach Art. 15 DS-GVO.

Diese Pflichten bestehen nicht bei einer heimlichen Videoüberwachung von Beschäftigten. Diese ist wegen ihres hohen Eingriffsgewichts allerdings nur in seltenen Fällen zulässig. Nach § 26 Abs. 1 Satz 2 BDSG kann das der Fall sein, wenn der konkrete Verdacht einer begangenen strafbaren Handlung zulasten des Arbeitgebers besteht und weniger einschneidende Mittel zur Aufklärung des Verdachts erfolglos ausgeschöpft wurden, die Videoüberwachung also das einzig verbleibende Mittel und sie somit nicht unverhältnismäßig ist.

Letztlich ist die Bewertung der Zulässigkeit einer Videoüberwachung immer im Einzelfall mittels einer Interessenabwägung vorzunehmen.

Eine rechtswidrige Videoüberwachung von Beschäftigten verwirklicht in der Regel den Ordnungswidrigkeitentatbestand des Art. 83 Abs. 5 Buchstabe d)

DS-GVO. Die LDI NRW kann in diesem Fall Geldbußen verhängen.

Eine Überwachung von Beschäftigten im Betrieb durch Videotechnik stellt einen massiven Eingriff in deren grundrechtlich geschütztes allgemeines Persönlichkeitsrecht dar und ist daher nur unter strengen Voraussetzungen zulässig. Nach Möglichkeit sind Kameras durch technische Maßnahmen so einzustellen, dass eine dauerhafte Beobachtung der Beschäftigten ausgeschlossen ist. Bei Uneinsichtigkeit der Arbeitgeber kann mit einer aufsichtlichen Anordnung die Veränderung bzw. gänzliche Einstellung der Videoüberwachung angeordnet werden und/oder ein Ordnungswidrigkeitsverfahren eingeleitet werden.

8. Beratung öffentlicher Stellen in Fragen des Datenschutzes

Die LDI NRW kontrolliert öffentliche Stellen hinsichtlich der Einhaltung des Datenschutzes, legt jedoch auch weiterhin großen Wert darauf, sie präventiv zu beraten. Dies gilt auch und gerade im Zusammenhang mit der Umsetzung der Datenschutz-Grundverordnung.

Die Neuregelung des Datenschutzrechts löste und löst auch bei den öffentlichen Stellen in NRW eine Fülle von Auslegungs- und Anwendungsfragen aus. Im Vorfeld des Stichtages 25. Mai 2018 haben wir die wesentlichen Änderungen in dem Neun-Punkte-Papier „Auf dem Weg zum neuen Datenschutzrecht – Anregungen für öffentliche Stellen in NRW“ zusammengefasst. Ferner haben wir in der Folgezeit einen „Leitfaden für öffentliche Stellen in Nordrhein-Westfalen“ und eine Gegenüberstellung der alten und neuen Rechtsgrundlagen („Synopse der Rechtsgrundlagen“) für die Verarbeitung personenbezogener Daten erstellt. Alle Papiere finden sich auf unserer Homepage www.ldi.nrw.de.

Ergänzend dazu erfolgte ein Angebot zur Kooperation an die kommunalen Spitzenverbände in NRW, die dieses gerne aufgegriffen haben. So vermittelte die LDI NRW auf mehreren Veranstaltungen Informationen und Hilfestellungen für die tägliche Praxis. Der Austausch über aktuelle Fragen der Rechtsanwendung sowie über Praxiserfahrungen hilft dabei beiden Seiten. Das Angebot besteht auch weiterhin fort und ergänzt so andere Treffen mit öffentlichen Stellen, wie etwa den jährlichen Erfahrungsaustausch mit den nordrhein-westfälischen Hochschuldatenschutzbeauftragten und mit dem Justizministerium NRW.

Die LDI NRW wird die öffentlichen Stellen im Rahmen des Möglichen auch weiterhin bei der Sicherstellung des Datenschutzes aktiv und präventiv unterstützen. Dies geschieht sowohl durch Beratungen im Einzelfall als auch durch Fortsetzung des Erfahrungsaustausches sowie durch die Veröffentlichung von allgemeinen Informationen auf der Homepage.

9. Innere Sicherheit und Justiz

9.1 Änderungen bereichsspezifischer Gesetze im Sicherheits- und Justizbereich

Im Zuge der Umsetzung der Richtlinie (EU) 2016/680 (JI-RL) wurden umfangreiche materiell-rechtliche Gesetzesnovellierungen vorgenommen. Im Rahmen der Beteiligung im Vorfeld der Einbringung der Gesetzentwürfe und als geladene Expertin bei Anhörungen des Landtags hat die LDI NRW zahlreiche zum Teil gravierende Bedenken geäußert, denen im Ergebnis nicht hinreichend Rechnung getragen wurde.

Zur Umsetzung der JI-RL wurden neben dem Datenschutzgesetz NRW (DSG NRW – siehe hierzu unter 1.3) auch mehrere bereichsspezifische Normen im Sicherheits- und Justizbereich angepasst bzw. neu geschaffen. Dies betrifft das Polizeigesetz Nordrhein-Westfalen (PolG NRW), das Verfassungsschutzgesetz NRW (VSG NRW) sowie das neu geschaffene Justizvollzugsdatenschutzgesetz (JVollzDSG NRW):

Anpassungen des PolG NRW

Im Jahr 2018 wurden in kurzen Abständen zwei Gesetzentwürfe zur Änderung des PolG NRW in den Landtag eingebracht, so dass beide Entwürfe parallel beraten wurden. Dieses gestufte Verfahren, bei dem es zum Teil Überschneidungen gab, erschwerte nicht nur die Beratungstätigkeit der LDI NRW, sondern auch die Transparenz für die Bürgerinnen und Bürger in NRW ganz erheblich.

Der erste Entwurf (des Gesetzes zur Stärkung der Sicherheit in Nordrhein-Westfalen – Sechstes Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen – LT-Drs. 17/2351) sah eine erhebliche Ausweitung der polizeilichen Befugnisse im Bereich der Gefahrenabwehr vor. Erst der zweite Entwurf (des Gesetzes zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen und des Gesetzes über Aufbau und Befugnisse der Ordnungsbehörden – LT-Drs. 17/2576) hatte die erforderliche Anpassung des PolG NRW an die JI-RL zum Gegenstand. Diese von der LDI NRW kritisierte Vorgehensweise führte dazu, dass die Umsetzungsfrist der JI-RL zum 8. Mai 2018 deutlich überschritten wurde.

Die beschlossenen Gesetzesänderungen geben vor allem in materiell-rechtlicher Hinsicht Anlass für Kritik: Dies gilt in besonderem Maße für das oben genannte Sechste Änderungsgesetz zum PolG NRW (siehe unsere Stellungnahme an den Landtag vom 30. Mai 2018 - Landtag-Stellungnahme 17/645). So ist fraglich, ob das Gesetz den umfassenden Vorgaben des Bundesverfassungsgerichts in dessen Urteil zum Bundeskriminalamtsgesetz aus dem Jahr 2016 (sogenanntes BKAG-Urteil – BVerfGE 141, 220) in angemessener Weise Rechnung trägt. Dies gilt insbesondere bezüglich der Einhaltung des Bestimmtheits- und Verhältnismäßigkeitsgrundsatzes.

Mit den im Gesetzgebungsverfahren eingebrachten Änderungen wurden zwar noch einige Verbesserungen in gesetzestechnischer Hinsicht und bezüglich der Reichweite der neuen Eingriffsbefugnisse vorgenommen. Die Kritik der LDI NRW wurde hierdurch jedoch nicht vollständig ausgeräumt. Besonders problematisch ist aus unserer Sicht weiterhin die Einführung der Quellen-Telekommunikationsüberwachung;
wichtige Fragen zur damit einhergehenden Beeinträchtigung der globalen IT-Sicherheit sind nach wie vor ungeklärt. Gleiches gilt für die erhebliche Ausweitung der Möglichkeiten polizeilicher Videoüberwachung im öffentlichen Raum nach § 15a PolG NRW.

Bezüglich des Gesetzes zur Umsetzung der JI-RL im Polizeibereich ist vor allem zu bemängeln, dass die schon in Teil 3 des DSG NRW fehlenden erforderlichen Befugnisse der LDI NRW (siehe hierzu schon unter 1.3) auch mit diesem Gesetz nicht eingeführt wurden. Nicht hinzunehmen ist zudem die Streichung der Benachrichtigungspflicht im äußerst praxisrelevanten Bereich der Bestandsdatenauskünfte nach dem Telekommunikationsgesetz, die wir auch in unserer Stellungnahme an den Landtag vom 4. September 2018 bemängelt hatten (siehe Landtag-Stellungnahme 17/791). Insgesamt weist dieses Gesetz eine wenig aussagekräftige Begründung auf, die die künftige praktische Anwendung des PolG NRW deutlich erschweren dürfte.

Änderungen des Verfassungsschutzgesetzes NRW

Mit dem Nordrhein-Westfälischen Datenschutz-Anpassungs- und Umsetzungsgesetz EU (siehe hierzu unter 1.3) erfolgte auch eine Änderung des VSG NRW. Aufgrund der Stellungnahme der LDI NRW vom 12. April 2018 im Gesetzgebungsverfahren (siehe Landtag-Stellungnahme 17/508, S. 50 f.) wurden einige Verbesserungen vorgenommen. Ein erhebliches Risiko für eine Absenkung des Datenschutzniveaus bringt jedoch die neu geschaffene Regelung des § 15 Abs. 3 Satz 3 VSG NRW mit sich. Sie erlaubt der Verfassungsschutzbehörde, die Kontrollmöglichkeit der LDI NRW unter erleichterten Voraussetzungen einzuschränken als dies bisher nach § 22 Abs. 2 DSG NRW alte Fassung in Verbindung mit § 31 VSG NRW alte Fassung möglich war. Die bisherige Regelung sah ein zweistufiges Verfahren und die Beteiligung der obersten Landesbehörde vor. Zudem mussten Daten einer Person betroffen sein, der von der verantwortlichen Stelle Vertraulichkeit besonders zugesichert worden war. Nunmehr kann die Kontrollmöglichkeit der LDI NRW in einem einstufigen Verfahren und durch die Verfassungsschutzbehörde selbst ausgeschlossen werden.

Schaffung eines eigenen Datenschutzgesetzes für den Justizvollzugsbereich

Mit dem JVollzDSG NRW wurden erstmals alle Datenschutzvorschriften der Vollzugsgesetze in NRW in einem Gesetz zusammengefasst. Diesen Ansatz begrüßen wir ausdrücklich (siehe auch unsere Stellungnahme an den Landtag vom 4. September 2018 – Landtag-Stellungnahme 17/696).

Auch zur inhaltlichen Umsetzung der JI-RL gab es wenig Anlass zu Kritik. Zum

Umgang mit zweckändernden Verarbeitungen sind in Abstimmung mit der LDI NRW neuartige Vorschriften geschaffen worden. Diese sehen besondere Abwägungserfordernisse vor, um die Vorgaben des Bundesverfassungsgerichts (BVerfG) umzusetzen. Entgegen unserer Empfehlung wurden vergleichbare Abwägungserfordernisse allerdings an anderen Stellen des Gesetzes nicht geschaffen. Dies eröffnet im Ergebnis die Möglichkeit bestimmter zweckändernder Verarbeitungen personenbezogener Daten im Vollzugsbereich entgegen den diesbezüglichen Vorgaben des BVerfG.

Neben der Umsetzung der JI-RL wurden mit dem Gesetz neue Eingriffsbefugnisse in das Grundrecht auf informationelle Selbstbestimmung geschaffen. Auch wenn aus Sicht der LDI NRW auf einige dieser Befugnisse hätte verzichtet werden können, konnten wir im Gesetzgebungsverfahren dennoch eine Vielzahl an Änderungen erreichen, um die Eingriffsintensität der Maßnahmen abzumildern.

Als problematisch sehen wir weiterhin insbesondere die faktische Abschaffung des Direkterhebungsgrundsatzes an. Zwar ist weiter festgeschrieben, dass personenbezogene Daten grundsätzlich bei der betroffenen Person zu erheben sind. Als gleichwertige Möglichkeit ist nunmehr die Erhebung bei öffentlichen Stellen vorgesehen. Hierbei handelt es sich allerdings gerade um die Erhebung bei Dritten.

Der Sicherheitsbereich hat im Zuge der Umsetzung der JI-RL gewichtige notwendige Änderungen erfahren. Diese Umsetzung hätte jedoch teils auch deutlich differenzierterer Vorschriften in den bereichsspezifischen Regelungen bedurft. Viele der ohne einen dahingehenden Regelungsbedarf der JI-RL zusätzlich geschaffenen Eingriffsbefugnisse sind dagegen problematisch. Im Zuge der Beteiligung der LDI NRW im Gesetzgebungsverfahren konnten zwar Verbesserungen erreicht werden. Es sind jedoch in allen genannten Vorschriften Regelungen verblieben, die wir kritisch sehen.

9.2 Entschließungen der Datenschutzkonferenz zum Datenschutz im Sicherheitsbereich

Die Datenschutzkonferenz (DSK) hat zu verschiedenen Themen aus dem Sicherheitsbereich Entschließungen gefasst.

Neues Bundeskriminalamtgesetz – Informationspool beschneidet Grundrechte

Im Zuge der Umsetzung der Richtlinie (EU) 2016/680 (JI-RL) wurde auf Bundesebene auch das Bundeskriminalamtgesetz (BKAG) angepasst. Gleichzeitig wurden darin Vorgaben des Bundesverfassungsgerichts aus dem sogenannten BKAG-Urteil (BVerfGE 141, 220) umgesetzt. Das Gesetz enthält jedoch auch Erweiterungen der Befugnisse des BKA und sieht die Umstellung der bisherigen Verbunddateien auf ein einheitliches Datenspeicherungssystem vor. Die DSK hat die als besonders kritisch erachteten Punkte in der Entschließung „Neues Bundeskriminalamtgesetz – Informationspool beschneidet Grundrechte“ vom 16. März 2017 zusammengefasst (Abdruck im Anhang).

Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken

Im Jahr 2017 starteten verschiedene Pilotprojekte zum Einsatz von Videokameras zur biometrischen Gesichtserkennung. Das wohl prominenteste Pilotverfahren ist das am Berliner Bahnhof Südkreuz. Neben der biometrischen Gesichtserkennung verfügen die Kamerasysteme häufig auch über Möglichkeiten, auffällige Bewegungsmuster zu erkennen. Die DSK sieht die neue Technik kritisch und bemängelt vor allem das Fehlen einer Rechtsgrundlage für den Einsatz. Sie hat daher am 30. März 2017 die Entschließung „Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken“ verabschiedet (Abdruck im Anhang).

Keine anlasslose Vorratsspeicherung von Reisedaten

Der Gerichtshof der Europäischen Union (EuGH) hat am 26. Juli 2017 ein Gutachten (Nr. 1/15) zum Fluggastdaten-Abkommen der EU mit Kanada erstellt. Darin erklärte er die langfristige Speicherung von Daten sämtlicher Fluggäste (Passenger Name Records – PNR-Daten) für nicht mit der Europäischen Grundrechtecharta vereinbar. Damit hat der EuGH seine bisherige Position bekräftigt und der anlasslosen Vorratsdatenspeicherung von personenbezogenen Daten erneut eine klare Absage erteilt. Die DSK hat dies zum Anlass genommen, mit der Entschließung „Keine anlasslose Vorratsspeicherung von Reisedaten“ vom 9. November 2017 an sämtliche Entscheidungsträger zu appellieren, bestehende Regelungen zu ändern und geplante Regelungen – wie beispielsweise das neue EU Entry-Exit-System (EES) – nicht in der vorgesehenen Form umzusetzen (Abdruck im Anhang).

Zuverlässigkeitsüberprüfungen bei öffentlichen und privaten Veranstaltungen nur im erforderlichen Maß und nach einem rechtsstaatlichen und transparenten Verfahren

In den vergangenen Jahren haben Sicherheitsüberprüfungen im Zusammenhang mit öffentlichen und privaten Großveranstaltungen stark zugenommen. Diese werden regelmäßig durch die Polizeibehörden vorgenommen und betreffen etwa Ausstellerinnen und Aussteller, Gastronominnen und Gastronome sowie Handwerkerinnen und Handwerker. Die DSK hat am 26. April 2018 die Entschließung „Zuverlässigkeitsüberprüfungen bei öffentlichen und privaten Veranstaltungen nur im erforderlichen Maß und nach einem rechtsstaatlichen und transparenten Verfahren“ gefasst (Abdruck im Anhang). Sie kritisiert vor allem, dass die Überprüfungen bisher häufig ohne gesetzliche Rechtsgrundlage, sondern vielmehr auf Basis von problematischen Einwilligungserklärungen in Verfahren erfolgen, die keinen hinreichenden Rechtschutz gewähren.

Der Vorschlag der EU-Kommission für eine E-Evidence-Verordnung führt zum Verlust von Betroffenenrechten und verschärft die Problematik der sog. Vorratsdatenspeicherung

Im April 2018 hat die Europäische Kommission Vorschläge für eine E-Evidence-Verordnung (Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen – COM (2018) 225 final) vorgelegt. Damit möchte sie eine Alternative zum bisher maßgeblichen förmlichen Rechtshilfeverfahren schaffen, bei dem Ermittlungsbehörden sich zunächst an zuständige Behörden im Land des Dienstleisters wenden mussten. Die Ermittlungsbehörden sollen die Anbieter von Telekommunikations- und Internetdienstleistungen nunmehr direkt und grundsätzlich ohne Einschaltung von Behörden am Sitz des Dienstleisters zur Herausgabe einer Vielzahl personenbezogener Daten verpflichten können. Dies soll für Dienstleister aus anderen Mitgliedstaaten der EU und sogar aus Staaten außerhalb der EU (sogenannten Drittstaaten) gelten.

Die DSK weist in ihrer Entschließung „Der Vorschlag der EU-Kommission für eine E-Evidence-Verordnung führt zum Verlust von Betroffenenrechten und verschärft die Problematik der sog. Vorratsdatenspeicherung“ vom 7. November 2018 auf eine Reihe kritischer Punkte des Verordnungsentwurfs hin (Abdruck im Anhang). Sie fordert aufgrund der Vielzahl der noch bestehenden Probleme den Stopp des Gesetzgebungsverfahrens.

Es hat einige bedenkliche Entwicklungen im Sicherheitsbereich gegeben, auf die die DSK jeweils mit Entschließungen reagiert hat. Ein mehrfach kritisierter Punkt waren hierbei neuartige Eingriffe durch die Sicherheitsbehörden ohne darauf zugeschnittene spezielle Ermächtigungsgrundlagen.

9.3 Ausweitung der Videoüberwachung durch die Polizei

Die Videoüberwachung nach § 15a Polizeigesetz Nordrhein-Westfalen (PolG NRW) wurde in mehreren nordrhein-westfälischen Großstädten deutlich ausgeweitet. Wir haben diese Maßnahmen umfassend überprüft.

§ 15a PolG NRW erlaubt der Polizei, zur Verhütung von Straftaten einzelne öffentlich zugängliche Orte, an denen wiederholt Straftaten begangen wurden und deren Beschaffenheit die Begehung von Straftaten begünstigt, mittels Bildübertragung zu beobachten und die übertragenen Bilder aufzuzeichnen. Zudem müssen als weitere Voraussetzung Tatsachen die Annahme rechtfertigen, dass an diesem Ort weitere Straftaten begangen werden.

Bereits im 23. Bericht (siehe unter 5.3) haben wir aufgezeigt, dass unter anderem wegen der Vorkommnisse in der Silvesternacht 2015/2016 die Videoüberwachung von Kriminalitätsschwerpunkten durch die Polizei intensiviert wurde bzw. werden sollte. Gleichzeitig haben wir eine Überprüfung aller neuen Maßnahmen zur Videoüberwachung angekündigt.

Neben der rechtlichen Überprüfung nach Aktenlage umfassten unsere Kontrollen auch jeweils eine Inaugenscheinnahme der Situation am Ort der Videoüberwachung. Inzwischen konnten wir diese Überprüfungen in Aachen, Essen, Dortmund, Duisburg, Düsseldorf und Köln weitgehend abschließen.

In einem Fall kam es dabei zu erheblichen zeitlichen Verzögerungen. Während eine Polizeibehörde bereits im Dezember 2016 die ersten Kameras in Betrieb genommen hatte, konnte erst im September 2018 der Ortstermin stattfinden. Gründe hierfür waren bis dahin fehlende Unterlagen sowie terminliche Abstimmungsprobleme. Im Rahmen der Kontrolle stellte sich heraus, dass seit Februar 2018 die Videoüberwachung 24 Stunden täglich durchgeführt wird. Dies widersprach den vorgelegten Unterlagen.

Die Begründung dieser zeitlichen Ausweitung der Videoüberwachung konnte bislang nicht überzeugen. Daher haben wir empfohlen, diese Maßnahme rückgängig zu machen und zu den vorherigen eingeschränkten Betriebszeiten zurückzukehren.

Insgesamt zeigte sich insbesondere im Rahmen der mit den Verantwortlichen geführten Gespräche eine große Kooperationsbereitschaft. Positiv nahmen wir wahr, dass die Verantwortlichen konstruktiv mit den von uns ausgesprochenen Empfehlungen umgingen. So setzten sie wichtige Anregungen unmittelbar um. Dazu gehören beispielsweise die vollständige Verpixelung privater Wohnbereiche, eine ausreichende Beschilderung oder die zeitlich konkret definierte Löschung von Screenshots.

Die Ausweitung der Videoüberwachung sehen wir weiterhin grundsätzlich kritisch. Die konkrete Handhabung in der Praxis wurde durch unsere Beratung in vielen Fällen weniger eingreifend gestaltet. Dies führen wir auf die gute Kom-

munikation mit den Polizeidienststellen und deren Bereitschaft zurück, datenschutzrechtlichen Hinweisen zu Verbesserungen nachzukommen.

9.4 Überprüfung von Datenspeicherungen im Zusammenhang mit dem G-20-Gipfel im Juli 2017 in Hamburg

Im Nachgang zum G-20-Gipfel überprüften wir – wie auch einige Datenschutzaufsichtsbehörden anderer Bundesländer – Datenspeicherungen bei Polizei und Verfassungsschutz. Hintergrund war, dass diese Speicherungen Grundlage für die Verweigerung der Akkreditierung für Journalistinnen und Journalisten beim G-20-Gipfel gewesen sein könnten.

