Freistaat
SACHSEN

Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten

Berichtszeitraum: 1. April 2017 bis 31. Dezember 2018

Sächsischer Landtag DRUCKSACHE 7/800
7. Wahlperiode

Schutz des Persönlichkeitsrechts

Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten

Berichtszeitraum: 1. April 2017 bis 31. Dezember 2018

Dem Sächsischen Landtag

vorgelegt zum 19. Dezember 2019

gemäß Artikel 59 der Datenschutz-Grundverordnung

Vorbemerkung zum Sprachgebrauch in diesem Bericht:

Logisch ist zu unterscheiden zwischen biologischem und grammatischem Geschlecht (sexus und genus). Es wäre ein Verlust, diese Unterscheidung aufzugeben; sie erleichtert das Verständnis von Texten und hilft, sich auf das Wesentliche zu konzentrieren. Frauen bitte ich, sich auch von scheinbar männlichen, in Wahrheit nur generellen Bezeichnungen gemeint zu wissen: Bauherr, Lehrer, Beamter, Betroffener etc. (Übrigens gibt es auch den umgekehrten Fall: Der [männliche] Entbindungspfleger ist eine Hebamme i. S. v. § 53 Absatz 1 Nummer 3 StPO.)

Herausgeber: Sächsischer Datenschutzbeauftragter
Andreas Schurig
Devrientstraße 5 Postfach 11 01 32
01067 Dresden 01330 Dresden
Telefon: 0351/85471-100
Fax : 0351/85471-109

Besucheranschrift: Devrientstraße 5
01067 Dresden

Herstellung: Staatsbetrieb Sächsische Informatik Dienste

Bildnachweis
(Motiv auf Umschlagseite): © sdecoret - stock.adobe.com

Inhalt

Schutz des Persönlichkeitsrechts

Tätigkeitsbericht
des
Sächsischen Datenschutzbeauftragten

Teil 1

19. Tätigkeitsbericht
Schutz des Persönlichkeitsrechts im öffentlichen Bereich
- Berichtszeitraum: 1. April 2017 bis 24. Mai 2018 -

9. Tätigkeitsbericht
Schutz des Persönlichkeitsrechts im nicht-öffentlichen Bereich
- Berichtszeitraum: 1. April 2017 bis 24. Mai 2018 -

Inhaltsverzeichnis Teil 1

1 Schutz des Persönlichkeitsrechts im öffentlichen Bereich

1.1 Inneres

1.1.1 Kommunale Selbstverwaltung

1.1.1.1 Auskunftsersuchen gemäß § 93 Abgabenordnung (AO)

Ein privater Arbeitgeber machte mich darauf aufmerksam, dass eine Gemeinde sich mit einem Auskunftsersuchen gemäß § 93 Abgabenordnung (AO) an ihn gewandt und um Beantwortung der angegebenen Fragen in Bezug auf einen namentlich genannten Arbeitnehmer gebeten hätte. Aus dem Auskunftsersuchen ging für ihn nicht hervor, ob die Auskunft für die Besteuerung des Auskunftspflichtigen oder für die Besteuerung anderer Personen angefordert werde (§ 93 Absatz 2 AO). Weiterhin war für den Hinweisgeber nicht ersichtlich, ob die Kämmerei - Sachgebiet Vollstreckung des Landratsamtes Finanzbehörde nach § 6 AO sei.

Da für ihn weder der Zweck der Datenübermittlung noch die Zuständigkeit des Landratsamtes eindeutig erkennbar waren, hatte er Zweifel, ob er die angeforderten Daten des Arbeitnehmers übermitteln durfte.

Auf der Ebene der Kommunen sind die Gemeinde-, Kreis- oder Stadtsteuerämter und die Gemeinde-, Kreis- oder Stadtkassen für die Realisierung der Gemeindesteuern zuständig und somit unter den Finanzbehördenbegriff nach § 6 AO zu subsumieren.

Ich forderte die zuständige Stelle auf, die Vorlagen bzw. Textbausteine, die im Rahmen von Vollstreckungsmaßnahmen verwendet und an Arbeitgeber von Vollstreckungsschuldnern versendet werden, entsprechend § 93 Absatz 2 AO zu ergänzen. Weiterhin regte ich an, eine Erklärung aufzunehmen, dass auf der Ebene der Kommunen die Gemeinde-, Kreis- oder Stadtsteuerämter und die Gemeinde-, Kreis- oder Stadtkassen für die Realisierung der Gemeindesteuern zuständig sind und somit unter den Finanzbehördenbegriff nach § 6 AO zu subsumieren sind.

1.1.2 Statistikwesen

1.1.2.1 Verdienststatistik

Immer wieder erreichen mich Anfragen zu einer Datenabfrage des Statistischen Landesamts zur Verdienststatistik. Dabei regt sich insbesondere Widerstand bei der Abfrage von Daten zu den Beschäftigten, konkret bei der Abfrage der Rentenversicherungsnummern.

Die diesbezügliche Datenerhebung des Statistischen Landesamtes Sachsen dient der Durchführung der Bundesstatistik der Arbeitsverdienste und Arbeitskosten.

Rechtsgrundlage hierfür ist das Gesetz über die Statistik der Verdienste und Arbeitskosten (VerdStatG), das seit 1. Januar 2007 in Kraft ist.

Das Bundesverfassungsgericht hat in seinem Urteil zum Volkszählungsgesetz 1983 (Urteil vom 15.12.1983, NJW 1984, 419ff.) festgelegt, dass das Recht auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse eingeschränkt werden kann. Diese Einschränkungen bedürfen jedoch einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Der Gesetzgeber hat dabei den Grundsatz der Verhältnismäßigkeit zu beachten und organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

Das Statistische Landesamt - als die gemäß § 2 Absatz 1 Nummer 2 und § 3 Absatz 2 Nummer 1 Sächsisches Statistikgesetz für die Durchführung einer solchen Bundesstatistik zuständige Behörde - ist dabei auch berechtigt, vom Auskunftspflichtigen die Daten in einer Form zu erheben, bei der Name und die Anschrift erkennbar bleiben. Denn auch dies ist mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar: Nach der Rechtsprechung des Bundesverfassungsgerichts gewährt das aus Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG abzuleitende Grundrecht auf informationelle Selbstbestimmung keinen Anspruch auf Datenerhebung in einer Form, die den Auskunftsgebenden nicht erkennen lässt. Zu den Schranken, die das Bundesverfassungsgericht dem – auch vom Gericht nicht in Frage gestellten – Recht des Staates, für statistische Zwecke Daten zu erheben, gezogen hat, gehört gerade nicht das Verbot, Daten nur mittels eines Verfahrens zu erheben, bei dem der Auskunftsverpflichtete von vornherein anonym bleibt. Als notwendige Sicherung des Rechts auf informationelle Selbstbestimmung bei der Erhebung statistischer Daten durch den Staat fordert das Bundesverfassungsgericht vielmehr nur Vorkehrungen bei der Durchführung und Organisation der Datenerhebung und -verarbeitung einschließlich Trennungs- bzw. Löschungsregelungen.

Im Einzelnen:

- Die Abfrage von Geburtsdatum, Geschlecht und Einkommen der Beschäftigten findet ihre Rechtsgrundlage in § 4 VerdStatG.
- Zulässige Hilfsmerkmale der Erhebungen sind ausdrücklich nach § 7 Nummer 3 VerdStatG die Versicherungsnummern der gesetzlichen Rentenversicherung der in die Erhebung nach § 4 einbezogenen Beschäftigten oder, wenn keine Versicherung in der gesetzlichen Rentenversicherung vorliegt, die Namen der Beschäftigten; gibt der Auskunftspflichtige die Namen der Beschäftigten an, hat er die Beschäftigten unverzüglich darüber zu unterrichten.

- Die Abfrage der streitgegenständlichen Angaben beruht mithin auf gesetzlicher Grundlage. Einen datenschutzrechtlichen Verstoß kann ich daher nicht feststellen.

1.1.3 Polizei

1.1.3.1 Gemeinsames Kompetenz- und Dienstleistungszentrum (GKDZ)

Mit abschließender Unterzeichnung vom 8. September 2017 schlossen die Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen den Staatsvertrag für den Aufbau eines gemeinsamen Zentrums zur Telekommunikationsüberwachung. Das Gemeinsame Kompetenz- und Dienstleistungszentrum (GKDZ) soll nach derzeitigem Planungsstand (12.12.2018) 2020 seinen Wirkbetrieb aufnehmen und neben seinem Hauptsitz in Leipzig auch eine Außenstelle in Dresden bekommen. Für die fünf Bundesländer stellt das geplante Zentrum eines der bedeutendsten Ergebnisse der seit 15 Jahren bestehenden Sicherheitskooperation dar. Die polizeiliche Telekommunikationsüberwachung wird in Zukunft unter dem Dach des GKDZ gebündelt, so dass eigene Technik in den einzelnen Ländern nicht mehr vorgehalten werden muss. Angesichts sich rasant entwickelnder Telekommunikations- und Verschlüsselungstechnologien bieten sich den Ermittlungsbehörden der Länder technische Synergien bei der Aufklärung schwerster Straftaten und dem vorbeugenden Schutz der Bevölkerung. Unabhängig von der technischen Lösung bleiben Entscheidungen und Anordnungskompetenzen zur Telekommunikationsüberwachung weiterhin in der Hoheit des jeweiligen Landes. Vollzugspolizeiliche Befugnisse werden der Anstalt nicht übertragen. Zudem werden die Daten für jedes Bundesland getrennt verarbeitet und gespeichert. Die Anstalt fungiert in diesem Sinne als zentrale Dienstleisterin der Trägerländer. Da das GKDZ hierbei personenbezogene Daten im Auftrag verarbeitet, gelten die jeweiligen Vorschriften über den Datenschutz des auftraggebenden Landes. Die Rechte der jeweiligen Landesdatenschutzbeauftragten bleiben unberührt. Auch die parlamentarischen Kontrollrechte bleiben erhalten.

Nachdem der GKDZ-Staatsvertrag am 28. Dezember 2017 mit der Hinterlegung aller Ratifizierungsurkunden bei der Sächsischen Staatskanzlei in Kraft getreten war, erfolgte die Gründung des GKDZ als rechtsfähige Anstalt des öffentlichen Rechts auf der konstituierenden Sitzung des Verwaltungsrates GKDZ am 11. Januar 2018. Auf dieser wurden die Geschäftsordnung und die Satzung beschlossen sowie ein Vorstand bestellt. Das GKDZ ist seitdem rechts- und geschäftsfähig und Bestandteil der mittelbaren Landesverwaltung.

Bereits in der frühen Planungsphase des Projekts wurden die Datenschutzbeauftragten der fünf Trägerländer informiert. Meine Kollegen und ich hatten jeweils Gelegenheit, gegenüber ihren Innenressorts zum Entwurf des Staatsvertrages Stellung zu nehmen. Darüber hinaus habe ich im Namen der Datenschutzbeauftragten der beteiligten Länder

sowohl gegenüber dem Sächsischen Staatsministerium des Innern als auch gegenüber dem Innenausschuss des Sächsischen Landtages Anregungen, z. B. auf Festschreibung des Ziels einer strikten, fehlertoleranten Mandantentrennung und des Betretungsrechts des zuständigen Landesdatenschutzbeauftragten zu Kontrollzwecken gedrungen. Ferner habe ich auf die textliche Aufnahme des Schutzes des Kernbereichs privater Lebensgestaltung sowie auf die Präzisierung der Regelungen zum technisch-organisatorischen Datenschutz hingewirkt. Meine – unsere – Vorschläge haben Eingang in die Endfassung des Staatsvertrages gefunden und waren auch Gegenstand des Entschließungsantrages zum Zustimmungsgesetz des Sächsischen Landtages (Drs. 6/11534). Im weiteren Fortgang hat das SMI regelmäßig zum Umsetzungsstand der Anstalt auch hinsichtlich der technisch-organisatorischen und personellen Feinplanung und zur Durchsetzung einer strikten und zuverlässigen Mandantentrennung gemäß § 13 GKDZ-Staatsvertrag berichtet. Die Ankündigung einer detaillierten Unterrichtung zur Feinplanung erfolgte im Dezember 2018. Der Termin ist für Februar 2019 vorgesehen. Dort sollen die Grundzüge der technisch-organisatorischen Umsetzung und zu klärender technischer Anforderungen vorgestellt und diskutiert werden und eine Abstimmung zur weiteren Vorgehensweise erfolgen. Eine vollständige datenschutzrechtliche Bewertung des Projekts kann natürlich erst nach Vorlage und Prüfung der die Vorgaben des Staatsvertrages und des Verfassungsrechts umsetzenden, ergänzenden Unterlagen und Festlegungen (Benutzungsordnung, Sicherheitskonzept, Verfahrensverzeichnis, Zugriffsberechtigungskonzept, Datenflussmodelle, Pflichtenheft etc.) erfolgen. Bisher kann ich jedoch Einbeziehung und Information durch das SMI bzw. die Anstalt positiv hervorheben.

1.1.3.2 Zuverlässigkeitsüberprüfungen im Rahmen von Akkreditierungen bei Großveranstaltungen

Zunehmend werden im Rahmen von öffentlichen und privaten Veranstaltungen Personen, die auf dem Veranstaltungsgelände z. B. als Ordner oder Kellner tätig werden wollen, durch Sicherheitsbehörden auf ihre Zuverlässigkeit überprüft. Alleinige Grundlage ist hier in den meisten Fällen immer noch die Einwilligung der betroffenen Person. Nur in wenigen Bundesländern gibt es bisher eine gesetzliche Grundlage für solche Verfahren. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat die Gesetzgeber und Verantwortlichen im April 2018 erneut nachdrücklich aufgefordert, für ein rechtstaatliches und transparentes Verfahren solcher Zuverlässigkeitsüberprüfungen zu sorgen, das auf das absolut erforderliche Maß beschränkt bleibt. Dies betrifft sowohl den Umfang der Überprüfung als auch den betroffenen Personenkreis. Generell dürfen Zuverlässigkeitsüberprüfungen nur bei solchen Veranstaltungen eingesetzt werden, die aufgrund ihrer spezifischen Ausprägung infolge einer belastbaren Gefahrenprognose als besonders gefährdet bewertet werden können. Korrespondierend müssen die personenbezogenen Daten der Bewerber, die aus den polizeilichen Informa-

tionssystemen zur Bewertung herangezogen werden, nicht nur eine ausreichende Qualität haben, es dürfen auch nur hinreichend gewichtige Delikte einbezogen werden. Ferner müssen Anhörungsrechte der betroffenen Person verankert werden. Im Berichtszeitraum hat meiner Kenntnis nach keine Zuverlässigkeitsüberprüfung durch sächsische Polizeidienststellen stattgefunden. Auch in Sachsen besteht hierfür keine spezifische Rechtsgrundlage. Ein Rückgriff auf die allgemeinen Polizeibefugnisse ist aus meiner Sicht nicht befriedigend. Die Datenübermittlungsbefugnis nach § 44 Absatz 1 SächsPolG würde der Rolle der Polizei als Zentralstelle bei einer eigenen Zuverlässigkeitsüberprüfung in Sachsen nicht gerecht.

Im Berichtszeitraum häuften sich auch die Fälle einer Datenübermittlung nach § 44 Absatz 1 SächsPolG, über die ich gemäß § 44 Absatz 3 SächsPolG unterrichtet wurde. Hierbei handelt es sich um die Mitwirkung der sächsischen Polizei bei einer fremden, von einer anderen Stelle durchgeführten Zuverlässigkeitsüberprüfung in der Form der Datenübermittlung. Hiernach kann der sächsische Polizeivollzugsdienst personenbezogene Daten an öffentliche und nichtöffentliche Stellen zum Zwecke einer Zuverlässigkeitsüberprüfung übermitteln. Konkret handelte es sich hierbei um Veranstaltungen (Musikfestivals, zentrale Feierlichkeiten) in anderen Bundesländern, die von den dortigen Sicherheitsbehörden als besonders gefährdet eingestuft wurden. Die für die Zuverlässigkeitsüberprüfung am jeweiligen Ort zuständige zentrale Stelle (LKA oder örtliche Polizeidienststelle) forderte – nach einem vorher festgelegten und dem Bewerber bekanntgegebenen Kriterienkatalog – die in PASS oder IVO gespeicherten Informationen zu einem Bewerber an, um sie dann ggf. unter Zusammenführung mit Informationen aus anderen Bundesländern dahingehend zu bewerten, ob bezüglich der Zulassung des Bewerbers auf das Veranstaltungsgelände Bedenken bestehen. Da die Einstufung als besonders gefährdete Veranstaltung durch mich nicht immer nachvollzogen werden konnte, entschloss ich mich, die Umstände eines konkreten Übermittlungsverfahrens beim LKA Sachsen zu kontrollieren. Dabei kam ich mit dem LKA übereinstimmend zu folgenden Ergebnissen: Das Instrument der Zuverlässigkeitsüberprüfung muss sparsam eingesetzt werden, die Anfragen durch die Zentralstelle müssen besser begründet werden, wenn die Einstufung als besonders gefährdete Veranstaltung nicht auf der Hand liegt, muss die angefragte Stelle vor der Übermittlung hierzu ggf. rückfragen.

Weiter wies ich daraufhin, dass im Hinblick auf das Auskunftsrecht der betroffenen Person zu dokumentieren sei, welche Daten wann wohin übermittelt wurden und diese Dokumentation eine angemessene Zeit aufzubewahren ist. Dies ist insbesondere für abgelehnte Bewerber relevant.

Der behördliche Datenschutzbeauftragte des LKA ist Mitglied einer Bund-Länder-Arbeitsgruppe, die eine stufenweise Erarbeitung von bundeseinheitlichen Mindeststan-

dards bei Zuverlässigkeitsprüfungen anstrebt. In der nächsten Sitzung dieses Gremiums wird er meine Anregungen thematisieren.

1.1.4 Verfassungsschutz

1.1.4.1 Einbeziehung des LfV zur Überprüfung von Projekten, die durch das Programm „Weltoffenes Sachsen“ gefördert werden sollen

Ein Bürger machte mich auf die Antwort der Staatsregierung auf eine parlamentarische Anfrage aufmerksam und behauptete, dass Demokratieprojekte durch das Landesamt für Verfassungsschutz (LfV) ausgespäht würden.

Zunächst war nach kurzer Recherche festzustellen, dass die Kleine Anfrage LT-Drs. 6/13482 behördlich veranlasste Überprüfungen von Trägern von Demokratieprojekten, die eine Förderung durch das Landesprogramm „Weltoffenes Sachsen für Demokratie und Toleranz" („WOS“) beantragt hatten, durch das Landesamt für Verfassungsschutz (LfV) zum Inhalt hatte. Fragestellungen und Antworten boten allerdings keinerlei Anhaltspunkte für ein Ausspähen von Demokratieprojekten durch das LfV.

Gleichwohl nahm ich den Hinweis und die Antwort der Staatsregierung auf die o.g. Kleine Anfrage, in der es u.a. hieß, dass eine Überprüfung von nichtextremistischen Trägern durch das LfV nicht stattfinde, dass aber nach der Förderrichtlinie des Landesprogramms ein Zuwendungsempfänger nach seiner Satzung oder seinem tatsächlichen Verhalten keine Bestrebungen im Sinne des § 3 Absatz 1 des Sächsischen Verfassungsschutzgesetzes (SächsVSG) unterhalten oder fördern dürfe und dass zur Prüfung dieser Fördervoraussetzung durch die Bewilligungsbehörden regelmäßig eine Abfrage beim LfV Sachsen erfolge, ob und inwiefern dort Erkenntnisse zu den zur Förderung vorgeschlagenen Projekten bzw. Projektträgern vorliegen, die eine Förderung infrage stellen bzw. ausschließen könnten, zum Anlass, mich an das Sächsische Staatsministerium des Innern (SMI) zu wenden und nachzufragen, ob solche Überprüfungen die Übermittlung personenbezogener Daten umfassten.

Der Fall greift ein Thema auf – die Rechtmäßigkeit (oder Rechtswidrigkeit) der Übermittlung personenbezogener Daten an das LfV zur Überprüfung von Fördermittelantragstellern –, das ich mit dem SMI bereits im Jahr 2011 im Zusammenhang mit der damals von Antragstellern geforderten „Demokratieerklärung“ in umfangreichem Schriftwechsel diskutiert hatte.

Im aktuellen Vorgang habe ich das SMI für den Fall, dass personenbezogene Daten übermittelt werden, um Nennung der Rechtsgrundlagen gebeten und darauf hingewiesen, dass landesrechtliche Mitwirkungsaufgaben des LfV Sachsen in § 2 Absatz 2 SächsVSG (abschließend) bestimmt werden. Eine Mitwirkung des LfV Sachsen nach dieser Vorschrift setzt eine Unterrichtung der betroffenen Personen voraus (§ 2 Absatz 3

Satz 1 SächsVSG). Daneben habe ich angemerkt, dass weder Vorschriften der Sächsischen Haushaltsordnung noch die Förderrichtlinie des Landesprogramms „WOS“ gesetzliche Bestimmungen im Sinne von § 2 Absatz 2 Satz 1 Nummer 6 SächsVSG darstellen (diese Vorschrift erfasst gesetzlich vorgesehene Mitwirkungen wie in § 7 Absatz 3 LuftSiG oder § 12b Absatz 3 AtG).

Das SMI teilte mir mit, dass die Bewilligungsbehörde zur Prüfung der Fördervoraussetzung, dass der Zuwendungsempfänger nach seiner Satzung oder seinem tatsächlichen Verhalten keine Bestrebungen im Sinne des § 3 Absatz 1 SächsVSG unterhalten oder fördern darf, zunächst selbst einen Abgleich mit den in den jährlichen Verfassungsschutzberichten genannten „Extremistischen Organisationen und Gruppierungen im Freistaat Sachsen“ vornehmen könne. Da diese Übersichten jedoch aus verschiedenen Gründen nicht immer aktuell und vollständig seien, habe das LfV in der Vergangenheit auf Bitten der für die Förderung zuständigen Stelle geprüft, ob es sich bei den antragstellenden Vereinen bzw. Trägern um Beobachtungsobjekte des LfV handele. Es habe lediglich ein Abgleich mit dem Bewertungsstand des LfV und keine inhaltliche „Tiefenprüfung“ konkreter Träger stattgefunden. Die Projekte selbst oder einzelne Mitarbeiterinnen und Mitarbeiter der Träger seien ausdrücklich kein Prüfungsgegenstand gewesen.