Zwischen Akkreditierung und Beginn des Gipfels machten Sicherheitsbehörden hinsichtlich mehrerer Medienvertreterinnen und -vertreter Sicherheitsbedenken geltend, die aus Erkenntnissen verschiedener deutscher Behörden resultierten. Diese Erkenntnisse führten dann in wenigen Fällen zum Verlust der Akkreditierung. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) bat uns im Kontext ihrer eigenen Prüfung, die sich auf das Bundeskriminalamt (BKA) bezog, mehrere dieser Fälle zu prüfen. Bei diesen sollten möglicherweise aus NRW stammende Daten für die Entscheidung des BKA über den Verlust der Akkreditierung maßgeblich gewesen sein. Wir haben als wesentliches Ergebnis unserer Kontrolle festgestellt, dass die aus NRW zugelieferten Informationen, die mittelbar im Zusammenhang mit dem Akkreditierungsverfahren standen, nicht zu beanstanden waren.

Der BfDI erstellt gemeinsam mit den betroffenen Bundesländern hierzu einen Gesamtbericht zur datenschutzrechtlichen Kontrolle des Akkreditierungsverfahrens beim G-20-Gipfel. Unsere Prüfergebnisse und Bewertungen der Einzelfälle werden darin einfließen.

Diese Prüfung führt anhand der Einzelfälle insgesamt klar vor Augen, dass jede Speicherung von Daten weitreichende Folgen haben kann. Deshalb muss bei der Erfassung in Datenbanken von Sicherheitsbehörden größtmögliche Sorgfalt walten. Wir werden in NRW auch zukünftig die Umsetzung datenschutzrechtlicher Vorgaben bei Polizei und Verfassungsschutz prüfen.

10. Gesundheit und Soziales

10.1 Informationen der Heilberufskammern zur Anwendung der DS-GVO in der ambulanten Versorgung

Rund 250.000 Angehörige der Heilberufe können sich mit Hilfe zahlreicher Informationsblätter der Heilberufskammern zur Reform des Datenschutzrechts in der ambulanten Versorgung über die Anforderungen nach der DS-GVO orientieren. Die Informationsblätter sind mit der LDI NRW abgestimmt.

Eine Arbeitsgemeinschaft, bestehend aus den nordrhein-westfälischen Heilberufskammern sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe, hat verschiedene Informationsblätter sowie mehrere ergänzende Mustertexte zu praxisrelevanten Datenschutzfragen erarbeitet. Beantwortet werden dabei Fragen zu datenschutzrechtlichen Schwerpunkten von A wie Auftragsverarbeitung bis V wie Verzeichnis von Verarbeitungstätigkeiten. Wir haben an der Erarbeitung dieser Informationsblätter maßgeblich mitgewirkt und diese inhaltlich mit der Arbeitsgemeinschaft abgestimmt.

Über die Multiplikatoren der Heilberufskammern und der Kassenärztlichen Vereinigungen wird ein erheblicher Verbreitungsradius dieser Informationen erreicht. Die Angehörigen der Heilberufe können sich auf der Homepage ihrer Kammer über die relevanten datenschutzrechtlichen Fragen des Praxisalltags informieren. Sie sind gut beraten, wenn sie sich daran orientieren.

10.2 Verfahren der Gutachterkommission bei den Ärztekammern und der Haftpflichtversicherer

Verfahren vor den Gutachterkommissionen für ärztliche Behandlungsfehler können grundsätzlich ohne Beteiligung der Haftpflichtversicherer der Ärzte datenschutzgerecht durchgeführt werden.

Patientinnen und Patienten sehen in der Regel viele Vorteile des Verfahrens vor den Gutachterkommissionen für ärztliche Behandlungsfehler, die gemäß § 6 Abs. 1 Nr. 9 des Heilberufsgesetzes NRW bei den Ärztekammern zu errichten sind: Das Verfahren ist kostenlos und nicht-öffentlich. Die Kommission würdigt die Beweise, und die von ihr durchgeführte Begutachtung ist für die Prognose der Erfolgsaussichten eines möglicherweise folgenden Prozesses von Bedeutung. Auf diese Weise setzen mutmaßlich Geschädigte und ihre Ärzte, die sich gegen den betreffenden Vorwurf wehren wollen, zunächst vor einer objektiven Stelle außergerichtlich auseinander.

Durch einige Eingaben von Bürgerinnen und Bürgern wurde jedoch deutlich, dass dieses „Gleichgewicht der Kräfte“ bei der Gutachterkommission der Ärztekammer Nordrhein dadurch gestört war, dass auf Seiten der Ärzte – neben ihrer Rechtsvertretung – schon hier dessen Haftpflichtversicherer auftrat, was nach den „Allgemeinen Versicherungsbedingungen Haftpflicht“ eigentlich erst für den Zivilprozess vorgesehen ist. Die betroffenen Patientinnen und Patienten hatten nur die Möglichkeit, bereits zu Beginn des Kommissionsverfahrens in die Übermittlung ihrer besonders geschützten Gesundheitsdaten an den Versicherer als unbeteiligten Dritten einzuwilligen und behandelnde Ärzte von der Schweigepflicht zu entbinden. Andernfalls sollte das Verfahren vor der Gutachterkommission erst gar nicht eröffnet werden.

Die Ärztekammer Nordrhein wurde auf das datenschutzrechtliche Problem der mutmaßlich fehlenden Freiwilligkeit der Einwilligung aufmerksam gemacht. Im Übrigen ist auch keine Rechtsgrundlage für die geplante Datenübermittlung erkennbar.

Ihre Einwilligungs- und Schweigepflichtentbindungserklärung im Rahmen der Antragsstellung hat die Ärztekammer Nordrhein erfreulicherweise nun so konzipiert, dass die Betroffenen ein Wahlrecht besitzen, ob der Haftpflichtversicherer des jeweiligen Arztes in das Verfahren eingebunden wird oder nicht. Sofern die Beteiligung abgelehnt wird, hindert dies nicht die Durchführung des Verfahrens vor der Kommission.

10.3 Gültigkeitsdauer einer Einverständniserklärung zur Rechnungserstellung durch eine Abrechnungsgesellschaft

Ärztinnen und Ärzte beauftragen oft externe Dienstleistungsunternehmen mit der Abrechnung ihrer ärztlichen Leistungen. Hierfür müssen sie zuvor eine wirksame Einverständniserklärung der jeweils betroffenen Person einholen. Das einmal erklärte Patienteneinverständnis gilt jedoch nicht unbegrenzt.

Die Verarbeitung personenbezogener Daten ist immer an den von der Legitimationsgrundlage vorgegebenen Zweck gebunden, hier der Einwilligung. Damit geht notwendigerweise auch in zeitlicher Hinsicht eine Konkretisierung des Sachzusammenhangs einher, in dem die Verarbeitung der personenbezogenen Daten erfolgen soll.

Für den Fall der wiederholten Verarbeitung personenbezogener Daten für gleichgelagerte Verarbeitungszwecke reicht eine vor der Erhebung und Verarbeitung der Daten eingeholte Einwilligung, die alle Verarbeitungsvorgänge erfasst, zwar grundsätzlich aus. Diese kann jedoch nicht unbegrenzt gelten. Auch eine Formulierung im Einwilligungsformular, mit der die Patientin bzw. der Patient erklärt zu wissen, „dass die Erklärung auch für zukünftige Behandlungen gilt und vor jeder neuen Behandlung widerrufen werden kann“, ist dahingehend auszulegen, dass sie sich nur auf einen zum Zeitpunkt der Erklärung überschaubaren Sachzusammenhang und Zeitraum beziehen kann. Dieser wird allgemein bei Einwilligungen in die Verarbeitung personenbezogener Daten bei zwei Jahren angenommen.

Dieser Zeitraum ist auch in Bezug auf Patientendaten als die maximal angemessene Frist zu betrachten. Insbesondere wenn die behandelten Personen die Praxis über einen längeren Zeitraum nicht aufgesucht hat, ist eine Erneuerung der Einwilligungserklärung auch nach einem kürzeren Zeitraum empfehlenswert. Ansonsten ist nicht sichergestellt, dass die Betroffenen den Inhalt ihrer Einwilligungserklärung noch vor Augen haben.

Zwar mag einer in regelmäßiger Behandlung befindlichen Person im Einzelfall bewusst sein, eben diese Erklärung abgegeben zu haben. Auch in solch einem Fall wird jedoch üblicherweise durch die Arztpraxis regelmäßig überprüft, ob die gespeicherten Patientendaten noch aktuell sind. Jedenfalls bei einer notwendigen Aktualisierung der Daten sollte Anlass bestehen, auch die Einwilligung in die Datenverarbeitung zu erneuern.

Die Beweislast für eine wirksame Patienteneinwilligung obliegt der Ärztin bzw. dem Arzt als die für die Datenverarbeitung verantwortliche Person. Liegt der Datenverarbeitung keine rechtswirksame Einwilligung zugrunde, kann dies geahndet werden.

10.4 Rezeptbestellungen mittels WhatsApp

Zu dem in der Praxis immer häufiger vorkommenden Serviceangebot für Apothekenkunden, Rezeptdaten mittels WhatsApp zu übermitteln, erreichen uns vermehrt Anfragen sowohl von besorgten Bürgerinnen und Bürgern als auch von Apotheken. Die LDI NRW sieht die Nutzung von WhatsApp für die damit einhergehende Übermittlung von Gesundheitsdaten sehr kritisch und rät den Kundinnen und Kunden sowie den Apotheken von einer solchen Nutzung ab (zur grundsätzlichen Problematik siehe 23. Bericht unter 12.6).

Die Datenschutzverantwortung für die Eröffnung des Kommunikationsweges WhatsApp liegt bei den Apothekerinnen und Apothekern als verantwortliche Stellen im Sinne des Artikels 4 Nr. 7 DS-GVO. Sie müssen insbesondere die erforderlichen technischen und organisatorischen Maßnahmen gemäß Artikel 5 Abs. 1 Buchstabe f) DS-GVO zur Gewährleistung des Datenschutzes und der Datensicherheit treffen. Dies ist in Bezug auf die in Rede stehenden personenbezogenen Daten der Kundinnen und Kunden deshalb so wichtig, weil es sich hierbei um besonders schutzbedürftige Gesundheitsdaten im Sinne des Art. 9 Abs. 1 in Verbindung mit Art. 4 Nr. 15 DS-GVO handelt.

Darüber hinaus besteht für die oben genannte Berufsgruppe auch eine berufsrechtliche Verschwiegenheitsverpflichtung, der durch die Verwendung von WhatsApp aus unserer Sicht nicht ausreichend Rechnung getragen werden kann.

Die Nutzung von WhatsApp zur Übermittlung von Rezept- und Bestelldaten unterliegt schon deswegen datenschutzrechtlichen Bedenken, weil hier besonders schutzbedürftige personenbezogene Daten übermittelt werden. Denn allein aus der Tatsache, dass jemand Apothekenkundin oder -kunde ist und eine Bestellung vornimmt, ergibt sich bereits, dass es sich bei den Kundendaten um Gesundheitsdaten handelt oder handeln kann.

Die Einholung einer gemäß Art. 9 Abs. 2 Buchstabe a) DS-GVO erforderlichen informierten Einwilligungserklärung dürfte in der Praxis eher schwierig sein, weil die Apotheken selbst tatsächlich keine ausreichenden Aussagen über die Datenverarbeitung bei dem genutzten Messengerdienst treffen können.

Auch kann durch die bloße Nutzung von WhatsApp keine konkludente Einwilligung der Kunden unterstellt werden. Denn die Annahme einer bloß konkludenten Willensbekundung ist dem Datenschutzrecht fremd. Erforderlich ist in diesem Zusammenhang zumindest eine eindeutige, bestätigende, informierte und unmissverständliche Handlung bezogen auf den konkreten Fall (siehe Erwägungsgrund 32).

Ob es im Weiteren neben der speziellen Rechtsgrundlage des Artikels 9 DS-GVO die Möglichkeit gibt, auch noch auf die allgemeine Bestimmung des Artikels 6 DS-GVO zurückzugreifen, erscheint schließlich fraglich.

Die Durchführung einer Ende-zu-Ende-Verschlüsselung, die WhatsApp immer betont, löst die aufgezeigten Probleme nicht umfassend.

In der Praxis wurde den jeweils betroffenen Apotheken geraten, davon abzusehen, die Nutzung von WhatsApp aktiv zu bewerben, zumal Apothekerinnen und Apotheker gegenüber ihren Kunden auch berufsrechtlich zur Verschwiegenheit verpflichtet sind. Bei unaufgefordert eingehenden WhatsApp-Nachrichten von Kunden wurde angeregt, zumindest einen anderen Antwortweg zu wählen.

11. Datensicherheit

11.1 Meldungen von Datenschutzverstößen nach Art. 33 DS-GVO

Seit Inkrafttreten der DS-GVO haben uns im Vergleich zu den Vorjahren sehr viel mehr Meldungen zu Datenschutzverstößen erreicht. Dabei ist die Unsicherheit bei den Verantwortlichen groß, welcher Verstoß zu melden ist und welcher nicht. Aus dieser Unsicherheit heraus melden viele sicherheitshalber auch eher unbedeutende Datenpannen, um möglichen Sanktionen vorzubeugen.

Von Mai bis Dezember 2018 sind uns mehr als 1.200 Datenpannen nach Art. 33 DS-GVO über das auf unserer Website dafür neu bereitgestellte Formular gemeldet worden. Im Zeitraum von Januar bis Mai 2018 erhielten wir hingegen nur 61 Meldungen nach § 42a Bundesdatenschutzgesetz – alte Fassung (BDSG a. F.).

Diese Unterschiede erklären sich dadurch, dass § 42a BDSG a. F. nur dann eine Meldepflicht begründet, wenn personenbezogene Daten aus den in der Rechtsvorschrift explizit genannten Kategorien einem Dritten unrechtmäßig zur Kenntnis gelangen und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Art. 33 DS-GVO erfasst hingegen alle personenbezogenen Daten, die Art ihrer Verletzung wird außerdem nicht eingeschränkt und eine Meldung ist bereits erforderlich, wenn die Verletzung wahrscheinlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen wird.

Bei den uns nach Art. 33 DS-GVO vorliegenden Meldungen handelt es sich häufig um Fehladressierungen von Postsendungen, nicht verschlossene Briefumschläge, Fehladressierungen von E-Mails oder auch den Versand von E-Mails mit offenen Verteilerlisten. Ursache für solche Pannen waren zumeist Irrtümer oder Nachlässigkeiten von Mitarbeitern, also menschliche Fehlhandlungen.

Art. 33 Abs. 1 der DS-GVO fordert die Meldung einer Verletzung des Schutzes personenbezogener Daten, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Dies bedeutet, dass eine Meldung unterbleiben kann, wenn der Eintritt eines Schadens für die von der Verletzung betroffenen natürlichen Personen nicht wahrscheinlich ist. Mit anderen Worten: Eine Meldung ist nicht erforderlich, wenn die Datenschutzverletzung im konkreten Fall gar keinen Schaden zur Folge haben kann oder wenn ein möglicher Schaden wahrscheinlich nicht eintreten wird. Da aber in den meisten Fällen ein Schaden oder dessen Eintrittswahrscheinlichkeit nicht gänzlich ausgeschlossen werden kann, ist für eine vorliegende Datenschutzverletzung zunächst die Risikostufe auf der Grundlage einer **Risikoanalyse** zu ermitteln.

Die ermittelte Risikostufe entscheidet dann darüber, ob eine Meldung an die Aufsichtsbehörde erforderlich ist.

Das Kurzpapier (siehe hierzu unter 1.1) Nr. 18 „Risiko für die Rechte und Freiheiten natürlicher Personen“ der Datenschutzkonferenz beschreibt den Prozess der Risikoanalyse. Es ist zudem eine hilfreiche Leitlinie für die Entscheidung, ob bei einer konkret vorliegenden Datenschutzverletzung eine Meldung an die zuständige Aufsichtsbehörde zu erfolgen hat.

Das Kurzpapier stellt klar, dass es eine vollständig risikolose Datenverarbeitung nicht geben kann. Insofern ist die in Art. 33 DS-GVO gewählte Formulierung „nicht zu einem Risiko“ von ihrem Sinn und Zweck ausgehend als „nur zu einem geringen Risiko führend“ zu verstehen. Damit ergeben sich für die Risikobeurteilung die Abstufungen „geringes Risiko“, „Risiko“ und „hohes Risiko“.

Kommt der Verantwortliche in seiner Risikoanalyse zu dem Ergebnis, dass nur ein geringes Risiko vorliegt, ist keine Meldung an die Aufsichtsbehörde erforderlich. Ein geringes Risiko liegt vor, wenn sowohl der mögliche Schaden als auch dessen Eintrittswahrscheinlichkeit als gering bis überschaubar eingeschätzt werden. Der Bereich des geringen Risikos wird in dem Kurzpapier durch eine Risikomatrix veranschaulicht.

Es können allerdings auch Situationen eintreten, in denen der Eintritt des Schadens relativ wahrscheinlich ist oder der potentielle Schaden besonders schwer wiegen würde. In solchen Fällen ist eine besonders sorgfältige Einzelfallbetrachtung notwendig.

Beispiel:
Ein Laptop mit medizinischen Befunden wird einem Arzt entwendet. Die Daten auf der Festplatte des Laptops sind mit einem kryptographischen Verfahren nach dem Stand der Technik sicher verschlüsselt.

Eine Offenbarung der auf dem Laptop gespeicherten Befunde würde für die betroffenen Patienten einen hohen Schaden bedeuten. Allerdings ist davon auszugehen, dass der Schadenseintritt höchst unwahrscheinlich ist, wenn die Befunde – im obigen Sinne – sicher verschlüsselt sind. In diesem Fall kann der Verantwortliche nach eigenem Ermessen von einer Meldung bei der Aufsichtsbehörde absehen.

Kommt ein Verantwortlicher im Rahmen der Risikobewertung zu dem Ergebnis, dass keine Meldung bei der Aufsichtsbehörde erforderlich ist, so hat er dennoch den Datenschutzvorfall und die Ergebnisse seiner Risikoanalyse intern zu dokumentieren und die entsprechenden Maßnahmen zu ergreifen, um einen solchen Vorfall zukünftig zu vermeiden.

Datenschutzvorfälle, die nur ein geringes Risiko für die Rechte und Freiheiten der Betroffenen darstellen, müssen der Aufsichtsbehörde nicht gemeldet werden. Allerdings sind der Datenschutzvorfall, die Ergebnisse der Risikoanalyse und die getroffenen Maßnahmen vom Verantwortlichen intern zu dokumentieren.

11.2 Sicherheitslücken in Onlineshop-Software

Fehlerfreie Software ist selten. Im Fall von Sicherheitslücken ist dies datenschutzrechtlich relevant, da hierüber Dritte Zugriff auf personenbezogene Daten erlangen oder diese manipulieren können. Werden Sicherheitslücken öffentlich, lassen Angriffe in der Regel nicht lange auf sich warten. Das gilt auch für OpenSource-Software für Onlineshops, die Zahlungsdaten verarbeiten. Umso wichtiger ist es, die eingesetzte Software aktuell zu halten.

Sehr viele Onlineshops basieren auf der OpenSource-Software „Magento“. Veraltete Versionen enthalten bekannte Schwachstellen und müssen aktualisiert werden. Das Computer Emergency Response Team der Bundesverwaltung — CERT-Bund hat über die betroffenen Provider deutschlandweit über 1.000 Shopbetreiber auf bestehende Probleme mit ihrer Installation hingewiesen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Anfang 2017 festgestellt, dass diese Lücken in vielen Fällen weiterhin bestehen.

Aufgrund der enormen Tragweite des Problems hat die LDI NRW weiter recherchiert und 24 verantwortliche Stellen in Nordrhein-Westfalen identifiziert, die einen verwundbaren Onlineshop betrieben.

Diese 24 Stellen haben wir angeschrieben, auf das Problem aufmerksam gemacht und zur Stellungnahme aufgefordert. In den meisten Fällen wurde das Problem daraufhin kurzfristig behoben. Aus einigen Antworten ging hervor, dass kein Bewusstsein vorhanden war, welche Risiken sich aus dem Betrieb eines Onlineshops ergeben und welche technischen und organisatorischen Maßnahmen zu ergreifen sind, um diese zu minimieren. In einem Fall verhängten wir ein Bußgeld, da die verantwortliche Stelle nicht auf unser Schreiben reagierte.

Veraltete Onlineshop-Software ist eine Gefahr für den Datenschutz. Vielen Betreibern ist nicht bekannt, dass Onlineshops regelmäßige Sicherheitsupdates erfordern.

11.3 Digitale Erpressung – jetzt auch analog

Software, die die Festplatte verschlüsselt und ein Lösegeld für die Daten fordert, ist weit verbreitet. Neu hingegen ist die Forderung von Schweigegeld, um die Veröffentlichung gekaperter Daten zu vermeiden.

Erpressungsversuche mit Daten sind kein neues Phänomen. Bereits der 23. Bericht beschäftigt sich unter 13.4 mit Ransomware, die Daten verschlüsselt und verspricht, die Daten gegen Lösegeld freizugeben. Ein geeignetes Backup-Konzept schützt vor dieser Bedrohung: Sollte Ransomware trotz geeigneter Sicherheitsmaßnahmen Daten verschlüsseln, können sie nach Bereinigung des Systems aus dem Backup zurückgespielt werden.

Verantwortliche mussten nach § 42a Bundesdatenschutzgesetz – alte Fassung unter gewissen Umständen die unrechtmäßige Kenntniserlangung von Daten an die LDI NRW melden. Art. 33 der DS-GVO greift diesen Grundsatz auf und erweitert die Meldepflicht. Anhand solcher Meldungen haben wir festgestellt, dass sich das Vorgehen der Angreifenden weiterentwickelt hat.

In einigen Fällen wurden die Verantwortlichen damit bedroht, dass erlangte Daten im Internet veröffentlicht würden, wenn kein Schweigegeld gezahlt werde. Teilweise versuchten die Erpresser, ihrer Forderung mit Beispieldatensätzen Nachdruck zu verleihen.

In einem Großteil dieser Fälle gelang der Zugriff auf die Daten entweder über mit Malware infizierte Computer oder über schlecht gewartete Onlineshops.

In einzelnen Fällen waren physische Einbrüche, beispielsweise in eine Arztpraxis, der Weg an die Daten. In mindestens einem dieser Fälle kann nicht ausgeschlossen werden, dass mit dem Einbruch gezielt eine Erpressung vorbereitet wurde.

Ebenfalls zu verzeichnen waren Erpressungsversuche, bei denen die Beispieldatensätze plausibel waren, der Verantwortliche aber kein Datenleck identifizieren konnte.

Unabhängig von der Quelle der Daten waren die Erpresserschreiben teilweise individuell gestaltet.

Bei Erhalt eines Erpresserschreibens ist in jedem Fall zu überprüfen, auf welchem Weg die Angreifenden in den Besitz der Daten kommen konnten und ob personenbezogene Daten betroffen sind. Ist dies der Fall, ist der Vorfall nach Art. 33 der DS-GVO regelmäßig an die zuständige Aufsichtsbehörde zu melden. Gegebenenfalls sind darüber hinaus die Betroffenen zu informieren (Art. 34 der DS-GVO). Zudem sollte eine Strafanzeige in Erwägung gezogen werden.

Unsere Hinweise zur Reduktion der Risiken von Angriffen mit Ransomware aus dem 23. Bericht haben weiterhin Bestand. Insbesondere sind Backups unverzichtbar, um verlorengegangene Daten wiederherzustellen. Gegenstand von Drohungen ist mittlerweile oft die Veröffentlichung sensibler Daten im

Internet. Kriminelle gelangen nicht nur über IT-Sicherheitslücken an die Daten, sondern verschaffen sich auch physisch Zugriff. Eine wirksame Zugangssicherung ist daher weiterhin essentieller Bestandteil jedes Sicherheitskonzepts. Sollte ein Erpressungsversuch im Zusammenhang mit personenbezogenen Daten stehen, ist zu prüfen, ob eine Meldepflicht nach Art. 33 der DS-GVO oder eine Benachrichtigungspflicht nach Art. 34 der DS-GVO besteht. Unabhängig davon sollte ebenfalls in Erwägung gezogen werden, Strafanzeige zu erstatten.

2. Teil: Informationsfreiheitsbericht

Überblick

Die Sicherstellung der Informationsfreiheit ist seit 2002 die zweite wichtige Aufgabe der LDI NRW. Erfreulicherweise hat das Bundesverfassungsgericht in seinem Beschluss vom 20. Juni 2017 (Az. 1 BvR 1978/13) nunmehr ausdrücklich festgestellt, dass die **Informationsfreiheit** ebenfalls ein **Grundrecht** ist. Siehe hierzu unter 1. Die „kleine Schwester" Informationsfreiheit hat also denselben Verfassungsrang wie der „große Bruder" Datenschutz.

Wie wichtig Bürgerinnen und Bürgern die Informationsfreiheit ist, belegt die Tatsache, dass das Anrufungsrecht im Informationsfreiheitsgesetz NRW (IFG NRW) seit Bestehen dieses Gesetzes noch nie so häufig genutzt wurde wie in diesem Berichtszeitraum. Die wichtigste Aufgabe der LDI NRW ist es dabei, zwischen der antragstellenden Person und der auskunftspflichtigen Stelle zu vermitteln. Siehe zu einigen **Erfahrungen aus der Beratungspraxis** unter 4 und 5.

Wie im letzten Bericht angekündigt, habe ich zudem das **Beratungsangebot** für auskunftspflichtige Stellen durch Vorträge mit Erfahrungsaustausch erweitert, zunächst im kommunalen Bereich. Diese Veranstaltungen, die sehr gut angenommen werden, dienen zugleich dem Zweck, die Informationsfreiheit weiter in NRW zu etablieren. Siehe hierzu unter 3.

Die Eingaben aus den verschiedensten Bereichen zeigen, dass viele Menschen ein starkes Interesse daran haben, Verwaltungsentscheidungen und politische Prozesse im Rahmen eines Informationszugangs unmittelbar nachvollziehen zu können. Die vielen individuellen Auskunftsverlangen könnten überflüssig werden, wenn öffentliche Stellen verpflichtet würden, Informationen in größerem Umfang proaktiv zu veröffentlichen.

Seit Jahren weise ich darauf hin, dass es an der Zeit ist, das bewährte IFG NRW in diesem Sinne endlich zu einem **Transparenzgesetz** weiterzuentwickeln. Eine tatsächliche Entwicklung in diese Richtung ist jedoch bedauerlicher Weise auch in den vergangenen zwei Jahren nicht zu erkennen gewesen. Hier ist der Gesetzgeber dringend gefordert. Bei einer solchen Novellierung könnten zugleich eine grundsätzliche Modernisierung des IFG NRW in Angriff genommen werden und notwendige Korrekturen und Klarstellungen erfolgen. Siehe hierzu unter 6, 7 und 8.

Selbstverständlich biete ich bei einer Fortentwicklung des Gesetzes auf der Basis jahrelanger Praxiserfahrung gern meine fachliche Beratung an.

Eine moderne Verwaltung muss für die Bevölkerung transparent sein und darf nicht den Anschein von Geheimniskrämerei erwecken. In Zeiten der digital basierten Kommunikation, in der sich „Fake News" über Massenmedien und Social Media rasant verbreiten, ist es umso wichtiger, dass Bürgerinnen und Bürger Informationen unmittelbar aus deren Quelle beziehen können. Der ausschließlich „antragsgesteuerte" Informationszugang nach dem IFG NRW

hinkt den Entwicklungen in anderen Ländern deutlich hinterher und reicht vielen Informationssuchenden schon längst nicht mehr aus.

Das IFG NRW wird im Jahr 2020 volljährig, und es ist nunmehr vordringliche Aufgabe des Gesetzgebers, das Gesetz den Anforderungen einer modernen Informationsgesellschaft entsprechend zu novellieren und so dem Informationsinteresse der Bürgerinnen und Bürger umfassend Rechnung zu tragen.

1. Bundesverfassungsgericht (BVerfG): Informationsfreiheit hat Verfassungsrang!

Das BVerfG hat in seinem Beschluss vom 20. Juni 2017, Az. 1 BvR 1978/13, festgestellt, dass es sich bei der Informationsfreiheit um ein Grundrecht handelt. Damit hat es zugleich einen langjährigen dogmatischen Streit um den Rang und die verfassungsrechtliche Ableitung der Informationsfreiheit entschieden.

Den Verfassungsrang leitet das BVerfG aus Art. 5 Abs. 1 Satz 1 Halbsatz 2 des Grundgesetzes (GG) ab. Dort heißt es: „Jeder hat das Recht, (…) sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten." Das BVerfG stellt hierzu fest, dass eine Informationsquelle dann allgemein zugänglich ist, „wenn sie geeignet und bestimmt ist, der Allgemeinheit, also einem individuell nicht bestimmbaren Personenkreis, Informationen zu verschaffen". Eine solche Bestimmung als Informationsquelle ist allerdings nur insoweit gegeben, als der Landes- bzw. Bundesgesetzgeber tatsächlich ein IFG erlassen hat. In der Konsequenz dieser Entscheidung gewinnt die Informationsfreiheit erheblich an Gewicht, da Auslegung und Anwendung der gesetzlichen Ausnahmetatbestände (in NRW sind dies die §§ 6 bis 9 IFG NRW) nun auch im Licht der grundrechtlich garantierten Informationsfreiheit erfolgen müssen. Die Informationsfreiheit hat damit denselben verfassungsrechtlichen Rang wie der Datenschutz, der in NRW bereits seit 1978 ausdrücklichen Verfassungsrang genießt. In Art. 4 Abs. 2 der Verfassung für das Land NRW heißt es: "Jeder hat Anspruch auf Schutz seiner personenbezogenen Daten. Eingriffe sind nur im überwiegenden Interesse der Allgemeinheit aufgrund eines Gesetzes zulässig." Im GG ist der Datenschutz im Übrigen in Art. 2 Abs. 1 in Verbindung mit Art 1 GG verankert.

Der Beschluss des höchsten deutschen Gerichts ist zu begrüßen, weil damit eine erhebliche Aufwertung der Informationsfreiheit verbunden ist. Wie sich dies in der Verwaltungspraxis auswirkt, bleibt abzuwarten. Zudem stellt sich die Frage, wie dieses Grundrecht in den Ländern ohne IFG – dies sind bislang immerhin noch drei: Bayern, Niedersachsen und Sachsen – gewährleistet und geschützt werden kann.

2. Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)

Die IFK – das Pendant zur Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – tagte im Jahr 2017 unter Vorsitz von Rheinland-Pfalz und im Jahr 2018 unter Vorsitz von Baden-Württemberg insgesamt viermal.

Wie immer wurden auf den Sitzungen der IFK aktuelle Fragen zur Informationsfreiheit erörtert. Alle Protokolle der IFK mit den dazugehörigen Protokollen der vorbereitenden Arbeitskreissitzungen sind auf unserer Homepage www.ldi.nrw.de veröffentlicht. Folgende Entschließungen wurden von der IFK verabschiedet:

In der Entschließung „Mit Transparenz gegen ‚Fake-News'" vom 13. Juni 2017 fordert die IFK alle öffentlichen Stellen in Deutschland auf, sich ihrer Verantwortung für die Informationsfreiheit bewusst zu sein und durch größtmögliche Transparenz – sowohl auf Antrag als auch proaktiv – die Bürgerinnen und Bürger in ihrer politischen Willensbildung zu unterstützen.

Mit der Entschließung „Soziale Teilhabe braucht konsequente Veröffentlichung von Verwaltungsvorschriften!" vom 16. Oktober 2018 appelliert die IFK an alle Sozialleistungsträger, „Verwaltungsvorschriften antragsunabhängig, zeitnah und benutzerfreundlich zu veröffentlichen, soweit sie dazu nicht bereits gesetzlich verpflichtet sind".

Zwei weitere Entschließungen wurden allein durch die Landesbeauftragten für die Informationsfreiheit gefasst:

Die „Grundsatzpositionen" vom 6. Oktober 2017 beinhalten mehrere Forderungen an die Bundespolitik.

Mit der Entschließung „Open Data: Gesetzentwurf der Bundesregierung greift zu kurz!" vom 24. April 2017, wird der Deutschen Bundestag aufgefordert, statt des von der Bundesregierung vorgelegten Entwurfs eines Open-Data-Gesetzes (Erstes Gesetz zur Änderung des E-Government-Gesetzes) das Informationsfreiheitsgesetz des Bundes zu einem umfassenden Transparenzgesetz weiterzuentwickeln.

Die Entschließungen sind im Anhang abgedruckt.

Die IFK wird auch weiterhin für die Stärkung und den Ausbau der Informationsfreiheit in Deutschland eintreten.

3. Informationsfreiheitsrechtliche Beratung und Schulung durch die LDI NRW

Seit 2016 bieten wir Vorträge und Schulungen für Beschäftigte von Behörden an.

Nicht nur Antragstellerinnen und Antragsteller können sich zur Vermittlung an uns wenden, sondern auch öffentliche Stellen haben selbstverständlich die Möglichkeit, uns bei informationsfreiheitsrechtlichen Fragen zu kontaktieren.

Das war schon immer so. Im Jahr 2016 haben wir darüber hinaus begonnen, Vorträge und Schulungen zum Informationsfreiheitsgesetz NRW (IFG NRW) anzubieten. So haben wir auch im Berichtszeitraum entsprechende Einladungen mehrerer Kommunen sowie eines kommunalen Spitzenverbandes erhalten und gerne wahrgenommen. Sowohl bei den kreisfreien wie kreisangehörigen Gemeinden besteht Beratungsbedarf bezüglich des IFG NRW. Der formlose Erfahrungsaustausch der öffentlichen Stellen mit der LDI NRW zu praktischen Fragestellungen ist zudem eine gute Möglichkeit, um die jeweiligen Perspektiven und Standpunkte kennenzulernen und damit letztendlich den freien Zugang zu Informationen zu stärken. Dadurch ergibt sich ein konstruktiver Austausch, wie zum Beispiel über Auslegungsfragen zum Schutz von Betriebs- und Geschäftsgeheimnissen. Das Beratungs- und Schulungsangebot und das damit verbundene gegenseitige Kennenlernen bewirken zudem, dass seitdem manche der beteiligten Kommunen erst einmal eine Vorabberatung der LDI NRW zu Auslegungsfragen in Anspruch nehmen, bevor ein Antrag vorschnell abgelehnt wird. Solche Beratungen bieten auch die Möglichkeit, den auskunftspflichtigen Stellen die Perspektive der Antragstellenden näherzubringen.

Insgesamt haben wir mit unserem Angebot sehr positive Erfahrungen gemacht und freuen uns auf einen weiterhin kooperativen und konstruktiven Austausch mit anderen öffentlichen Stellen.

Unser Beratungs- und Schulungsangebot für informationspflichtige Stellen ist ein Baustein, um die Informationsfreiheit in NRW weiter zu stärken.

4. Die Grenzen der Informationsfreiheit

Das Informationsfreiheitsgesetz NRW (IFG NRW) eröffnet den Zugang zu einer großen Bandbreite von Informationen. Die Reichweite dieses Zugangsanspruchs ist allerdings auch nicht unbegrenzt, was bei Bürgerinnen und Bürgern immer wieder zu Enttäuschungen führt. Diese Grenzen ergeben sich unmittelbar aus dem Gesetz und lassen sich nicht durch dessen Auslegung verschieben.

Im Folgenden werden einige Grenzen des IFG NRW aufgezeigt, die in unserer Praxis regelmäßig eine Rolle spielen.

„Wieso, weshalb, warum…?“ sind keine Fragen, auf die nach Maßgabe des IFG NRW eine Antwort erteilt werden muss.

Sinn und Zweck des Informationszugangsanspruchs nach dem IFG NRW ist es, die Transparenz behördlichen Handelns zu erhöhen. Hierdurch sollen Nachvollziehbarkeit und Akzeptanz behördlicher Entscheidungen gefördert werden. Darüber hinaus soll die Mitsprache der Bürgerinnen und Bürger in Bezug auf das Handeln staatlicher Organe dadurch optimiert werden, dass ihnen eine verbesserte Argumentationsgrundlage an die Hand gegeben wird. In diesem Sinn dient das Informationszugangsrecht einer – wenn auch mittelbaren – Kontrolle staatlichen Handelns. Voraussetzung für einen Informationszugang ist aber stets, dass überhaupt eine Information im Sinne des § 4 Abs. 1 IFG NRW bei der Behörde vorhanden ist. Eine Erstellung von Informationen und Begründungen kann dagegen nicht beansprucht werden. In der Praxis erhalten wir häufig Eingaben von Bürgerinnen und Bürgern, die Begründungen zu Entscheidungen begehren. Sie haben indes nur dann einen Anspruch auf Informationszugang, wenn die Begründung zu einer Entscheidung dokumentiert ist und damit vorliegt. Die öffentlichen Stellen sind nicht verpflichtet, zusätzliche Erläuterungen oder Erklärungen abzugeben (siehe auch 22. Bericht unter 12.2).

Es gibt keinen Anspruch auf Zugang zu eventuell in der Zukunft vorliegenden Informationen.

Antragstellende haben keinen Anspruch auf Zugang zu Informationen, die erst zukünftig erstellt oder vorliegen werden; das IFG NRW sieht – wie oben ausgeführt – nur einen Zugang zu bereits vorhandenen Informationen vor. So wurde in einem Fall ein Dauerantrag auf Zugang zu zukünftigen Demonstrationsanmeldungen gestellt. Da diese Informationen zum Zeitpunkt der Antragsstellung nicht vorlagen, wurde der Antrag zu Recht abgelehnt.

Nicht alle Institutionen unterfallen (uneingeschränkt) dem Anwendungsbereich des IFG NRW.

Für den Landtag, die Gerichte, die Behörden der Staatsanwaltschaft, den Landesrechnungshof und die Staatlichen Rechnungsprüfungsämter gilt das Gesetz bereits nach dem ausdrücklichen Wortlaut des § 2 Abs. 2 IFG NRW nur, soweit sie Verwaltungsaufgaben wahrnehmen. Weitere Einschränkungen sieht § 2 Abs. 3 IFG NRW für Forschungseinrichtungen, Hochschulen und Prüfungseinrichtungen vor.

Darüber hinaus gibt es einige weitere öffentliche Stellen mit Sitz in NRW, auf die das IFG NRW keine Anwendung findet. So unterfällt beispielsweise der „ARD ZDF Deutschlandradio Beitragsservice“ nicht dem IFG NRW. Diese Stelle, die seit dem 1. Januar 2013 den Rundfunkbeitrag einzieht, hat zwar ihren Sitz in Köln, aber das IFG NRW findet auf diese nicht rechtsfähige Gemeinschaftseinrichtung keine Anwendung. Lediglich der WDR als Mitglied des Beitragsservices und Anstalt des öffentlichen Rechts des Landes NRW unterfällt dem Anwendungsbereich dieses Gesetzes. Ebenso besteht nach dem IFG NRW kein Anspruch auf Informationszugang gegenüber dem Deutschlandradio. Es handelt sich bei dieser Stelle um eine von den Ländern errichtete und getragene gemeinnützige rechtsfähige Körperschaft des öffentlichen Rechts. Damit ist sie jedoch keine informationspflichte Stelle des Landes NRW. Im Ergebnis sind so einige öffentliche Stellen mit Sitz in NRW dem Anwendungsbereich des IFG NRW entzogen.

Das IFG NRW ist ein Werkzeug, um Transparenz in Bezug auf Verwaltungshandeln zu schaffen, kann jedoch nicht alle Fragen der Antragstellenden beantworten.

5. Zivilrechtlich geschlossene Verträge unterfallen dem Informationsfreiheitsgesetz NRW (IFG NRW)

Immer noch sehen einige öffentliche Stellen den Anwendungsbereich des IFG NRW in Bezug auf zivilrechtlich geschlossene Verträge nicht als eröffnet an. Dabei handelt es sich um eine Frage, die längst obergerichtlich geklärt wurde.

Zu dieser Thematik hatten wir uns bereits im 22. Bericht (unter 12.6) geäußert und in einem Fall eine Beanstandung ausgesprochen.

Gleichwohl stellen wir nach wie vor fest, dass einige öffentliche Stellen den Zugang zu privatrechtlich geschlossenen Verträgen mit dem Hinweis ablehnen, es handele sich nicht um eine Verwaltungstätigkeit der Behörde im Sinne des § 2 Abs. 1 Satz 1 IFG NRW. Dabei ist der Begriff der Verwaltungstätigkeit nach der Rechtsprechung des Oberverwaltungsgerichts NRW weit auszulegen (Beschluss vom 31. Januar 2005, Az. 21 E 1487/04). Unabhängig von der Rechtsform des Handelns der öffentlichen Stelle kommt es allein darauf an, dass sich das Handeln als Wahrnehmung einer Verwaltungsaufgabe – im Gegensatz zu Aufgaben der Legislative oder der Judikative – darstellt. Daher unterfallen etwa auch Miet-, Kauf- und Erbbaurechtsverträge dem Anwendungsbereich des IFG NRW. Die an uns herangetragenen Fälle zeigen jedoch, dass die Definition des Anwendungsbereichs in § 2 Abs. 1 IFG NRW klarer gefasst werden sollte.

Auch wenn öffentliche Stellen privatrechtlich handeln, unterfallen sie der Informationspflicht nach dem IFG NRW.

6. Auslagenerhebung ohne gesetzliche Grundlage

Das Bundesverwaltungsgericht (BVerwG) hat in seinem Urteil vom 20. Oktober 2016, Az. 7 C 6.15, festgestellt, dass die Regelungen der Informationsgebührenverordnung des Bundes über die Erhebung von Auslagen mangels einer ausreichenden gesetzlichen Ermächtigungsgrundlage unwirksam sind. Dies hat mittelbar auch Auswirkung auf NRW.

Das Urteil des BVerwG bezieht sich zwar unmittelbar auf das Informationsfreiheitsgesetz des Bundes, betrifft gleichermaßen aber auch NRW, dessen Informationsfreiheitsgesetz (IFG NRW) eine vergleichbare Regelung zur Erstattung von Kosten enthält. § 11 Abs. 2 IFG NRW ermächtigt zum Erlass einer die Gebühren regelnden Rechtsverordnung. Nicht umfasst von der Ermächtigung ist jedoch die Regelung zur Erstattung von Auslagen, da § 11 Abs. 2 IFG NRW ausdrücklich nur „Gebühren“, nicht aber auch „Auslagen“ benennt. Auslagen sind Kosten, die die Behörde etwa für die Anfertigung von Kopien und Ausdrucken erhebt. Mangels Ermächtigungsgrundlage ist nach aktueller Gesetzeslage die Erhebung von Auslagen nach § 11 Abs. 2 IFG NRW in Verbindung mit § 3 Verwaltungsgebührenordnung zum IFG NRW rechtswidrig. Im Ergebnis bedeutet dies für informationspflichtige Stellen in NRW, dass sie gegenwärtig nicht dazu berechtigt sind, von Antragstellenden eine Auslagenerstattung zu fordern.

Sollen informationspflichtige Stellen die Möglichkeit erhalten, im Rahmen der Gewährung von Informationszugangsansprüchen eine Auslagenerstattung zu beanspruchen, ist der Gesetzgeber gefordert, die Regelung in § 11 Abs. 2 IFG NRW entsprechend anzupassen.

7. Befugnisse der Informationsfreiheitsbeauftragten durch Gesetzesreform beschnitten

Vor Wirksamwerden der DS-GVO am 25. Mai 2018 waren die Aufgaben und Befugnisse der Informationsfreiheitsbeauftragten durch einen Verweis auf die im Datenschutzgesetz NRW (DSG NRW) normierten Aufgaben und Befugnisse der Datenschutzbeauftragten geregelt. Die mit der DS-GVO verbundenen Änderungen des Datenschutzrechts haben eine Anpassung des IFG NRW erforderlich gemacht. Nun hat das Gesetz im neu gestalteten § 13 Informationsfreiheitsgesetz NRW (IFG NRW) zwar eine Vollregelung erhalten. Dennoch ist dabei einiges auf der Strecke geblieben.