Ich habe die Ausführungen des SMI so verstanden, dass die für die Förderung zuständige Stelle lediglich organisationsbezogene, aber keine personenbezogenen Anfragen an das LfV richtet, ob dort zu einem Antragsteller einer Förderung entgegenstehende Erkenntnisse vorliegen. Dagegen wäre aus datenschutzrechtlicher Sicht nichts einzuwenden, da in das Individualgrundrecht auf informationelle Selbstbestimmung nicht eingegriffen würde. Vorsorglich habe ich das SMI noch einmal darauf hingewiesen, dass hingegen für personenbezogene Anfragen und Übermittlungen – in diesem Fall läge ein Eingriff in das Grundrecht der einzelnen in der Anfrage bzw. Übermittlung genannten Person vor – eine Rechtsgrundlage fehlte und ein Austausch personenbezogener Informationen zwischen Bewilligungsbehörde und LfV anlässlich von Förderanträgen unzulässig wäre. Die gesetzlichen Voraussetzungen für Übermittlungen nach dem Sächsischen Verfassungsschutzgesetz wären nicht erfüllt – weder für Übermittlungen an das LfV noch in umgekehrter Richtung –, aber auch die von Antragstellern zu unterzeichnende datenschutzrechtliche „Einwilligungserklärung“ könnte mangels Bestimmtheit eine Übermittlung an das LfV nicht rechtfertigen. Die „Einwilligungserklärung“ bezog sich auch auf die „Übermittlung der Daten an die an der Bewilligung, Auszahlung und Verwaltung der Zuwendung beteiligten Stellen innerhalb und außerhalb des Sächsischen Staatsministeriums des Innern und die Verarbeitung der übermittelten Daten durch diese Stellen“, wozu „insbesondere der Bund, die Sächsische Aufbaubank (SAB) und der Sächsische Rechnungshof zählen“ könnten. Betroffene Personen können danach

allerdings nicht erkennen, an welche konkreten Stellen ihre Daten übermittelt werden, insbesondere Verfassungsschutzbehörden werden an keiner Stelle erwähnt.

Das SMI bestätigte mir daraufhin, dass lediglich organisationsbezogene, aber keine personenbezogenen Anfragen an das LfV erfolgten, und sagte zu, die für die Förderung zuständige Stelle nochmals entsprechend zu informieren.

1.1.5 Ausländerwesen

1.1.5.1 Akteneinsicht in Ausländerakten

Im Rahmen mehrerer Beschwerden von Betroffenen bzw. deren Rechtsanwälten wurde ich um datenschutzrechtliche Prüfung teilweiser verwehrter Akteneinsicht in ausländerrechtlichen Verfahren gebeten. Im 14. (Beitrag 5.12.2) und 17. Tätigkeitsbericht (Beitrag 5.13.1) hatte ich schon einmal zu diesem Thema berichtet.

Im Berichtszeitraum wurde in einigen Fällen den Betroffenen die Einsicht in bestimmte Aktenteile mit der Begründung verwehrt, dass diese Akten auch „personenbezogene Daten Dritter“ enthielten. Eine zuständige Ausländerbehörde hatte mehrere Seiten der Hauptakte mit dem Hinweis, diese enthielten „personenbezogene Daten Dritter“, entfernt und in eine Nebenakte genommen, welche im Rahmen der Akteneinsichtnahme nicht zugänglich war.

Zwar enthielten die betreffenden Seiten tatsächlich personenbezogene Daten Dritter, es war jedoch seitens der Behörde die notwendige Prüfung unterblieben, ob ein berechtigtes Interesse dritter Personen gemäß § 29 Absatz 2 VwVfG überhaupt vorlag, die ein Verwehren des Einsichtsrechts begründen könnten.

Die Akteneinsicht – im aufenthaltsrechtlichen Verfahren ist mangels spezieller Vorschrift § 29 VwVfG einschlägig – sichert ein rechtstaatliches Verfahren und ist für den Beteiligten Grundlage und Voraussetzung einer effektiven Ausübung seiner Rechte. Dies muss bei der vor der Einsichtsgewährung vorzunehmenden Abwägung zwischen dem Geheimhaltungsinteresse der Ausländerbehörde und dem Informationsinteresse des Beteiligten besondere Berücksichtigung finden.

In einem konkreten Fall wurden Blätter aus der Akte entfernt, die Angaben zur geschiedenen Ehefrau betrafen. Ein besonderes Geheimhaltungsinteresse war im konkreten Fall nicht erkennbar, insbesondere weil davon ausgegangen werden musste, dass dieses Datum (Geburtsdatum) dem Beteiligten bekannt war. Eine solche Prüfung muss jedoch in jedem Fall gesondert erfolgen, da auch „persönliche Verhältnisse“ vorliegen können, die u. U. sehr „persönlich“ und damit schützenswert auch gegenüber dem geschiedenen Ehepartner sind.

In einem anderen Fall war ein ausgefüllter Fragebogen zur Ehebefragung in aufenthaltsrechtlichen Verfahren aus den Akten entnommen worden. Stattdessen sollte die Befragung in der Form eines „Antwortprotokolls“ zu den Akten genommen werden.

Mit der Herausnahme der Blätter sollte die Verbreitung formalisierter bzw. standardisierter Fragen, die Erkenntnisse darüber erbringen sollen, ob eine bloße „Scheinehe“ besteht, unterbunden werden. Durch die Herausnahme der Fragebögen sah sich der Betroffene in seinem Recht auf informationelle Selbstbestimmung verletzt.

Grundsätzlich kann ich das Anliegen der Ausländerbehörde nachvollziehen, dass solche Fragebögen nicht „öffentlich zirkulieren“ dürfen, um eine gezielte Vorbereitung auf entsprechende Fragen zu unterbinden, die eine behördliche Einschätzung, ob eine Eheschließung ausschließlich zum Zwecke des Erhalts eines Aufenthaltstitels vorliegt, erschweren würde.

Doch auch in einem solchen Fall muss eine Abwägung zwischen dem verfahrensrechtlichen Informationsinteresse des Beteiligten und seinem Recht auf informationelle Selbstbestimmung einerseits und dem Geheimhaltungsinteresse der Ausländerbehörde andererseits stattfinden.

Grundsätzlich bestehen aus rein datenschutzrechtlicher Sicht gegen ein Verfahren, bei dem die mittels standardisierter Fragen bei Dritten erhobenen Daten, einschließlich derer mit Doppelbezug, dem Betroffenen in Form eines „Antwortprotokolls“ zugänglich gemacht werden, keine durchgreifenden Bedenken. Allerdings, und das habe ich den betreffenden Ausländerbehörden mitgeteilt, muss sichergestellt sein, dass dem Beteiligten durch ein solches Verfahren keine ihn betreffenden personenbezogenen Daten vorenthalten werden.

In einem solchen „Antwortprotokoll“ muss zudem abgesichert sein, dass, wenn erhobene Daten nur bzw. erst im Zusammenhang mit der betreffenden Fragestellung verständlich sind bzw. Erkenntniswert aufweisen, auch die entsprechenden Fragen offengelegt werden.

Meiner Bitte um Berücksichtigung dieser Hinweise kamen die Ausländerbehörden anstandslos nach.

1.2 Justiz

1.2.1 Datenschutzrechtliche Fälle aus dem Justizvollzug

Während in den letzten Jahren ein starker Rückgang von datenschutzrechtlichen Beschwerden Gefangener zu verzeichnen ist, nutzen die Justizvollzugsanstalten die Möglichkeit datenschutzrechtlicher Beratung regelmäßig, was ich sehr begrüße.

Im Berichtszeitraum erteilte ich Auskünfte unter anderem zu den folgenden Themen. Bereits jetzt ist allerdings darauf hinzuweisen, dass eine Änderung der Rechtslage bevorsteht. Die datenschutzrechtlichen Bestimmungen in den verschiedenen Sächsischen Justizvollzugsgesetzen werden weitgehend aufgehoben bzw. entnommen und in einem einheitlichen Sächsischen Justizvollzugsdatenschutzgesetz zusammengefasst. Auch nachfolgend erwähnte Vorschriften werden dabei verändert, an der grundsätzlichen Gültigkeit der folgenden Überlegungen ändert sich jedoch nichts.

1. Umgang mit Gesundheitsdaten von Gefangenen

Medizinische Daten von Gefangenen unterliegen auch im Justizvollzug einem besonderen Schutz. Verschiedene gesetzliche Bestimmungen tragen der Schutzbedürftigkeit der höchstpersönlichen Angaben über den Gesundheitszustand des Gefangenen sowie dem besonderen Vertrauensverhältnis zwischen Arzt und Patient Rechnung. So unterliegt der Anstaltsarzt auch gegenüber dem Anstaltsleiter und der Aufsichtsbehörde grundsätzlich der ärztlichen Schweigepflicht (§ 98 Absatz 2 Satz 1 SächsStrafVollzG). Gesundheitsakten über Gefangene sind vom Anstaltsarzt zu führen; sie sind getrennt von den Gefangenenpersonalakten aufzubewahren und besonders zu sichern (§ 100 Absatz 3 und 4 SächsStrafVollzG). Die Einsicht in die Gesundheitsunterlagen und ihre Übermittlung sind nur unter den Voraussetzungen von § 98 Absatz 2 und 3 SächsStrafVollzG zulässig. Die Übermittlungsbeschränkung des § 96 Absatz 7 SächsStrafVollzG, der u.a. auf den Schutz von Gesundheitsangaben nach § 98 Absatz 2 SächsStrafVollzG verweist, läuft nicht dadurch ins Leere, dass die entsprechenden Angaben in einer Akte enthalten sind und – bei einem falschen Verständnis von § 100 Absatz 5 SächsStrafVollzG – mit der Akte herauszugeben wären.

Eine Einschränkung der ärztlichen Schweigepflicht im Justizvollzug findet sich in der gesetzlich bestimmten Offenbarungspflicht nach § 98 Absatz 2 Satz 2 SächsStrafVollzG sowie in der Offenbarungsbefugnis nach § 98 Absatz 2 Satz 3 SächsStrafVollzG. Erstere kommt zur Anwendung, wenn der Anstaltsarzt an vollzuglichen Entscheidungen und Maßnahmen mitwirkt, etwa im Rahmen der Aufnahmeuntersuchung des Gefangenen. Insoweit erhebt der Arzt Gesundheitsdaten aufgrund gesetzlicher Bestimmungen, der Gefangene ist weniger (freiwilliger) Patient als vielmehr eine „behördlich untersuchte Person“. Die Offenbarungsbefugnis des Anstaltsarztes hingegen knüpft an Fälle der Gesundheitsfürsorge an, an Angaben aus Untersuchungen also, die der Gefangene als Patient erbeten bzw. veranlasst hat. Entsprechend höher ist die Voraussetzung für eine Offenbarung, soweit die Aufgabenerfüllung der Anstalt oder der Aufsichtsbehörde in Rede steht.

Zulässig ist allerdings auch eine Offenbarung aufgrund einer Schweigepflichtentbindungserklärung durch den Gefangenen. Zwar ist eine Einwilligung von Gefangenen in

Verarbeitungen ihrer Daten aufgrund der Besonderheiten des Justizvollzugs und des Sonderrechtsverhältnisses zwischen Staat (Anstalt) und Gefangenem stets kritisch und mit größter Vorsicht zu betrachten, allerdings gibt es keinen Grund, einen Gefangenen anders (schlechter) zu stellen als eine Person in Freiheit, die – insbesondere wenn es zu ihrem Vorteil ist – ihren Arzt hinsichtlich sie betreffender Gesundheitsdaten selbstverständlich von seiner Schweigepflicht entbinden kann.

Adressat einer Offenbarung des Anstaltsarztes nach § 98 Absatz 2 SächsStrafVollzG ist grundsätzlich nur der Anstaltsleiter, der letztendlich die Gesamtverantwortung für den Vollzug trägt. Eine so klare Reduzierung des Adressatenkreises dient nicht nur dem Schutz der Gesundheitsdaten und damit des Gefangenen, sondern auch des Arztes selbst, für den grundsätzlich das Verbot unbefugter Offenbarung von Patientengeheimnissen nach § 203 Absatz 1 Nummer 1 StGB gilt. Allerdings kann der Anstaltsleiter nach § 98 Absatz 3 Satz 2 SächsStVollzG die unmittelbare Offenbarung gegenüber bestimmten Anstaltsbediensteten allgemein anordnen. Voraussetzung wären die Zulässigkeit der Offenbarung zu einem Zweck nach § 98 Absatz 2 SächsStrafVollzG und eine ausdrückliche, den Adressaten bestimmende Anordnung des Anstaltsleiters.

2. Akteneinsichtsgesuche (ehemaliger) Gefangener

Mitunter wollen ehemalige Gefangene Auskünfte aus oder Einsicht in ihre noch aufbewahrten Gefangenenpersonalakten nehmen. Auskunft an Betroffene über die zu ihrer Person gespeicherten Daten wird nach § 102 SächsStrafVollzG i.V.m. § 18 SächsDSG erteilt; Akteneinsicht erhalten Betroffene nach dieser Vorschrift, soweit eine Auskunft für die Wahrnehmung ihrer rechtlichen Interessen nicht ausreicht und sie hierfür auf die Einsichtnahme angewiesen sind.

Grundsätzlich spielt es keine Rolle, ob das Auskunftsersuchen oder der Antrag auf Akteneinsicht von einem aktuell im Vollzug befindlichen oder einem ehemaligen Gefangenen gestellt wird; die gesetzliche Vorschrift orientiert sich allein an der Betroffenheit, also daran, dass zu der Person Daten verarbeitet werden (bei ehemaligen Gefangenen in aller Regel nur in der Verarbeitungsvariante der Speicherung bzw. Aufbewahrung der Daten).

Aus datenschutzrechtlicher Sicht ist eine großzügige Praxis hinsichtlich der Gewährung von Einsicht für Betroffene in ihre Gefangenenpersonalakten wünschenswert. Es ist – trotz dem Wortlaut der Vorschrift – kaum verständlich, weshalb dem Gefangenen nur nach Darlegung bestimmter rechtlicher Umstände Einsicht in die zu ihm selbst geführte Akte gewährt werden soll. Durch die Sammlung ihn betreffender Informationen ist der Gefangene ohnehin stets in seinem (Grund)Recht auf informationelle Selbstbestimmung betroffen. Es ist auch nicht zu befürchten, dass dem Gefangenen schützenswerte Daten

Dritter oder aus Sicherheitsgründen geheim zu haltende Informationen durch die Akteneinsicht offenbart werden müssten, denn die Beschränkungen des § 18 Absatz 5 SächsDSG, die im Rahmen von § 102 SächsStrafVollzG zu beachten sind, gelten auch für die Akteneinsicht.

Jedenfalls in seine Gesundheits- und Therapieakten (§ 100 Absatz 2 und 3 SächsStrafVollzG) sollte der Gefangene grundsätzlich ohne Beschränkung Einsicht nehmen können. Allenfalls, wenn der Einsichtnahme erhebliche therapeutische Gründe oder erhebliche Rechte Dritter entgegenstehen, sollte die Einsicht – hinsichtlich der betroffenen Aktenteile – versagt werden dürfen. Damit würde der Gefangene Patienten in Freiheit gleichgestellt, die nach diesen Maßgaben ihre Patientenakte einsehen können. Eine Schlechterstellung von Gefangenen ist kaum zu begründen und liefe dem Grundsatz, dass das Leben im Vollzug den allgemeinen Lebensverhältnissen soweit wie möglich anzugleichen ist (§ 3 Absatz 4 SächsStrafVollzG), zuwider.

Eine Sonderstellung nehmen auch Gefangenenakten aus der Zeit der DDR ein. Immer wieder kommt es vor, dass Menschen, die in der DDR in einer Strafvollstreckungseinrichtung inhaftiert waren, Einsicht in die sie betreffenden Unterlagen aus jener Zeit begehren. Zwar ist auch hier formal die Vorschrift des § 102 SächsStrafVollzG einschlägig. Allerdings muss berücksichtigt werden, dass es sich um Akten aus einer „anderen Zeit“, einem anderen Rechtssystem handelt. Gefangenen standen damals nicht die heute bestehenden Möglichkeiten offen, ihre Behandlung oder sie betreffende vollzugliche Maßnahmen gerichtlich überprüfen zu lassen. Vermutlich werden Einsichtsgesuche, die heute gestellt werden und Akten aus den 1980er Jahren betreffen, häufig der Aufarbeitung der eigenen Geschichte dienen (worin streng genommen keine Wahrnehmung rechtlicher Interessen im Sinne von § 102 SächsStrafVollzG läge). Möglicherweise dienen sie aber auch der Prüfung, ob eventuell Ansprüche nach dem Strafrechtlichen Rehabilitierungsgesetz bestehen (dann wäre die Wahrnehmung rechtlicher Interessen ohne Weiteres zu bejahen).

Ich plädiere hier für eine sehr großzügige Praxis der Einsichtsgewährung unabhängig von der Darlegung eines besonderen Interesses; Einschränkungen sollten allenfalls erfolgen, wenn schutzwürdige Rechte Dritter dies erfordern. Personalakten, Gesundheitsakten und Krankenblätter von Gefangenen, die zwischen dem 30. Januar 1933 und dem 2. Oktober 1990 inhaftiert waren, sind nach § 4 Absatz 2 der Sächsischen Justizschriftgutverordnung bis zum Ablauf des Jahres 2020 aufzubewahren. Diese besonders lange und an die politischen und rechtlichen Besonderheiten in diesem Zeitraum anknüpfende Aufbewahrungsfrist dient nicht zuletzt der Vereinfachung des Zugriffs von Betroffenen auf Informationen aus diesen Unterlagen. Dieser Gedanke sollte auch bei der tatsächlichen Gewährung der Einsicht Richtschnur sein.

3. Mitteilungen an konsularische Vertretungen der Heimatstaaten von Gefangenen

Gelegentlich wendet sich die Auslandsvertretung des Heimatlandes eines Gefangenen an eine Justizvollzugsanstalt und bittet um Informationen über ihren Staatsangehörigen.

Besonderheiten gegenüber Übermittlungen von Angaben zu Gefangenen nach den Vorschriften der Sächsischen Justizvollzugsgesetze ergeben sich in solchen Fällen aus dem Wiener Übereinkommen vom 24. April 1963 über konsularische Beziehungen (WÜK). Gemäß Artikel 36 Absatz 1 Buchstabe b WÜK haben die zuständigen Behörden des Empfangsstaats die konsularische Vertretung des Entsendestaats auf Verlangen des Betroffenen unverzüglich zu unterrichten, wenn in deren Konsularbezirk ein Angehöriger dieses Staates festgenommen, in Straf- oder Untersuchungshaft genommen oder ihm anderweitig die Freiheit entzogen ist. Zuständig für eine solche Mitteilung ist beim Vollzug von Freiheitsstrafe, Jugendstrafe, Sicherungsverwahrung, Jugendarrest oder aufgrund eines Vollstreckungshaftbefehls die zuständige Justizvollzugsanstalt (Nummer 5 Buchstabe b) der „Verwaltungsvorschrift des Sächsischen Staatsministeriums der Justiz über die Unterrichtung konsularischer Vertretungen über strafrechtlich begründete Freiheitsentziehungen gegen Angehörige ihres Staates“). Hinsichtlich bestimmter Staaten besteht eine völkerrechtliche Verpflichtung zur Unterrichtung der konsularischen Vertretung auch ohne oder gegen den Willen des Betroffenen (die Liste dieser Staaten findet sich in der Anlage der vorgenannten VwV).

Nach Nummer 3 Buchstabe a der o.g. VwV ist die ausländische Vertretung unverzüglich, in dringenden Fällen fernmündlich im Voraus, über die Tatsache der Freiheitsentziehung zu unterrichten. Weiter heißt es dort: „Sofern der betroffene ausländische Staatsangehörige schriftlich die Zustimmung erklärt, können auch der Grund der Verhaftung und der gegen ihn erhobene Tatvorwurf mitgeteilt werden. Von einer weiter gehenden Unterrichtung der konsularischen Vertretung, auch durch Übersendung von Unterlagen, ist abzusehen. Zeigt sich eine konsularische Vertretung an zusätzlichen Mitteilungen interessiert, ist sie auf die Möglichkeit hinzuweisen, mit dem Betroffenen Verbindung aufzunehmen.“

Diese Bestimmungen sollen – allein – sicherstellen, dass eine konsularische Betreuung des Gefangenen durch eine Stelle seines Heimatlandes erfolgen kann; sie kommen unabhängig von landesrechtlichen Übermittlungsvorschriften zur Anwendung. Datenschutzrechtlich bedeutsam ist dabei die Beschränkung auf eine bloße Unterrichtung über die Tatsache der Freiheitsentziehung. Grund der Verhaftung und Tatvorwurf darf die Anstalt nur mit schriftlicher Zustimmung des Gefangenen mittteilen, weitergehende Angaben darf sie auf Grundlage des WÜK gegenüber konsularischen Vertretungen des Heimatstaats des Gefangenen nicht machen.

Ob in sonstigen Fällen Justizvollzugsanstalten direkt an Stellen anderer EU-Mitgliedstaaten oder an Drittstaaten und internationale Organisationen personenbezogene Daten von Gefangenen übermitteln dürfen, richtet sich in formeller Hinsicht – Zuständigkeit – nach der Art von eventuellen Auskunftsersuchen und den anzuwendenden Rechtsvorschriften (z.B. Gesetz über die internationale Rechtshilfe in Strafsachen i. V. m. der Verwaltungsvorschrift des Sächsischen Staatsministeriums der Justiz über die Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten) und in materieller Hinsicht nach den Übermittlungsvorschriften in den Sächsischen Justizvollzugsgesetzen und künftig im Justizvollzugsdatenschutzgesetz.

1.2.2 Umfangreiche TKÜ-Maßnahmen erfordern besondere Sorgfalt bei der Einhaltung gesetzlicher Löschungs- und Benachrichtigungsverpflichtungen

Nachdem Ende 2016 in den Medien über die Einstellung eines Ermittlungsverfahrens wegen Bildung einer kriminellen Vereinigung und über umfangreiche Telekommunikationsüberwachungen in diesem Verfahren berichtet worden war und ich auf eine erste allgemeine Anfrage an die Generalstaatsanwaltschaft Dresden eine plausible Antwort zum Umfang der Maßnahmen erhalten hatte, erreichten mich Anfang 2017 datenschutzrechtliche Petitionen von ehemaligen Beschuldigten, die erfahren hatten, dass Drittbetroffene der TKÜ-Maßnahmen (Personen, gegen die sich nicht die TKÜ-Anordnung selbst richtet, die aber mit überwachten Personen bzw. Anschlüssen kommunizierten und dadurch von der Überwachung erfasst wurden) nach einer Benachrichtigung und einem Antrag auf gerichtliche Überprüfung der Telekommunikationsüberwachung teilweise noch vor ehemaligen Beschuldigten Einsicht in größere Bestandteile der Verfahrensakten erhalten hätten.