So fehlen im aktualisierten IFG NRW etwa die Befugnisse der LDI NRW zu beraten, zu informieren und Empfehlungen unabhängig von einer Beanstandung zu geben. Zwar leiten wir aus dem allgemeinen in § 13 Abs. 1 IFG NRW normierten Mandat, für die Sicherstellung des Rechts auf Information zuständig zu sein, auch diese Aufgaben ab. Dennoch wäre eine explizite Zuweisung – wie etwa in § 22 Abs. 1 Satz 2 DSG NRW alte Fassung oder im jetzigen § 27 Abs. 1 DSG NRW für die Belange des Datenschutzes – wünschenswert. Zudem kann die LDI NRW nach dem aktuellen § 13 Abs. 6 Satz 2 IFG NRW nur „bei Verstößen gegen die Informationspflicht“ eine Beanstandung aussprechen. Diese Formulierung nimmt etwa Verstöße wegen der Festsetzung überhöhter Gebühren im Zusammenhang mit einem Informationszugangsantrag aus. Das war in der Vergangenheit anders: Bis zum 25. Mai 2018 konnten wir „Verstöße gegen die Vorschriften dieses Gesetzes“ beanstanden. Die ohnehin limitierten Möglichkeiten erfahren dadurch eine zusätzliche Einschränkung, die nicht nachvollziehbar ist. Zu begrüßen wäre es außerdem gewesen, bei dieser Gelegenheit weitere Befugnisse, wie etwa die Beanstandung bei Verstößen gegen Veröffentlichungspflichten, festzuschreiben.

Auch in Bezug auf die Aufgaben und Befugnisse der LDI NRW besteht akuter Nachbesserungsbedarf. Bei einer künftigen Reform des IFG NRW sollten diese Punkte berücksichtigt werden.

8. Reformbedarf des Informationsfreiheitsgesetzes NRW (IFG NRW)

Das IFG NRW hat sich grundsätzlich bewährt, bedarf jedoch teilweise der Überarbeitung und zeitgemäßen Fortentwicklung.

2002 hat NRW als viertes Land nach Brandenburg (1998), Berlin (1999) und Schleswig-Holstein (2000) ein IFG erhalten und gehörte damit zu den Vorreitern. Nun – 17 Jahre später – ist das IFG NRW in die Jahre gekommen, und es bedürfte an der einen oder anderen Stelle dringend einer Modernisierung.

Grundsätzlicher Reformbedarf ergibt sich etwa hinsichtlich der Weiterentwicklung zu einem Transparenzgesetz, das öffentliche Stellen verbindlich dazu verpflichten würde, bestimmte Informationen antragsunabhängig im Internet zu veröffentlichen (siehe dazu ausführlich im 23. Bericht unter 16.2). Nach wie vor fehlt es auch noch an der Zuständigkeit der LDI NRW in Bezug auf das Umweltinformationsgesetz NRW – in diesem Bereich gibt es seit Bestehen des Gesetzes im Jahr 2007 keine unabhängige Aufsichtsbehörde.

Konkreter Reformbedarf ergibt sich etwa aus der Tatsache, dass die in § 4 Abs. 1 IFG NRW geregelte Antragsberechtigung auf natürliche Personen begrenzt ist. Dies ist vor allem im Vergleich mit anderen IFG nicht mehr zeitgemäß: So ist zum Beispiel in Bremen, Brandenburg, Hamburg und im Bund „jeder“ antragsberechtigt – also unabhängig davon, ob es sich um eine natürliche oder juristische Person handelt. In derselben Norm sollte der Begriff der „amtlichen Information“ um den Zusatz „amtlichen“ reduziert werden, da diese Formulierung dazu verleitet, den Zugang zu Informationen in den Fällen zu verweigern, in denen es sich um das Tätigwerden in privatrechtlichen Angelegenheiten handelt.

Des Weiteren bedarf es einer Konkretisierung der in § 12 IFG NRW normierten Veröffentlichungspflichten öffentlicher Stellen: Bislang sind diese zwar bereits verpflichtet, Geschäftsverteilungspläne und Organigramme zu veröffentlichen. Ausdrücklich verankert werden sollte dabei aber die Verpflichtung, diese Übersichten inklusive Namen und dienstlicher Kontaktdaten der Beschäftigten mit Außenkontakten zu veröffentlichen, damit für Bürgerinnen und Bürger transparent ist, wen sie wie erreichen können. Gerade in diesem Bereich ist darüber hinaus ein Vollzugsdefizit zu beobachten: Nicht wenige öffentliche Stellen des Landes kommen ihrer Veröffentlichungspflicht nicht ausreichend oder sogar gar nicht nach. Insofern wäre an die Einhaltung des Grundsatzes der Gesetzmäßigkeit der Verwaltung nach Art. 20 Abs. 3 Grundgesetz zu erinnern: Danach ist die Verwaltung an Recht und Gesetz gebunden.

Neben einigen redaktionellen Überarbeitungen ergibt sich Änderungsbedarf auch im Nachgang zum NRWDSAnpUG-EU aus dem Jahr 2018 (siehe hierzu unter 7). Außerdem bedarf es einer gesetzlichen Grundlage für Ausla-

generhebungen (siehe hierzu unter 6). Darüber hinaus sollten die Definitionen des Anwendungsbereichs in § 2 IFG NRW klarer gefasst werden (siehe hierzu unter 5).

Einst unter den Vorreitern auf dem Feld der Informationsfreiheit ist das IFG NRW – im Vergleich zu Ländern wie etwa Hamburg oder Rheinland-Pfalz mit ihren Transparenzgesetzen – ins Hintertreffen geraten und bedarf unbedingt einer Modernisierung.

Anhang zum Datenschutzbericht

Presseinformation der LDI NRW vom 29. März 2018 – Datenschutz-Grundverordnung im Verein

Die Europäische Datenschutz-Grundverordnung (DS-GVO) wird am 25.Mai 2018 direkt anwendbares Recht. Nationale Regelungsspielräume bestehen nur noch in einem begrenzten Umfang. Die bisher für Vereine einschlägigen Regelungen des deutschen Datenschutzrechts werden damit weitgehend durch die Verordnung ersetzt. Ergänzende nationale Regelungen wie etwa des neuen Bundesdatenschutzgesetzes (BDSG 2018) treten am 25. Mai 2018 in Kraft.

Helga Block, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und Vorsitzende der Datenschutzkonferenz, gibt auf regelmäßig gestellte Fragen Antworten.

Ergänzend sind auf unserer Internetseite www.ldi.nrw.de weitere Informationen abrufbar.

1. Wieso wurde das europäische Datenschutzrecht reformiert?
„Bislang war Datenschutz europäisch durch eine Richtlinie geregelt. Ziel der Richtlinie war es, einen Mindeststandard für den Datenschutz in Europa festzulegen, der in allen Mitgliedstaaten durch eigene, nationale Gesetze sichergestellt werden sollte. Dies lief nicht immer einheitlich. In den Mitgliedstaaten gab es 28 nationale Umsetzungs- und Anwendungsvarianten der Richtlinie. Die EU entschloss sich daher zur Reform des Datenschutzrechts in Form einer Verordnung. Diese gilt unmittelbar und ohne Umsetzung in nationales Recht in den Mitgliedstaaten. Ziel ist ein harmonisierter Datenschutz auf hohem Niveau. Das Datenschutzrecht war aber auch an die veränderten gesellschaftlichen Gegebenheiten anzupassen."

2. Sind auch Vereine von dieser Neuregelung betroffen?
„Ja. Jeder Verein, der personenbezogene Daten verarbeitet, ist betroffen – auch nicht eingetragene oder nicht rechtsfähige Vereine."

3. Was sind personenbezogen Daten?
„Beispiele sind neben Namen, Anschrift und Geburtsdaten auch die Mitgliedschaft im Verein als solche oder deren Dauer sowie Platzierungen in Wettkämpfen. Nach Art. 4 Nr. 1 sind alle Informationen umfasst, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen."

4. Hat die Datenschutz-Grundverordnung nur Auswirkungen auf den Gesamtverein oder auch auf die Untergliederungen wie Abteilungen und unselbständigen Ortsgruppen?
„Die Verordnung gilt im gesamten Verein, also sowohl bei mehrstufigen Vereinsorganisationen, etwa Orts- Landes- und Bundesverband, als auch in den unselbständigen Abteilungen des einzelnen Vereins. In unselbstständigen Untergliederungen muss aber

in der Regel weder ein eigener Datenschutzbeauftragter bestellt noch ein eigenes Verarbeitungsverzeichnis geführt werden. Dies erfolgt auf Ebene des Gesamtvereins."

5. Welche Änderungen erwarten die Vereine? Was sollten Vereine jetzt veranlassen?

„Die bisher für Vereine geltenden Regelungen des deutschen Datenschutzrechts werden weitgehend durch die Verordnung ersetzt. Viele Grundsätze des bislang geltenden Rechts finden sich jedoch auch in der Verordnung wieder. Vorhandene Strukturen und Prozesse in Vereinen, die sich an dem geltenden Datenschutzrecht ausrichten, machen sich jetzt also bezahlt. Hier geht es oft nur um Anpassungen im Einzelfall. Vereine hingegen, die das Thema Datenschutz bislang vernachlässigt haben, haben viel nachzuholen um ihre Organisation datenschutzgerecht zu gestalten. In einigen Vereinen haben sich über die Jahre vermutlich an verschiedenen Stellen eine Vielzahl personenbezogener Daten angesammelt. Ausgangspunkt sollte also zunächst eine Bestandsaufnahme sein. Welche Mitgliederdaten, Listen über Platzierungen oder aber auch Beschäftigtendaten liegen im Verein vor? Im nächsten Schritt ist dann für jede einzelne Information zu prüfen, ob der Verein mit dieser überhaupt umgehen darf. Auch unter der Verordnung gilt dabei das Prinzip des „Verbots mit Erlaubnisvorbehalt". Das bedeutet, dass Daten nur dann erhoben oder weitergegeben werden dürfen, wenn die betroffene Person entweder eingewilligt hat oder eine sonstige Rechtsgrundlage dies erlaubt. Die Datenschutzkonferenz hat für die Umsetzung der Verordnung einen Maßnahmenplan veröffentlicht, abrufbar auf unserer Internetseite www.ldi.nrw.de."

6. Muss der Verein seine Mitglieder jetzt umfangreicher informieren?

„Die Verordnung soll besonders die Rechte der Bürgerinnen und Bürger stärken. Ihre Rechte können sie jedoch nur dann wahrnehmen, wenn sie wissen, dass personenbezogene Daten über sie verarbeitet werden. Die neuen Informationspflichten sind deshalb umfangreicher und auch von Vereinen zu beachten. Immer dann wenn Daten der Mitglieder erhoben werden, etwa im Antrag auf Mitgliedschaft, müssen die in Art. 13 genannten Informationen mitgeteilt werden. So ist insbesondere über Art, Umfang und Zweck der Datenerhebung aber auch über die Rechte der Betroffenen zu informieren. Bislang war auf Vereinsformularen zum Datenschutz oft nur der Hinweis zu lesen, dass die Daten „unter Beachtung des Datenschutzrechts" verarbeitet werden. Das reicht so nicht aus."

7. Braucht jeder Verein künftig einen Datenschutzbeauftragten?

„Grundsätzlich gilt hier: Wer bisher einen Datenschutzbeauftragten bestellen musste, muss dies in der Regel auch weiterhin. Allgemeine Aussagen darüber hinaus sind schwierig, denn große und kleine Vereine übernehmen in vielen Feldern gesellschaftliche Verantwortung. Im Einzelfall ist deshalb zu prüfen, ob nach den Vorgaben des Artikels 37 der Verordnung oder § 38 des neuen Bundesdatenschutzgesetzes ein Datenschutzbeauftragter zu bestellen ist. Sportvereine oder Vereine die Gesundheitsdaten verarbeiten, kann etwa eine Pflicht nach Art. 37 Abs. 1 lit. c treffen, da ihre Kerntätigkeit möglicherweise in der Verarbeitung besonderer Kategorien von Daten gemäß

Art. 9 liegt. Zudem besteht eine Benennungspflicht nach § 38 Abs. 1 Satz 1 des neuen Bundesdatenschutzgesetzes, wenn regelmäßig mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Unabhängig von der Pflicht zur Bestellung eines Datenschutzbeauftragten, empfehlen wir, dass es im Verein zumindest eine Ansprechpartnerin oder einen Ansprechpartner gibt, die oder der sich in Fragen des Datenschutzes auskennt. Auch die freiwillige Bestellung eines Datenschutzbeauftragten ist möglich und zu empfehlen."

8. Wer kann zum Datenschutzbeauftragten bestellt werden?

„Zunächst muss die oder der Datenschutzbeauftragte unabhängig und weisungsfrei sein. Vorstandsmitglieder scheiden damit aus. Artikel 37 Absatz 5 verlangt als Voraussetzung eine ausreichende Qualifizierung und Fachwissen. Das bezieht sich aber nicht nur auf die gesetzlichen Grundlagen. Weil viele Daten heute elektronisch verarbeitet werden, sollte Mann oder Frau sich auch mit IT-Systemen und IT-Sicherheitsmaßnahmen auskennen. Wie vertieft diese Kenntnisse sein müssen, ist auch hier wieder eine Frage des Einzelfalles. Je komplexer die Datenverarbeitungen sind oder je mehr sensible Daten vorhanden sind, desto höhere Anforderungen sind an das notwendige Fachwissen des Datenschutzbeauftragten zu stellen. Werden etwa umfangreich Gesundheitsdaten verarbeitet ist eine höhere Qualifikation erforderlich, als in Vereinen, die lediglich eine Mitgliederliste mit Kontaktdaten führen."

9. Darf ein Verein personenbezogene Daten demnächst überhaupt noch weitergeben?

„Es kommt im Einzelfall darauf an, welche personenbezogenen Daten zu welchem Zweck und an wen übermittelt werden. Ausgangspunkt sollte hier zunächst sein, dass Vereinsmitglieder davon ausgehen dürfen, dass Informationen über sie nur zur Verwaltung und Betreuung der Mitgliedschaft genutzt werden und den Verein nicht verlassen. Wurden die personenbezogenen Daten rechtmäßig erhoben, ist weiter zu prüfen, ob die Betroffenen in die Weitergabe ihrer Daten eingewilligt haben oder aber eine andere Rechtsgrundlage vorliegt. Beabsichtigt der eigenständige Einzelverein etwa seine Mitgliederliste an den Dachverein zu übersenden, verlassen die Informationen den Verein. Es erfolgt eine Weitergabe an Dritte. Dies ist nicht ohne weiteres möglich. Als Lösung kommt etwa eine ausdrückliche Regelung in der Vereinssatzung in Betracht. Bei einer Weitergabe innerhalb des Vereins, zum Beispiel zwischen den Vereinsmitgliedern, kann ein Blick auf den festgelegten Vereinszweck weiterhelfen. Die Weitergabe an Vereinsmitglieder ist grundsätzlich möglich, wenn der Vereinszweck eine besondere persönliche Verbundenheit zwischen den Vereinsmitgliedern vorschreibt oder die persönliche Kontaktpflege der Mitglieder einen wesentlichen Bestandteil darstellt. Die Weitergabe sollte aber mit dem Hinweis erfolgen, dass diese nur für Vereinszwecke erfolgt."

10. Dürfen Informationen noch per E-Mail verschickt werden?

„Eine E-Mail ist vergleichbar mit einer Postkarte. Die Möglichkeit, dass unbefugte Dritte mitlesen, kann nicht ganz ausgeschlossen werden. Vereine sind nach Art. 32 aber

verpflichtet die personenbezogenen Daten durch geeignete und angemessene Maßnahmen zu schützen. Grundsätzlich empfehlen wir deshalb E-Mails mit personenbezogenen Daten nur verschlüsselt zu senden. Und bei der Nutzung von E-Mail-Verteilern sollte die BCC-Funktion, auch Blindkopie-Funktion genannt, verwendet werden."

11. Welche Dokumentationspflichten gib es? Muss ein Verarbeitungsverzeichnis geführt werden?

„Die Verordnung sieht als eine neue Dokumentationspflicht das so genannte Verarbeitungsverzeichnis vor. Dieses geht über das bisherige Datenschutzrecht hinaus. Das Verarbeitungsverzeichnis soll der Transparenz und dem Nachweis der Einhaltung der Datenschutzvorschriften nach innen und nach außen gegenüber der Datenschutzaufsicht dienen. Im Verarbeitungsverzeichnis sind alle datenschutzrelevanten Prozesse aufzuführen. Nach Artikel 30 ist dies regelmäßig von jedem Verantwortlichen also auch von Vereinen zu führen. Bestehende Verarbeitungsübersichten nach dem bis Mai geltenden Bundesdatenschutzgesetz sind eine gute Grundlage für das Verarbeitungsverzeichnis. Sie sind jedoch gemäß der Verordnung anzupassen. Hinweise und Muster der Datenschutzkonferenz sind auf unserer Internetseite abrufbar."

12. Was passiert, wenn gegen die Grundverordnung verstoßen wird? Drohen dem Vorstand dann Strafen?

„Die Verordnung ist bereits am 25. Mai 2016 in Kraft getreten und wird am 25. Mai 2018 direkt anwendbares Recht. Damit hatten alle Betroffenen zwei Jahre Vorbereitungszeit. Vereine werden die Verordnung zu beachten haben und die Datenschutzaufsichtsbehörden können dies kontrollieren. Dazu haben wir zahlreiche Untersuchungs- und Abhilfebefugnisse und können diese auch mit Zwangsmitteln durchsetzen. Schwerpunktmäßig werden wir die Vereine jedoch weiter beraten und sensibilisieren."

Entschließungen der Datenschutzkonferenz 2017/2018

93. Konferenz vom 29./30. März 2017

▪ Göttinger Erklärung der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) vom 30. März 2017 – Vom Wert des Datenschutzes in der digitalen Gesellschaft

Datenschutz ist zurzeit in aller Munde: Mit der Europäischen Datenschutzreform werden ab Mai 2018 in der ganzen Europäischen Union neue einheitliche Regeln gelten. Gegenwärtig sind die Gesetzgeber in Bund und Ländern mit Hochdruck da-bei, das nationale Recht an die Europäischen Vorgaben anzupassen. Zugleich schreitet die Digitalisierung der Gesellschaft mit großen Schritten voran, etwa mit dem Internet der Dinge, der Wirtschaft 4.0 und künstlicher Intelligenz, und fordert die Wahrung des Datenschutzes und die Gewährleistung der Persönlichkeitsrechte heraus. Auch der Staat erweitert fortwährend seine Befugnisse zur Verarbeitung personenbezogener Daten, sei es zur Bekämpfung des Terrorismus und zur Gewährleistung der öffentlichen Sicherheit, sei es bei der Digitalisierung staatlicher Dienstleistungen.

Dabei gerät aber leichtfertig eines aus dem Blick: Datenschutz ist ein Grundrecht, wie die Meinungsfreiheit oder die Eigentumsgarantie. Es bindet alle Staatsgewalten unmittelbar, schützt die Menschenwürde und die freie Entfaltung der Persönlichkeit und kann auch Aspekte der Teilhabe und Chancengleichheit betreffen. Alle gesetzlichen Regelungen, sowie die Geschäftsmodelle und Anwendungen auch im Bereich der Wirtschaft, haben dies zu berücksichtigen. Immer häufiger stellen aber Verantwortliche in Politik und Wirtschaft dieses grundrechtlich geschützte Recht auf informationelle Selbstbestimmung implizit oder sogar explizit in Frage. Datenschutz wird als Hindernis diskreditiert.

Dies betrachtet die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder mit großer Sorge. Es befremdet sehr, wenn Mitglieder der Bundesregierung und andere Stimmen in der Politik in letzter Zeit immer wieder betonen, es dürfe kein Zuviel an Datenschutz geben und das Prinzip der Datensparsamkeit könne nicht die Richtschnur für die Entwicklung neuer Produkte sein. Stattdessen wird für eine vermeintliche Datensouveränität geworben, deren Zielrichtung aber im Unklaren bleibt.

Die Konferenz betont, dass Informationen über Personen keine Ware sind wie jede andere und nicht allein auf ihren wirtschaftlichen Wert reduziert werden dürfen. Gerade in Zeiten von Big Data, Algorithmen und Profilbildung bieten die digitalen Informationen ein nahezu vollständiges Abbild der Persönlichkeit des Menschen. Mehr denn je muss

daher die Menschenwürde auch im digitalen Zeitalter der zentrale Maßstab staatlichen und wirtschaftlichen Handelns sein. Zu einer menschenwürdigen und freien Entfaltung der Persönlichkeit gehört die freie Selbstbestimmung über das eigene Ich.

„Datensouveränität" verstanden als eigentumsähnliche Verwertungshoheit kann daher nur zusätzlich zum Recht auf informationelle Selbstbestimmung greifen, dieses jedoch keinesfalls ersetzen.

Die Konferenz fordert daher alle Entscheidungsträger in Politik und Wirtschaft auf, den hohen Wert des Rechts auf informationelle Selbstbestimmung für eine freiheitliche Gesellschaft zu achten und sich nachdrücklich vertrauensbildend für die Persönlichkeitsrechte einzusetzen. Datenschutz stellt kein Hindernis für die Digitalisierung dar, sondern ist wesentliche Voraussetzung für deren Gelingen.

Die Entwicklung datenschutzkonformer IT-Produkte und -Verfahren muss nachhaltig gefördert werden, um den Datenschutz zu einem Qualitätsmerkmal der europäischen Digitalwirtschaft zu machen.

▪ Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken

In Pilotprojekten wird derzeit der Einsatz von Videoüberwachungssystemen erprobt, die erweiterte Möglichkeiten der Verhaltensauswertung und der Identifizierung von Beobachteten bieten. Neben der Mustererkennung steht besonders die biometrische Gesichtserkennung im Fokus dieser Projekte. Dies verschärft die ohnehin schon vorhandene Problematik derartiger neuer Überwachungsverfahren, mit denen „abweichendes Verhalten" erkannt werden soll.

Der Einsatz von Videokameras mit biometrischer Gesichtserkennung kann die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, gänzlich zerstören. Es ist kaum möglich, sich solcher Überwachung zu entziehen oder diese gar zu kontrollieren.

Anders als bei konventioneller Videoüberwachung könnten Passanten mit dieser Technik nicht nur beobachtet und anhand bestimmter Muster herausgefiltert werden, sondern während der Überwachung anhand von Referenzbildern (Templates) automatisiert identifiziert werden. Damit wird eine dauerhafte Kontrolle darüber möglich, wo sich konkrete Personen wann aufhalten oder bewegen und mit wem sie hierbei Kontakt haben. Ermöglicht wird so die Erstellung von umfassenden Bewegungsprofilen und die Verknüpfung mit anderen über die jeweilige Person verfügbaren Daten.

Neben den genannten massiven gesellschaftspolitischen Problemen bestehen auch erhebliche rechtliche und technische Bedenken gegen den Einsatz solcher Überwa-

chungstechniken. Biometrische Identifizierung arbeitet mit Wahrscheinlichkeitsaussagen; bei dem Abgleich zwischen ermitteltem biometrischen Merkmal und gespeichertem Template sind falsche Identifizierungen keine Seltenheit. Beim Einsatz dieser Technik durch Strafverfolgungsbehörden kann eine falsche Zuordnung dazu führen, dass Bürgerinnen und Bürger unverschuldet zum Gegenstand von Ermittlungen und konkreten polizeilichen Maßnahmen werden. Dieselbe Gefahr besteht, falls sie sich zufällig im öffentlichen Raum in der Nähe von gesuchten Straftätern oder Störern aufhalten.

Es gibt keine Rechtsgrundlage für die Behörden von Bund und Ländern für den Einsatz dieser Technik zur Gefahrenabwehr und Strafverfolgung. Die bestehenden Normen zum Einsatz von Videoüberwachungstechnik erlauben nur den Einsatz technischer Mittel für reine Bildaufnahmen oder -aufzeichnungen, nicht hingegen für darüber hinausgehende Datenverarbeitungsvorgänge. Aufgrund des deutlich intensiveren Grundrechtseingriffs, der durch Videotechnik mit erweiterter Auswertung einhergeht, können die bestehenden gesetzlichen Regelungen nicht analog als Rechtsgrundlage herangezogen werden, da sie für einen solchen Einsatz verfassungsrechtlich zu unbestimmt sind.

Nach der Rechtsprechung des Bundesverfassungsgerichts sind Maßnahmen mit großer Streubreite ein erheblicher Grundrechtseingriff. So verlangt das Bundesverfassungsgericht bereits für das automatisierte Erfassen von KFZ-Kennzeichen zwecks Abgleichs mit dem Fahndungsbestand eine normenklare und verhältnismäßige Rechtsgrundlage, die einen anlasslosen und flächendeckenden Einsatz ausschließt. Da bereits die allgemeine Regelung zur Videoüberwachung nicht zur Erfassung von KFZ-Kennzeichen ermächtigt, muss dies erst recht für die viel stärker in die Grundrechte Betroffener eingreifende Videoüberwachung zwecks Abgleichs biometrischer Gesichtsmerkmale einzelner Personen gelten. Ein Einsatz der Videoüberwachung mit Gesichtserkennung darf daher auf derzeitiger Grundlage auch im Rahmen eines Pilotbetriebs nicht erfolgen.

94. Konferenz vom 8./9. November 2017

▪ Umsetzung der DSGVO im Medienrecht

Das Inkrafttreten der Datenschutzgrundverordnung (DSGVO) und deren Geltungsbeginn im Mai 2018 verlangt eine Anpassung der medienrechtlichen Datenschutzbestimmungen an die neuen Vorgaben. Dabei muss dem hohen Stellenwert der Meinungs- und Informationsfreiheit sowie der Presse-, Rundfunk- und Medienfreiheit gemäß Art. 5 Grundgesetz (GG) und Art. 11 EU-Grundrechtecharta (GRCh) für die freiheitliche demokratische Grundordnung ebenso Rechnung getragen werden wie dem Recht auf Informationelle Selbstbestimmung gemäß Art. 1 i.V.m. Art. 2 GG und dem Recht auf Schutz personenbezogener Daten gemäß Art. 8 GRCh. Kollisionen der Schutzbereiche der Grundrechte sind im Sinne einer praktischen Konkordanz aufzulösen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist daher auf die Anpassungsklausel des Art. 85 DSGVO hin. Danach können die Mitgliedstaaten Ausnahmen und Abweichungen von bestimmten Vorgaben der DSGVO normieren, wenn „dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen“. Das sich daraus ergebende Regel-Ausnahme-Verhältnis bedeutet, dass die Vorgaben der DSGVO grundsätzlich auch auf sämtliche Verarbeitungen personenbezogener Daten zu grundrechtlich besonders geschützten journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken angewendet werden sollen.

Bei der Umsetzung von Art. 85 DSGVO gilt es insbesondere folgende Anforderungen zu beachten:

- Ausnahmen oder Abweichungen von der Anwendung der DSGVO auf die Verarbeitung personenbezogener Daten im journalistischen Bereich müssen notwendig sein, um freie Meinungsäußerung und Informationsfreiheit gemäß Art. 11 GRCh sicherzustellen.
- Einen regelhaften Vorrang der Presse-, Rundfunk- und Medienfreiheit sieht die DSGVO nicht vor. Sie verlangt vielmehr, einen angemessenen Ausgleich zwischen den Grundrechten herzustellen, wenn diese in Widerstreit geraten (vgl. 153. Erwägungsgrund der DSGVO).
- Die Grundsätze des Datenschutzes (Art. 5 DSGVO) müssen hinreichend Beachtung finden. Jedenfalls steht es nicht im Einklang mit dem Recht auf Schutz personenbezogener Daten, wenn die Grundsätze des Datenschutzes im Journalismus in weitem Umfang ausgeschlossen werden. Eine Regelung kann keinesfalls als notwendig i. S. d. DSGVO angesehen werden, wenn sie zum Zwecke der Abwägung mit der Meinungs- und Informationsfreiheit die Transparenzrechte und In-

terventionsmöglichkeiten für betroffene Personen sowie Verfahrensgarantien über eine unabhängige Aufsicht missachtet.
- Über den eingeräumten Gestaltungsspielraum geht es hinaus, wenn die Verarbeitung personenbezogener Daten durch Hilfsunternehmen zu undifferenziert vom Geltungsbereich der DSGVO ausgenommen wird, ohne dass diese Aktivitäten unmittelbar der journalistischen Tätigkeit dienen. Die Reichweite der journalistischen Tätigkeit bedarf zudem einer Konkretisierung.
- Die künftige Aufsicht über den Datenschutz beim Rundfunk ist unabhängig auszugestalten. Sie bedarf wirksamer Abhilfebefugnisse bei Datenschutzverstößen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher für die Anpassung von RundfunkStaatsverträgen, Presse- und Mediengesetzen:

- Die gesetzlichen Anpassungen i. S. d. Art. 85 DSGVO müssen konkret und spezifisch – bezogen auf die jeweiligen Normen und Vorgaben der DSGVO – Ausnahmen und Abweichungen regeln und diese begründen.
- Bei der Ausübung der jeweiligen Regelungskompetenz ist das europäische Datenschutzrecht zwingend zu beachten. Eine faktische Beibehaltung der bisherigen nationalen Rechtslage würde dem nicht gerecht.

Keine anlasslose Vorratsspeicherung von Reisedaten

Der Gerichtshof der Europäischen Union (EuGH) hat in seinem Gutachten vom 26. Juli 2017 (Gutachten 1/15) zum Fluggastdaten-Abkommen der EU mit Kanada die langfristige Speicherung von Fluggastdaten (Passenger Name Records -PNR-Daten) sämtlicher Passagiere für nicht mit der Europäischen Grundrechtecharta vereinbar erklärt und seine Position zu anlasslosen Speicherungen personenbezogener Daten bekräftigt. Er erteilt damit einer anlasslosen Vorratsdatenspeicherung von personenbezogenen Daten erneut eine klare Absage. Die Aussagen des EuGH sind nicht nur auf alle geltenden PNR-Instrumente übertragbar und stellen Anforderungen an die Anpassung des Fluggastdatengesetzes, sie betreffen auch die auf europäischer Ebene angestrebte Einrichtung eines Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS), die ebenfalls weitreichende anlasslose Speicherungen beabsichtigen.

Zwar hält der EuGH es grundsätzlich für zulässig, Fluggastdaten automatisiert zu übermitteln und auszuwerten, um Personen zu ermitteln, die eine potentielle Gefahr für die öffentliche Sicherheit darstellen und bei ihrer Einreise einer gewissenhaften Kontrolle unterzogen werden sollen. Das gilt jedoch nicht für sensible Daten, die Rückschlüsse etwa auf die rassische und ethnische Herkunft, religiöse Überzeugungen oder das Sexualleben ermöglichen. Der Übermittlungszweck rechtfertigt auch nicht automatisch die weitere Verwendung und Speicherung der Daten. Die übermittelten Daten haben vielmehr ihren Zweck erfüllt, wenn sich während des Aufenthaltes keine konkre-

ten Anhaltspunkte für geplante terroristische oder andere schwere Straftaten ergeben haben. In diesem Fall sieht der EuGH keine Rechtfertigung für eine weitere Speicherung der Daten.

Das Fluggastdatengesetz, mit dem die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von PNR-Daten zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität umgesetzt wurde, geht insbesondere durch die Einbeziehung der innereuropäischen Flüge, die im Widerspruch zu dem Grundsatz des freien Personenverkehrs im Schengen-Raum steht, noch über den verpflichtenden Teil der Richtlinie hinaus.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) sieht in den vom EuGH ausgesprochenen Feststellungen zur Rechtslage einen unverzichtbaren Maßstab für die Verordnungsvorschläge zur Einrichtung eines neuen Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS).

Mit dem EES sollen alle Ein- und Ausreisen sowie Einreiseverweigerungen von Drittstaatlern in die EU zentral erfasst und für mehrere Jahre gespeichert werden (einschließlich biometrischer Identifizierungsmerkmale). Im ETIAS sollen zum Zwecke der Erleichterung der Grenzkontrollen vorab Daten von einreisewilligen visabefreiten Drittstaatlern erhoben und ebenfalls für mehrere Jahre zentral gespeichert werden. In beiden Datenbanken sollen also Daten, die im Rahmen der Einreise und Grenzkontrolle erhoben werden, ebenso wie nach dem PNR-Abkommen, ohne konkreten Anlass zentral für einen langen Zeitraum vorgehalten werden. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hält dies nicht für vertretbar.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert die jeweils zuständigen Gesetzgeber auf, zeitnah und konsequent sämtliche PNR-Instrumente der EU im Sinne der EuGH-Rechtsprechung nachzubessern, insbesondere das deutsche Fluggastdatengesetz.

Sie fordert die Bundesregierung zudem auf, sich auf europäischer Ebene für eine den Anforderungen der EU-Grundrechtecharta und der Rechtsprechung des EuGH entsprechende Ausgestaltung der angestrebten Systeme EES und ETIAS einzusetzen.

95. Konferenz vom 25./26. April 2018

▪ Zuverlässigkeitsüberprüfungen bei öffentlichen und privaten Veranstaltungen nur im erforderlichen Maß und nach einem rechtsstaatlichen und transparenten Verfahren

Zunehmend werden im Rahmen von öffentlichen und privaten Veranstaltungen Personen, die in unterschiedlichen Funktionen auf einem Veranstaltungsgelände tätig werden wollen oder sonst Zutritt zu Sicherheitszonen begehren (beispielsweise Anwohner), durch Sicherheitsbehörden auf ihre Zuverlässigkeit überprüft. Auch bei privaten Veranstaltungen fordern die Polizeien die Veranstalter bisweilen dazu auf, dafür zu sorgen, dass alle im

Rahmen der Veranstaltung Tätigen einer solchen Prüfung unterzogen werden. In den

meisten Fällen ist alleinige Grundlage für diese Maßnahmen immer noch die Einwilligung der Betroffenen.

Bereits vor mehr als zehn Jahren haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 25./26. Oktober 2007 darauf hingewiesen, dass allein die Einwilligung der Betroffenen in eine Zuverlässigkeitsüberprüfung keine legitimierende Grundlage für solche tiefen Eingriffe in das Recht auf informationelle Selbstbestimmung darstellen kann. Die wiederholten Forderungen nach Schaffung gesetzlicher Grundlagen haben seitdem die Gesetzgeber nur weniger Bundesländer aufgegriffen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert die Gesetzgeber und die Verantwortlichen deshalb erneut nachdrücklich auf, für ein rechtsstaatliches und transparentes Verfahren solcher Zuverlässigkeitsüberprüfungen zu sorgen, das auf das absolut erforderliche Maß beschränkt bleibt, sowohl was den Umfang der Überprüfung als auch den betroffenen Personenkreis betrifft. Dabei sind insbesondere folgende Rahmenbedingungen zu beachten:

Zuverlässigkeitsüberprüfungen nur aufgrund einer spezifischen Rechtsgrundlage
Die Gesetzgeber werden aufgefordert, bereichsspezifische Rechtsgrundlagen zu schaffen, die den Grundsatz der Verhältnismäßigkeit beachten und aus denen sich die Voraussetzungen und der Umfang der Überprüfungen klar und für die Bürgerinnen und Bürger erkennbar ergeben.

Zuverlässigkeitsüberprüfungen nur im erforderlichen Maß
Anwendung, Umfang, Kreis der betroffenen Personen und die Datenverarbeitung sind auf das Erforderliche zu beschränken. Generell dürfen Zuverlässigkeitsüberprüfungen nur bei solchen Veranstaltungen eingesetzt werden, die aufgrund ihrer spezifischen

Ausprägung infolge einer belastbaren Gefahrenprognose als besonders gefährdet bewertet werden.
Korrespondierend müssen die personenbezogenen Daten, die in den zum Abgleich herangezogenen Dateien und Informationssystemen gespeichert sind, nicht nur eine ausreichende Qualität haben, es dürfen auch nur hinreichend gewichtige Delikte in die Überprüfung einbezogen werden. Zudem müssen die Kriterien, die zur Annahme von Sicherheitsbedenken führen, einen konkreten Bezug zu den abzuwehrenden Gefahren haben.

Zuverlässigkeitsüberprüfungen nur in einem transparenten Verfahren
Die Rechte und Freiheiten der betroffenen Personen müssen durch ein transparentes Verfahren gewährleistet werden. Dazu müssen insbesondere Anhörungsrechte der betroffenen Personen rechtlich verankert werden. Im praktischen Verfahren kann im Einzelfall auch die Einrichtung einer Clearingstelle sinnvoll sein. Zudem sollten zumindest die Datenschutzbeauftragten der Verantwortlichen frühzeitig vorab beteiligt werden, damit eine datenschutzrechtliche Beratung für eine datensparsame Ausgestaltung und Beschränkung des konkreten Verfahrens stattfinden kann.

▪ Facebook-Datenskandal – Neues Europäisches Datenschutzrecht bei Sozialen Netzwerken durchsetzen!

Im März 2018 wurde in der Öffentlichkeit bekannt, dass über eine von November 2013 bis Mai 2015 mit Facebook verbundene App nach Angaben des Unternehmens Daten von 87 Millionen Nutzern weltweit, davon 2,7 Millionen Europäern und etwa 310.000 Deutschen erhoben und an das Analyseunternehmen Cambridge Analytica weitergeben wurden. Dort wurden sie offenbar auch zur Profilbildung für politische Zwecke verwendet.

Aus diesem Anlass hat der national zuständige Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ein Bußgeldverfahren gegen Facebook eingeleitet. Er steht dabei in engem Austausch mit seinen europäischen Kollegen, insbesondere mit dem Information Commissioner's Office in Großbritannien sowie der Artikel-29-Gruppe. Der Datenskandal um Facebook und Cambridge Analytica wirft ein Schlaglicht auf den Umgang mit Millionen Nutzerdaten. Zudem dokumentieren die Vorgänge um Cambridge Analytica, dass Facebook über Jahre hinweg den Entwicklern von Apps den massenhaften Zugriff auf Daten von mit den Verwendern der Apps befreundeten Facebook-Nutzenden ermöglicht hat. Das geschah ohne eine Einwilligung der Betroffenen. Tatsächlich ist der aktuell diskutierte Fall einer einzelnen App nur die Spitze des Eisbergs. So geht die Zahl der Apps, die das Facebook-Login-System nutzen, in die Zehntausende. Die Zahl der davon rechtswidrig betroffenen Personen dürfte die Dimension des Cambridge-Analytica-Falls in dramatischer Weise sprengen und dem Grunde nach alle Facebook-Nutzenden betreffen. Das Vorkommnis zeigt zudem die

Risiken für Profilbildung bei der Nutzung sozialer Medien und anschließendes Mikrotargeting, das offenbar zur Manipulation von demokratischen Willensbildungsprozessen eingesetzt wurde.

Die Datenschutzkonferenz fordert aus diesen offenbar massenhaften Verletzungen von Datenschutzrechten Betroffener folgende Konsequenzen zu ziehen:

- Soziale Netzwerke müssen ihre Geschäftsmodelle auf die neuen europäischen Datenschutzregelungen ausrichten und ihrer gesellschaftliche Verantwortung nachkommen. Dazu gehört auch, angemessene Vorkehrungen gegen Datenmissbrauch zu treffen.
- Facebook muss den wahren Umfang der Öffnung der Plattform für App-Anbieter in den Jahren bis 2015 offenlegen und belastbare Zahlen der eingestellten Apps sowie der von dem Facebook-Login-System betroffenen Personen nennen. Ferner gilt es Betroffene über die Rechtsverletzungen zu informieren.
- In Zukunft muss Facebook sicherstellen, dass die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) rechtskonform umgesetzt werden: Die Vorstellung von Facebook zur Einführung der automatischen Gesichtserkennung in Europa lässt erhebliche Zweifel aufkommen, ob das Zustimmungsverfahren mit den gesetzlichen Vorgaben insbesondere zur Einwilligung vereinbar ist. Wenn Facebook die Nutzenden dazu drängt und es ihnen wesentlich leichter macht, der biometrischen Datenverarbeitung zuzustimmen, als sich ihr zu entziehen, führt dies zu einer unzulässigen Beeinflussung des Nutzers.
- Die Reaktionen auf datenschutzwidriges Verhalten sind dabei nicht allein auf den Vollzug des Datenschutzrechts beschränkt, sondern betreffen auch das Wettbewerbs- und Kartellrecht. Die Forderung nach einer Entflechtung des Facebook-Konzerns wird in dem Maße zunehmen, wie sich dieser durch die systematische Umgehung des Datenschutzes wettbewerbswidrige Vorteile auf dem Markt digitaler Dienstleistungen zu verschaffen versucht. Es bedarf europäischer Initiativen, um monopolartige Strukturen im Bereich der sozialen Netzwerke zu begrenzen und Transparenz von Algorithmen herzustellen.

Weil Datenverarbeitungsprozesse zunehmend komplexer und für Betroffene intransparenter werden, kommt der Datenschutzaufsicht eine elementare Rolle zu. Ihre fachliche Expertise ist gefragt, sie muss organisatorisch und personell in der Lage sein, beratend und gestaltend tätig zu sein. Ein starkes Datenschutzrecht und effektive Aufsichtsbehörden vermindern gemeinsam die Risiken für die Bürgerinnen und Bürger in der digitalen Gesellschaft. Sollten Facebook und andere soziale Netzwerke nicht bereit sein, den europäischen Rechtsvorschriften zum Schutz der Nutzenden nachzukommen, muss dies konsequent durch Ausschöpfung aller vorhandenen aufsichtsbehördlichen Instrumente auf nationaler und europäischer Ebene geahndet werden.

96. Konferenz vom 7./8. November 2018

▪ Der Vorschlag der EU-Kommission für eine E-Evidence-Verordnung führt zum Verlust von Betroffenenrechten und verschärft die Problematik der sog. Vorratsdatenspeicherung

Mit ihrem Vorschlag für eine E-Evidence-Verordnung (Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM (2018) 225 final)) möchte die EU-Kommission eine Alternative zum förmlichen Rechtshilfeverfahren schaffen und den Ermittlungsbehörden einen schnelleren Zugang zu Kommunikationsdaten ermöglichen. Die Strafverfolgungsbehörden der EU-Mitgliedstaaten sollen die Befugnis erhalten, Anbieter von Telekommunikations- und Internetdienstleistungen in anderen Mitgliedstaaten der EU und auch in Staaten außerhalb der EU (Drittstaaten) unmittelbar zur Herausgabe von Bestands-, Zugangs-, Transaktions- und Inhaltsdaten zu verpflichten.

Die DSK weist hierzu auf die kritische Stellungnahme des Europäischen Datenschutzausschusses hin (https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-commission-proposals-european-production-and_de). Diese stellt bereits das Vorliegen einer Rechtsgrundlage in Frage. Mit Besorgnis sieht die DSK vor allem auch die vorgeschlagene Abkehr vom Grundsatz der doppelten bzw. beiderseitigen Strafbarkeit.

Erstmals im Bereich der internationalen Zusammenarbeit in Strafsachen soll die Herausgabe von Daten nicht mehr davon abhängig sein, ob die verfolgte Tat dort, wo die Daten ersucht werden, überhaupt strafbar ist. Im Ergebnis könnten Unternehmen mit Sitz in Deutschland also zur Herausgabe von Daten an Ermittlungsbehörden in anderen EU-Mitgliedstaaten verpflichtet werden, obwohl die verfolgte Tat in Deutschland überhaupt keine Straftat ist. Das könnte zum Beispiel ein in Deutschland erlaubter Schwangerschaftsabbruch sein oder eine politische Meinungsäußerung, wenn diese im ersuchenden Staat strafbewehrt ist.

Zu befürchten ist hierbei auch, dass Drittstaaten die Regelung der EU als Blaupause für eigene Regelungen heranziehen werden. Provider in EU-Mitgliedstaaten würden sich dann vermehrt Herausgabeanordnungen von Drittstaaten ausgesetzt sehen, mit denen möglicherweise Straftaten aus einer völlig anderen Rechtstradition verfolgt werden.

Kritisch sieht die DSK auch, dass im Regelfall jegliche Information und Beteiligung der Justizbehörden des Staates, in dem der Provider seinen Sitz hat, unterbleibt und damit ein wichtiges verfahrensrechtliches Korrektiv fehlt. Ob die Rechtmäßigkeit eines Ersuchens überprüft wird, hängt im vorgeschlagenen Verfahren ausschließlich vom Verhalten der Provider ab. Nur wenn sich das Unternehmen weigert, Daten zu übermitteln,

muss der ersuchende Staat bei den Behörden vor Ort um Vollstreckungshilfe bitten. Nur dann können diese noch in das Verfahren eingreifen. Werden Daten herausgegeben, erlangen die zuständigen Justizbehörden hiervon jedoch keine Kenntnis. Der Vorschlag sieht keine Informationspflicht gegenüber den Behörden am Sitz des Unternehmens vor. Provider verfolgen aber in der Regel wirtschaftliche Interessen und unterliegen in ihren Entscheidungen anderen Verpflichtungen als die Justizbehörden Hierdurch werden Betroffene deutlich schlechter gestellt.