Daraufhin wandte ich mich erneut an die Generalstaatsanwaltschaft und diskutierte den Umfang der Akteneinsicht für Drittbetroffene bzw. deren Rechtsanwälte. In dieser Konstellation gilt es, das berechtigte Interesse Drittbetroffener zu erfahren, aufgrund welcher Umstände TKÜ-Maßnahmen angeordnet wurden, sowie das schutzwürdige Interesse von Beschuldigten und Dritten, deren Daten sich in den Ermittlungsakten finden, abzuwägen und in angemessenen Ausgleich zu bringen. Im Ergebnis der Erörterungen mit der Generalstaatsanwaltschaft konnte eine Einigung über den Umfang der Akteneinsicht für Drittbetroffene erzielt werden, die unter Beachtung der einschlägigen Rechtsprechung des Bundesgerichtshofes sowohl Interessen der Drittbetroffenen als auch Belange der ehemaligen Beschuldigten angemessen berücksichtigt.

Aufgrund von neuerlichen Hinweisen in datenschutzrechtlichen Petitionsvorgängen und Medienberichten über Journalisten und Rechtsanwälte, die von den TKÜ-Maßnahmen mitbetroffen gewesen sein sollen, wandte ich mich im Sommer 2017 erneut an die Ge-

neralstaatsanwaltschaft. Daneben erhielt ich Hinweise darauf, dass zum Teil ganz erheblich mitbetroffene Dritte nicht benachrichtigt worden sein sollen; auch diese Hinweise habe ich aufgegriffen und mich dazu im frühen Herbst 2017 an die Generalstaatsanwaltschaft Dresden gewandt.

Meine Prüfung konzentrierte sich nachfolgend auf die Frage, ob die gesetzliche Pflicht zur unverzüglichen Löschung der Aufzeichnungen von Kommunikation aus dem Kernbereich privater Lebensgestaltung oder mit bestimmten Berufsgeheimnisträgern eingehalten wurde, und ob bei der Benachrichtigung von Drittbetroffenen den gesetzlichen Vorgaben entsprochen wurde.

Das Ermittlungsverfahren war im Herbst 2013 wegen des Anfangsverdachts der Bildung einer kriminellen Vereinigung zunächst durch die Staatsanwaltschaft Dresden eingeleitet worden. Im November 2015 wurde das Verfahren, das sich gegen 14 Beschuldigte aus Leipzig richtete, durch die Generalstaatsanwaltschaft Dresden übernommen. Diese stellte im Oktober 2016 das Ermittlungsverfahren hinsichtlich aller Beschuldigten nach § 170 Absatz 2 StPO ein.

Polizeiliche Ermittlungshandlungen nahm das Operative Abwehrzentrum (OAZ) vor, das eine Organisationseinheit der Polizeidirektion Leipzig war und im Oktober 2017 in das Polizeiliche Terrorismus- und Extremismus-Abwehrzentrum (PTAZ) überführt wurde, das dem Landeskriminalamt Sachsen (LKA) angehört.

Von Dezember 2013 bis August 2014 erließ das Amtsgericht Dresden auf Anträge der Staatsanwaltschaft Dresden insgesamt 26 Anordnungen zur Überwachung der Telekommunikation von Beschuldigten des Verfahrens gemäß § 100a StPO, wobei es sich um Erst- und Folgeanordnungen handelte. Die Durchführung der richterlich angeordneten Maßnahmen begann im Dezember 2013, die letzte Maßnahme wurde im November 2014 beendet.

Im Rahmen dieser verdeckten Ermittlungsmaßnahmen wurde die überwachte Kommunikation aufgezeichnet, 56.118 Verkehrs- und 838 Bestandsdatensätze wurden erhoben. In den mir vorgelegten Ermittlungsunterlagen fanden sich keine Hinweise auf besondere Abreden zwischen Staatsanwaltschaft Dresden und OAZ zum Vorgehen beim Erkennen von Kommunikationsaufzeichnungen, die den Kernbereich privater Lebensgestaltung oder besonders geschützte Berufsgeheimnisträger betreffen. Löschungen von Aufzeichnungen über Kommunikation in diesen sensiblen Bereichen wurden erst zwischen der später zuständigen Generalstaatsanwaltschaft Dresden und dem OAZ thematisiert. Nach Absprache im Juli 2016 informierte das OAZ die Generalstaatsanwaltschaft über aufgezeichnete Gespräche, die (möglicherweise) dem Kernbereich zuzurechnen waren bzw. mit Berufsgeheimnisträgern geführt worden waren. Im September 2016 bat daraufhin

die Generalstaatsanwaltschaft um Löschung der betreffenden Gesprächsaufzeichnungen. Das OAZ kam dieser Bitte nach.

Vor dieser Löschung im Herbst 2016 wurden seit Beginn der TKÜ-Maßnahmen im Dezember 2013 keine Aufzeichnungen gelöscht. Mit anderen Worten: Aufgezeichnete Kommunikationsinhalte, die nach § 100a Absatz 4 Satz 3 StPO a. F. (jetzt § 100d Absatz 2 Satz 2 StPO) und § 160a Absatz 1 Satz 3 i.V.m. Satz 5 StPO unverzüglich hätten gelöscht werden müssen, wurden zum Teil über zweieinhalb Jahre gespeichert.

Ende September 2016 bat die Generalstaatsanwaltschaft das OAZ, zur Vorbereitung von Benachrichtigungen eine Liste von betroffenen Anschlussinhabern zu erstellen. Im Oktober 2016 hielt die Generalstaatsanwaltschaft fest, dass unmittelbar betroffene Anschlussinhaber eine Benachrichtigung erhalten sollen und dass die Benachrichtigung der Regelfall sei und nur ausnahmsweise unterbleiben könne, etwa, wenn der Anschlussinhaber Arbeitgeber des Betroffenen oder der Nutzer nicht identifizierbar sei.

Im Rahmen der Bearbeitung bei mir eingegangene datenschutzrechtlicher Petitionen ehemaliger Beschuldigter und Drittbetroffener häuften sich allerdings Hinweise, dass von TKÜ-Maßnahmen zum Teil ganz erheblich Mitbetroffene nicht benachrichtigt worden waren. Es stellte sich heraus, dass die Polizei grundsätzlich zu hohe Anforderungen an die Übereinstimmung zwischen Nutzer und Anschlussinhaber gestellt hatte.

So sei, wie die Polizei mir mitteilte, ihr eine eindeutige Zuordnung von Anschlussinhaberin und Nutzerin in einem Fall, in dem 324 Kommunikationsereignisse aufgezeichnet (darunter auch kernbereichsrelevante Kommunikation) und über 500 Seiten Protokolle gefertigt worden waren, nicht möglich gewesen, obwohl als Nutzerin eine Person mit einer alltäglichen, üblichen Abkürzung eines voll ausgeschriebenen Vornamens erfasst worden war und die Bestandsdatenerhebung eine Person mit zur Abkürzung passenden Vornamen und einem Nachnamen als Anschlussinhaberin ergeben hatte.

In einem anderen Fall war ein Drittbetroffener als Inhaber der Rufnummer eines Mobilfunkanschlusses gespeichert und zu seiner Person 24 Kommunikationsereignisse erfasst worden. Bestandsdaten wurden erhoben, die dabei erlangte Anschrift stimmte mit der Anschrift aus dem Sächsischen Melderegister überein. Der Polizei waren damit Vor- und Nachname des Drittbetroffenen bekannt. In der aufgezeichneten Kommunikation war der Betroffene auch mit seinem zutreffenden Vornamen angesprochen worden. Gleichwohl soll dies für eine hinreichend sichere Identifizierung des Anschlussnutzers nicht ausreichend gewesen sein.

In diesen und weiteren der Generalstaatsanwaltschaft vorgetragenen Einzelfällen wurde durch letztere die nachträgliche Benachrichtigung von Mitbetroffenen veranlasst.

Meine umfangreiche datenschutzrechtliche Prüfung des Vorgangs umfasste Akteneinsichten, längeren Schriftwechsel mit den beteiligten Behörden sowie mündliche Erörterungen.

Im Sommer 2018 habe ich nach alledem das Landeskriminalamt wegen der Verletzung seiner Mitwirkungspflichten bei der Einhaltung von Verfahrensregelungen im Rahmen von Maßnahmen der Telekommunikationsüberwachung (TKÜ) nach § 100a StPO gemäß § 29 Absatz 1 SächsDSG gegenüber dem Sächsischen Staatsministerium des Innern förmlich beanstandet. Ebenso erging eine Beanstandung der Staatsanwaltschaft Dresden wegen Verstößen gegen die gesetzliche Pflicht, Aufzeichnungen von Kommunikation aus dem Kernbereich privater Lebensgestaltung bzw. mit besonders geschützten Berufsgeheimnisträgern unverzüglich zu löschen, gegenüber dem Sächsischen Staatsministerium der Justiz.

Das Unterlassen von Löschungen aufgezeichneter Kommunikation, die den Kernbereich privater Lebensgestaltung betraf bzw. mit besonders geschützten Berufsgeheimnisträgern geführt wurde, in der Phase der Verfahrensleitung der Staatsanwaltschaft Dresden verstieß gegen gesetzliche Löschungsverpflichtungen nach § 100a Absatz 4 Satz 3 StPO a. F. (jetzt § 100d Absatz 2 Satz 2 StPO) und § 160a Absatz 1 Satz 3 i.V.m. Satz 5 StPO. Die Staatsanwaltschaft als „Herrin des Ermittlungsverfahrens“ ist für derartige Löschungen zuständig. Von ihrer Verantwortung wird sie nicht dadurch entbunden, dass sie dabei auf die Zuarbeit der ermittlungsführenden Polizeidienststelle angewiesen ist. Letztere führt die TKÜ-Maßnahmen tatsächlich durch und erhält zuerst Kenntnis vom Inhalt der überwachten Kommunikation.

Die im Nachgang zum Urteil des Bundesverfassungsgerichts zum „Großen Lauschangriff“ (Urteil vom 3. März 2004 - 1 BvR 2378/98), in dem Begriff und Schutz des Kernbereichs privater Lebensgestaltung eine zentrale Rolle spielen, erarbeiteten Verwaltungsvorschriften sehen vor, dass die ermittlungsführende Stelle bei Feststellung der Aufzeichnung entsprechender Informationen dies bei der zuständigen Staatsanwaltschaft anzeigt, um eine Entscheidung (der Staatsanwaltschaft) über die Löschung herbeizuführen.

Seitens des OAZ unterblieben derartige Informationen und Anregungen an die verfahrensleitende Staatsanwaltschaft Dresden vollständig. Selbst nach Beendigung der letzten TKÜ-Maßnahme im November 2014 verging ein Jahr, ohne dass entsprechende Anzeigen an die Staatsanwaltschaft Dresden erfolgten. Dass dies aber angesichts der Erhebung kernbereichs- und berufsgeheimnisrelevanter Kommunikationsinhalte seit Dezember 2013 hätte geschehen müssen, um der gesetzlichen Pflicht zur unverzüglichen Löschung nachkommen zu können, liegt auch unter Berücksichtigung des Umstands, dass

nicht sämtliche Aufnahmen sofort angehört und protokolliert werden und so den Ermittlern nicht sofort nach Erlangung zur Kenntnis gelangen, auf der Hand.

Die Staatsanwaltschaft ihrerseits darf sich nicht stillschweigend darauf verlassen, dass die ermittlungsführende Polizeidienststelle ihre Zuarbeiten stets mit der erforderlichen Sorgfalt erledigt; auch in diesem Punkt leitet die Staatsanwaltschaft das Verfahren und hat – ggf. durch Hinweise oder Nachfragen – sicherzustellen, dass die Handlungen vorgenommen werden, die die Erfüllung gesetzlicher Verpflichtungen ermöglichen. Dies gilt insbesondere, wenn sich die Staatsanwaltschaft generell die Entscheidung über die Löschung von Aufzeichnungen vorbehält. Die Besprechungen zwischen Staatsanwaltschaft Dresden und dem OAZ hätten für entsprechende Hinweise oder Nachfragen ebenso Gelegenheit geboten wie der Schriftwechsel zwischen beiden Stellen. Auch die bloße Anzahl der Anordnungen nach § 100a StPO, die in der Regel jeweils eine Überwachung der Telekommunikation für den Zeitraum von drei Monaten vorsahen, musste nahelegen, dass bei einem derart hohen Aufkommen an überwachter und aufgezeichneter Kommunikation auch gesetzlich besonders geschützte Kommunikation betroffen sein würde, sodass – wenn nicht schon bei Absprachen zum Vorgehen noch vor den ersten TKÜ-Maßnahmen – zumindest im Lauf des Jahres 2014 ein klarer Hinweis der Staatsanwaltschaft an das OAZ erforderlich gewesen wäre.

Der Staatsanwaltschaft Dresden war aus polizeilichen Anregungen weiterer TKÜ-Anordnungen sowie aus Berichten des OAZ bekannt, dass Telekommunikation antrags- und anordnungsgemäß tatsächlich von Dezember 2013 an überwacht, aufgezeichnet und ausgewertet wurde. Gleichwohl ergingen keine Hinweise oder Nachfragen zu eventuellen Aufzeichnungen von Kommunikation aus dem Kernbereich privater Lebensgestaltung oder mit Berufsgeheimnisträgern. Wegen der Versäumnisse sowohl seitens der Polizei als auch seitens der Staatsanwaltschaft wurden Aufzeichnungen gesetzlich besonders geschützter Kommunikation entgegen unmissverständlichen gesetzlichen Vorgaben nicht unverzüglich, sondern erst nach vielen Monaten und – nach dem Übergang der Zuständigkeit für das Ermittlungsverfahren – auf Veranlassung der Generalstaatsanwaltschaft Dresden gelöscht.

Der Schutz des Kernbereichs privater Lebensgestaltung und von bestimmten Berufsgeheimnissen vor einem verdeckten Eindringen staatlicher Stellen ist rechtstaatlich essentiell. Die gesetzliche Befugnis zum Eingriff in Kommunikationsgrundrechte besteht in der aktuellen Ausgestaltung nur, weil zugleich andere gesetzliche Vorschriften vor unverhältnismäßigen und verfassungswidrigen Eingriffen schützen. Ein laxer Umgang mit diesen Schutzregelungen verletzt nicht nur Grundrechte der Betroffenen, sondern beschädigt auch die Reputation der Strafverfolgungsbehörden.

Hinsichtlich des Vorwurfs, durch zu hohe Anforderungen an die Identität von Anschlussinhabern und tatsächlichen Anschlussnutzern bei der Erstellung der Liste von zu benachrichtigenden Personen (Beteiligte der überwachten Kommunikation nach § 101 Absatz 4 Satz 1 Nummer 3 StPO) Mitteilungen an Mitbetroffene und damit deren Rechtsschutzmöglichkeiten vereitelt zu haben, habe ich von einer Beanstandung des LKA gegenüber dem Sächsischen Staatsministerium des Innern abgesehen.

Zwar halte ich den seinerzeitigen Ansatz des OAZ, die Übereinstimmung „lediglich“ des Vornamens von Anschlussinhaber und Nutzer als nicht ausreichend für eine die Benachrichtigung rechtfertigende Feststellung der Übereinstimmung anzusehen und nur nach ein-eindeutiger Verifizierung eine Benachrichtigung anzuregen, für grob falsch und geeignet, die gesetzliche Regelung zu unterlaufen und zum Teil erheblich Mitbetroffenen Rechtsschutzmöglichkeiten faktisch zu verwehren. Insbesondere die oben aufgeführten Beispiele verdeutlichen, dass zu hohe Anforderungen an Hinweise auf die Identität von Anschlussinhaber und Nutzer zu unvertretbaren Ergebnissen führen und gesetzliche Schutzvorschriften ins Leere laufen lassen.

Allerdings habe ich anerkannt, dass OAZ und Generalstaatsanwaltschaft sich über das Vorgehen bei der Benennung von zu benachrichtigenden Personen überhaupt austauschten. Ich vermute, dass dabei beide Seiten davon ausgingen, dass ihre jeweilige Position hinsichtlich der Feststellungen der Übereinstimmung von Anschlussinhaber und Nutzer durch die jeweils andere Behörde berücksichtigt und umgesetzt bzw. gebilligt werde, dass tatsächlich aber insoweit – unerkannte – Differenzen bestanden. Des Weiteren habe ich anerkannt, dass nach Einstellung des Ermittlungsverfahrens bereits vor Einleitung meiner datenschutzrechtlichen Prüfung eine relativ große Zahl an Mitbetroffenen benachrichtigt wurde und keine Anhaltspunkte für eine systematische Umgehung von Benachrichtigungspflichten vorlagen.

Das LKA hat mich im Rahmen meiner Kontrolle darüber informiert, dass es Maßnahmen ergriffen habe, um aufgezeigte Verstöße gegen gesetzliche Vorschriften künftig zu vermeiden. Dazu gehörten Sensibilisierungs- und Schulungsmaßnahmen für mit TKÜ-Maßnahmen befasste Mitarbeiter und die Überarbeitung bzw. Fortschreibung verwaltungsinterner bzw. behördenübergreifender Richtlinien zur Durchführung von TKÜ-Maßnahmen. Das Sächsische Staatsministerium der Justiz hat die Beanstandung zum Anlass genommen, den Generalstaatsanwalt des Freistaates Sachsen aufzufordern, eine entsprechende Sensibilisierung der Mitarbeiter der Staatsanwaltschaften in Sachsen durchzuführen.

Ich gehe danach davon aus, dass sächsische Staatsanwaltschaften und Polizeidienststellen in aktuellen und künftigen Ermittlungsverfahren besonderes Augenmerk auf die Einhaltung grundrechtsschützender Verfahrensvorschriften legen. Neben der Stärkung

der Rechte von Betroffenen kann dadurch auch die Begrenzung – vermeidbaren – nachträglichen Aufwands durch behördliche und gerichtliche Überprüfungen erreicht werden.

1.3 Gesundheit und Soziales

1.3.1 Sozialwesen

1.3.1.1 Antragsformular zum Unterhaltsvorschussgesetz

Im Rahmen einer Eingabe musste ich Ende 2017 ein Landratsamt auf eine Korrektur des bei der Behörde zum Einsatz kommenden Antragsformulars nach dem Unterhaltsvorschussgesetz - auf welches wegen § 68 Nummer 14 SGB I die Regelungen des SGB Anwendung finden - aufmerksam machen:

Die Kreisfreien Städte sowie Landratsämter sind im Rahmen ihres Aufgabenbereichs auch für die Bewilligung des Unterhaltsvorschusses zuständig, welcher für Kinder von 12 Jahren bis unter 18 Jahren bis zu 268 Euro betragen kann.

Für ein Kind besteht zwischen 12 und 18 Jahren dabei zusätzlich die Voraussetzung, dass das Kind nicht auf Leistungen nach dem SGB II angewiesen ist oder der alleinerziehende Elternteil im SGB II-Bezug ein eigenes Bruttoeinkommen von mindestens 600 Euro monatlich erzielt.

Von dem genannten Unterhaltsvorschussbeitrag sind bei Kindern, die keine allgemeinbildende Schule mehr besuchen, unter bestimmten Voraussetzungen auch andere Einkommen des Kindes abzuziehen. Einkommen von Kindern, die noch eine allgemeinbildende Schule besuchen, bleibt von vornherein unberücksichtigt.

Insoweit sind Angaben zu Einkünften des Kindes nur anzugeben, wenn das Kind ab 15 Jahren keine allgemeinbildende Schule mehr besucht. Bis zum Ende des Schulbesuchs, der durch Vorlage eines schriftlichen Nachweises des Schulbesuchs zu belegen ist (soweit nicht bereits mit Antragstellung erfolgt), müssen daher für die betreffenden Kinder keine Angaben zu weiteren Einkünften erfolgen.

Diese müssen dann auch nicht im Rahmen einer Mitwirkungspflicht angegeben werden, es sei denn, der Schulbesuch wird – entgegen der bisherigen Angaben gegenüber dem Jugendamt - vorzeitig abgebrochen.

Insoweit war das seinerzeit zum Einsatz kommende Antragsformular bei der Beantragung von Leistungen nach dem UVG zu überarbeiten, da in diesem generell Angaben zu Einkünften des Kindes von 15 bis 17 Jahren erhoben wurden, ohne dass dabei differenziert wurde, ob das betreffende Kind noch eine allgemeinbildende Schule besucht oder nicht.

Ich habe insoweit auf ein entsprechendes Antragsformular des Jugendamts der Landeshauptstadt Dresden, Sachgebiet Unterhaltsvorschuss, Stand: 07/2017, dort unter 2. auf Seite 3 oben, verwiesen. Dort ist klargestellt, dass nachfolgende Angaben, die Einkünfte des Kindes betreffen, nur erforderlich sind, wenn das Kind keine allgemeinbildende Schule mehr besucht.

Das betreffende Landratsamt hat zeitnah meine Hinweise aufgegriffen und das Formular überarbeitet. Abschließend habe ich gegenüber der Behörde daher nur noch darauf hingewiesen, dass die Anpassung auch bereits laufende Vorgänge betrifft.

1.3.1.2 Vorlage des Schulzeugnisses im Rahmen eines Feststellungsverfahrens nach dem SGB IX

Der Vater eines behinderten Kindes hatte sich an mich gewandt. Im Rahmen einer Überprüfung, inwieweit die Behinderung seines Kindes fortbesteht, war er aufgefordert worden, eine Kopie des letzten Schulzeugnisses seines Kindes vorzulegen.

Der Landkreis hat mir in seiner Stellungnahme mitgeteilt, dass im vorliegenden Fall zusätzlich zu den angeforderten medizinischen Befunden vom gesetzlichen Vertreter ein aktuelles Schulzeugnis angefordert worden sei, da ein Entwicklungsrückstand zu Gleichaltrigen vorliegt und mit dem Zeugnis eine bessere Aussage zum Ausmaß des vorliegenden Entwicklungsrückstandes zu treffen sei.