Provider als Adressaten eines Ersuchens sehen sich künftig nicht mehr den Justizbehörden des eigenen Staates gegenüber, sondern müssen sich mit den Behörden des anordnenden Staates auseinandersetzen. Den Betroffenen wiederum steht, wenn überhaupt, nur ein Rechtsbehelf im ersuchenden Mitgliedsstaat zu, dessen Rechtsordnung ihnen in der Regel aber fremd ist.

Ein besonderes Verfahren ist vorgesehen, wenn sich Provider mit Sitz in Drittstaaten darauf berufen, dass die angeordnete Übermittlung gegen das dortige Recht verstößt. Für diesen Fall sieht der Vorschlag eine gerichtliche Überprüfung im anordnenden Staat vor. Wenn das Gericht zu der Auffassung gelangt, dass tatsächlich ein Rechtskonflikt vorliegt, muss es die zuständigen Behörden im Zielstaat der Anordnung beteiligen. Das Ergebnis der Konsultation ist für das Gericht verbindlich. Diese Regelung ist ausdrücklich zu begrüßen. Denn auch hier wird eine Blaupause geschaffen für die Frage, welche Rechte europäische Unternehmen in der umgekehrten Situation haben sollten, wenn sie aus Drittstaaten auf der Grundlage von deren Gesetzen (wie z.B. US-Cloud-Act) zu einer Übermittlung verpflichtet werden und welche Verbindlichkeit eine Konsultation der zuständigen Behörden in Europa für Gerichte in Drittstaaten haben sollte.

Besonders kritisch ist jedoch, dass in Deutschland Telekommunikationsdienstleister verpflichtet sind, u.a. sämtliche Verkehrsdaten für zehn Wochen zu speichern. Aus diesen Daten lassen sich genaue Schlüsse auf das Privatleben der Betroffenen, insbesondere deren Kontakt- und Interessenprofil ziehen. Die Problematik dieser sog. Vorratsdatenspeicherung verschärft sich deutlich, wenn ausländische Strafverfolgungsbehörden einen direkten Zugriff auf derartige Informationen erhalten.

Die DSK appelliert daher an alle im Gesetzgebungsverfahren Beteiligten, den Vorschlag für eine E-Evidence-Verordnung zu stoppen!

Entschließungen zwischen den Konferenzen 2017/2018

▪ 24. Januar 2017 – Novellierung des Personalausweisgesetzes – Änderungen müssen bürger- und datenschutzfreundlich realisiert werden!

Die Bundesregierung plant grundlegende Änderungen des Personalausweisrechts. Nach dem vom Bundeskabinett beschlossenen Gesetzentwurf (BR-Drs. 787/16) werden das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger übergangen und Datenschutz sichernde Standards unterlaufen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher insbesondere folgende datenschutzrechtliche Anforderungen zu berücksichtigen:

- Die obligatorische Aktivierung der eID-Funktion ist dann hinnehmbar, wenn dauerhaft sichergestellt ist, dass daraus keine verpflichtende Nutzung der eID-Funktion des Personalausweises resultiert. Die Entscheidung über die Nutzung der eID-Funktion muss allein bei den Bürgerinnen und Bürgern liegen. Deren Selbstbestimmungsrecht muss gewahrt bleiben.
- An der bisherigen Verpflichtung der Ausweisbehörden, Bürgerinnen und Bürger über die eID-Funktion des Personalausweises schriftlich zu unterrichten, sollte festgehalten werden. Nur durch eine bundesweit einheitliche Vorgabe zu einer solchen Information wird sichergestellt, dass alle Bürgerinnen und Bürger in hinreichend verständlicher Form aufgeklärt werden.
- Vor einer Datenübermittlung aus dem Personalausweis müssen die Bürgerinnen und Bürger Kenntnis über den Zweck der Übermittlung erhalten; zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung müssen die Betroffenen stets – wie bislang – nachvollziehen können, in welchem konkreten Kontext ihre Identitätsdaten übermittelt werden. Zudem sollte die bisherige Möglichkeit, die Übermittlung einzelner Datenkategorien auszuschließen, beibehalten werden.
- Die Einführung von organisationsbezogenen Berechtigungszertifikaten bei Diensteanbietern wird abgelehnt. Um sicherzustellen, dass Diensteanbieter nur die für den jeweiligen Geschäftsprozess erforderlichen Angaben übermittelt bekommen, sollte an der aktuellen Rechtslage festgehalten werden, nach der der antragstellende Diensteanbieter die Erforderlichkeit der aus der eID-Funktion des Personalausweises zu übermittelnden Angaben nachweisen muss und an den jeweils festgelegten Zweck gebunden ist.
- Berechtigungszertifikate dürfen nur an Diensteanbieter erteilt werden, die Datenschutz und Datensicherheit gewährleisten. Daher sollten antragstellende Diensteanbieter nach wie vor durch eine Selbstverpflichtung die Erfüllung dieser Anforderungen schriftlich bestätigen und nachweisen müssen.
- Die maßgeblichen Regelungen für die mit der Anlegung und Nutzung von Servicekonten einhergehende Erhebung und Verarbeitung von Identitätsdaten aus dem

Personalausweis sowie die sicherheitstechnischen Rahmenbedingungen sollten im Personalausweisgesetz getroffen werden.

- Die Voraussetzungen für die Erstellung und Weitergabe von Personalausweisablichtungen sollten gesetzlich konkreter normiert werden. Insbesondere das Prinzip der Erforderlichkeit ist durch eine verpflichtende Prüfung der Notwendigkeit der Anfertigung einer Ablichtung sowie durch eine Postitivliste von Erlaubnisgründen zu stärken. Die Einwilligung der Betroffenen als alleinige Voraussetzung birgt die Gefahr, dass in der Praxis Ablichtungen angefertigt werden, obwohl sie nicht erforderlich sind. Zudem dürfte fraglich sein, ob betroffene Personen in eine solche Maßnahme stets informiert und freiwillig einwilligen können.
- Die zum 1. Mai 2021 vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste wird abgelehnt. Bisher dürfen zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten insbesondere die Polizei- und Ordnungsbehörden Lichtbilder automatisiert abrufen, wenn die Personalausweisbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährdet. Diese gesetzlichen Einschränkungen für das Abrufverfahren sollen nun entfallen. Zudem sollen alle Nachrichtendienste künftig voraussetzungslos Lichtbilddaten abrufen können. Die bisherige Rechtslage ist völlig ausreichend.

- 15. März 2017 – Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtssicher und datenschutzkonform gestalten!

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesgesetzgeber auf, mit dem derzeit vorliegenden Gesetzentwurf der Bundesregierung „zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ (BR-Drs. 163/17) den Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtsicher und datenschutzkonform zu gestalten.

Die Schweigepflicht ist Grundlage des für die Berufsausübung notwendigen Vertrauensverhältnisses. Aber auch Berufsgeheimnisträger können heute nicht mehr wirtschaftlich agieren, ohne die moderne Informations- und Kommunikationstechnik zu nutzen. Kaum ein Anwalt oder Arzt verfügt über das notwendige Spezialwissen, um diese Technik selbst zu warten und vor ständig neuen Bedrohungen abzusichern. Der vorliegende Gesetzentwurf will deshalb eine Praxis legalisieren, die aus Gründen der Praktikabilität längst etabliert ist. Der strafrechtliche Schutz von Privatgeheimnissen soll die Beauftragung externer Dienstleister durch Berufsgeheimnisträger nicht länger erschweren. Im Gegenzug sollen diese Auftragnehmer künftig einer strafrechtlich sanktionierten Verschwiegenheitspflicht unterliegen. Dennoch versäumt es der Gesetzent-

wurf, insbesondere mit der vorgeschlagenen Formulierung zu § 203 StGB, klare Verhältnisse zu schaffen. Bisher sorgte unter Ärzten – und mitunter sogar Anwälten – der Umstand für Verwirrung, dass das, was datenschutzrechtlich legitim war, noch längst nicht strafrechtlich erlaubt sein musste. Was nach dem Gesetzentwurf nunmehr strafrechtlich erlaubt sein soll, könnte wiederum nach der neuen Europäischen Datenschutz-Grundverordnung mit empfindlichen Bußgeldern in Millionenhöhe sanktioniert werden. Denn es ist weder mit dem Schutzzweck von § 203 StGB vereinbar, noch datenschutzrechtlich zulässig, dass Berufsgeheimnisträger, wie im neuen § 203 StGB vorgesehen, die Verantwortung für die Datenverarbeitung ohne Einwilligung der Betroffenen an externe Dienstleister übertragen. Nicht absehbar ist zudem, ob die Zeugnisverweigerungsrechte und das Beschlagnahmeverbot in einem weiteren Gesetzgebungsverfahren entsprechend weitgehend auf alle denkbaren Dienstleister ausgeweitet werden, die an der Berufsausübung durch Berufsgeheimnisträger mitwirken.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder dringt daher darauf, den Gesetzentwurf nachzubessern und die geplanten straf- und berufsrechtlichen Regelungen mit den datenschutzrechtlichen Vorschriften zu synchronisieren. Es muss Berufsgeheimnisträgern möglich sein, externe Dienstleister zu Rate zu ziehen. Im Sinne der ungestörten Berufsausübung der Berufsgeheimnisträger und des Rechts auf informationelle Selbstbestimmung der Betroffenen sollten die Pflichten, die den Berufsgeheimnisträger dabei aus unterschiedlichen Rechtsgebieten treffen, aber soweit als möglich gleichlaufend ausgestaltet werden.

▪ 16. März 2017 – Gesetzesentwurf zur Aufzeichnung von Fahrdaten ist völlig unzureichend!

Die Bundesregierung hat im Januar 2017 einen Entwurf zur Novellierung des Straßenverkehrsgesetzes (BT Drs. 18/11300) vorgelegt, um die Nutzung automatisierter Fahrfunktionen auf Deutschlands Straßen zu erlauben. Dabei sollen Fahrdaten aufgezeichnet werden, anhand derer bewertet werden kann, zu welchem Zeitpunkt das Auto jeweils durch den Fahrer oder durch eine „automatisierte Fahrfunktion“ gesteuert wurde und wann ein Fahrer die Aufforderung zur Übernahme der Steuerung erhalten hat. Ebenfalls aufgezeichnet werden sollen Daten zu technischen Störungen automatisierter Fahrfunktionen. Mit den Daten soll sich nach einem Unfall klären lassen, ob die Technik und damit der Hersteller oder der Fahrer für einen Unfall verantwortlich war. Welche Daten dies sind und wie das Speichermedium ausgestaltet werden soll, regelt der Gesetzentwurf nicht.

Auf Verlangen der nach Landesrecht für Verkehrskontrollen zuständigen Behörden müssen die Fahrdaten diesen Behörden übermittelt werden. Die Fahrdaten sind auch Dritten zu übermitteln, wenn diese glaubhaft machen können, dass sie die Fahrdaten zur Geltendmachung, Abwehr oder Befriedigung von Rechtsansprüchen aus Unfällen

benötigen. Unklar ist, wer die Daten übermitteln muss. Es bleibt ebenfalls unbestimmt, ob ggf. auch die Behörden Fahrdaten übermitteln dürfen.

Im Gesetzesentwurf sind außerdem weder die Zwecke noch die zu übermittelnden Daten hinreichend konkretisiert. Weiterhin geht nicht hervor, wie die Integrität, Vertraulichkeit und Verfügbarkeit bei der Aufzeichnung und Übermittlung der Fahrdaten sichergestellt werden soll.

Sollte der Entwurf in der vorgelegten Form in Kraft treten, besteht in Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion die Gefahr elektronischer Fahrtenschreiber, die personenbezogene Profile bilden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Gesetzgeber zu einer dem datenschutzrechtlichen Bestimmtheitsgebot genügenden Novellierung des Straßenverkehrsgesetzes und zur Stärkung der Datenschutzrechte der Fahrer auf.

Sofern man eine Datenverarbeitung überhaupt für erforderlich hält, ist folgendes zu regeln:

- die abschließende Aufzählung derjenigen Daten, die aufgezeichnet und gespeichert werden dürfen,
- die Bestimmung des für die Verarbeitung Verantwortlichen,
- die Ergänzung einer Übermittlungs-/Zugriffsregelung für den Fahrer/Halter,
- die Konkretisierung der Daten, die den nach Landesrecht zuständigen Behörden zu übermitteln sind,
- die datenschutzgerechte Ausgestaltung des Speichermediums, insbesondere die Festlegung einer angemessenen Speicherdauer anhand der Erforderlichkeit und des Zwecks der Beweisführung für die Haftung,
- eindeutige Festlegungen für die Trennung der Daten von den in den Fahrzeugdatenspeichern der Fahrzeuge gespeicherten Daten,
- die Konkretisierung der Zwecke für die Übermittlung der gespeicherten Daten,
- die Nennung des Adressaten für das Übermittlungsverlangen,
- die abschließende Nennung berechtigter Übermittlungsempfänger und ihrer jeweiligen Verarbeitungsbefugnisse mit im Übrigen strikter Zweckbindung und
- die Konkretisierung des Löschzeitpunkts der übermittelten Daten.

▪ 16. März 2017 – Neues Bundeskriminalamtgesetz – Informationspool beschneidet Grundrechte

Der „Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes“ (BT-Drs. 18/11326 und 18/11163; BR-Drs. 109/17) ändert das polizeiliche Daten-

schutzrecht grundlegend und betrifft Polizeibehörden in Bund und Ländern gleichermaßen. Er beschränkt sich nicht darauf, die Vorgaben des Bundesverfassungsgerichts aus dem Urteil vom 20. April 2016 zum Bundeskriminalamtgesetz und aus der neuen EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres umzusetzen. Tatsächlich nimmt er sogar wichtige Datenschutzregeln und Verfahrenssicherungen zurück, die der Gesetzgeber nach dem Volkszählungsurteil des Bundesverfassungsgerichts geschaffen hatte.

Der Entwurf ändert den bisherigen Informationsverbund für alle Polizeibehörden grundlegend. Dieser ist nicht mehr nach Dateien untergliedert und führt zu unverhältnismäßig weitreichenden Speicherungen. In dieser Form ist dies weder durch das Urteil des Bundesverfassungsgerichts zum BKAG noch durch die EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres veranlasst. Das Urteil des Bundesverfassungsgerichts fordert, den Zweck der jeweiligen Ermittlungsmaßnahmen bei allen weiteren Schritten zu berück-sichtigen, bei denen die ermittelten Daten verwendet werden. Nicht im Einklang damit steht es, Verfahrenssicherungen und datenschutzrechtliche Rahmenbedingungen aufzugeben.

Abzulehnen ist insbesondere der vorgesehene Verzicht auf Errichtungsanordnungen. Diese sind bislang Ausgangspunkt sowohl für datenschutzrechtliche Kontrollen als auch die Selbstkontrolle der Polizeibehörden. In ihnen wird festgelegt, zu welchen Zwecken personenbezogene Daten gespeichert sind. Dies ist eine wesentliche verfassungsrechtliche Vorgabe. Die neuen Regeln führen zu umfassenden themenübergreifenden Verknüpfungen und Abgleichen aller gespeicherten Personen. Sie verkürzen die Kontrollmöglichkeiten der Datenschutzaufsichtsbehörden von Bund und Ländern.

Ebenso sind die künftig durch die geplante „Mitziehautomatik“ erheblich längeren Speicherfristen abzulehnen. Die geplante Neuregelung hat zur Folge, dass alte Speicherungen – auch zu Personen, die lediglich im Verdacht standen, eine Straftat begangen zu haben und die nicht verurteilt wurden – bei jedem neuen Speicheranlass ungeprüft weiter fortgeschrieben werden. Dafür soll es schon genügen, wenn die betroffene Person als Zeuge oder Kontaktperson erneut in Erscheinung tritt. Auch dies verstößt gegen das durch die ständige Rechtsprechung des Bundesverfassungsgerichtes bekräftigte Übermaßverbot.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert daher, den Gesetzentwurf in der parlamentarischen Beratung datenschutzkonform zu überarbeiten!

▪ 6. Juni 2018 – Die Zeit der Verantwortungslosigkeit ist vorbei: EuGH bestätigt gemeinsame Verantwortung von Facebook und Fanpage-Betreibern

Die unabhängigen Datenschutzbehörden des Bundes und der Länder begrüßen das Urteil des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018, das ihre langjährige Rechtsauffassung bestätigt.

Das Urteil des EuGH zur gemeinsamen Verantwortung von Facebook und den Betreibern einer Fanpage hat unmittelbare Auswirkungen auf die Seitenbetreiber. Diese können nicht mehr allein auf die datenschutzrechtliche Verantwortung von Facebook verweisen, sondern sind selbst mitverantwortlich für die Einhaltung des Datenschutzes gegenüber den Nutzenden ihrer Fanpage.

Dabei müssen sie die Verpflichtungen aus den aktuell geltenden Regelungen der Datenschutz-Grundverordnung (DS-GVO) beachten. Zwar nimmt das Urteil Bezug auf die frühere Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr, doch die vom EuGH festgestellte Mitverantwortung der Seitenbetreiber erstreckt sich auf das jeweils geltende Recht, insbesondere auf die in der DS-GVO festgeschriebenen Rechte der Betroffenen und Pflichten der Verarbeiter.

Im Einzelnen ist Folgendes zu beachten:

- Wer eine Fanpage besucht, muss transparent und in verständlicher Form darüber informiert werden, welche Daten zu welchen Zwecken durch Facebook und die Fanpage-Betreiber verarbeitet werden. Dies gilt sowohl für Personen, die bei Facebook registriert sind, als auch für nicht registrierte Besucherinnen und Besucher des Netzwerks.
- Betreiber von Fanpages sollten sich selbst versichern, dass Facebook ihnen die Informationen zur Verfügung stellt, die zur Erfüllung der genannten Informationspflichten benötigt werden.
- Soweit Facebook Besucherinnen und Besucher einer Fanpage durch Erhebung personenbezogener Daten trackt, sei es durch den Einsatz von Cookies oder vergleichbarer Techniken oder durch die Speicherung der IP-Adresse, ist grundsätzlich eine Einwilligung der Nutzenden erforderlich, die die Anforderung der DS-GVO erfüllt.
- Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage-Betreibern ist in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtung der DS-GVO erfüllt. Diese Vereinbarung muss in wesentlichen Punkten den Betroffenen zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen können.

Für die Durchsetzung der Datenschutzvorgaben bei einer Fanpage ist die Aufsichtsbehörde zuständig, die für das jeweilige Unternehmen oder die Behörde zuständig ist, die die Fanpage betreibt. Die Durchsetzung der Datenschutzvorgaben im Verantwortungsbereich von Facebook selbst obliegt primär der irischen Datenschutzaufsicht im Rahmen der europäischen Zusammenarbeit.

Die deutschen Aufsichtsbehörden weisen darauf hin, dass nach dem Urteil des EuGH dringender Handlungsbedarf für die Betreiber von Fanpages besteht. Dabei ist nicht zu verkennen, dass die Fanpage-Betreiber ihre datenschutzrechtlichen Verantwortung nur erfüllen können, wenn Facebook selbst an der Lösung mitwirkt und ein datenschutzkonformes Produkt anbietet, das die Rechte der Betroffenen wahrt und einen ordnungsgemäßen Betrieb in Europa ermöglicht.

Beschlüsse der Datenschutzkonferenz

▪ 23. März 2018 – Übermittlung von E-Mail-Adressen durch Onlineversandhändler an Postdienstleister

Die Übermittlung von E-Mail-Adressen durch Onlinehändler an Postdienstleister ist nur bei Vorliegen einer Einwilligung der Kunden in eben diese Übermittlung rechtmäßig. Die Praxis hat gezeigt, dass es vielen Onlinehändlern möglich ist, die Zustellinformationen selbst an den Kunden weiterzugeben bzw. einen Link zur Sendungsverfolgung in die eigene Bestellbestätigung einzubinden. Dies stellt jedenfalls eine objektiv zumutbare Alternative dar. Aus dem gleichen Grund wird auch die Erforderlichkeit im Rahmen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG bzw. Art. 6 Abs. 1 Satz 1 lit. f DS-GVO verneint.

▪ 23. März 2018 – Mahnung durch Computeranruf

Eine telefonische Mahnung durch Computeranruf ist wegen der hohen Gefahr, dass eine andere als die betroffene Person die Nachricht erhält und so personenbezogene Daten unbefugt offenbart werden, unzulässig.

▪ 23. März 2018 – Kontaktloses Bezahlen

Kontaktloses Bezahlen ist derzeit in vielen Varianten möglich. Der zugrunde liegende Übertragungsstandard Near Field Communication (NFC) wird für Geld- und Kreditkarten sowie für mobiles Bezahlen z.B. mit dem Smartphone genutzt. Die Datenschutzaufsichtsbehörden begleiten die Entwicklung aus datenschutzrechtlicher und –technischer Sicht. So wurde bereits im Beschluss des Düsseldorfer Kreises vom 19. September 2012 zu „Near Field Communication (NFC) bei Geldkarten“ auf die datenschutzrechtlichen Grundanforderungen hingewiesen. Mittlerweile sind die Verantwortlichen vielen dieser Forderungen nachgekommen bzw. mit deren Umsetzung befasst.

Die grundsätzlichen Forderungen bezüglich kontaktloser Bezahlverfahren lassen sich wie folgt zusammenfassen:

Die Notwendigkeit einer Datenschutz-Folgenabschätzung ist nach Artikel 35 DS-GVO zu prüfen.

Die Karten ausgebenden Institute sind verpflichtet, umfassende und verständliche Informationen für Nutzerinnen und Nutzer über Datenhaltung und -verarbeitung bereitzustellen. Bei Bezahlverfahren, die ein Smartphone voraussetzen, ist weiterhin über

die damit einhergehenden besonderen Risiken zu informieren. Zudem sind Hinweise zur Risikominimierung zu geben.

Die Kundinnen und Kunden sind darüber zu unterrichten, dass eine kostenlose Schutzhülle in der Standardversion zur Verfügung steht.

Es muss sichergestellt sein, dass durch Voreinstellung die NFC-Funktion zunächst deaktiviert ist. Den Kundinnen und Kunden muss ermöglicht werden, die NFC-Funktion jederzeit abschalten zu können. Alternativ können auch Karten ohne NFC-Funktion angeboten werden, ohne dass für Kundinnen und Kunden Mehrkosten entstehen.

Um das unberechtigte Auslesen etwaiger personenbeziehbarer Daten zu verhindern, ist die drahtlose Kommunikation zwischen (virtueller) Karte und Terminal zu verschlüsseln. Die (Kredit-)Wirtschaft wird aufgefordert, die zurzeit laufenden Arbeiten an einer internationalen Spezifikation der Verschlüsselung weiterhin zu forcieren. Auch bleiben weitere Maßnahmen zur technisch-organisatorischen Absicherung von NFC-basierten Konzepten – wie z.B. die Randomisierung der Kartennummer – fortgesetzt aktuell.

Es sollte grundsätzlich keine Möglichkeit des kontaktlosen Auslesens einer wiederkehrenden Kennziffer (z.B. Kartennummer) möglich sein, die unter Umständen zu Zwecken der Profilbildung herangezogen werden kann.

Bei Bezahlverfahren, die ein Smartphone voraussetzen, ist die Bezahl-App von den ausgebenden Kreditinstituten aktuell zu halten. Die Kundinnen und Kunden sind dazu anzuhalten, nur die aktuellen Software- und Betriebssystemversionen einzusetzen. Bei nicht aktualisierten Software- und Betriebssystemversionen ist mindestens kontinuierlich und unübersehbar darauf hinzuweisen, wenn die Anwendungen zu Sicherheitsrisiken führen.

Die Karten ausgebenden Institute werden darauf hingewiesen, dass etwaige auf der Karte vorhandene Drittanwendungen, die geeignet sind, das Pseudonymisierungskonzept des Bezahlsystems zu unterlaufen, eine neue datenschutzrechtliche Bewertung erforderlich machen. Zudem sind die Drittanbieter darauf hinzuweisen, dass und wie eine mögliche Depseudonymisierung infolge unsachgemäßer Belegung von Datenfeldern zu vermeiden ist.

▪ 23. März 2018 – Einmeldung offener und unbestrittener Forderungen in eine Wirtschaftsauskunftei unter Geltung der DS-GVO

Die Zulässigkeit einer Einmeldung beurteilt sich künftig nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO.

Hierzu ist es notwendig, dass die Einmeldung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Zudem dürfen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen. Das bedeutet, dass eine Abwägung unter Berücksichtigung dieser Kriterien im Einzelfall vorzunehmen ist.

Im Rahmen dieser Einzelfallprüfung entfalten die nachfolgenden Fallgruppen eine Indizwirkung für eine zulässige Einmeldung:

1. Die Forderung ist durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden oder es liegt ein Schuldtitel nach § 794 der Zivilprozessordnung vor.
2. Die Forderung ist nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden.
3. Der Betroffene hat die Forderung ausdrücklich anerkannt.
4. Der Betroffene ist nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden, die erste Mahnung liegt mindestens vier Wochen zurück, der Betroffene ist zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden und der Betroffene hat die Forderung nicht bestritten.
5. Das der Forderung zugrunde liegende Vertragsverhältnis kann aufgrund von Zahlungsrückständen fristlos gekündigt werden und der Betroffene ist zuvor über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden.

Zusätzliche Anhaltspunkte oder Hinweise können ggf. zu einer anderen Abwägung führen. Darüber hinaus muss eine Kompatibilitätsprüfung nach Art. 6 Abs. 4 DS-GVO erfolgen, weil die personenbezogenen Daten zunächst für einen anderen Zweck –zur Durchführung eines Rechtsgeschäfts und nicht zur Einmeldung bei einer Auskunftei – verarbeitet wurden. Der Betroffene muss also zuvor durch die Auskunftei-Vertragspartner über die Möglichkeit der Einmeldung unterrichtet worden sein, denn es darf nur das eingemeldet werden, womit der Betroffene vernünftigerweise rechnen muss (Erwägungsgrund 47 der DS-GVO).

▪ 23. März 2018 – Keine fortlaufenden Bonitätsauskünfte an den Versandhandel

Auskunfteien dürfen Bonitätsauskünfte gemäß Art. 6 Abs. 1 S. 1 lit. f DSGVO grundsätzlich nur erteilen, wenn es zur Wahrung eines berechtigten Interesses eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Besteht zwischen diesem Dritten (also dem anfragenden Unternehmen) und dem Betroffenen ein Dauerschuldverhältnis, aufgrund dessen das anfragende Unternehmen während der gesamten Dauer des Bestehens ein finanzielles Ausfallrisiko trägt (z.B. Ratenzahlungskredit, Girokonto, Energielieferungs-, Telekommunikationsvertrag), so dürfen Bonitätsauskünfte nicht nur zu dem Zeitpunkt erteilt werden, zu dem der Betroffene ein solches Vertragsverhältnis beantragt hat, sondern während der gesamten Laufzeit des Vertragsverhältnisses und bis zur Erfüllung sämtlicher Pflichten des Betroffenen. Bei jeder dieser weiteren Auskünfte sind jedoch im Einzelfall die Voraussetzungen des Art. 6 Abs. 1 S. 1 lit. f DS-GVO strikt zu beachten.

Das heißt vor jeder Übermittlung sind die konkreten berechtigten Interessen des Dritten gegen die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person abzuwägen.

Ein Versandhandelsgeschäft stellt als solches kein Dauerschuldverhältnis dar. Die aufgrund der bisherigen Erfahrungen mit den Kunden möglicherweise bestehende Wahrscheinlichkeit und darauf gegründete Erwartung, dass der Kunde nach der ersten Bestellung wiederholt bestellen wird, und die zur Erleichterung der Bestellvorgänge möglicherweise erfolgte Einrichtung eines „Kundenkontos“ rechtfertigten es nicht, ein Versandhandelsgeschäft mit einem Dauerschuldverhältnis gleichzusetzen.

Ein berechtigtes Interesse seitens des Versandhandels gem. Art. 6 Abs. 1 S. 1 lit. f DS-GVO ist demnach nur gegeben, wenn aufgrund eines konkreten Bestellvorgangs ein finanzielles Ausfallrisiko vorliegt.

Nach Vertragsschluss sind Bonitätsauskünfte an Versandhändler dann nicht zu beanstanden, wenn ein Ratenzahlungskredit vereinbart wurde oder noch ein offener Saldo besteht. In allen anderen Fällen ist das Rechtsgeschäft nach Abwicklung des einzelnen Kaufgeschäftes für den Versandhandel abgeschlossen, ein berechtigtes Interesse an Bonitätsauskünften ist dann nicht mehr zu belegen. Damit sind Nachmeldungen oder sonstige Beauskunftungen in dieser Konstellation rechtlich unzulässig.

▪ 23. März 2018 – Aufzeichnung von Telefongesprächen

Die Aufzeichnung von Telefongesprächen ist datenschutzrechtlich in aller Regel nur mit Einwilligung auch des externen Gesprächspartners zulässig. Eine datenschutzrechtlich wirksame Einwilligung im Sinne von Art. 4 Nr. 11 DS-GVO setzt voraus, dass der externe Gesprächspartner vor Beginn der beabsichtigten Aufzeichnung gefragt wird, ob er mit der Aufzeichnung einverstanden ist, und falls er einverstanden ist, gebeten wird, sein Einverständnis beispielsweise durch Aussprechen eines „Ja“ oder durch eine aktive bestätigende Handlung (etwa durch das Betätigen einer Telefontaste) ein-

deutig zum Ausdruck zu bringen. Diese Einwilligung umfasst nicht eine biometrische Auswertung.

Die bloße Einräumung einer Widerspruchsmöglichkeit und das anschließende Fortsetzen des Telefonats stellen keine datenschutzrechtlich wirksame Einwilligung im Sinne der DS-GVO dar. Da der datenschutzrechtlich Verantwortliche nachweisen können muss, dass die betroffene Person eine wirksame Einwilligung erteilt hat (Art. 7 Abs. 1 DS-GVO), muss er auch nachweisen können, dass die betroffene Person die Einwilligung „in informierter Weise“ abgegeben hat (vgl. Art. 4 Nr. 11 DS-GVO). Die Aufzeichnung betrifft regelmäßig auch Beschäftigte. Insoweit gelten besondere Anforderungen. Sie sind nicht Gegenstand dieses Beschlusses.

▪ 26. April 2018 – Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Abs. 1 lit. C Datenschutz-Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs

1. Betreibt ein einzelner Arzt, Apotheker oder sonstiger Angehöriger eines Gesundheitsberufs eine Praxis, Apotheke oder ein Gesundheitsberufsunternehmen und sind dort einschließlich seiner Person in der Regel mindestens 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt, besteht eine gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten (DSB).

2. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, ist in der Regel nicht von einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne von Art. 37 Abs. 1 lit. c DS-GVO auszugehen – in diesen Fällen ist unter Berücksichtigung von Punkt 3 dann kein DSB zu benennen, wenn weniger als 10 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind.

3. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, bei denen ein hohes Risiko für die Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten zu erwarten ist, ist eine Datenschutzfolgenabschätzung vorgeschrieben und damit zwingend ein Datenschutzbeauftragter zu benennen. Dies kann neben einer umfangreichen Verarbeitung (z.B. große Pra-

xisgemeinschaften), die ohnehin nach Art. 37 Abs. 1 lit. c DS-GVO zu einer Benennungspflicht führt, beispielsweise beim Einsatz von neuen Technologien, die ein hohes Risiko mit sich bringen, der Fall sein. Der Datenschutzbeauftragte ist damit auch dann zu benennen, wenn weniger als 10 Personen ständig mit der Verarbeitung personenbezogener Daten zu tun haben.

4. Der Begriff „Gesundheitsberuf“ ist im Sinne der Aufzählung nach § 203 Abs. 1 StGB auszulegen und umfasst die in § 203 Abs. 1 Nr. 1, 2, 4 und 5 StGB aufgezählten Berufsbilder.

▪ 11. Juni 2018 – Verarbeitung von Positivdaten zu Privatpersonen durch Auskunfteien

Handels- und Wirtschaftsauskunfteien können sog. Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage des Art. 6 Abs. 1 lit. f DS-GVO erheben. Denn bei Positivdaten – das sind Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben – überwiegt regelmäßig das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung ihrer Daten zu bestimmen. Werden die Daten von einem Verantwortlichen an eine Auskunftei übermittelt, ist insoweit bereits die Übermittlung dieser Daten nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO regelmäßig unzulässig.

Will eine Auskunftei Positivdaten zu Privatpersonen erheben, bedarf es dafür im Regelfall einer wirksamen Einwilligung der betroffenen Personen im Sinne des Art. 7 DS-GVO. Auf die hohen Anforderungen an die Freiwilligkeit nach Art. 7 Abs. 4 DS-GVO wird hingewiesen. Sofern die Auskunftei oder ihre Vertragspartner zu diesem Zweck eine für eine Vielzahl von Fällen vorformulierte Einwilligungsklausel verwenden, die als Allgemeine Geschäftsbedingung im Sinne des § 305 BGB zu werten ist, muss eine entsprechende Einwilligung darüber hinaus den Anforderungen des § 307 BGB genügen.

Besonderheiten für Kreditinstitute:

Es wird für zulässig angesehen, wenn Kreditinstitute aufgrund von Art. 6 Abs. 1 S. 1 lit. f DSGVO – wie bisher durch § 28 a Abs. 2 BDSG gesetzlich erlaubt – personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung von Kredit- und Giroverträgen sowie Garantiegeschäften (insbesondere Bürgschaften) an Auskunfteien übermitteln, es sei denn, dass im Einzelfall das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Übermittlung gegenüber den Interessen der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt.

Diese Besonderheit für Kreditinstitute begründet sich mit den speziellen Bonitätsprüfungsverpflichtungen der Kreditinstitute nach dem Kreditwesengesetz sowie gesamtgesellschaftlichen Gesichtspunkten des Schutzes der betroffenen Personen vor Überschuldung. Die betroffene Person ist vor Abschluss des Vertrages über die damit verbundene Datenübermittlung an Auskunfteien zu unterrichten.

Dies gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben.

Ebenso ist die Übermittlung von Daten zu allgemeinen Konditionenanfragen, die der Herstellung von Markttransparenz dienen, an Auskunfteien unzulässig; hierzu kann auch keine rechtswirksame Einwilligung der betroffenen Person eingeholt werden.

Die Übermittlung von Daten an Auskunfteien für Bonitätsabfragen ist nach Art. 6 Abs. 1 S. 1 lit. b DS-GVO zulässig, wenn dies zur Durchführung eines Beratungsvertrages oder einer vorvertraglichen Maßnahme, die auf Anfrage der betroffenen Person erfolgt, erforderlich ist mit dem Ziel, Konditionen, die auf eine bestimmte Person zugeschnittenen werden, zu überprüfen.

Nachträgliche Änderungen von Tatsachen hat das Kreditinstitut gemäß Art. 19 DS-GVO der Auskunftei unverzüglich nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. Die Auskunftei hat das betreffende Kreditinstitut über die Löschung der ursprünglich übermittelten Daten zu unterrichten.

Zur Einmeldung von Dauerschuldverhältnissen außerhalb des KWG werden im AK Auskunfteien noch weitere Abstimmungen erfolgen.

▪ 5. September 2018 – Ablehnung der Behandlung durch Ärztinnen und Ärzte bei Weigerung der Patientin oder des Patienten, die Kenntnisnahme der Informationen nach Art. 13 DSGVO durch Unterschrift zu bestätigen

Die Datenschutzaufsichtsbehörden des Bundes und der Länder sprechen sich dagegen aus, dass Ärztinnen und Ärzte oder andere Angehörige von Gesundheitsberufen die Behandlung ablehnen oder die Verweigerung der Behandlung androhen, wenn die Patientin oder der Patient die Informationen nach Art. 13 DSGVO nicht mit ihrer oder seiner Unterschrift versieht. Eine solche Praxis ist nicht mit der DSGVO vereinbar.

Die Informationspflicht nach Art. 13 DSGVO bezweckt lediglich, dass der Patientin bzw. dem Patienten die Gelegenheit gegeben wird, die entsprechenden Informationen

einfach und ohne Umwege zu erhalten. Sie oder er muss diese jedoch nicht zur Kenntnis nehmen, wenn sie oder er dies nicht möchte.

Um seinen Nachweispflichten gegenüber der Aufsichtsbehörde nachzukommen, kann der Verantwortliche das Aushändigen der Information vermerken oder einen konkreten Verfahrensablauf betreffend die Umsetzung der Informationspflicht dokumentieren, aus dem hervorgeht, wie die Patientin oder der Patient die Informationen im Regelfall erhält.

▪ 5. September 2018 – Beschluss der DSK zu Facebook Fanpages

Mit Urteil vom 5. Juni 2018 hat der Gerichtshof der Europäischen Union (EuGH), Aktenzeichen C-210/16, entschieden, dass eine gemeinsame Verantwortlichkeit von Facebook-Fanpage-Betreiberinnen und Betreibern und Facebook besteht. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Entschließung vom 6. Juni 2018 deutlich gemacht, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen – insbesondere für die Betreiberinnen und Betreiber einer Fanpage – ergeben.

Bei einer gemeinsamen Verantwortlichkeit fordert die Datenschutz-Grundverordnung (DSGVO) unter anderem eine Vereinbarung zwischen den Beteiligten, die klarstellt, wie die Pflichten aus der DSGVO erfüllt werden.

Seit dem Urteil des EuGH sind drei Monate vergangen. Zwar hat Facebook einige Änderungen in seinem Angebot – zum Beispiel bezüglich der Cookies – vorgenommen, doch weiterhin werden auch bei Personen, die keine Facebook-Nutzerinnen und Nutzer sind, Cookies mit Identifikatoren gesetzt, jedenfalls wenn sie über die bloße Startseite einer Fanpage hinaus dort einen Inhalt aufrufen.

Auch werden nach wie vor die Fanpage-Besuche von Betroffenen nach bestimmten, teilweise voreingestellten Kriterien im Rahmen einer sogenannten Insights-Funktion von Facebook ausgewertet und den Betreiberinnen und Betreibern zur Verfügung gestellt.

Der EuGH hat unter anderem hervorgehoben, dass „die bei Facebook unterhaltenen Fanpages auch von Personen besucht werden können, die keine Facebook-Nutzer sind und somit nicht über ein Benutzerkonto bei diesem sozialen Netzwerk verfügen. In diesem Fall erscheint die Verantwortlichkeit des Betreibers der Fanpage hinsichtlich der Verarbeitung der personenbezogenen Daten dieser Personen noch höher, da das bloße Aufrufen der Fanpage durch Besucher automatisch die Verarbeitung ihrer personenbezogenen Daten auslöst.“

Offizielle Verlautbarungen vonseiten Facebooks, ob und welche Schritte unternommen werden, um einen rechtskonformen Betrieb von Facebook-Fanpages zu ermöglichen, sind bisher ausgeblieben. Eine von Facebook noch im Juni 2018 angekündigte Vereinbarung nach Art. 26 DSGVO (Gemeinsam für die Verarbeitung Verantwortliche) wurde bislang nicht zur Verfügung gestellt. Die deutschen Datenschutzaufsichtsbehörden wirken daher auf europäischer Ebene auf ein abgestimmtes Vorgehen gegenüber Facebook hin.

Auch Fanpage-Betreiberinnen und Betreiber müssen sich ihrer datenschutzrechtlichen Verantwortung stellen. Ohne Vereinbarung nach Art. 26 DSGVO ist der Betrieb einer Fanpage, wie sie derzeit von Facebook angeboten wird, rechtswidrig.

Daher fordert die DSK, dass nun die Anforderungen des Datenschutzrechts beim Betrieb von Fanpages erfüllt werden. Dazu gehört insbesondere, dass die gemeinsam Verantwortlichen Klarheit über die derzeitige Sachlage schaffen und die erforderlichen Informationen den betroffenen Personen (= Besucherinnen und Besucher der Fanpage) bereitstellen.

Eine gemeinsame Verantwortlichkeit bedeutet allerdings auch, dass Fanpage-Betreiberinnen und Betreiber (unabhängig davon, ob es sich um öffentliche oder nicht-öffentliche Verantwortliche handelt) die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und dies nachweisen können. Zudem können Betroffene ihre Rechte aus der DSGVO bei und gegenüber jedem Verantwortlichen geltend machen (Art. 26 Abs. 3 DSGVO).

Insbesondere die im Anhang aufgeführten Fragen müssen deshalb sowohl von Facebook als auch und von Fanpage-Betreiberinnen und Betreibern beantwortet werden können.

▪ 5. September 2018 – Anwendung der DSGVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien

Die Konferenz nimmt das Ergebnis der Beratungen des Arbeitskreises Grundsatzfragen des Datenschutzes zur Kenntnis und empfiehlt für die weitere Rechtspraxis, die im Folgenden aufgeführten Positionierungen bei der Tätigkeit als Aufsichtsbehörde zu Grunde zu legen:

1. Soweit Datenverarbeitungen von Parlamenten (auch deren Organe einschließlich der Abgeordneten) den parlamentarischen Kerntätigkeiten zuzuordnen sind, findet die DSGVO keine Anwendung.

2. Parlamente (auch deren Organe einschließlich der Abgeordneten) unterliegen bei der Ausübung originär parlamentarischer Kerntätigkeiten nur dann datenschutzrechtlichen Vorgaben und der Aufsicht der Aufsichtsbehörde, wenn sich dies aus einer klaren gesetzlichen Regelung ergibt.

3. Die Einordnung von Tätigkeiten der Parlamente (auch deren Organe einschließlich der Abgeordneten) als verwaltende und fiskalische in Abgrenzung zur parlamentarischen Kerntätigkeit bedarf jeweils einer Bewertung im Einzelfall.

4. Soweit keine gesetzlichen Grundlagen für die parlamentarische Kerntätigkeit bestehen, wäre eine Datenschutzordnung des Parlaments zu empfehlen, die sich an der DSGVO orientieren sollte. Eine Beratung durch die Aufsichtsbehörde sollte in jedem Fall unbenommen bleiben.

5. Parteien als nicht-öffentliche Stellen sind grundsätzlich Normadressaten der DSGVO und unterliegen damit der Aufsicht der Aufsichtsbehörden. Eine mögliche Berücksichtigung ihres besonderen Status im Rahmen der Gesetzesanwendung bleibt unberührt.

Pressemitteilung der Vorsitzenden der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

25. Mai 2018 – Zeitenwende im Datenschutz Neues Datenschutzrecht: Vorsicht, aber keine Panik!

Ab heute ist die europäische Datenschutz-Grundverordnung anzuwenden. Mit ihr treten das neue Bundesdatenschutzgesetz und zahlreiche Ländergesetze in Kraft. Der selbst gesetzte Anspruch der Verordnung ist hoch: stärkere Datenschutzrechte der etwa 510 Millionen Bürgerinnen und Bürger der Europäischen Union auf der einen Seite. Auf der anderen Seite soll der freie Verkehr personenbezogener Daten im in einer der größten Volkswirtschaft der Welt aus Gründen des Datenschutzes weder eingeschränkt noch verboten werden. Die Verordnung muss nunmehr beweisen, ob sie in diesem Spannungsverhältnis bestehen wird. Vom ersten Kommissionsentwurf vor über sechs Jahren, über die Veröffentlichung am 4. Mai 2016 und zuletzt verstärkt auf der Zielgeraden hin zur Anwendung wurde über die Verordnung viel diskutiert. Ein reformiertes Datenschutzrecht ist aber gerade in Zeiten von Big Data und der Digitalisierung richtig und wichtig, um der Gefährdung der Freiheit der Menschen, über ihre Daten selbst zu bestimmen, entgegenzuwirken. Im Rahmen der Verordnung müssen Vereine jedoch auch weiter ihre unverzichtbaren gesellschaftlichen Aufgaben erfüllen und Unternehmen wettbewerbsfähige Geschäftsmodelle der Zukunft entwickeln können.