Da der Grad der Behinderung die Auswirkungen auf die Teilhabe am Leben in der Gesellschaft widerspiegelt (§ 152 SGB IX), seien bei Jugendlichen nicht nur ärztliche Befundberichte, sondern auch Leistungseinschätzungen von Bildungs- und Erziehungseinrichtungen in Bezug auf den Lebensbereich „Schule" von Bedeutung. Diese würden vom versorgungsärztlichen Dienst ausgewertet und in die Einschätzung zum Ausmaß der Teilhabebeeinträchtigung einbezogen. Zeugnisse als pädagogische Dokumente enthalten wichtige Hinweise auf die sich aus Gesundheitsstörungen ergebende Befähigung zur Einordnung und Anpassung an Regellebensbereiche - wie sie von den versorgungsmedizinischen Grundsätzen als Bewertungsmaßstab definiert sind - und stellten somit wertvolle Ergänzungen ärztlicher Quellen dar.

Ich habe gegenüber dem Petenten abschließend noch darauf hingewiesen, dass auch nach der obergerichtlichen Rechtsprechung die Beiziehung von Schulzeugnissen bei der Festlegung eines Grades der Behinderung rechtens ist (siehe LSG Sachsen-Anhalt, L 7 SB 72/12, Urteil vom 19.2.2014).

1.4 Technischer und organisatorischer Datenschutz

1.4.1 Ende-zu-Ende-Verschlüsselung mit dem System SIDAS v4 - Sicherer Datenaustausch Sachsen

Im Berichtszeitraum bat mich der Staatsbetrieb Sächsische Informatik Dienste (SID) um eine abschließende Datenschutzprüfung seiner zentralen Cloud-Speicherlösung „Sicherer Datenraum Sachsen“ (SiDaS V4)[1]. Das System SiDaS V4 ist ein virtueller Datenraum, in welchem die Daten webbasiert gespeichert, verwaltet und zwischen den Anwendern ausgetauscht werden können. Es steht den Mitarbeitern der Landesverwaltung Sachsen zur Verfügung.

Die zum Einsatz kommende Cloudlösung ist für den sicheren verschlüsselten Datenaustausch zwischen den öffentlichen Stellen des Freistaates Sachsen und Unternehmen, Bürgern oder sonstigen Dritten konzipiert. Insbesondere können damit auch große Dateien über einen verschlüsselten Datenraum sicher versenden werden, der Zugriff auf verschlüsselte virtuelle Datenräume organisiert werden oder auch Dateien sicher per passwortgesichertem Download-Link an Dritte versendet werden. Im System SiDaS kann optional eine zusätzliche clientseitige Verschlüsselung (Triple-Crypt-Technologie) zur Ende-zu-Ende-Verschlüsselung aktiviert werden. Die Datenhaltung erfolgt ausschließlich im Rechenzentrum des SID in Sachsen. Jede Behörde kann als separater Mandant eingerichtet werden und den Behördendatenraum selbst administrieren und verwalten.

Ich habe das System SiDaS geprüft und festgestellt, dass eine Verarbeitung von personenbezogenen Daten durch das System datenschutzgerecht möglich ist. Entsprechend der überprüften technischen und organisatorischen Systeminformationen ist die Sicherheit als ausreichend gegeben unter der Voraussetzung anzusehen, dass für die Übermittlung von personenbezogenen Daten die Nutzung des verschlüsselten Data Room erfolgt (derzeit mit der Verschlüsselung Triple-Crypt™Technology)[2]. Ferner müssen die Nutzungs- und Datenschutzvorgaben zum System gemäß der abzuschließenden Leistungsvereinbarung mit dem SID in der jeweiligen Behörde eingehalten und umgesetzt werden.

Vor dem Einsatz des Systems in einer Behörde sind der Schutzbedarf der zu übermittelnden Daten von der datenverarbeitenden Stelle festzustellen und die erforderlichen Datenschutzmaßnahmen festzulegen und umzusetzen. Der Nutzer, der die Daten bereitstellt, trägt die Verantwortung für die Zulässigkeit der Datenübermittlung. Die Anwender des Systems SiDaS stehen in der Verantwortung, die datenschutzrechtlichen Anfor-

[1] https://www.sid.sachsen.de/sidas.html
[2] Kurzgutachten ULD (https://www.datenschutzzentrum.de/uploads/guetesiegel/kurzgutachten/g150402/g150402-rezertifizierung-DRACOON-2018.pdf)

derungen zu beachten und beim Hochladen, Speichern, Nutzen oder Weiterleiten von Daten mittels des SiDaS umzusetzen. Ferner ist für das System ein auf die Behörde ausgerichtetes Berechtigungskonzept zu erstellen, welches sicherstellt, dass nur die dafür vorgesehenen Personen Zugriff auf die entsprechenden Daten oder virtuellen Datenräume haben.

Für die Übermittlung von personenbezogenen oder besonders sensiblen Daten empfehlen die Datenschutzbeauftragten der Länder Lösungen umzusetzen, die auf eine konsequente Ende-zu-Ende-Verschlüsselung setzen. Daher empfehle ich, bei dem System SiDaS generell die Voreinstellung des verschlüsselten Data Room mit Triple Crypt Technology zur Übermittlung personenbezogener oder besonders sensibler Daten zu nutzen. Eine Übermittlung über den unverschlüsselten Datenraum ist nur in begründeten Ausnahmen zulässig.

Ich empfehle die Nutzer jeder Behörde in einem Datenschutzmerkblatt ausreichend zu sensibilisieren, wie die sichere Einsatzumgebung, insbesondere die Verschlüsselung, richtig zu nutzen ist.

1.5 Ordnungswidrigkeitenverfahren

Vom 1. April 2017 bis zum Ablauf des 24. Mai 2018 war ich im öffentlichen Bereich zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach

- § 38 Sächsisches Datenschutzgesetz (§ 38 Absatz 3 Satz 1 SächsDSG),
- § 16 Absatz 2 Nummer 2 bis 5 Telemediengesetz (§ 15 Nummer 2 OWiZuVO i. V. m. § 16 Absatz 2 Nummer 2 bis 5 TMG)
- § 111 Absatz 1 Nummer 1 des Vierten Buches Sozialgesetzbuch – Gemeinsame Vorschriften für die Sozialversicherung – (§ 15 Nummer 3 OWiZuVO i. V. m. § 111 Absatz 1 Nummer 1 SGB IV) und
- § 85 des Zehnten Buches Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (§ 15 Nummer 4 OwiZuVO i. V. m. § 85 SGB X).

Im Berichtszeitraum waren im öffentlichen Bereich insgesamt 65 Bußgeldverfahren anhängig. Davon wurden im Berichtszeitraum 12 mit einem Bußgeld und eines mit einem Verwarngeld abgeschlossen.

Drei Verfahren sind nach eingelegtem Einspruch gegen den Bußgeldbescheid dem zuständigen Amtsgericht vorgelegt worden. Die Entscheidungen stehen derzeit noch aus.

Berichtszeitraum		**01.04.2017 – 24.05.2018**
anhängig gesamt		**65**
davon	Verfahren aus vorherigem Berichtszeitraum	15
	neu eingegangene Verfahren	50
abgeschlossen		**25**
davon	mit Bußgeld	12
	mit Verwarnungsgeld	1
	eingestellt/von Verfolgung abgesehen	12
noch in Bearbeitung		40
Summe rechtskräftige Bußgelder/ Verwarnungsgelder in €		**5.760**

Bei Hochrechnung auf den bisherigen Berichtszeitraum von zwei Jahren ergibt sich ein gleichbleibendes (hohes) Aufkommen von Ordnungswidrigkeitenverfahren im öffentlichen Bereich. Die Summe der rechtskräftigen Buß- und Verwarngelder belief sich auf 5.760 Euro.

Sowohl der personelle Engpass als auch der stetig steigende Bearbeitungsaufwand im Bereich der Ordnungswidrigkeiten wirken sich negativ auf die Dauer der Verfahren aus. Es konnten im Vergleich zum vergangenen Berichtszeitraum weniger Verfahren abgeschlossen werden, was wiederum zu einer niedrigeren Summe der festgesetzten Geldbußen führte.

Geprüft bzw. geahndet wurden

- unbefugte Verarbeitungen (insbesondere in Form der Übermittlung oder Nutzung) nicht offenkundiger personenbezogener Daten (§ 38 Absatz 1 Nummer 1 Buchstabe a SächsDSG),
- unbefugte Abrufe nicht offenkundiger personenbezogener Daten für sich oder einen anderen (§ 38 Absatz 1 Nummer 1 Buchstabe c SächsDSG) und
- unbefugte Erhebungen oder Verarbeitungen nicht allgemein zugänglicher Sozialdaten (§ 85 Absatz 2 Nummer 1 SGB X).

Die unbefugten Verarbeitungen oder Abrufe nicht offenkundiger personenbezogener Daten (§ 38 Absatz 1 Nummer 1 Buchstabe a und c SächsDSG) gingen zudem, nach

entsprechender Verpflichtung gemäß § 6 Absatz 2 SächsDSG, in der Regel mit einer Verletzung des Datengeheimnisses nach § 6 Absatz 1 Satz 1 oder 2 SächsDSG einher (Ordnungswidrigkeitentatbestand nach § 38 Absatz 1 Nummer 3 SächsDSG).

Nach wie vor handelt es sich zum Großteil (ca. 82 %) um Ordnungswidrigkeitenverfahren gegen Bedienstete der sächsischen Polizei wegen unbefugter Abrufe personenbezogener Daten aus den der Polizei zur Verfügung stehenden Datenbanken, z. B. zu Freunden, Kollegen, Nachbarn oder anderen Bekannten. Dieser Umstand erklärt sich aus dem überdurchschnittlichen Anzeigeverhalten der Polizeidirektionen, die datenschutzrechtliches Fehlverhalten ihrer Bediensteten konsequent verfolgen. Er besagt nicht, dass andere Teile der Verwaltung weniger datenschutzrechtliche Ordnungswidrigkeiten begehen. Des Weiteren standen Bedienstete von Jobcentern der Bundesagentur für Arbeit, die in meinen Zuständigkeitsbereich fallen, unter Verdacht, nicht allgemein zugängliche Sozialdaten ohne dienstlichen Anlass erhoben oder verarbeitet zu haben (Ordnungswidrigkeitentatbestand nach § 85 Absatz 2 Nummer 1 SGB X). Auch bestand gegenüber Bediensteten unterschiedlichster Behörden der Verdacht, nicht offenkundige personenbezogene Daten unbefugt verarbeitet zu haben.

Zwei Ordnungswidrigkeitenverfahren gegen sächsische Polizeibeamte aus dem vorherigen Berichtszeitraum, die nach eingelegtem Einspruch gegen den Bußgeldbescheid an das zuständige Amtsgericht abgegeben worden sind, wurden im Berichtzeitraum gerichtlich entschieden. In beiden Fällen sind den Betroffenen Geldbußen wegen ordnungswidrigen Handelns auferlegt worden.

In einem der beiden Fälle, welcher neben Recherchen zu Dritten auch Recherchen zur eigenen Person des Betroffenen in den polizeilichen Auskunfts- bzw. Informationssystemen umfasste, begründet das Amtsgericht Borna sein Urteil vom 26. September 2017 unter anderem folgendermaßen:

„Das Abrufen nicht offenkundiger personenbezogener Daten ist nur zulässig, wenn deren Kenntnis zur Aufgabenerfüllung der abrufenden Person erforderlich ist, d. h. nur dann, wenn die Erfüllung der gesetzlichen − also die sich aus einer dienstlichen Anweisung ergebende – Aufgabe, ohne die konkrete Datenerhebung nicht möglich ist. Selbst wenn die polizeilichen Auskunfts- bzw. Informationssysteme IVO, PASS, INPOL, Schengen und ZEVIS zu den täglichen Arbeitsmitteln eines Polizeibeamten zählen und die darin gespeicherten Daten generell zugänglich sind, muss für jede Datenverarbeitung und für jeden Datenabruf eine dienstliche Notwendigkeit gegeben sein (OLG Bamberg, a.a.O.).“

Die getroffenen Feststellungen des AG Borna stellen dabei im Wesentlichen auf ein Urteil des OLG Bamberg, Beschluss vom 27.04.2010, Az. 2 Ss 531/10, ab.

Ausschließlich die Eigenschaft, Polizeibeamtin oder -beamter zu sein, die oder der zur Abwehr von Gefahren und zur Verfolgung von Straftaten nach § 1 SächsPolG verpflichtet ist, reicht demnach regelmäßig nicht aus, um sämtliche technisch möglichen Datenabrufe zu rechtfertigen. So wie der gesamte Polizeivollzugsdienst nur die personenbezogenen Daten verarbeiten darf, die zur Erfüllung seiner Aufgaben erforderlich sind (§ 43 Absatz 1 Satz 1 SächsPolG), ist auch der einzelne Polizeibedienstete nur berechtigt, die zur Erfüllung seiner konkreten dienstlichen Aufgabe erforderlichen Daten zu verarbeiten. Das vorgenannte Urteil bestätigt nochmals, dass sich Polizeibeamtinnen und -beamte grundsätzlich innerhalb ihrer konkreten Aufgabenzuweisung und Zuständigkeiten zu bewegen haben.

Bezüglich der Recherchen zur eigenen Person des Betroffenen bekräftigte das Amtsgericht Borna zudem in seinem Urteil:

„Der Erfüllung des Tatbestandes des unbefugten Abrufs nicht offenkundiger personenbezogener Daten steht grundsätzlich auch nicht entgegen, dass der Betroffene zu seiner eigenen Person recherchiert hat. Der Abruf von Daten aus geschützten Dateien ist nicht einwilligungsfähig, insbesondere polizeiliche Auskunftssysteme können mehr Angaben über Personen enthalten, als diesen bekannt ist. Die polizeiliche Vorgangsdatei enthält Vorgänge, die einzelne polizeiliche Tätigkeit veranlasst haben und daher Informationen über laufende Ermittlungen sowie über Personalien der beteiligten Personen hinausgehende weitere Feststellungen, wie etwa zur Kontrolle und Rechtfertigung polizeilichen Einschreitens, zur Beweissicherung und als Hintergrundwissen für zukünftige polizeiliche Maßnahmen. Die dort gespeicherten Daten betreffen damit rein polizeiinterne Informationen, die der betroffenen Person selbst nicht bekannt sind. Die dortige Datenspeicherung erfolgt daher auch nicht mit Einwilligung des Betroffenen, sondern auf Grund bereichsspezifischer Regelung. Die gespeicherten Daten dienen damit ausschließlich dienstlichen Interessen und nicht privaten Interessen der gespeicherten Person (vgl. OLG Bamberg a.a.O.). Schließlich kann bei Recherchen mit der Eingabe der eigenen Personalien nicht davon ausgegangen werden, dass nur Daten zur eigenen Person abgerufen werden. Vielmehr enthalten Speicherungen zu Vorgängen regelmäßig die Informationen über verschiedene Personen. Gespeichert werden in IVO Angaben zu Beschuldigten, Verdächtigen, Vermissten oder hilflosen Personen, Zeugen, Geschädigten, Opfern, Haltern, Fahrern, Insassen und Unfallbeteiligte im Zusammenhang mit Fahrzeugen oder anderem. Über die Recherche nach einem Namen gelangt man zu diesen Vorgängen. Personenbezogene Daten von anderen Beteiligten werden dabei ebenfalls zugänglich gemacht.“

Unabhängig davon steht Personen zum Zweck der Selbstauskunft § 51 SächsPolG zur Verfügung. Dies gilt auch für Polizeibeamte, sofern sie Auskünfte über polizeiliche Speicherungen zu ihrer Person erhalten wollen.

Des Weiteren stellte das Amtsgericht Borna fest, dass es nicht darauf ankommt, ob die abgerufenen personenbezogenen Daten an Dritte weitergegeben oder die Daten mit Schädigungsabsicht abgerufen worden sind. Der Tatbestand des § 38 Absatz 1 Nummer 1 Buchstabe c SächsDSG als auch des § 38 Absatz 1 Nummer 3 SächsDSG ist bereits erfüllt, wenn die Daten unbefugt für sich selbst oder auch für einen anderen abgerufen werden bzw. diesbezüglich das Datengeheimnis verletzt wird.

In dem zweiten Fall berücksichtigte das AG Torgau mit Urteil vom 19. September 2017 bei der Festsetzung der Geldbuße, dass Verstöße gegen die datenschutzrechtlichen Bestimmungen in hohem Maße geeignet sind, das Vertrauen der Allgemeinheit in den Umgang öffentlicher Stellen mit personenbezogenen Daten zu beeinträchtigen und – im konkreten Fall – das Ansehen der Polizei empfindlich zu schädigen.

Die Ahndung von Ordnungswidrigkeiten im öffentlichen Bereich ist daher nach wie vor unabdingbar. Die Bediensteten der Behörden und sonstigen öffentlichen Stellen in Sachsen sind auch zukünftig zu ihrer besonderen Pflichtenwahrung und Vorbildwirkung zu ermahnen.

2 Datenschutzaufsicht im nicht-öffentlichen Bereich

Als Sächsischem Datenschutzbeauftragten oblag mir auch die Datenschutzaufsicht nach § 38 BDSG über nicht-öffentliche Stellen im Anwendungsbereich des Dritten Abschnitts des BDSG (§ 30a Satz 1 SächsDSG). Zudem hatte man mir zugleich die Funktion der Verwaltungsbehörde nach § 36 Absatz 2 OWiG (vgl. § 15 OWiZuVO) übertragen, d. h. ich war auch für die Verfolgung von Ordnungswidrigkeiten nach den §§ 43 BDSG, 16 Absatz 2 Nummer 2 bis 5 TMG und 130 OWiG zuständig.

Als Datenschutzaufsichtsbehörde überwachte ich die Durchführung des Datenschutzes bei nicht-öffentlichen Stellen und öffentlich-rechtlichen Wettbewerbsunternehmen und habe dabei die Einhaltung der Regelungen des BDSG sowie anderer Datenschutzvorschriften kontrolliert, soweit sie die automatisierte Verarbeitung personenbezogener Daten oder aber die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht-automatisierten Dateien regelten.

Soweit im Rahmen des vorliegenden Abschnitts 2 des Tätigkeitsberichts auf das BDSG Bezug genommen wird, ist damit stets das – am 25. Mai 2018 außer Kraft getretene – Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I Satz 66), zuletzt geändert durch Artikel 10 Absatz 2 des Gesetzes vom 31. Oktober 2017 (BGBl. I Satz 3618), gemeint.

Die einzelnen Aufgaben leiteten sich wie folgt aus dem BDSG ab:

- **Registerführung** (§ 38 Absatz 2 Satz 1 BDSG)
  Die Aufsichtsbehörden führten das Register der nach § 4d BDSG meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4e Satz 1 BDSG.

- **Anlass- und Regelkontrollen** (§ 38 Absatz 1 Satz 1 BDSG)
  Die Datenschutzaufsichtsbehörden durften, soweit die grundsätzlichen Anwendungsvoraussetzungen des Bundesdatenschutzgesetzes erfüllt waren, alle nicht-öffentlichen Stellen kontrollieren. Es mussten weder hinreichende Anhaltspunkte für eine Datenschutzverletzung vorliegen, noch war auf eine meldepflichtige Tätigkeit als Kontrollvoraussetzung abzustellen. Während sich **Anlasskontrollen** nichtsdestoweniger auf (vermutete) Verstöße gegen datenschutzrechtliche Vorschriften konzentrierten, deckten (anlassfreie) **Regelkontrollen** ausgewählte branchenspezifische Schwerpunkte oder aber das gesamte Spektrum datenschutzrechtlicher Vorschriften ab.

- **Beratungstätigkeit (§§ 4g, 4d, 38 Absatz 1 Satz 2 BDSG)**
  Gesetzlich verankert war die Beratungsfunktion in § 4g Absatz 1 Satz 2 BDSG (Aufgaben des Beauftragten für den Datenschutz) sowie in § 4d Absatz 6 Satz 3 BDSG (Meldepflicht/Vorabkontrolle), wonach sich der betriebliche Datenschutzbeauftragte jeweils in Zweifelsfällen an die Aufsichtsbehörde wenden konnte. Darüber hinaus regelte § 38 Absatz 1 Satz 2 BDSG auch generell, dass die Aufsichtsbehörde die Datenschutzbeauftragten und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse berät.

- **Prüfung der Verhaltensregeln von Berufsverbänden** (§ 38a BDSG)
  Ferner konnten sich auch Berufs- und Unternehmensverbände an die Aufsichtsbehörde wenden, um von ihnen erarbeitete Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen auf die Vereinbarkeit mit geltendem Datenschutzrecht prüfen zu lassen.

- **Genehmigung von Datenübermittlungen in Drittstaaten** (§ 4c Absatz 2 BDSG)
  § 4b BDSG regelte die Übermittlung personenbezogener Daten ins Ausland. Für den konkreten Fall, dass personenbezogene Daten in Drittstaaten ohne angemessenes Datenschutzniveau übermittelt werden sollten, stellte § 4c BDSG einen Ausnahmekatalog bereit, der vermeiden sollte, dass der Wirtschaftsverkehr mit diesen Staaten unangemessen beeinträchtigt wurde. Über diesen Katalog hinausgehende Ausnahmen waren von der Aufsichtsbehörde zu genehmigen.

- **Öffentlichkeitsarbeit** (§ 38 Absatz 1 Satz 6 BDSG)
  Die Aufsichtsbehörden für den nicht-öffentlichen Bereich hatten regelmäßig, spätestens jedoch alle zwei Jahre, einen Tätigkeitsbericht zu veröffentlichen.

- **Stellungnahmen zu Unterlassungsklagen** (§ 12a UKlaG)
  Werden personenbezogene Daten eines Verbrauchers zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens einer Auskunftei, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben, verarbeitet oder genutzt und ist dazu bei dem zuständigen Gericht eine zivilrechtliche Verbandsklage anhängig, hat mich das Gericht vor einer Entscheidung anzuhören.

Im Rahmen ihrer Tätigkeit konnten die Aufsichtsbehörden nach pflichtgemäßem Ermessen von folgenden Durchsetzungs- bzw. Sanktionsbefugnissen Gebrauch machen:

- **Unterrichtung des Betroffenen** und **Anzeige** der für den Verstoß verantwortlichen Stelle **bei den zuständigen Ahndungs- und Verfolgungsbehörden** (§ 38 Absatz 1 Satz 6 BDSG)

- **Anordnung von Maßnahmen** zur Beseitigung festgestellter technischer oder organisatorischer Mängel und von Verstößen bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten (§ 38 Absatz 5 Satz 1 BDSG)

- Verhängung von **Zwangsgeldern** zur Durchsetzung angeordneter Maßnahmen zur Mängelbeseitigung (§ 38 Absatz 5 Satz 2 BDSG) bis hin zur Untersagung der Erhebung, Verarbeitung oder Nutzung einzelner Verarbeitungsverfahren

- Aufforderung zur **Abberufung des betrieblichen Datenschutzbeauftragten** (§ 38 Absatz 5 Satz 3 BDSG)

- Erlass förmlicher und damit vollstreckbarer **Auskunftsheranziehungsbescheide**, gegebenenfalls auch verbunden mit der Verhängung von Zwangsgeldern, zur Durchsetzung der Erfüllung der gegenüber der Behörde bestehenden Auskunftspflichten (vgl. § 38 Absatz 3 BDSG) der verantwortlichen Stellen

- Erlass förmlicher und damit vollstreckbarer Duldungsanordnungen, gegebenenfalls auch verbunden mit der Verhängung von Zwangsgeldern, zur Durchsetzung der Betretungs- und Besichtigungsrechte der Aufsichtsbehörde (§ 38 Absatz 4 Sätze 1, 2 und 4 BDSG)

- Durchführung von **Ordnungswidrigkeitenverfahren** nach dem Bundesdatenschutzgesetz, den datenschutzrechtlichen Tatbeständen des Telemediengesetzes sowie nach § 130 OWiG (§ 15 OWiZuVO)

- eigenständiges Strafantragsrecht bei BDSG-Straftatbeständen (§ 44 Absatz 2 BDSG)

Meine örtliche Zuständigkeit war auch als Aufsichtsbehörde nach § 38 BDSG gemäß § 3 VwVfG auf den Freistaat Sachsen beschränkt. Für die Kontrollzuständigkeit maßgeblich war, wo die Daten verarbeitet wurden, d. h. wo die einzelnen Verarbeitungshandlungen jeweils stattfanden. Ich war also immer dann zuständig, wenn sich die tatsächliche in der Verarbeitung personenbezogener Daten bestehende Geschäftstätigkeit der verantwortlichen Stelle im Freistaat Sachsen abgespielt hat oder wenn am Unternehmenssitz im Freistaat Entscheidungen darüber getroffen wurden, in welcher Weise im Unternehmen personenbezogene Daten verarbeitet werden sollen. Ohne Bedeutung war dabei, wo der von der Datenverarbeitung Betroffene seinen Wohnsitz hat.

2.1 Verfahrensregister

Die Aufsichtsbehörde führt ein Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen mit den Angaben gemäß § 4e Satz 1 (§ 38 Absatz 2 Satz 1 BDSG).

Die Meldepflicht nach § 4d BDSG traf zum einen alle Unternehmen, die personenbezogene Daten geschäftsmäßig zum Zweck der (gegebenenfalls auch anonymisierten) Übermittlung speichern – dies sind in erster Linie Wirtschaftsauskunfteien, Adresshändler sowie Markt- und Meinungsforschungs-institute. Zum anderen unterlagen auch solche Unternehmen der Meldepflicht, die höchstens neun Arbeitnehmer mit der automatisierten Datenverarbeitung für eigene Zwecke beschäftigen, diese Datenverarbeitung weder durch die Einwilligung der Betroffenen noch durch die Zweckbestimmung eines Vertragsverhältnisses gedeckt, und im Übrigen auch keine Vorabkontrolle erforderlich ist.

Zum Stichtag 24. Mai 2018 lagen insgesamt 35 Registermeldungen von 22 Unternehmen vor, die

- in 6 Fällen Verfahren von Handels- und Wirtschaftsauskunfteien,
- in 23 Fällen Verfahren von Markt- und Meinungsforschungsinstituten

sowie in je einem Fall den Betrieb eines Verfügungszentralregisters, eines Widerspruchsregisters, eines Adresshandels, eines Bewertungsportals, eines Handwerkerpools sowie eines Verfahrens zur Videoüberwachung betrafen.

Das bei mir geführte Verfahrensregister war in dem in § 38 Absatz 2 BDSG beschriebenen Umfang öffentlich gewesen und konnte folglich von jedem eingesehen werden. Innerhalb des Berichtszeitraums hatte ich aber kein solches Verlangen zu verzeichnen.

Am 25. Mai 2018 ist das BDSG in der bisherigen Fassung außer Kraft getreten. Da weder das neue BDSG (Bundesdatenschutzgesetz vom 30. Juni 2017, BGBl. I Satz 2097, in Kraft seit dem 25. Mai 2018) noch die seit dem 25. Mai 2018 anwendbare Datenschutz-Grundverordnung eine dem § 4d Absatz 1 BDSG vergleichbare Regelung zur Meldepflicht enthalten, habe ich das bei mir nach § 38 Absatz 2 BDSG geführte Register zum 25. Mai 2018 aufgelöst und die (ehemals) meldepflichtigen Stellen entsprechend unterrichtet.

Verantwortliche (und Auftragsverarbeiter) sind nach Artikel 30 DSGVO zwar auch weiterhin zur Führung eines (internen) Verzeichnisses von Verarbeitungstätigkeiten verpflichtet, müssen mir dieses aber nunmehr nur noch auf Anforderung zur Verfügung stellen (Artikel 30 Absatz 4 DSGVO).

2.2 Regelaufsicht

Die Aufsichtsbehörde kontrolliert die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht-automatisierten Dateien regeln, einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Absatz 5 (§ 38 Absatz 1 Satz 1 BDSG).

Nachdem ich im letzten Berichtszeitraum wieder einige – wenn auch fast ausschließlich im schriftlichen Verfahren – anlassfreie Kontrollen hatte durchführen können, ist die Anzahl der Regelkontrollen im aktuellen Berichtszeitraum erneut auf das vollkommen unzureichende Niveau der vorangegangenen Jahre gefallen. Die Ursache dafür ist u. a. darin zu suchen, dass mir ein nur befristet auf Abordnungsbasis zur Verfügung gestellter Mitarbeiter, zwar planmäßig, aber eben auch ersatzlos, wieder abgezogen worden ist, und mir daher schlichtweg die personellen Kapazitäten zur Vornahme weiterer anlassfreier Kontrollaktionen – welcher Art auch immer – gefehlt haben. Hinzu kam, dass gegen Ende des Berichtszeitraums ohnehin alle meine – unverändert deutlich zu gering bemessenen – Ressourcen in der Vorbereitung des Übergangs zur Datenschutz-Grundverordnung einerseits sowie meiner Selbstständigkeit als oberste Staatsbehörde (§ 15 Absatz 1 SächsDSDG) andererseits gebunden waren.

Berichtszeitraum	01.01.09 31.12.10	01.01.11 31.03.13	01.04.13 31.03.15	01.04.15 31.03.17	01.04.17 24.05.18
Anzahl Regelkontrollen	2	7	0	133	3

Die durch mich dennoch durchgeführten drei Regelkontrollen betrafen für das elektronisch geführte Grundbuch abrufberechtigte Unternehmen aus dem Immobilien- und Finanzsektor. Dabei handelte es sich um die Fortsetzung einer 2016 begonnenen Kontrollaktion; Inhalt und Ergebnisse dieser Kontrollen sind insoweit unverändert geblieben, sodass an dieser Stelle für weitere Informationen auf den 8. Tätigkeitsbericht, Punkt 3.3, verwiesen werden kann.

2.3 Anlassaufsicht

Die Aufsichtsbehörde kontrolliert die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht-automatisierten Dateien regeln, einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Absatz 5 (§ 38 Absatz 1 Satz 1 BDSG).

Während Regelkontrollen (anlassfreie Kontrollen) ohne konkreten Anhaltspunkt für eine Datenschutzverletzung durchgeführt werden, beruhen Anlasskontrollen regelmäßig auf solchen Anhaltspunkten, in erster Linie auf Eingaben Betroffener, resultieren darüber hinaus zu einem geringen Anteil aber auch aus Hinweisen Dritter, Presse- oder Internetveröffentlichungen oder bereits durchgeführten Überprüfungen.

Im Berichtszeitraum waren insgesamt 573 anlassbedingte Aufsichtsvorgänge bei mir anhängig, 79 Fälle resultierten dabei noch aus dem letzten Berichtszeitraum.

		01.01.09 31.12.10	01.01.11 31.03.13	01.04.13 31.03.15	01.04.15 31.03.17	**01.04.17 24.05.18**
Neueingänge		648	904	807	749	**494**
zzgl. Übernahme Vorjahr		29	14	26	91	**79**
anhängige Sachverhalte gesamt		677	918	833	840	**573**
davon	mit örtlichen Kontrollen	68	162	98	106	**51**
	Verstöße	152	324	259	292	**132**
	keine Zuständigkeit	160	180	124	150	**89**
	noch in Bearbeitung	14	26	91	79	**112**

Die vorstehende Tabelle fasst den Umfang meiner anlassbedingten Kontrolltätigkeit im Berichtszeitraum zusammen und stellt deren Entwicklung im Vergleich zu den Vorjahren dar.

Wenn man die Zahlen dieser Übersicht zur besseren Vergleichbarkeit durchgängig auf einen Zweijahreszeitraum bezieht, ergibt sich folgendes Bild:

	01.01.09 31.12.10	01.01.11 31.03.13	01.04.13 31.03.15	01.04.15 31.03.17	**01.04.17 24.05.18**
Neueingänge	648	803*	807	749	**861***
zzgl. Übernahme Vorjahr	29	14	26	91	**79**
anhängige Sachverhalte gesamt	677	817*	833	840	**940***

* Vergleichswerte (Zweijahreszeitraum), rechnerisch ermittelt!

Aus der Zusammenstellung ist abzulesen, dass die Gesamtzahl der Aufsichtsvorgänge nach einem geringfügigen Rückgang im letzten Berichtszeitraum auf einen neuen Spitzenwert gestiegen ist. Noch nie vorher hatte ich im nicht-öffentlichen Bereich eine solche hohe Anzahl von Eingaben zu bearbeiten. Es ist nur schwer einzuschätzen, ob dies

seine Ursache in einer gewachsenen Sensibilität der Betroffenen, möglicherweise auch in Verbindung mit der bevorstehenden Änderung des maßgeblichen Rechtsrahmens (BDSG/DSGVO), oder in einem nachlässigeren Umgang der verantwortlichen Stellen mit den für sie geltenden datenschutzrechtlichen Vorschriften hat. Jedenfalls aber zeigt die bereichsspezifische Analyse der bearbeiteten Vorgänge, dass Aspekte der Videoüberwachung einen erheblichen Anteil an dieser Steigerung haben. Die diesbezügliche Technik ist schon seit Längerem äußerst kostengünstig auch in Discountern zu erhalten und viele Anwender sehen darin ein einfaches Mittel zur Erhöhung ihrer Sicherheit oder zur Lösung (tatsächlich wohl eher zur Verschärfung) ihrer Nachbarschaftsprobleme.

Ein derart hoher Zuwachs an Eingaben führt – bei unverändert unzureichendem Personalbestand – schon fast erwartungsgemäß auch zu einer weiteren Erhöhung der auch schon in den letzten Berichtszeiträumen sehr hohen Anzahl noch zur (abschließenden) Bearbeitung anstehender Aufsichtsvorgänge. Mit 112 offenen Vorgängen ist leider auch insoweit ein neuer Spitzenwert erreicht. Praktisch bedeutet dies für die Betroffenen deutlich verlängerte Bearbeitungszeiten und damit im Fall der Feststellung von Datenschutzverstößen auch deutlich längere Zeiten, in denen diese nicht geahndet und auch nicht auf deren Unterbindung hingewirkt werden kann. Die große Anzahl der offenen Verfahren ist natürlich auch die logische Folge der hohen Arbeitsbelastung meiner Mitarbeiter im nicht-öffentlichen Bereich; schon seit Längerem kann ich feststellen, dass sich das diesbezügliche Verhältnis zwischen nicht-öffentlichen und öffentlichen Bereich deutlich in Richtung nicht-öffentlicher Bereich verschoben hat. Aktuell ist festzustellen, dass mich im nicht-öffentlichen Bereich etwa doppelt so viele Eingaben erreichen wie im öffentlichen Bereich.

Anlasskontrollen führe ich im Regelfall im schriftlichen Verfahren durch, daneben kontrolliere ich die verantwortlichen Stellen – falls dies vom Sachverhalt her angezeigt ist – oftmals aber auch vor Ort. So habe ich im Berichtszeitraum in immerhin 57 Fällen örtliche Überprüfungen bei insgesamt 51 verantwortlichen Stellen durchgeführt.

Den Schwerpunkt meiner anlassbedingten Kontrolltätigkeit bilden unverändert Videoüberwachungsfälle, deren relative Anzahl um 18 % gestiegen ist. Noch größere (relative) Steigerungen habe ich im Gesundheitswesen (+ 74 %), in der Werbung (+ 64 %) sowie in der Wohnungswirtschaft (+ 46 %) beobachten können, während in den übrigen Bereichen keine derart gravierenden Veränderungen feststellbar waren bzw. dort prozentuale Auswertungen infolge der geringen absoluten Fallzahlen wenig aussagekräftig sein würden.

Im Einzelnen verteilten sich die Schwerpunkte meiner anlassbedingten Kontrolltätigkeit (ohne Altfälle) im Berichtszeitraum wie folgt:

1.	Videoüberwachung	104 Fälle
2.	Betroffenenrechte	64 Fälle
3.	Beschäftigtendatenschutz	33 Fälle
4.	Gesundheitswesen	23 Fälle
5.	Wohnungswirtschaft	22 Fälle
6.	Internet	20 Fälle
7.	Dienstleistungen	18 Fälle
8.	Werbung	13 Fälle
9.	Vereine und Verbände	10 Fälle

An den ersten drei Positionen hat es mithin keine Veränderungen gegeben: Unangefochtener Spitzenreiter bei den Eingaben ist nun schon seit mehreren Jahren die Videoüberwachung, gefolgt von Eingaben zu Betroffenenrechten, insbesondere zur Auskunft nach § 34 BDSG, und Eingaben im Bereich des Arbeitnehmerdatenschutzes.

Bei deutlich mehr als jedem dritten Aufsichtsfall (ca. 36 %, letzter Berichtszeitraum: 38 %) habe ich im Ergebnis einen Verstoß gegen datenschutzrechtliche Vorschriften feststellen müssen. Die bereichsspezifische Auswertung zeigt dabei bei den ersten beiden Positionen eine Übereinstimmung mit den eingegangenen Eingaben, wobei der prozentuale Anteil festgestellter Verstöße jedenfalls in diesen beiden Fällen etwas zurückgegangen ist. In Bezug auf die absoluten Zahlen ergibt sich im Hinblick auf die bei meinen Kontrollen festgestellten Verstöße folgendes Ranking:

1.	Videoüberwachung	42 Verstöße (42 %)
2.	Betroffenenrechte	26 Verstöße (38 %)
3.	Datengeheimnis	10 Verstöße (---)
4.	Datenschutzbeauftragter	7 Verstöße (---)
5.	Internet	7 Verstöße (37 %)

Die bezüglich der betrieblichen Datenschutzbeauftragten festgestellten Verstöße betrafen fast ausnahmslos die Bestellungspflicht. Ebenso wie beim Datengeheimnis ist dabei keine prozentuale Angabe möglich, da keine unmittelbar auf diese Punkte gerichteten

Kontrollen durchgeführt worden sind, sondern es sich dabei regelmäßig um Nebenerkenntnisse aus mit einem anderen Schwerpunkt durchgeführten Überprüfungen gehandelt hat (vgl. dazu 8. TB, Punkt 8.16.1).

Soweit es sich bei den festgestellten Datenschutzverstößen um allgemein interessierende Fallgestaltungen handelt, die in den vorangegangenen Tätigkeitsberichten noch nicht thematisiert worden sind oder einer nochmaligen erweiterten Erörterung bedürfen, werden diese unter Punkt 8 näher beschrieben.

2.4 Beratungstätigkeit

Die Aufsichtsbehörde berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse (§ 38 Absatz 1 Satz 2 BDSG).

Dazu korrespondierende Vorschriften sind in § 4g Absatz 1 Sätze 1 bis 3 BDSG:

Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er kann die Beratung nach § 38 Absatz 1 Satz 2 in Anspruch nehmen.

und in § 4d Absatz 6 Satz 3 BDSG enthalten:

Bei der Durchführung der Vorabkontrolle hat sich der Beauftragte für den Datenschutz in Zweifelsfällen an die Aufsichtsbehörde zu wenden.

Mit 440 Anfragen sind dieses Mal mehr als dreimal so viel Beratungsanliegen an mich herangetragen worden wie noch im vorangegangenen Berichtszeitraum. Dies entspricht absolut einem Anstieg des Beratungsvolumens auf 324% des vorhergehenden Berichtszeitraums, relativ (hochgerechnet auf den besser vergleichbaren Zweijahreszeitraum) bedeutet das sogar einen Anstieg auf 564%, mithin das 5,5-fache. Dies hat mich – ebenso wie die Aufsichtsbehörden in den anderen Bundesländern – zwar nicht unbedingt überrascht, jedoch zweifelsfrei überfordert. Mit den vorhandenen personellen Ressourcen war ich schon im letzten Berichtszeitraum absolut am Limit, d. h. es ist mir (bis heute) praktisch unmöglich gewesen, alle diese Anfragen vollumfänglich und zeitnah zu beantworten. Die Politik hatte es leider versäumt, hier vorausschauend Vorsorge zu treffen und mir die immer wieder eingeforderten zusätzlichen Stellen rechtzeitig zuzugestehen.

Berichtszeitraum / Beratungsfälle	01.01.09 31.12.10	01.01.11 31.03.13	01.04.13 31.03.15	01.04.15 31.03.17	**01.04.17 24.05.18**
absolut	87	122	146	136	**440**
relativ (Zweijahreszeit-raum)	87	108*	146	136	**767***

*Vergleichswert (Zweijahreszeitraum), rechnerisch ermittelt!

Die Vielzahl telefonischer Anfragen, die auch sofort durch telefonische Beratung erledigt werden konnten, ist in diesen Zahlen noch nicht einmal enthalten – hierüber wurde keine Statistik geführt.

Es liegt auf der Hand, dass der weitaus größte Teil des Zuwachses an meiner Beratungstätigkeit der zum Ende des Berichtszeitraums anstehenden Umstellung auf die Datenschutz-Grundverordnung zuzuschreiben ist. Bereits im Januar 2018 war ein deutlich verstärktes Beratungsaufkommen festzustellen, welches sich dann zum Mai hin exorbitant steigerte – allein im Mai 2018 sind mehr als 200 Anfragen per Post oder E-Mail bei mir eingegangen.

Schwerpunkte bei diesen bereits auf die DSGVO bezogenen Anfragen waren folgende Themen:

- Verpflichtung zur Benennung eines betrieblichen Datenschutzbeauftragten insbesondere bei Arztpraxen, Apotheken und Vereinen
- Vollzug der Meldepflicht in Bezug auf benannte Datenschutzbeauftragte
- Umsetzung der Informationspflichten nach Artikel 13 DSGVO, insbesondere auch im Hinblick auf die Bestätigung der Kenntnisnahme
- Einordung als Auftragsverarbeiter nach Artikel 28 DSGVO in verschiedenen Fallgestaltungen, u. a. bei Steuerberatern und medizinischen Laboren
- datenschutzkonforme Gestaltung von Websites
- Notwendigkeit des Einholens von Einwilligungen gemäß Artikel 7 DSGVO
- Umsetzung der DSGVO in Klein- und mittelständischen Unternehmen
- neue datenschutzrechtliche Anforderungen an Vereine
- Notwendigkeit einer Datenschutz-Folgenabschätzung
- Anfertigung und Verbreitung von Fotografien auf Sport- und anderen Veranstaltungen

Im Übrigen bildeten auch bei den Beratungen Zulässigkeitsfragen in Bezug auf (geplante) Videoüberwachungen einen wesentlichen Bestandteil meiner Aufsichtstätigkeit im Berichtszeitraum. Diesbezüglich erreichten mich insgesamt 25 Anfragen, d. h. fast genauso viel wie im vorangegangenen 10 Monate längeren Berichtszeitraum. In Bezug auf die verbleibenden Beratungsfälle waren keine besonderen Schwerpunkte feststellbar.

2.5 Prüfung den Datenschutz betreffender Verhaltensregeln von Berufsverbänden

Gemäß § 38a BDSG überprüft die Aufsichtsbehörde ihr von Berufsverbänden und anderen, bestimmte Gruppen verantwortlicher Stellen vertretenden Vereinigungen unterbreiteten Entwürfe für interne datenschutzrechtliche Verhaltensregeln auf ihre Vereinbarkeit mit dem geltenden Datenschutzrecht.

Im Berichtszeitraum sind an mich keine derartigen Anliegen herangetragen worden.

2.6 Genehmigung von Datenübermittlungen in Drittstaaten

Sofern personenbezogene Daten in Drittstaaten ohne angemessenes Datenschutzniveau übermittelt werden sollen und keiner der in § 4c Absatz 1 BDSG aufgeführten Ausnahmetatbestände erfüllt ist, kann die Aufsichtsbehörde entsprechende Datenübermittlungen genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist (§ 4c Absatz 2 BDSG).

Als Garantien für den Schutz des Rechts auf informationelle Selbstbestimmung als Teil des zivilrechtlichen Persönlichkeitsrechts waren der Aufsichtsbehörde dazu entsprechende Vertragsklauseln oder verbindliche Unternehmensregelungen vorzulegen. Im Berichtszeitraum sind an mich jedoch keine derartigen Anträge gestellt worden.

Wurden die von der Europäischen Kommission festgelegten Standardvertragsklauseln verwendet, war eine Genehmigung der Datenübermittlungen durch die Aufsichtsbehörde nicht mehr erforderlich. Nach wie vor gibt es drei derartige Standvertragsklauseln (siehe *http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm*):

- Standardvertragsklauseln für die Datenübermittlung (2001/497/EG)
- Alternative Standardvertragsklauseln für die Datenübermittlung (nicht anwendbar für Beschäftigtendaten) (2004/915/EG)
- Standardvertragsklauseln für Auftragsdatenverarbeitung

(2010/87/EU)

Bei einer Reihe von Staaten hat die Europäische Kommission bereits formell festgestellt, dass dort ein im Sinne des § 4b BDSG angemessenes Datenschutzniveau gegeben ist. Zu diesen Ländern zählen Andorra, Argentinien, die Färöer, Guernsey, Israel, die Isle of Man, die Vogtei Jersey, Kanada (mit Einschränkungen), Neuseeland, die Schweiz, Uruguay sowie die USA (Privacy Shield), vgl. dazu *https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.*

Bei einer Übermittlung in diese Länder bzw. an die den jeweiligen Regelungen unterfallenden Stellen (Kanada, USA) ist ebenso wie bei der Verwendung der Standardvertragsklauseln keine Genehmigung durch die Aufsichtsbehörde erforderlich.