Datenschutz-Grundverordnung und Bundesdatenschutzgesetz

Die Europäische Datenschutz-Grundverordnung wird direkt anwendbares Recht und ersetzt damit weitgehend das deutsche Datenschutzrecht. Nationale Regelungsspielräume bestehen nur noch in einem begrenzten Umfang. Das neue Bundesdatenschutzgesetz setzt einzelne Regelungsaufträge der Verordnung um und schafft ergänzende Vorschriften dort, wo Öffnungsklauseln der Verordnung es erlauben. Es tritt zeitgleich in Kraft. Beispiel Datenschutzbeauftragte: Die Verordnung erlaubt es, die Pflicht zur Benennung eines Datenschutzbeauftragte in nationalen Ausführungsgesetzen auf weitere Stellen auszudehnen. Der Bundesgesetzgeber hat diesen Regelungsspielraum im neuen Bundesdatenschutzgesetz genutzt, um die Pflicht zur Benennung von betrieblichen Datenschutzbeauftragte dem in Deutschland bestehenden „Status quo“ anzupassen.

Sanktionen und Beratung

Im Vordergrund der Debatte stehen häufig die Befürchtungen, dass Verstöße gegen die Verordnung in Zukunft mit Geldbußen in Millionenhöhe geahndet werden können. Unerwähnt bleibt dabei oft, dass die Verordnung den Aufsichtsbehörden einen „Werkzeugkasten“ in die Hände gegeben hat, um jeden Einzelfall datenschutzrechtlicher Missstände angemessen zu beheben. Geldbußen sind darin nur eine von vielen Möglichkeiten. An erster Stelle steht die Beratung. Auch von Sanktionen werden die Auf-

sichtsbehörden Gebrauch machen – jedoch mit Augenmaß. Für die konkrete Bestimmung der Höhe eines Bußgeldes wird eine Vielzahl von Aspekten einzubeziehen sein: Art, Schwere und Dauer des Verstoßes, aber auch, ob und wie mit den Aufsichtsbehörden zusammengearbeitet wurde, um Verstößen abzuhelfen, und ob diese eigenständig mitgeteilt wurden.

Europäischer Datenschutzausschuss und Datenschutzkonferenz
Die nationalen Datenschutzbehörden werden in einem neuen Format zusammenarbeiten: Der Europäische Datenschutzausschuss soll gewährleisten, dass die Rechtsauslegung europaweit vereinheitlicht wird. Im Einzelfall werden seine Entscheidungen verbindlich sein. Die Datenschutzkonferenz wird in Deutschland auch in Zukunft schwerpunktmäßig praxisgerechte Auslegungs- und Anwendungsfragen zur Verordnung klären.

Als besonders hilfreich haben sich die Kurzpapiere erwiesen – Ausführungen der Datenschutzkonferenz, wie nach ihrer Auffassung die Verordnung im praktischen Vollzug zu besonders praxisrelevanten Themen angewendet werden sollte. Von der Praxis besonders gefragt sind die Kurzpapiere Datenschutzbeauftragte (Nr. 12), Beschäftigtendatenschutz (Nr. 14), Videoüberwachung (Nr. 15) und insbesondere der Maßnahmenplan „DS-GVO“ für Unternehmen (Nr. 8).

Helga Block, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und Vorsitzende der Datenschutzkonferenz: „Die Forderungen an die Aufsichtsbehörden, Klarheit in strittige Auslegungs- und Anwendungsfragen der Datenschutz-Grundverordnung zu bringen, sind berechtigt. Diese Auslegungen stehen jedoch unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.“

Datenschutzreform vollendet?
Die neue Verordnung spricht viele Themen an, ohne sie explizit zu regeln. Insbesondere im Hinblick auf die elektronische Kommunikation soll die ePrivacy-Verordnung die Datenschutz Grundverordnung präzisieren und ergänzen. Die ePrivacy-Verordnung wird das deutsche Telekommunikationsgesetz und Telemediengesetz in der bisherigen Form teilweise ersetzen, bzw. auch hier wird eine Anpassung des deutschen Gesetzgebers notwendig sein. Mit dem Inkrafttreten im Jahr 2018 ist jedoch nicht mehr zu rechnen. Die derzeit herrschenden Unklarheiten müssen schnell mit klaren Gesetzen beseitigt werden.

Anhang zum Informationsfreiheitsbericht

Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

13. Juni 2017 – Mit Transparenz gegen „Fake-News“

Internet und soziale Medien eröffnen zunehmend auch Möglichkeiten für die gezielte Verbreitung von Falschmeldungen zur Beeinflussung der politischen Meinungs- und Willensbildung. Eine informierte und kritische Gesellschaft benötigt jedoch vielfältige, freie und qualitativ aussagekräftige Informationen für eine umfassende gesellschaftliche und politische Teilhabe. Da die öffentlichen Stellen der Länder und des Bundes über solche Informationen verfügen, kommt ihnen insoweit eine Schlüsselrolle zu. Deshalb ist es von zentraler Bedeutung, dass staatliche Institutionen transparent agieren, um das Vertrauen in die Demokratie und in deren Akteure zu stärken. Für den Prozess der politischen Meinungs- und Willensbildung sind verlässliche und solide Informationen eine unverzichtbare Voraussetzung.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland appelliert an alle öffentlichen Stellen in Deutschland, sich ihrer Verantwortung für die Informationsfreiheit bewusst zu sein und durch größtmögliche Transparenz – sowohl auf Antrag als auch proaktiv – die Bürgerinnen und Bürger in ihrer politischen Willensbildung zu unterstützen. Sie wirbt dafür, dass sich öffentliche Stellen in Deutschland noch stärker öffnen, auf die Informationswünsche der Bürgerinnen und Bürger eingehen, mit behördlichen Dokumenten valide und qualitätsvolle Informationen aus vertrauenswürdiger Quelle bereitstellen und die Kontrolle durch die Bürgerinnen und Bürger ermöglichen.

Damit kann auch bewusst gestreuten Fehlinformationen, mit denen die Manipulation des Meinungsbildes und die Schwächung demokratischer Institutionen verfolgt wird, aktiv und aufgeklärt im öffentlichen Diskurs entgegengetreten werden.

16. Oktober 2018 – Soziale Teilhabe braucht konsequente Veröffentlichung von Verwaltungsvorschriften!

Eine offene und transparente Verwaltungskultur ist eine Voraussetzung dafür, dass sich Bürgerinnen und Bürger und Staat auf Augenhöhe begegnen. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert die Sozialleistungsträger auf,

Verwaltungsvorschriften antragsunabhängig, zeitnah und benutzerfreundlich zu veröffentlichen, soweit sie dazu nicht bereits gesetzlich verpflichtet sind.[1]

Soziale Teilhabe aller Menschen in unserer Gesellschaft folgt aus dem im Grundgesetz verankerten Sozialstaatsprinzip. Ausdruck dieses Prinzips ist ein soziales Sicherungssystem, das durch Sozialleistungen auf Grundlage der Sozialgesetzbücher einen Grundstandard an sozialer Sicherheit gewährleisten soll. Nur informierte Bürgerinnen und Bürger können sie betreffende Entscheidungen von Sozialleistungsträgern verstehen, Ansprüche geltend machen, aber auch Pflichten wahrnehmen.

Alle Sozialleistungsträger bedienen sich Verwaltungsvorschriften, um innerhalb ihrer Behörde eine einheitliche Bearbeitungs- bzw. Entscheidungspraxis sicherzustellen. Verwaltungsvorschriften sind interne Weisungen, die regeln, wie Gesetze auszulegen und anzuwenden sind. Zwar binden Verwaltungsvorschriften unmittelbar nur die Verwaltung selbst; die auf ihrer Grundlage getroffenen Entscheidungen wirken aber nach außen. Verwaltungsvorschriften sind daher bekannt zu geben, damit „der Betroffene (…) sich des Inhalts der durch sie für ihn begründeten Rechte und Pflichten vergewissern“[2] kann. So agieren in diesem Bereich etwa die Bundesagentur für Arbeit sowie die Deutsche Rentenversicherung, die aktuelle Weisungen veröffentlichen. Viele andere Sozialleistungsträger geben die Informationen hingegen allenfalls auf Antrag heraus.

[1] Gesetzliche Verpflichtungen bestehen derzeit in: Hamburg, Bremen, Rheinland-Pfalz, Schleswig-Holstein (ab 1.1.2020).
[2] Urteil des Bundesverwaltungsgerichts vom 25.11.2004, Az. 5 CN 1.03.

Entschließungen der Informationsfreiheitsbeauftragten der Länder

24. April 2017 – Open Data: Gesetzentwurf der Bundesregierung greift zu kurz!

Die Informationsfreiheitsbeauftragten der Länder fordern den Deutschen Bundestag auf, statt des von der Bundesregierung vorgelegten Entwurfs eines Open-Data-Gesetzes (Erstes Gesetz zur Änderung des E-Government-Gesetzes) das Informationsfreiheitsgesetz des Bundes zu einem umfassenden Transparenzgesetz zu entwickeln. Bereits im Dezember letzten Jahres hat die Konferenz der Informationsfreiheitsbeauftragten in Deutschland ihre Bedenken angesichts des geplanten Open-Data-Gesetzes in einer Entschließung zum Ausdruck gebracht. Das mittlerweile fortgeschrittene Gesetzgebungsverfahren bietet Anlass, noch einmal ausdrücklich auf folgende Bedenken hinzuweisen:

Der Deutsche Bundestag hat sich am 31. März 2017 in erster Lesung mit dem Entwurf der Bundesregierung für ein Erstes Gesetz zur Änderung des E-Government-Gesetzes (BTDrucksache 18/11614) befasst. Bund und Länder hatten am 14. Oktober 2016 vereinbart, Open Data zu stärken. Dabei verpflichteten sich die Länder, Open-Data-Gesetze nach dem Beispiel der Bundesregelung zu erlassen. Die Ergebnisse im aktuellen Gesetzgebungsverfahren auf Bundesebene werden daher erhebliche Auswirkungen auf die Landesgesetzgebung haben.

Neben Rohdaten auch Dokumente aktiv veröffentlichen
Der Entwurf richtet sich ausschließlich auf die Bereitstellung von Rohdaten. Informationen, die aus sich heraus verständlich sind, zum Beispiel Verträge, Gutachten, Stellungnahmen und ähnliche Dokumente, sind davon nicht umfasst. Für das von der Bundesregierung angestrebte Ziel der Stärkung zivilgesellschaftlicher Teilhabe ist dies aber ein entscheidender Gehalt des Gesetzes.

Transparenzregelungen gehören in Transparenzgesetze
Die Informationsfreiheitsbeauftragten der Länder sind der Ansicht, dass das Informationsfreiheitsgesetz des Bundes der richtige Standort für eine Open-Data-Regelung wäre. Die Aufnahme von Open-Data-Regelungen in das E-Government-Gesetz des Bundes fördert zwar den Open-Data-Gedanken. Dabei darf jedoch nicht übersehen werden, dass die Behörden des Bundes nach wie vor verpflichtet bleiben, amtliche Informationen nach Maßgabe des Informationsfreiheitsgesetzes des Bundes zur Verfügung zu stellen. Eine zusätzliche Einzelregelung für offene Daten passt nicht in das bislang informationstechnisch orientierte EGovernment-Gesetz. Statt die Regelung dort einzufügen, sollten die vorgesehenen Regelungen im Informationsfreiheitsgesetz verankert werden. Dieses würde so zu einem modernen Transparenzgesetz, das erforderlichenfalls als weiteres Vorbild für die Landesgesetzgebung dienen könnte. Jede weite-

re Zersplitterung der ohnehin bereits unübersichtlichen Regelungen zum Informationszugang sollte vermieden werden.

Keine zusätzlichen Ausnahmen
Der Gesetzentwurf verweist zwar auf die Ausnahmetatbestände des Informationsfreiheitsgesetzes, enthält aber noch weitere Ausnahmen. Beispielsweise sollen nur Daten veröffentlicht werden, die außerhalb der Behörde liegende Verhältnisse betreffen. Das mit dem Gesetzentwurf verfolgte Ziel nach „mehr Teilhabe interessierter Bürgerinnen und Bürger und eine intensivere Zusammenarbeit der Behörde mit diesen“ dürfte damit nicht erreicht werden. Es erscheint insgesamt inkonsequent, Open Data durch Ausnahmen zu beschränken, die über die Regelung des Informationsfreiheitsgesetzes hinausgehen. Hiervon ist abzusehen. Die Weiterentwicklung der Informationsfreiheit kann nur im Abbau von Ausnahmen bestehen, nicht in deren Ausweitung.

Individueller Anspruch auf Veröffentlichung
Der Regierungsentwurf gewährt keinen individuellen Anspruch auf die Veröffentlichung von Daten. Ein solcher Anspruch, der von jedermann einklagbar wäre, ist als effektives Korrektiv zu einer reinen Selbstverpflichtung der öffentlichen Stellen jedoch unverzichtbar.

Für die Länder, die amtliche Informationen auf der Grundlage von Informationsfreiheitsgesetzen bereits in Informationsregistern zur Verfügung stellen, wie auch für die anderen Länder kann das geplante Open-Data-Gesetz in dieser Form keine Vorbildfunktion entfalten. Die Weiterentwicklung des Informationsfreiheitsgesetzes des Bundes zu einem Transparenzgesetz mit den dazugehörigen Open-Data-Regelungen könnte dagegen eine entsprechende Signalwirkung für die Länder haben.

Die Informationsfreiheitsbeauftragten der Länder fordern den Bundestag eindringlich auf, den eingeschlagenen Sonderweg zu überdenken.

6. Oktober 2017 – Grundsatzpositionen der Landesbeauftragten für die Informationsfreiheit

Informationen sind die Basis einer Demokratie. Sie sind Grund- und Treibstoff des Prozesses der öffentlichen Meinungsbildung. Transparenz schafft Vertrauen zwischen Politik, Verwaltung und Bevölkerung. Das Recht auf Zugang zu Informationen stellt ein zentrales Element zur Regelung des Informationsflusses von staatlichen Stellen zu Bürgerinnen und Bürgern in Deutschland dar. Die Informationsfreiheitsbeauftragten der Länder wenden sich mit den folgenden Forderungen zunächst an die Bundespolitik mit dem Ziel, dass sie im Rahmen ihrer Kompetenzen diesen Grundaussagen zur Geltung verhilft. Auch gegenüber der Landespolitik sollen diese Forderungen als grundsätzliche

Anregungen zur Weiterentwicklung und zum Ausbau der informatorischen Rechtsstellung des Einzelnen auch gegenüber der Landespolitik dienen.

I. Informationsfreiheit in die Verfassungen!

Der Anspruch auf freien Zugang zu amtlichen Informationen soll in das Grundgesetz und in die Landesverfassungen aufgenommen werden

In dem Beschluss vom 20. Juni 2017 (1 BvR 1978/13) stellt das Bundesverfassungsgericht fest, dass sich der Verfassungsrang der Informationszugangsfreiheit aus Art. 5 Abs. 1 Satz 1 Grundgesetz herleitet, jedenfalls soweit der Gesetzgeber eine einfachgesetzliche Regelung getroffen hat. Wer die Informationsfreiheit ernst nimmt, kann sie nicht in das Belieben des Gesetzgebers stellen. Deshalb ist die explizite Normierung im Grundgesetz erforderlich. Damit wäre für die Länder, die immer noch kein Recht auf voraussetzungslosen Zugang haben, die Pflicht verbunden, ein solches Recht einfachgesetzlich zu verankern. Auch im Jahr 2017 verfügt ein Viertel der Länder immer noch nicht über ein Informationsfreiheitsgesetz.

II. Ein Gesetz für den Informationszugang! Hin zu Transparenzgesetzen!

Zusammenfassung der verschiedenen Informationsfreiheitsgesetze in einem Gesetz und Weiterentwicklung zu Transparenzgesetzen mit umfassenden Veröffentlichungspflichten

Bestehende Informationszugangsansprüche in unterschiedlichen Informationsfreiheits bzw. Transparenz- und Fachgesetzen sollten verstärkt zusammengefasst werden. Die Ansprüche auf Einsicht in Verwaltungsakten und auf Zugang zu sonstigen Informationen öffentlicher Stellen sind derzeit auf eine Vielzahl von Einzelvorschriften verteilt: Sie finden sich in den Informationsfreiheitsgesetzen, in den Umweltinformationsgesetzen, im Verbraucherinformationsgesetz und in diversen weiteren Gesetzen. Dabei werden vergleichbare Sachverhalte unterschiedlich geregelt, etwa die Voraussetzungen für den Informationszugang, die Fristen zur Beantwortung von Anfragen, die Gebühren, welche für den Informationszugang zu entrichten sind, und die Rechte auf Anrufung der Informationsfreiheitsbeauftragten.

Diese Zersplitterung erschwert die Wahrnehmung der Informationsrechte und trägt zu Unsicherheiten bei der Rechtsanwendung durch die Behörden bei. Zukünftig sollten die Vorschriften so gestaltet werden, dass ein Höchstmaß an Transparenz und Bürgerfreundlichkeit erreicht wird.

Neben diesen anzustrebenden Erleichterungen für die Bürgerinnen und Bürger bei der Durchsetzung ihrer Informationszugangsansprüche ist die Weiterentwicklung der jeweiligen Informationsfreiheitsgesetze zu Transparenzgesetzen ein wichtiges Anliegen. Solche Gesetze verbinden den individuellen, antragsgebundenen Informationszugangsanspruch mit der Verpflichtung öffentlicher Stellen, bestimmte Informationen von

sich aus und antragsunabhängig auf Informationsplattformen im Internet zu veröffentlichen. Derartige gesetzliche Veröffentlichungspflichten erhöhen die Verwaltungstransparenz, die Nachvollziehbarkeit, Akzeptanz und Kontrolle behördlicher Entscheidungsprozesse.

Die Verwaltung soll zukünftig ihre Daten automatisch zur Verfügung stellen. Ausnahmen für die Nichtzurverfügungstellung müssen begründet werden. Das wirtschaftliche Potential von offenen Verwaltungsdaten wird bisher nicht ausreichend genutzt.

III. Nachrichtendienste ins IFG!

Erweiterung des Anwendungsbereichs der Informationsfreiheitsgesetze durch Abschaffung der Bereichsausnahme für die Nachrichtendienste

Die Informationsfreiheitsbeauftragten der Länder halten die in § 3 Nr. 8 IFG normierte Bereichsausnahme für die Nachrichtendienste für nicht erforderlich. Es läuft dem Transparenzgedanken zuwider, dass ein kompletter Verwaltungsbereich vom Informationsfreiheitsgesetz ausgenommen wird. Die Regelung führt dazu, dass die Nachrichtendienste im Fall eines Antrages nicht begründen müssen, warum eine Information nicht herauszugeben ist. Das bedeutet zudem, dass auch nicht-geheimhaltungsbedürftige Informationen zurückbehalten werden können.

Die Informationsfreiheitsbeauftragten stellen mit ihrer Forderung nicht den Geheimnisschutz an sich in Frage. Sie sind vielmehr der Ansicht, dass es ausreicht, wenn sich die Nachrichtendienste hinsichtlich der Herausgabe bzw. Nichtherausgabe von Informationen auf die Ausschlusstatbestände des Informationsfreiheitsgesetzes berufen können. Somit wären die Nachrichtendienste dazu verpflichtet, ihre Entscheidungen zu begründen.

Vergleiche mit Bundesländern wie beispielsweise Schleswig-Holstein, Rheinland-Pfalz und Mecklenburg-Vorpommern zeigen, dass die Verfassungsschutzbehörden auch ohne Bereichsausnahme nicht auf Geheimnisschutz verzichten müssen.

IV. Abschaffung unnötiger Ausnahmen!

Beschränkungen der Ausnahmeregelungen auf das verfassungsrechtlich zwingend gebotene Maß auf der Grundlage der Evaluierung des IFG Bund

Bei der Regelung ihrer Informationsfreiheitsgesetze haben sich zahlreiche Länder in der Vergangenheit am Informationsfreiheitsgesetz des Bundes orientiert, das für sie eine Vorbildfunktion hatte. Nach dessen Evaluierung im Jahr 2012 ergibt sich für den Bund und damit inzident auch für diejenigen Bundesländer, die mit ihrem Landesrecht dem Bund gefolgt waren, erheblicher Reformbedarf. So ist etwa eine Reduzierung und Harmonisierung der Ausschlussgründe, die einem Informationszugang entgegenstehen können, angezeigt. Zu viele, teilweise redundante und sich überschneidende Aus-

schlussgründe konterkarieren Open Data, Open Government und damit Bürgerbeteiligung und Demokratie. Eine allgemeine Güterabwägung zwischen Informations- und Geheimhaltungsinteresse (public interest test) ist daher als Korrektiv erforderlich.

V. Mehr Transparenz in der Drittmittelforschung!

Sicherstellung von Transparenz der Kooperationen zwischen privaten und wissenschaftlichen Einrichtungen

Unternehmensfinanzierte Forschung gewinnt zunehmende Bedeutung für die Hochschulen in der Bundesrepublik Deutschland. Deutschlandweit ist eine große Anzahl von Lehrstühlen direkt oder indirekt von Unternehmen finanziert. Oft sind Ziele und Umfang der Förderung für Außenstehende nicht erkennbar. Für eine Einordnung der Forschungsergebnisse und deren Bewertung ist die Kenntnis dieser Hintergründe jedoch bedeutsam. Die Freiheit von Forschung und Wissenschaft lebt von einer offenen Diskussion; die Geheimhaltung von Zusammenhängen kann diese Freiheiten einengen.

Einer verborgenen Einflussnahme auf Forschungsgegenstände, Forschungsergebnisse und auf deren Veröffentlichung kann durch eine konsequente Politik der Offenheit begegnet werden. Deshalb sollten Kooperationsverträge zwischen Wissenschaft und Unternehmen grundsätzlich offengelegt werden. Die Pflicht zur Veröffentlichung der Verträge darf nur zurücktreten, soweit und solange die Bekanntgabe geschützte Interessen beeinträchtigt.

Die regelmäßige Offenlegung der Finanzierung von Forschungsprojekten ist nach Auffassung der Informationsfreiheitsbeauftragten ein geeignetes Instrument, um die Freiheit der Forschung zu schützen, indem einseitige Abhängigkeiten oder auch nur deren Anschein vermieden werden. Eine bloße Selbstverpflichtung der Universitäten und Forschungseinrichtungen ist hierfür nicht ausreichend. Die Informationsfreiheitsbeauftragten der Länder fordern konsequente gesetzliche Regelungen zugunsten der Transparenz von drittmittelgeförderter Forschung in Bund und Ländern.

Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

www.ldi.nrw.de

Bericht 2019