Die Liste der US-Organisationen, die sich beim US-Handelsministerium durch Selbstzertifizierung zu den Grundsätzen des Privacy Shield bekannt haben, kann unter folgendem Link abgerufen werden: https://www.privacyshield.gov/list.

Im Vergleich zum vorangegangenen Berichtszeitraum sind keine Angemessenheitsentscheidungen zu weiteren Ländern getroffen worden; diesbezügliche Vorbereitungen liefen allerdings in Bezug auf Südkorea und Japan.

2.7 Ausgewählte Sachverhalte

2.7.1 Videoüberwachung

2.7.1.1 Dashcams

Innerhalb des Themenkomplexes Videoüberwachung entwickelt sich die Dashcam Problematik zunehmend zu einem Schwerpunkt. Nachdem ich bereits in den letzten beiden Tätigkeitsberichten (7./8. Tätigkeitsbericht, jeweils Punkt 8.1.1) über meine Bewertung informiert hatte, hat sich die diesbezügliche – bislang doch recht differenzierte – (zivilrechtliche) Rechtsprechung durch ein klarstellendes Urteil des Bundesgerichtshofes in einer die Position der Datenschutzaufsichtsbehörden stärkenden Weise entwickelt und gefestigt. Der BGH hat mit Urteil vom 15. Mai 2018 (VI ZR 233/17, juris) entschieden, dass

a. die permanente und anlasslose Aufzeichnung des Verkehrsgeschehens nicht mit den datenschutzrechtlichen Regelungen des Bundesdatenschutzgesetzes vereinbar,
b. die Verwertung von Dashcam-Aufzeichnungen, die ein Unfallbeteiligter vom Unfallgeschehen gefertigt hat, als Beweismittel im Unfallhaftpflichtprozess aber dennoch zulässig ist.

Diese Entscheidung mag dem ersten Eindruck nach widersprüchlich sein, trägt jedoch dem Umstand Rechnung, dass dem unstreitig bestehenden Gefährdungspotential des Einsatzes anlasslos und permanent aufzeichnender Videokameras nicht mit Beweisverwertungsverboten im Zivilprozess zu begegnen ist. Dies ist vielmehr Aufgabe des Datenschutzrechts (Rz. 52 des Urteils). Nach Auffassung des BGH bestehen die Risiken eines zunehmenden Einsatzes solcher Kameras in Privatfahrzeugen insbesondere in der Gefahr der Herstellung individueller Bewegungs- und Verhaltensprofile. Durch die Weiterleitung, Zusammenführung und anschließende Auswertung, unterstützt durch bereits heute verfügbare Gesichtserkennungssoftware, lassen sich die Aufzeichnungen einzelner Verkehrsteilnehmer zu aussagefähigen Profilen der betroffenen Person verdichten (aaO). Auf dieser Grundlage könnten Aussagen darüber gewonnen werden, wann sich Betroffene an welchen Orten aufgehalten, wohin und in welcher Begleitung, ggf. mit welchem Verkehrsmittel, sie sich bewegt haben (Rz. 26 des Urteils). Verschwindet der Betroffene aus dem Erfassungsbereich einer Kamera, könnte die nächste problemlos übernehmen.

Der BGH hat sich insoweit klar gegen die – auch von mir immer wieder festgestellte – ausufernde permanente und anlasslose Aufzeichnung des Verkehrsgeschehens positioniert. Eine solche ständige Aufzeichnung des gesamten Geschehens auf und entlang der Fahrstrecke ist zur Wahrnehmung berechtigter Interessen eines Fahrzeugführers weder nach § 28 Absatz 1 Satz 1 Nummer 2 noch nach § 6b Absatz 1 Satz 1 Nummer 3 BDSG erforderlich und deshalb gemäß § 4 Absatz 1 BDSG auch nicht zulässig (Rz. 19 des Urteils).

Beide Erlaubnissätze verlangen die Erforderlichkeit der Datenerhebung im Sinne eines zumutbaren mildesten Mittels, denn es ist technisch möglich, die dauerhafte Aufzeichnung zu vermeiden und lediglich eine kurzzeitige anlassbezogene Speicherung im Zusammenhang mit einem Unfallgeschehen vorzunehmen. Werden solche technischen Möglichkeiten zum Schutz der Persönlichkeitsrechte Dritter („Privacy by Design“) nicht genutzt, führt das dazu, dass die schutzwürdigen Interessen der anderen Verkehrsteilnehmer mit ihrem Recht auf informationelle Selbstbestimmung das Aufzeichnungsinteresse des Kamerabetreibers überwiegen (Rz. 25 des Urteils). Im Umkehrschluss hat der BGH damit zugleich Möglichkeiten eines rechtskonformen Einsatzes von Dashcams aufgezeigt. Werden diese lediglich im Sinne einer „Crashcam“ betrieben, dürften die datenschutzrechtlichen Bedenken jedenfalls vom Grundsatz her nicht mehr bestehen.

Dashcams werden nach meinen Erfahrungen allerdings zumeist so betrieben, dass einzig die Kapazität des jeweiligen Speichermediums das die Aufzeichnungsdauer begrenzende Kriterium ist. Videoaufzeichnungen mit einer Gesamtlänge von 10 Stunden und mehr sind keine Seltenheit; die Länge der einzelnen Videosequenzen reicht im Regelfall

von drei bis fünf Minuten – 30 Sekunden sind die Ausnahme; geringere Längen habe ich noch nicht feststellen können.

Ein solcher Betrieb einer Dashcam ist also zweifellos rechtswidrig und wird von mir im Rahmen diesbezüglicher Bußgeldverfahren verfolgt (Satz Punkt 13). Der BGH hat auf diese Ahndungsmöglichkeiten ausdrücklich hingewiesen: Verstöße gegen die datenschutzrechtlichen Bestimmungen können mit – hohen (vgl. dazu PM 88/2018 des BGH) – Geldbußen geahndet und vorsätzliche Zuwiderhandlungen gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht als Straftat verfolgt werden (Rz. 53 des Urteils). Darüber hinaus kann die Aufsichtsbehörde im Rahmen von § 38 Absatz 5 BDSG mit Maßnahmen zur Beseitigung von Datenschutzverstößen steuernd eingreifen (aaO).

Ich kann daher an dieser Stelle nur appellieren, sich gut zu überlegen, ob sich die Anschaffung einer Dashcam tatsächlich lohnt und ob die in Aussicht genommene Kamera überhaupt im Sinne des BGH-Urteils zu betreiben ist, d. h. die entsprechenden Betriebsmodi bereitstellt. Die von den Aufsichtsbehörden bei rechtswidrigem Betrieb von Dashcams festgesetzten Bußgelder jedenfalls könnten den ggf. in einem Zivilprozess erstrittenen finanziellen Vorteil auch wieder aufheben; höher als die Anschaffungskosten sind sie allemal.

Unabhängig davon gilt es auch einen weiteren Punkt zu überlegen: Dashcam-Aufzeichnungen können auch gegen den Betreiber verwendet werden. Wer garantiert, dass die Aufzeichnungen tatsächlich die eigene Unschuld beweisen? Wer garantiert, dass die Dashcam nicht im Falle eines Unfalls als Beweismittel sichergestellt oder gegen den Willen des Betreibers beschlagnahmt wird? Und schließlich ist noch zu berücksichtigen, dass permanente anlassfreie Dashcam-Aufzeichnungen auch ungewollte Einblicke in die Privatsphäre, teilweise sogar in die Intimsphäre des Betreibers ermöglichen, sei es im Rahmen von Unfallauswertungen, sei es bei Auswertungen nach einer Beschlagnahme wegen eines datenschutzwidrigen Betriebs Die Bußgeldbehörde muss sich natürlich die Aufzeichnungen anschauen, um den Tatnachweis zu führen; sie muss angeben, wann und wo die Dashcam genutzt worden ist. Dabei werden schnell Verhaltensmuster und Gewohnheiten erkennbar, Verkehrsordnungswidrigkeiten sichtbar, können Verwandte zugeordnet werden und dergleichen mehr. Besonders kritisch kann es werden, wenn in der Dashcam auch ein Mikrofon vorhanden und aktiviert war. Denn dann kommen zu rechtswidrigen Bildaufnahmen auch noch rechtswidrige Audioaufnahmen hinzu, sei es von Mitfahrern oder von Gesprächspartnern von über die Freisprechanlage geführten Telefonaten. Da steht dann plötzlich auch der Verdacht einer Straftat nach § 201 StGB im Raum. Es ist mir noch nicht untergekommen, dass ein Dashcam-Betreiber seine Mitfahrer oder Personen, mit denen er telefoniert hat, auf die Tatsache der Gesprächsaufzeichnung hingewiesen hat.

Darüber hinaus auch für andere Fallkonstellationen noch recht interessant und in Bezug auf immer wiederkehrende Gegenargumente bedeutsam sind einige weitere klarstellende Feststellungen bzw. Aussagen im oben benannten BGH-Urteil:

1. Videoaufnahmen von Fahrzeugen enthalten personenbezogene Daten im Sinne des § 3 Absatz 1 BDSG, also Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person, hier des Fahrzeughalters und ggf. auch des Fahrzeugführers. Für die Bestimmbarkeit genügt eine indirekte Identifizierbarkeit, etwa über eine Halterabfrage anhand des Fahrzeugkennzeichens (Rz. 21 des Urteils).
2. Mit der EuGH-Entscheidung vom 11. Dezember 2014 in der Sache Ryneš (C-212/13, juris) ist geklärt, dass eine Videoüberwachung, die sich auch nur teilweise auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre desjenigen gerichtet ist, der die Daten auf diese Weise verarbeitet, nicht als eine ausschließlich persönliche oder familiäre Tätigkeit angesehen werden kann (Rz. 22 des Urteils).
3. Nach diesem EuGH-Urteil stellt eine Überwachung mittels einer Videoaufzeichnung auf einer kontinuierlichen Speichervorrichtung zudem eine automatisierte Verarbeitung personenbezogener Daten dar (Rz. 22 des Urteils).
4. Im Sinne der §§ 6b und 28 BDSG kommt eine Güterabwägung zugunsten eines Dashcam-Betreibers überhaupt nur in Betracht, wenn eine Dashcam tatsächlich Datenschutzmechanismen zur Begrenzung auf kurzzeitige, anlassbezogene Aufzeichnungen aufweist und diese auch genutzt wurden (Rz. 25, 26 des Urteils). Ein Dashcam-Betreiber kann sich also nicht darauf berufen, dass das von ihm genutzte Gerät keine solchen Funktionalitäten aufweist.
5. Die Vorlage einer Videoaufnahme als Beweismittel bei Gericht oder der Bußgeldbehörde und ihre diesbezügliche Verwertung erfüllen grundsätzlich nicht den Tatbestand des „Verbreitens“ im Sinne von § 22 KunstUrhG (Rz. 57 des Urteils). Anders wäre es natürlich, wenn der Kamerabetreiber Teile der Aufnahmen im Internet verbreitet.

2.7.1.2 Aussichtsplattform

Nach dem Aufstieg auf eine denkmalgeschützte Aussichtsplattform musste ein Besucher unvermittelt feststellen, dass oberhalb der Plattform gleich mehrere Videokameras installiert waren, die dem Augenschein nach nicht nur die Plattform selbst, sondern das gesamte Areal um den Aussichtspunkt herum überwachten. Seiner Schilderung nach hatte es vor dem Aufstieg keinerlei Hinweise auf die Videoüberwachung gegeben; weder als Piktogramm, noch auf den ausgehändigten Flyern oder den Eintrittskarten.

Zu touristischen Zwecken betriebene Aussichtsplattformen sind öffentlich zugängliche Räume im Sinne von § 6b BDSG. Dass für den Aufstieg der Erwerb einer Eintrittskarte erforderlich ist, steht dem prinzipiell nicht entgegen. Auch entgeltpflichtige Bereiche fallen unter den Begriff des öffentlichen Raums im Sinne der Vorschrift (vgl. Scholz in: Simitis, BDSG 8. Aufl., Rdnr. 45 zu § 6b).

Nach § 6b Absatz 1 BDSG ist die (bloße) Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Eine (darüber hinausgehende) Videoaufzeichnung ist nach § 6b Absatz 3 BDSG nur zulässig, wenn auch diese zur Zweckerreichung erforderlich ist und auch insoweit keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Soweit der Betreiber für die Videoüberwachung präventive Zwecke angegeben hatte, war eine Aufzeichnung nicht erforderlich (§ 6b Absatz 3 BDSG). Dafür würden letztendlich sogar bloße Attrappen ausreichen. Wesentlich bedeutsamer wäre insoweit ein deutlicher, nicht zu übersehender Hinweis auf die Videoüberwachung gewesen (§ 6b Absatz 2 BDSG). Der unmittelbar vor Erreichen der Plattform auf einem groß mit „Lebensgefahr!“ überschriebenen Schild am Ende enthaltene Hinweis „Plattform wird videoüberwacht“ war insoweit jedenfalls nicht ausreichend. Er hob sich in keiner Weise von den übrigen Informationen ab und wird daher erfahrungsgemäß allzu leicht übersehen, ganz abgesehen davon, dass derjenige, der den doch recht anstrengenden Aufstieg bis kurz vor die Plattform bewältigt hat, an dieser Stelle wohl selbst dann nicht mehr umkehren würde, wenn er sich durch die Videoüberwachung in seinem Persönlichkeitsrecht beeinträchtigt fühlt. Auch für die darüber hinaus angegebenen Zwecke der Besuchersteuerung war eine Aufzeichnung nicht erforderlich. Hierfür genügt es regelmäßig, wenn das Kassenpersonal einen Monitor zur Beobachtung der Besucherdichte auf der Plattform zur Verfügung hat (§ 6b Absatz 1 Nummer 3 BDSG).

Im Ergebnis habe ich keine Zulässigkeit für eine Videoaufzeichnung gesehen. Es fehlte insoweit bereits an der Erforderlichkeit der Aufzeichnung zum Erreichen der verfolgten Zwecke (§ 6b Absatz 3 BDSG). Als milderes, weniger in das Persönlichkeitsrecht der Betroffenen eingreifendes Mittel genügt das bloße Monitoring. Soweit – wie mir der Betreiber auch mitgeteilt hatte – die Aufzeichnungen in der Vergangenheit auch dazu genutzt worden waren, um Lehrern das unangemessene Verhalten der von ihnen betreuten Schüler auf der Plattform zu verdeutlichen, konnte dies eine Aufzeichnung gleichfalls nicht rechtfertigen. Für das ordnungsgemäße Verhalten der Schüler auf der Aufsichtsplattform haben die begleitenden Lehrer bzw. Aufsichtspersonen selbst zu sorgen.

Letztendlich verdeutlichen derartige Vorfälle auch nur, dass die Aussichtsplattform nicht ausreichend deutlich als videoüberwacht gekennzeichnet war.

Ich habe der verantwortlichen Stelle daher aufgegeben, die Aufzeichnungsfunktion zu deaktivieren und die vorhandenen Aufzeichnungen zu löschen. Gegen die Einrichtung einer anlassbedingten Möglichkeit der temporären Aktivierung der Aufzeichnungsfunktion durch das Kassen- bzw. Einlasspersonal bestehen keine Einwände.

Soweit der Petent auch die Beobachtung der Umgebung der Aussichtsplattform vermutet hatte, konnte ich ihn beruhigen. Allein die Fokussierung der Kameras auf den Nahbereich der Aussichtsplattform verhinderte dies; abgesehen davon ermöglichte der Kamerawinkel lediglich (unscharfe) Horizontaufnahmen.

2.7.1.3 Schulcampus

Man stelle sich einen (privat betriebenen) Schulcampus vor, der an drei Seiten durch Schulgebäude und an der vierten Seite durch eine – insbesondere dem Fußgänger- und Fahrradverkehr dienende – Anliegerstraße mit seitlich angeordneten Parkflächen für das Schulpersonal begrenzt wird.

Nach einem Hinweis eines Passanten, dass an den Schulgebäuden installierte Videokameras auch auf diese Anliegerstraße gerichtet seien, habe ich mir selbst einen Eindruck von den örtlichen Gegebenheiten verschafft. Nach meinen eigenen Feststellungen wurde das gesamte Außengelände des Campus einschließlich der Anliegerstraße und den dortigen Parkflächen wohl annähernd flächendeckend mit Videokameras überwacht.

Das Gelände des Schulcampus war frei zugänglich, die Rechtmäßigkeit einer Videoüberwachung daher an § 6b BDSG zu messen. Gemäß dessen Absatz 1 Nummer 2 und 3 sowie Absatz 3 ist eine Beobachtung und Aufzeichnung in öffentlich zugänglichen Räumen mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für die Einordnung videoüberwachter Bereiche als öffentlich zugänglich und damit für die Anwendbarkeit des § 6b BDSG ist es unbeachtlich, in wessen Eigentum sich die überwachten Bereiche befinden. Vielmehr ist entscheidend, dass die betreffenden Bereiche von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten und genutzt werden können (Scholz in: Simitis, BDSG 8. Aufl., Rdnr. 42 zu § 6b). Die vom Betreiber offiziell genutzte Bezeichnung „Campus …“ unterstrich diese allgemeine Betretungsmöglichkeit. Die äußere Gestaltung des Geländes gab auch keinerlei Anlass, davon auszugehen, dass es sich um keinen solchen Bereich handeln könnte, d. h. der Betreiber hatte diesen Zugang selbst eröffnet.

Die Schüler konnten sich auf dem Campusgelände tatsächlich nicht bewegen, ohne dabei nicht ständig von einer Videokamera erfasst zu werden. Soweit als Zweck der Videoüberwachung die Prävention gegen Sachbeschädigungs- und Diebstahlsdelikte angegeben worden waren, wären bloße Attrappen vollkommen ausreichend gewesen. Soweit darüber hinaus auch eine Beweisführung im Schadensfall beabsichtigt worden war, wäre eine Aufzeichnung dafür zwar geeignet, jedoch jedenfalls tagsüber, insbesondere während des Schulbetriebs, in jedem Fall unverhältnismäßig gewesen, zumal es insoweit bekanntermaßen auch mildere Mittel wie eine entsprechende Aufsicht im Hofbereich gegeben hat. Zudem bestand die Möglichkeit, das Hofgelände durch geeignete Zutrittskontrollmaßnahmen für Dritte abzusperren. Vom Betreiber angeführte allgemeine Kriminalitätsstatistiken für ein ganzes Stadtgebiet können eine Videoüberwachung einer konkreten Liegenschaft grundsätzlich nicht begründen. Auch die von ihm angegebenen zwei Schadensfälle konnten eine Rundumüberwachung (zeitlich und örtlich) nicht rechtfertigen, zumal sie sich bezeichnender Weise am Wochenende bzw. in den Nachtstunden ereignet hatten. Alles in allem fehlte es also schon an der Erforderlichkeit zur Zweckerreichung.

Auch die Überwachung des Parkplatzbereiches begegnete erheblichen datenschutzrechtlichen Bedenken, da dieser Bereich auch von zahlreichen Passanten (Fußgänger, Radfahrer) genutzt wurde. Die diesbezügliche Videoüberwachung beschränkte sich keinesfalls nur auf die (nur) angemieteten Stellflächen, sondern erstreckte sich auch auf Bereiche (Grünflächen) außerhalb des Parkplatzes und den gesamten Durchgangsverkehr auf der Straße. Bezüglich der über die Parkflächen hinausgehenden Bereiche konnte der Betreiber noch nicht einmal ein berechtigtes Überwachungsinteresse geltend machen. Für die Stellflächen selbst hatte er zudem auch keine konkrete Gefährdungslage dargelegt, sondern wiederum nur auf die allgemeine Kriminalitätsstatistik verwiesen. Nur weil die Kriminalitätsstatistik zeigt, dass es bei geparkten Fahrzeugen immer wieder auch Einbruchs- und Sachbeschädigungsdelikte gibt, kann nicht jeder Ort, an dem ein Fahrzeug des Schulpersonals abgestellt wird, mittels Video überwacht werden. Dieser Logik folgend müsste jede Parkfläche in der Stadt videoüberwacht werden. Üblicherweise beschränkt sich die Nutzung dieser Stellflächen ohnehin auf die deutlich weniger gefährdeten Zeiten des Schulbetriebs. Auch insoweit fehlt es also an der Erforderlichkeit der Videoüberwachung.

Unbeschadet der vorstehenden Ausführungen standen auch schutzwürdige Betroffeneninteressen (insbesondere der Mitarbeiter und der Schüler) der Videoüberwachung des Schulcampus entgegen. Diese wurden bei jedem Aufenthalt im Hofbereich oder bei dessen Durchquerung von den Videokameras erfasst, ohne dass sie dies umgehen (Pflicht zur Erbringung der Arbeitsleistung bzw. verpflichtende Teilnahme am Schulbetrieb) oder die nachfolgende Verarbeitung oder Nutzung der über sie erstellten Videoauf-

zeichnungen beeinflussen oder verhindern konnten. Der Hofbereich war offensichtlich auch geradezu darauf ausgelegt, dass Mitarbeiter und Schüler dort ihre Pausenzeiten verbringen können. Die Gestaltung mit Wasserläufen, Trink- und Springbrunnen sowie zahlreichen Sitzgelegenheiten lud regelrecht dazu ein. Die Argumentation des Betreibers, dass es sich dabei nur um eine Verkehrsfläche handele, habe ich daher zurückgewiesen. An Orten, an denen Betroffene ihre Pausen oder auch (Teile) ihre(r) Freizeit verbringen (etwa nach Schulschluss), ist deren Interesse, dabei, also bei der Wahrnehmung von Freiheitsrechten, nicht von ihrem Arbeitgeber oder der Bildungseinrichtung per Video überwacht zu werden, als besonders schutzwürdig einzuordnen. Solche Orte sind – jedenfalls während dieser Zeiten – tatsächlich auch keine Orte mit einem tatsächlich erhöhten Gefährdungspotential für die Vermögenswerte des Eigentümers. Unter dem Druck der offensichtlichen Überwachung, deren tatsächlicher Umfang für die Betroffenen nicht ersichtlich und die vom Betreiber auch in keiner Weise kommuniziert worden war, werden sie ihr Verhalten bewusst oder unbewusst darauf einstellen und sind damit in der freien Entfaltung ihrer Persönlichkeit beeinträchtigt. Dies gilt weiterhin auch deshalb, weil die Aufzeichnung zunächst rein präventiv erfolgte, d. h. die Mitarbeiter und Schüler überhaupt keinen Anlass für eine Überwachung gegeben hatten, sondern diese in erster Linie gegen eine Gefährdung durch Dritte und in Zeiten außerhalb des Schulbetriebs bzw. der Arbeitszeiten gerichtet war.

Mit der Überwachung des Parkplatzbereiches griff der Betreiber darüber hinaus in besonderem Maße in die Rechte von Personen (Fußgänger, Radfahrer) ein, die mit ihm in keiner Weise etwas zu tun hatten, sondern lediglich den öffentlichen Weg entlang der Stellflächen nutzten, um an dahinterliegende Gebäude oder Erholungsflächen zu gelangen. Das verfassungsmäßige Recht auf informationelle Selbstbestimmung verbürgt das Recht des Einzelnen, sich insbesondere in der Öffentlichkeit frei und ungezwungen bewegen zu dürfen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden. Die sich daraus ergebenden schutzwürdigen Interessen der Betroffenen überwiegen dabei regelmäßig das Interesse des Betreibers an einer präventiven Überwachung seines Eigentums einerseits sowie der Beweissicherung im Fall von Sachbeschädigungen und Diebstählen andererseits. Auch nach der Rechtsprechung des Bundesgerichtshofs (Urteil vom 25. April 1995 – VI ZR 272/94, juris) haben Privatleute von notwehrähnlichen Situationen abgesehen nicht das Recht, durch Videoaufzeichnungen Passanten auf öffentlichen Wegen zu erfassen.

Im Ergebnis war der Betrieb der Videoüberwachungsanlage also in weiten Teilen unzulässig. Wäre der Betreiber seiner Pflicht zur Durchführung einer datenschutzrechtlichen Vorabkontrolle (§ 4d Absatz 5 Satz 1 BDSG) nachgekommen, hätte er dies selbst erkennen müssen. Eine solche Pflicht besteht nicht nur im Fall der Regelbeispiele des § 4d Absatz 5 Satz 2 BDSG, sondern immer dann, wenn automatisierte Verarbeitungen

besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Nach der diesbezüglichen Gesetzesbegründung (BT-Drs. 14/5793) liegen bei einer Videoüberwachung solche besonderen Risiken regelmäßig vor, wenn Überwachungskameras nicht punktuell, sondern durch die verantwortliche Stelle wie im vorliegenden Fall in größerer Zahl und zentral kontrolliert eingesetzt werden.

Um zu einem rechtskonformen Zustand zu gelangen, habe ich folgende Mindestmaßnahmen gefordert:

1. Die Videoüberwachung des Campusgeländes ist auf die Zeiten außerhalb des Schulbetriebes und der regulären Arbeitszeiten der Schulmitarbeiter sowie der dort ansässigen Unternehmen zu beschränken (Abend-/Nachtstunden, Wochenende).
2. Durch den Abbau von Kameras oder eine veränderte Ausrichtung ist sicherzustellen, dass sich die Überwachung auf das Campusgelände beschränkt, d. h. die Anliegerstraße einschließlich der Parkplätze nicht mehr überwacht wird.
3. Das Campusgelände ist deutlich als videoüberwacht zu kennzeichnen. Dabei ist insbesondere auch der Campus-Betreiber als verantwortliche Stelle anzugeben (§ 6b Absatz 2 BDSG).

2.7.1.4 Baustellenüberwachung

Aus ständig wiederkehrenden Presseveröffentlichungen ist allgemein bekannt, dass Bauunternehmen mit erheblichen Material-, Kraftstoff- und Maschinendiebstählen zu kämpfen haben. Es kommt daher wenig überraschend, dass diese ihre Baustellen zunehmend auch mit Videoüberwachungstechnik absichern. Grundsätzlich bestehen dagegen keine Einwände. Voraussetzung ist jedoch, dass derartige Videoüberwachungsanlagen datenschutzkonform betrieben werden. Dazu gehört u. a., dass

- die Videoüberwachung nur außerhalb des Baustellenbetriebs aktiv ist, mithin keine Überwachung der Bauarbeiter stattfindet,
- sich die Videoüberwachung auf die Baustelle selbst beschränkt und keine angrenzenden Nachbargrundstücke oder allgemein zugänglichen Bereiche erfasst und
- klar und deutlich auf die Videoüberwachung hingewiesen und dabei insbesondere die verantwortliche Stelle benannt wird.

Gerade Letzteres bereitet in der Praxis aber offensichtlich immer wieder Probleme. Mich haben mehrfach Beschwerden erreicht, bei denen zwar erkenn- (weithin sichtbare mobile Videoüberwachungstürme, z. B. Wellner-Boxen) oder spürbar (Gefährderansprachen über Lautsprecher) war, dass eine Videoüberwachung erfolgt, nicht aber, an wen man sich diesbezüglich für Rückfragen oder Beschwerden wenden konnte. Dabei

sollte eine deutliche Kennzeichnung – rechtzeitig vor Betreten des überwachten Baustellenbereichs – wegen der damit verbundenen Präventivwirkung doch auch für die Bauunternehmen von erheblichem Eigeninteresse sein.

Petenten monieren in diesem Zusammenhang regelmäßig die (unterstellte) Überwachung angrenzender öffentlicher Verkehrsbereiche. Oftmals liegen sie bei dieser Annahme aber falsch, weil man den Kameratürmen eben nicht ansehen kann, welche Bereiche sie tatsächlich absichern. Mitunter aber haben sie auch Recht. Ursache ist dabei zumeist die Umsetzung einer solchen Überwachungseinrichtung von einer Baustelle auf eine andere, ohne dass dabei die konkreten Systemeinstellungen für den Erfassungs- und Alarmierungsbereich an die neue Örtlichkeit angepasst werden. Dass dies unzulässig ist, bedarf sicher keiner größeren Erläuterung. Für die Absicherung einer Baustelle gegen Diebstahlsdelikte ist es ausreichend, wenn die eigentliche Baustelle überwacht wird. Es fehlt daher schon an der Erforderlichkeit der Überwachung angrenzender (allgemein zugänglicher) Bereiche, ganz abgesehen davon, dass schutzwürdige Betroffeneninteressen, nicht einer Videoüberwachung durch ein Bauunternehmen ausgesetzt zu werden, immer dann überwiegen, wenn sich die Betroffenen regelkonform außerhalb der Baustelle in öffentlichen Verkehrsbereichen bewegen (§ 6b Absatz 1 Nummer 2, 3, Absatz 3 BDSG).

2.7.1.5 Besondere Gefährdungslagen

Die zunehmende Gewaltbereitschaft in politisch extremen Kreisen äußert sich auch in Sachsen in häufigeren Anschlägen auf Partei- bzw. Bürgerbüros verschiedenster Couleur. Wände werden beschmiert, Farbtöpfe geworfen, Scheiben eingeschlagen, es kommt zu erheblichen Sachschäden. Bekennerschreiben kündigen weitere Anschläge an.

Zum Schutz der Büros installierte Videoüberwachungsanlagen beschränkten sich in der Vergangenheit auf die Innenbereiche bzw. die bloße Fassade der jeweiligen Gebäude, wobei angrenzende Verkehrsbereiche, insbesondere Gehwege, meist ausgenommen waren.

Die aus den eingangs geschilderten Geschehnissen abzuleitende erhöhte Gefährdungslage (vgl. dazu auch 8. TB, Punkt 8.1.4) führt nun – verständlicherweise – zu Bestrebungen, die Videoüberwachung weiter auszudehnen und so einerseits einen höheren Abschreckungseffekt zu erzielen und andererseits überhaupt die Chance zu haben, Beweismaterial in Bezug auf die vom öffentlichen Verkehrsraum aus agierenden Tätergruppen zu erlangen. Da sich die betroffenen Einrichtungen regelmäßig in den Innenstädten befinden und dort zumeist gut erreichbar direkt an viel frequentierten Straßen gelegen sind, bedingt eine solche Ausweitung der Videoüberwachung daher regelmäßig

und zwangsläufig auch eine Erfassung öffentlicher Verkehrsbereiche, insbesondere Gehwege.

Objektiv ist eine erhöhte Gefährdung politischer Objekte nicht von der Hand zu weisen. Die bekanntgewordenen Anschläge können bei der Interessenabwägung im Rahmen der Zulässigkeitsbetrachtung einer Videoüberwachungsanlage selbstverständlich nicht außer Betracht bleiben. Erst recht muss das gelten, wenn für das entsprechende Objekt eine Gefährdungseinschätzung des Landeskriminalamtes Sachsen und darauf aufbauend entsprechende baulich-technische Sicherheitsempfehlungen vorgelegt werden. In derartigen Konstellationen ist es daher durchaus möglich, vom Grundsatz, dass eine Videoüberwachung öffentlicher Verkehrsbereiche durch Private regelmäßig unzulässig ist, entsprechend abzuweichen. Dabei gelten folgende Maßgaben:

- Die Videoüberwachung von Außenbereichen wird auf die Abend- und Nachtstunden beschränkt; tagsüber dürfte die Gefahr eines (erneuten) Anschlags deutlich geringer sein.
- Auf der Grundlage des Hausrechts kann auch längerfristig zumindest ein schmaler Streifen (etwa 0,5 m) entlang der Gebäudeaußenfassade und beschränkt auf die Länge des jeweiligen Bürgerbüros per Video überwacht werden. Schutzwürdige Interessen Betroffener (Passanten) müssten unter diesen Umständen entsprechend zurücktreten (§ 6b Absatz 1 Satz 1 Nummer 2, Absatz 3 BDSG).
- Soweit dies im Einzelfall als nicht ausreichend zu betrachten sein sollte, wäre auf der Grundlage von § 6b Absatz 1 Satz 1 Nummer 3, Absatz 3 BDSG (Interessenabwägung) – jedenfalls temporär – auch eine darüber hinausgehende Videoüberwachung des Gehweges bis zu seiner Gesamtbreite begründbar. Passanten hätten dann zwar keine Möglichkeit mehr, dieser Videoüberwachung auszuweichen – zumal häufig auch ein Wechsel auf die gegenüberliegende Straßenseite nicht zumutbar ist –, jedoch wären sie nur kurz von der Videoüberwachung betroffen, was angesichts der besonderen Gefährdungslage für das Bürgerbüro jedenfalls vorübergehend hinzunehmen wäre.
- In jedem Fall sicherzustellen wäre – neben der zeitlichen Beschränkung – eine deutlich wahrnehmende Kennzeichnung des überwachten Bereiches (§ 6b Absatz 2 BDSG; dies hätte zugleich eine stark präventive Wirkung) sowie eine zeitnahe Löschung der erstellten Aufzeichnungen (max. Speicherdauer: 72 Stunden, § 6b Absatz 5 BDSG).

Gleichwohl gebe ich zu bedenken, dass eine solche Videoüberwachung die Wahrscheinlichkeit einer Täterermittlung erfahrungsgemäß kaum entscheidend erhöhen würde, denn potentielle Täter nutzen für derartige Anschläge üblicherweise die Dunkelheit und

werden daher – auch wegen der zusätzlich erfolgenden Maskierung – durch Videoaufzeichnungen im Regelfall kaum identifizierbar sein. Stattdessen erwarte ich eher, dass sich Unbeteiligte, also Passanten, an dieser Videoüberwachung des öffentlichen Raumes stören und dazu entweder beim jeweiligen Betreiber oder gleich bei mir vorstellig werden. Vor diesem Hintergrund sollten Vor- und Nachteile einer solchen Ausweitung der Videoüberwachung sorgfältig gegeneinander abgewogen werden.

2.7.1.6 Klingelkameras

Anfragen zu den Voraussetzungen eines datenschutzkonformen Betriebs einer Klingelkamera oder Videogegensprechanlage beantworte ich regelmäßig wie folgt:

- Die Kamera darf nur anlassbezogen durch das Klingeln an der Tür aktiviert werden können.
- Die Kamera darf nur den unmittelbaren Eingangsbereich (Nahbereich) vor der Tür erfassen.
- Die Kamera muss nach kurzer Zeit automatisch wieder deaktiviert werden.
- Es darf keine Übertragung des Livebildes über das Internet erfolgen.
- Es darf keine Aufzeichnung der Bilder möglich sein.

Sind diese Voraussetzungen erfüllt, ist weder § 6b BDSG als Spezialvorschrift für die Beobachtung öffentlich zugänglicher Räume noch das BDSG im Übrigen einschlägig; insbesondere fehlt es insoweit an einer Beobachtung im Sinne des § 6b BDSG.

2.7.1.7 Umfeld von Fußballstadien

An den Eingängen eines Fußballstadions waren deutlich sichtbar Domekameras angebracht, deren aktuelle Einstellungen – wenn überhaupt – nur bei sehr genauer Betrachtung erkennbar waren, die aber wegen ihrer Installationsorte ohne Weiteres auch öffentliche Verkehrsbereiche vor dem Stadion erfassen konnten.

Nach § 6b Absatz 1 Nummer 3 und Absatz 3 BDSG wäre eine solche Videoüberwachung nur zulässig, wenn dies für berechtigte Interessen des Betreibers erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Bei öffentlichen Verkehrsbereichen ist aber regelmäßig von überwiegenden schutzwürdigen Interessen der Betroffenen (Passanten, Fahrzeugführer), während der Nutzung solcher Bereiche nicht von nicht-öffentlichen Stellen überwacht zu werden, auszugehen.

Im Rahmen eines daraufhin durchgeführten Kontrollbesuches ist mir durch den Stadionbetreiber mitgeteilt worden, dass es sich bei den betreffenden Kameras um steuerbare

Videoüberwachungstechnik handelt, die im Zuge von Veranstaltungen in dem Stadion entweder von der Polizei selbst oder ausnahmsweise vom jeweiligen Veranstalter genutzt und insbesondere auch bedient wird. Zweck der Erfassung der vor dem Stadion gelegenen Verkehrsbereiche seien die Besucherstromsteuerung und die Freihaltung von Fluchtwegen sowie der Feuerwehrzufahrten.

In erster Linie würden die Videokameras natürlich bei Fußballspielen genutzt. Nach Ende des Spiels verblieben die Kameras in der letzten durch die Polizei benutzten Ausrichtung; allerdings könnten auch diesbezügliche Voreinstellungen, so genannte Pre-Sets festgelegt werden. Dies war vorliegend offensichtlich unterblieben, so dass es mehr oder weniger dem Zufall bzw. den mit der Bedienung beauftragten Polizeibeamten überlassen war, in welcher Stellung die Kameras bis zum nächsten Einsatz verblieben. Ich habe mich daraufhin mit dem Stadionbetreiber für die potentiell auch öffentliche Verkehrsbereiche erfassenden Videokameras auf datenschutzgerechte Grundeinstellungen verständigt, die der Betreiber dann anschließend auch technisch so eingerichtet hat. Zugleich hat er die Polizei auf deren zwingende Nutzung nach Veranstaltungsende hingewiesen. Nachdem die Polizei dies auch verbindlich zugesagt hat, ist nunmehr gewährleistet, dass außerhalb von Veranstaltungen, bei denen ohnehin die Polizei die Verfügungsgewalt über die Videoanlage hat, keine öffentlichen Verkehrsräume mehr überwacht werden.

Auch die Aufschaltung der Kamerabilder auf das vor Ort tätige Wachunternehmen begegnet (nunmehr) vom Grundsatz her keinen Bedenken mehr. Diesbezüglich hat der Stadionbetreiber sicherzustellen, dass der Wachdienst keinen Zugriff auf die Archivbilder hat und ihm ein Einschwenken der Kameras auf öffentliche Verkehrsbereiche (technisch) nicht möglich ist. Der am Empfangstresen platzierte Monitor ist durch geeignete technische und organisatorische Maßnahmen (Aufstellung, Spezialfolie für den Bildschirm, etc.) so zu sichern, dass Dritte (Besucher) möglichst wenig Einblick in die Überwachungsbilder nehmen können.

2.7.1.8 Wohnungseigentumsanlage

Eine Wohnungseigentumsanlage wies fünf Hauseingänge, eine Tiefgaragenzufahrt sowie einen auch von außen zugänglichen Fahrradkeller, also insgesamt sieben jeweils videoüberwachte Zugangsmöglichkeiten, auf. Alle Zugänge waren als videoüberwacht gekennzeichnet. Die unter unterschiedlichen Adressen geführten Gebäudeteile waren im Keller- und Tiefgaragenbereich miteinander verbunden. Die Nutzer (Eigentümer bzw. Mieter) der ca. 80 Wohneinheiten konnten das Gebäude nur über einen der o. g. sieben Zugänge betreten oder verlassen und mussten damit zwingend eine der sieben installierten Videokameras passieren. Es gab keine nicht videoüberwachte Zugangsmöglichkeit. Ein Mieter bat mich dazu um datenschutzrechtliche Bewertung. Ihm war mitgeteilt

worden, dass die Videoüberwachung auf der Grundlage eines Wohnungseigentümergemeinschafts-Beschlusses erfolge.

Bei den überwachten Bereichen handelte es sich nicht um öffentlich zugängliche Räume. Von der Überwachung betroffen waren vielmehr ausschließlich Bereiche, die bestimmungsgemäß nur von Eigentümern und Mietern sowie deren Besuchern betreten werden sollen. Im Bereich der Treppenhäuser waren die Videokameras hinter den Haustüren angeordnet und erfassten den Hausflur im Erdgeschoss im Bereich vor den Fahrstühlen bzw. des Treppenaufgangs. Die Haustüren waren verschlossen und konnten nur durch berechtigte Personen geöffnet werden. Die Tiefgaragenzufahrt war mit keiner besonderen Zutrittssperre für Dritte versehen, bestimmungsgemäß aber nur für die Nutzer der nicht-öffentlichen Tiefgarage vorgesehen. Die Kamera zur Sicherung des Fahrradkellers befand sich zwar an der Gebäudeaußenfront, erfasste aber ausschließlich den Treppenabgang zum Fahrradkeller. Auch dieser Bereich war daher von der Bestimmung her nicht öffentlich. Im Ergebnis war die datenschutzrechtliche Beurteilung ausschließlich auf der Grundlage von § 28 BDSG vorzunehmen; § 6b BDSG als Spezialvorschrift für öffentlich zugängliche Bereiche hingegen war nicht einschlägig.

Von den Erlaubnistatbeständen des § 28 Absatz 1 Satz 1 BDSG kam vorliegend nur die Nummer 2 in Betracht. Nach dieser Vorschrift ist eine Videoüberwachung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen am Ausschluss der Videoüberwachung überwiegt. Diese Voraussetzung war vorliegend aber nicht erfüllt; der Betrieb der Videoüberwachungsanlage verstieß gegen diese Vorschrift und war damit rechtswidrig:

Als Überwachungsinteresse der Wohnungseigentümergemeinschaft war die Verhinderung und Aufklärung von Schadensfällen und kriminellen Handlungen gegen das Gemeinschaftseigentum, sprich der Eigentumsschutz, benannt worden. In der Vergangenheit habe es mehrere, konkret aufgelistete Einbruchversuche sowie Sachbeschädigungen (Graffiti) gegeben. Grundsätzlich ergab sich aus diesen Vorfällen ein berechtigtes Überwachungsinteresse, jedoch fehlte es an der Erforderlichkeit.

Das Kriterium der Erforderlichkeit bestimmt sich im Sinne einer Verhältnismäßigkeitsprüfung auf der Grundlage der Merkmale Geeignetheit, Erforderlichkeit und Angemessenheit. Eine Videoüberwachung ist nach meinen Erkenntnissen zunehmend kaum noch geeignet, einen tatsächlichen Beitrag zur Täterermittlung zu leisten, da sich die Täter darauf eingestellt haben und unter entsprechender Vermummung im Schutz der Dunkelheit agieren. Für den insbesondere gegen Gelegenheitstäter gerichteten präventiven Einsatz einer Videoüberwachungsanlage hingegen bedarf es weder einer Videoauf-

zeichnung noch überhaupt eines Kameraeinsatzes. Insoweit fehlte es an der Erforderlichkeit; die äußere Kennzeichnung der Zugangsbereiche als videoüberwacht war dafür bereits ausreichend, zumal der genaue Standort der Kameras in den Treppenhäusern von außen gar nicht erkennbar war und somit ohnehin nicht abgeschätzt werden konnte, ob und an welcher Stelle genau tatsächlich eine Videoüberwachung stattfindet. In Verbindung mit weiteren, für potentielle Einbrecher unattraktiven Maßnahmen wie der durchgängigen Beleuchtung der zurückgesetzten Hauseingänge, kann auch ohne tatsächliche Videoüberwachung ein durchaus wirksamer Einbruchsschutz erreicht werden, ohne dabei die einzelnen Wohnungsnutzer einem ständigen, unangemessenen Überwachungsdruck auszusetzen.

Darüber hinaus bestand zweifelsfrei ein sehr gewichtiges schutzwürdiges Interesse der Betroffenen am Ausschluss der Videoüberwachung. Die Herstellung von Bildnissen einer Person, insbesondere die Erstellung von Videoaufzeichnungen, noch dazu in privatem Bereich (Wohnumfeld), stellt einen schwerwiegenden Eingriff in das Persönlichkeitsrecht und Selbstbestimmungsrecht der Betroffenen dar. Das von den Artikeln 1 und 2 GG geschützte allgemeine Persönlichkeitsrecht umfasst auch die Freiheit von ungewünschter Kontrolle oder Überwachung durch Dritte. Für den Nutzer bzw. Mieter einer Wohnung betrifft dies nicht nur die Freiheit, die eigene Wohnung bzw. das Haus zu betreten oder zu verlassen, ohne dass dies der Vermieter bzw. Eigentümer jederzeit überwachen und die An- oder Abwesenheit des Mieters feststellen kann. Es beinhaltet ebenso die Freiheit, ungestört und unüberwacht Besuch empfangen zu können. Dem Vermieter bzw. Eigentümer steht grundsätzlich kein Recht zu, dauerhaft überprüfen zu können, welche Personen wann und wie oft bei einem Wohnungsnutzer zu Besuch gewesen sind.

In der Wohnanlage mit ihren 80 Wohneinheiten waren mehr als 100, sehr wahrscheinlich sogar mehr als 200 Personen von der Videoüberwachung betroffen. Davon waren die wenigsten zugleich auch Eigentümer, die insoweit für den diesbezüglichen Beschluss verantwortlich zeichneten. Alle diese Personen wurden bei jedem Betreten oder Verlassen des Hauses von einer Videokamera erfasst; eine Ausweichmöglichkeit bestand nicht. Durch die Aufzeichnungen wurde für einen Zeitraum von 40 Tagen lückenlos dokumentiert, wann welcher Bewohner in welcher Begleitung oder mit welchen Gegenständen das Haus betreten oder verlassen hatte. Die WEG war jederzeit in der Lage, durch die Auswertung der Aufzeichnungen die (regelmäßige) An- oder Abwesenheit einzelner Bewohner und deren Zeitdauer bzw. Tageslage feststellen zu können. Ebenso konnte durch gezielte Auswertungen nachvollzogen werden, welche Bewohner wann welchen Besuch empfangen haben oder regelmäßig empfingen.

Ob und in welchem Umfang die Fertigung und Aufzeichnung derartiger Bilder rechtswidrig und damit unzulässig ist, ist unter Würdigung aller Umstände des Einzelfalls und durch Vornahme einer unter Berücksichtigung aller rechtlich, insbesondere auch verfassungsrechtlich geschützten Positionen der Beteiligten durchgeführten Güter- und Interessenabwägung zu bestimmen. Gemessen an dem langen Zeitraum, der den aufgelisteten Vorfällen zugrunde lag und der Tatsache, dass es sich um eine sehr große Wohnanlage mit insgesamt fünf Gebäudeteilen handelt, ergaben sich aus den dargelegten Einbruchsversuchen und Graffiti-Schmierereien keine Anhaltspunkte für eine besondere Gefährdungslage. Auch die unmittelbare Umgebung stellte keinen besonderen Kriminalitätsschwerpunkt dar. Dass es gerade in Stadtgebieten immer wieder einmal zu derartigen Vorkommnissen kommt, kann praktisch nicht verhindert werden. Für den Bereich der Tiefgaragenzufahrt und des Zugangs zum Fahrradkeller gab es – außer zwei Graffiti-Fällen – überhaupt keine insoweit maßgeblichen Vorfälle.

Die Interessen der Wohnungseigentümergemeinschaft an der Erhaltung ihres Eigentums, die grundsätzlich von Artikel 14 GG geschützt werden, verdrängten die schutzwürdigen, hier besonders gewichtigen Interessen der Wohnungsnutzer unter diesen Umständen nicht. Durch die Kameras in den Treppenhäusern, vor dem Fahrradkeller und vor der Tiefgarage war es diesen – mangels Ausweichmöglichkeiten – unmöglich, unbeobachtet ihre Wohnung zu erreichen oder zu verlassen. Aus Sicht der Betroffenen fand daher eine Rundumüberwachung ihres sozialen Lebens statt. Unbeachtlich war, dass diese Überwachung der Betroffenen in ihrer Sozialsphäre von der WEG so nicht beabsichtigt war. Eine technische Überwachung in einem Bereich, in dem die Betroffenen ohne Weiteres eindeutig (als Hausbewohner) identifizierbar sind, ist dabei insbesondere geeignet, deren Verhalten zunächst nur unmerklich, auf Dauer aber nachhaltig in negativer Hinsicht zu verändern (Verunsicherung). Der damit verbundene erhebliche Eingriff in das Persönlichkeitsrecht der Mieter wäre nur dann gerechtfertigt, wenn die Überwachung zur Abwehr von schwerwiegenden Beeinträchtigungen der WEG erforderlich ist und eine drohende Rechtsverletzung nicht anderweitig zu verhindern gewesen wäre. Dies war hier aber nicht der Fall.

Es war nicht ersichtlich, dass sich die Wohnungseigentümergemeinschaft auch nur ansatzweise mit einer solchen Interessenabwägung befasst hatte. Die Beschlüsse der WEG enthielten lediglich die pauschale Behauptung, dass die Voraussetzungen des (nicht einschlägigen) § 6b BDSG eingehalten würden. Eine datenschutzrechtliche Vorabkontrolle (§ 4d Absatz 5 BDSG), die zu dem oben dargestellten Ergebnis hätte kommen müssen, war nicht durchgeführt worden, obwohl dies wegen der Rundumüberwachung der Mieter zwingend erforderlich gewesen wäre. Einen für eine solche Vorabkontrolle verantwortlichen Datenschutzbeauftragten (§ 4d Absatz 6 BDSG) hatte die WEG entgegen §

4f Absatz 1 Satz 6 BDSG nicht bestellt und die Videoüberwachung im Übrigen auch nicht der Aufsichtsbehörde gemeldet (§ 4d Absatz 1 BDSG).

Die Hausverwaltung hat auf meine Einwände entsprechend reagiert und die Videoüberwachungsanlage sofort außer Betrieb genommen. Noch vorhandene Aufzeichnungen sind gelöscht worden. Bei der nächsten Eigentümerversammlung sind die zur Videoüberwachung gefassten Beschlüsse wieder aufgehoben worden. Allerdings sollten die Videokameras – somit als Attrappen – an ihren Installationsorten verbleiben. Um den Überwachungsdruck von den Bewohnern zu nehmen, hat die Hausverwaltung ein entsprechendes Informationsschreiben erstellt und an alle Haushalte verteilt.

2.7.1.9 Storchennest

Ein mit einer 360°-Videokamera versehenes Storchennest hoch oben auf einem Schornstein eines Betriebsgeländes – die Dome-Kamera war an einer Stange befestigt und blickte schräg von oben auf das Nest – erweckte den Argwohn der umliegenden Anwohner. Sie vermuteten, dass mit der Webcam nicht nur die Störche, sondern auch sie selbst überwacht werden könnten. Das betreffende Unternehmen teilte mir mit, dass es beabsichtige, die Videokamera als Webcam zu betreiben und auf diese Weise der Öffentlichkeit eine Beobachtung der Storchenfamilie zu ermöglichen. Der mir dazu vorgelegte Screenshot zeigte allerdings, dass die Kamera auch Bereiche außerhalb des Betriebsgeländes, insbesondere auch eine Straße und ein Nachbargrundstück, mit erfasste. Dies war natürlich unzulässig.

Nach § 6b Absatz 1 Nummer 3 BDSG ist eine Videoüberwachung öffentlich zugänglicher Bereiche nur zulässig, wenn dies zur Wahrung berechtigter Interessen des Betreibers für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen (hier: Passanten) überwiegen. Das berechtigte Interesse mag vorliegend letztendlich im Bereich der Werbung gelegen haben, denn die Aufnahmen der Webcam sollten der Öffentlichkeit über die Unternehmenshomepage zugänglich gemacht werden. Da aber in allgemein zugänglichen Bereichen regelmäßig von überwiegenden schutzwürdigen Interessen der Betroffenen auszugehen ist, hatte ich insoweit erhebliche Bedenken in Bezug auf die Rechtmäßigkeit des für diese Webcam vorgesehenen Erfassungsbereiches. Das verfassungsmäßige Recht auf informationelle Selbstbestimmung verbürgt das Recht des Einzelnen, sich insbesondere in der Öffentlichkeit frei und ungezwungen bewegen zu dürfen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden. Die sich daraus ergebenden schutzwürdigen Interessen der Betroffenen überwiegen das – im Verhältnis dazu eher gering zu gewichtende – Interesse an der Eigenwerbung.

Das Unternehmen hat daraufhin die insoweit kritischen Bereiche in seiner Webcam als Privatzonen markiert (Schwärzungen), sodass ich im Ergebnis keine Einwände gegen den Betrieb der Webcam zur Storchenbeobachtung mehr hatte. Um weiteren bzw. wiederholten Anwohnerbeschwerden aus dem Weg zu gehen, habe ich empfohlen, die Kamera außerhalb der Storchensaison entweder zu demontieren oder aber (zu Kontrollzwecken der Betroffenen) weiterhin in Betrieb zu lassen und die Kamerabilder auch unverändert auf der Website bereitzustellen.

Anmerkung am Rande:

Im konkreten Fall scheint es sich um sehr „persönlichkeitsrechtsbewusste“ Störche gehandelt zu haben. Das mir vom Geschäftsführer überlassene Foto mit der Gesamtansicht des oberen Bereiches des Schornsteins zeigte einen Storch, der sich nicht etwa im Nest, sondern oben auf der Webcam niedergelassen hatte. Möglicherweise war ihm die Beobachtung doch zu viel geworden.

2.7.2 Internet

2.7.2.1 Warnungen vor unseriösen Geschäftspraktiken

Ein Betroffener beschwerte sich bei mir, dass eine andere Person unter einem exakt seinem Namen entsprechenden Domainnamen eine Website betreiben würde. Alle Löschversuche seien bislang fehlgeschlagen.

Ich habe mir die Website daraufhin näher angeschaut und musste erkennen, dass es sich bei dem Betroffenen um eine inzwischen insolvente Person handelte, die in der Vergangenheit durch unseriöse Geschäftsgebaren zahlreiche Schulden bei einer Vielzahl von Gläubigern angehäuft hatte. Einer seiner Gläubiger hatte daraufhin diese Website unter dem Namen des Betroffenen (der besseren Auffindbarkeit wegen) erstellt und darüber Informationen zu diesen betreffenden Insolvenzverfahren, Strafverfahren, bisherige Verurteilungen, Unterhaltsverletzungen, vollstreckbares Vermögenswerten, Aufenthaltsorten u. ä. gesammelt und auch angeboten. Auf diese Weise sollte jedermann davor gewarnt werden, mit dem Betroffenen eine Geschäftsbeziehung einzugehen; Gläubiger und Opfer sollten bei der Durchsetzung ihrer Rechte und Interessen unterstützt werden.

Eine Rechtsgrundlage für diese Veröffentlichungen – letztendlich ein Internetpranger – war nicht ersichtlich.

Mit der betreffenden Website hatte der Gläubiger personenbezogene Daten des Betroffenen veröffentlicht, d. h. an einen unbestimmten weltweiten Empfängerkreis übermittelt. Als Zulässigkeitstatbestand dafür kam einzig § 28 Absatz 1 Satz 1 Nummer 2 BDSG, also eine Interessenabwägung, in Betracht. Ich konnte aber kein berechtigtes Interesse des Gläubigers entdecken, die von ihm über den Betroffenen gesammelten ne-

gativen Informationen, deren objektive Richtigkeit ich nicht in Frage gestellt habe, einer weltweiten Öffentlichkeit unaufgefordert und voraussetzungslos zur Verfügung zu stellen. Ich habe insbesondere bezweifelt, dass diese Internetveröffentlichung ihm oder anderen Gläubigern hilft, die noch offenen Forderungen gegenüber dem Betroffenen zu realisieren. Die betreffenden Informationen waren auch nicht wie von dem Gläubiger behauptet durch jedermann ohne Weiteres im Internet zu recherchieren, denn die von ihm benannten Quellen sind überwiegend nur bei Vorliegen besonderer Voraussetzungen nutzbar. So erfordern Auskünfte bei Handelsauskunfteien beispielsweise die Darlegung eines berechtigten Interesses; die Veröffentlichungen auf insolvenzbekanntmachungen.de sind uneingeschränkt nur über einen Zeitraum von zwei Wochen recherchierbar; Angaben zu strafrechtlichen Ermittlungsverfahren sind über allgemein zugängliche Quellen nicht zu erhalten.

Die Website ist daraufhin vom Netz genommen worden.

2.7.2.2 Kriegsgräberverzeichnis

Bei seinen zahlreichen Besuchen einer Kriegsgräberstätte, auf der auch ein Angehöriger seiner Familie beerdigt worden war, hatte ein Bürger die Beobachtung gemacht, dass noch immer viele Bürger einem Soldatenfriedhof vor allem deshalb einen Besuch abstatten, weil sie hoffen, doch noch einen Gefallenen aus ihrer Familie zu finden. Da ihm bekannt war, dass dies wiederholt auch schon zum Erfolg geführt hatte, war ihm die Idee gekommen, die ihm aus einer Kriegsgräberliste zugänglichen Informationen (Name, Geburts- und Todestag, Dienstgrad, Grablage) zu mehr als 200 namentlich bekannten Gefallenen ins Internet zu stellen. Er bat mich um Auskunft, ob dies möglich und was dazu aus datenschutzrechtlicher Sicht zu beachten sei. Die betreffenden Daten seien bereits seit 1946 an den Grabkennzeichen für jedermann ersichtlich.

Mit dem Hinweis, dass das Datenschutzrecht an dieser Stelle nicht einschlägig ist, und Fragen des postmortalen Persönlichkeitsschutzes allgemein zivilrechtlich – und nicht über meine Aufsicht – zu klären sind, habe ich dieses Beratungsgesuch wie folgt beantwortet:

Das für die Anwendung des Datenschutzrechts maßgebliche Grundrecht auf informationelle Selbstbestimmung ist höchstpersönlicher Natur und daher grundsätzlich nicht übertragbar; es endet mit dem Tod des Betroffenen. Allein die Menschenwürde als Teil des Rechts auf informationelle Selbstbestimmung wirkt über den Tod hinaus. Das lebzeitige Recht zur Selbstbewahrung, Selbstbestimmung und Selbstdarstellung geht in den Schutz des sozialen Geltungsanspruchs, d. h. den Schutz des Lebens- und Charakterbildes des Verstorbenen über. Das Andenken an den Verstorbenen wird – nur noch – gegen Angriffe auf seinen durch die Lebensleistung erworbenen Geltungswert und die ihm

als Mensch allgemein geschuldete Achtung geschützt. Die Dauer des postmortalen Persönlichkeitsschutzes lässt sich dabei nicht generell festlegen. Sie hängt von den Umständen des Einzelfalls ab. Das Schutzbedürfnis schwindet gemeinhin in dem Maße, in dem die Erinnerung an den Verstorbenen verblasst.

Die bloße Mitteilung von Name, Geburts- und Sterbedaten, sowie letzter Ruhestätte in Form eines öffentlichen Verzeichnisses einer Kriegsgräberstätte zum Zwecke der Findung Angehöriger beeinträchtigt einen im Zweiten Weltkrieg – also vor mehr als 70 Jahren – Gefallenen wohl nicht in seinem Achtungsanspruch und Geltungswert. Vielmehr handelt es sich um wertneutrale Daten ohne wertenden Bezug zu seiner Persönlichkeit. Dass die Daten durch eine Veröffentlichung im Internet einer breiteren Öffentlichkeit zugänglich gemacht und ggf. auch dauerhaft verfügbar gehalten werden, ändert an dieser Bewertung im Grundsatz nichts. Anderes gilt jedoch, wenn die Veröffentlichung geeignet ist, den Verstorbenen in einen nicht wertfreien Kontext zu rücken oder seine Persönlichkeit in einer nicht wertneutralen Weise zu vereinnahmen (z. B. „Helden“-Verehrung). Da jedenfalls bei deutschen Soldaten bestimmte Kriegsgräberstätten oder für die Personensuche zunächst auch nicht zwingend erforderliche Dienstgrade geeignet sind, diese Personen – über ihre allgemeine Beteiligung an einem verbrecherisch-menschenverachtenden Angriffskrieg hinaus – als im Besonderen fragwürdig erscheinen zu lassen, rate ich in solchen Fällen zur Zurückhaltung. Zwar können Systemträger gerade in Bezug auf diese Tätigkeit schwerlich einen besonderen Ehrschutz beanspruchen. Solange aber fehlerhafte Zuordnungen möglich bleiben oder das Maß individueller Verantwortung und Schuld differenziert betrachtet werden muss, sollte auch hier Zurückhaltung geübt werden.

2.7.2.3 Personalisierung der Digitalausgabe einer Zeitung

Zeitungsverlage räumen ihren Kunden zunehmend die Möglichkeit ein, die Tageszeitung als e-Paper im PDF-Format herunterzuladen. Einige Verlage personalisieren dabei die PDF-Ausgabe, indem sie in einer Kopfzeile auf der Titelseite den Kundennamen und die Kundennummer einfügen. Dies störte einen Kunden; er wandte sich gegen die – in seinen Augen unsinnige – Personalisierung der PDF-Ausgabe und wollte eine vollständige Übereinstimmung von Druck- und PDF-Version erreichen.

Nach meiner Auffassung bestehen keine grundsätzlichen datenschutzrechtlichen Bedenken gegen eine derartige Nutzung der Kundendaten.

Gemäß § 28 Absatz 1 Satz 1 Nummer 1 BDSG ist die Nutzung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn dies für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

Die Erforderlichkeit und das berechtigte Interesse des Verlages, die PDF-Version der Zeitung mit Namen und Kundennummer zu kennzeichnen, ergaben sich vorliegend aus den AGB, die der Kunde bei Abschluss des Online-Abos akzeptiert hatte. Dort heißt es, dass der Zugriff bei digitalen Abonnements auf drei parallele Sitzungen des jeweiligen Abonnenten beschränkt und jede darüber hinausgehende Nutzung und damit auch die digitale Weiterverarbeitung der Online-Ausgabe mit der Zeitung zu vereinbaren und aufschlagspflichtig ist.

Das heißt, dass der Verlag aufgrund des mit dem Kunden abgeschlossenen Vertrags berechtigt war, durch die Nutzung seiner personenbezogenen Daten sicherzustellen, dass er die als PDF heruntergeladene Online-Ausgabe der Zeitung nicht ohne gesonderte vertragliche Vereinbarung, z. B. über das Internet oder per E-Mail, an eine unbegrenzte Anzahl dritter Personen weiterverbreitet. Mildere Mittel zur Zweckerreichung sind nicht ersichtlich. Das Interesse des Kunden, von dieser Datennutzung verschont zu bleiben, weil die Papierausgabe ohne diese Namensangabe zugestellt wird, überwiegt insoweit nicht. Die Risiken einer vertragswidrigen Weiterverbreitung eines e-Papers sind deutlich größer als bei der Printversion einer Zeitung.

2.7.2.4 Vermittlung von Behördendiensten

Eine Petentin hat sich in Sorge um die Sicherheit ihren Sohn betreffender Daten an mich gewandt, nachdem sie festgestellt hatte, dass sie zwecks Beantragung einer (standesamtlichen) Geburtsurkunde für diesen versehentlich mit einem kommerziellen Internet-Vermittlungshelfer „ins Geschäft gekommen“ war. Nachdem sie den Irrtum bemerkt hatte, löste sie eine (kostenpflichtige) Stornierung aus und erhielt auch eine entsprechende Bestätigung. Sie bezweifelte mir gegenüber aber, dass diese Vorgehensweise legal war, da das einzige Ziel dieser Firma ihrer Meinung nach nur darin bestanden hätte, sich den Irrtum der Leute nutzbar zu machen und Stornogebühren zu verlangen.

Meine Prüfung hat ergeben, dass es sich um ein zulässiges Geschäftsmodell im Bereich Online-Dienstleistungen gehandelt hat. Zwar erschloss sich mir der Sinn des Angebots nicht so recht, da es kaum schwieriger erscheint, sich gleich direkt an die zuständige Behörde zu wenden, jedoch schien es offensichtlich einen Markt für diesen Service zu geben. Weil dabei natürlich stets auch sensible personenbezogene Daten verarbeitet werden, die generell den Reiz der Weiterveräußerung oder sonstiger missbräuchlicher Verwendung bieten, rate ich zwar regelmäßig zur Vorsicht gegenüber solchen Anbietern, jedoch habe ich als Aufsichtsbehörde im Übrigen ausschließlich das geltende Recht zu prüfen.

Von einem Internetnutzer kann erwartet werden, dass er sich vor Eingabe sensibler Daten über deren Empfänger Kenntnis verschafft. Dies vereitelte oder verschleierte der im

konkreten Fall auftretende Anbieter nicht. Insoweit waren in Hinblick auf die Datenerhebung keine persönlichkeitsrechtsschützenden Vorschriften verletzt worden. Und dafür, dass eine Datenverarbeitung entgegen der kommunizierten Zweckbestimmung erfolgte, konnten aus der bisherigen Aufsichtspraxis gleichfalls keine Anhaltspunkte entnommen werden. Fragen zur Stornierung und einer etwaigen Zahlungspflicht sind mir zuständigkeitshalber einer Klärung entzogen; derlei wäre auf zivilrechtlichen Wegen, ggf. mit Hilfe von Verbraucherschützern, zu klären.

Auch die von der Petentin gewünschte sofortige Löschung der zum Vorgang gespeicherten Daten konnte ich nicht unterstützen. Es war davon auszugehen, dass ein Vertrag zustande gekommen war, was wiederum bei der verantwortlichen Stelle kaufmännische Aufbewahrungsfristen ausgelöst hat. Anhaltspunkte, dass die an Stelle der Löschung tretende Nutzungsuntersagung (Sperrung) nicht befolgt worden sein könnte, haben ebenfalls nicht vorgelegen.

2.7.3 Arbeitnehmerdatenschutz

2.7.3.1 Datenaustausch zwischen potentiellem Arbeitgeber und Jobcenter

Im Rahmen einer Bewerbung auf ein Stellenangebot des Jobcenters kam es bei dem potentiellen privaten Arbeitgeber zu einem Bewerbungsgespräch mit dem SGB II-Bezieher. Kurz darauf erhielt der Petent vom Jobcenter die Aufforderung, zur „Auswertung Vorstellungsgespräch“ in der Behörde zu erscheinen. Es stellte sich heraus, dass der potentielle Arbeitgeber Angaben zum – offensichtlich negativen – Verlauf des Vorstellungsgesprächs gegenüber dem Jobcenter gemacht hatte.

Die Datenerhebungsbefugnis der SGB II-Behörde ergibt sich aus § 67 a Absatz 2 Nummer 2 Buchstabe b aa SGB X in Verbindung mit § 31 Absatz 1 Nummer 2 SGB II. Danach darf das Jobcenter Daten über das Vermittlungsergebnis erheben, da es gemäß § 31 Absatz 1 Nummer 2 SGB II auch die Aufgabe hat zu überprüfen, ob der Leistungsberechtigte durch sein Verhalten ggf. die Anbahnung eines Arbeitsverhältnisses – zum Beispiel durch unzureichende oder gar fehlende Bewerbungen oder sein Verhalten im Vorstellungsgespräch – verhindert (wovon das Jobcenter in diesem Fall offensichtlich ausgegangen war) und wofür der Leistungsträger die Beweislast trägt.

Die Rechtsgrundlage für die Auskunftserteilung und mithin für eine Datenübermittlung durch das Unternehmen, bei dem sich der Leistungsbezieher bewerben soll, an den Leistungsträger ergibt sich aus § 28 Absatz 2 Nummer 2a BDSG. Insoweit darf das betroffene Unternehmen nicht nur Angaben darüber machen, dass es zu keiner Einstellung gekommen ist, sondern auch zu den Gründen der fehlgeschlagenen Anstellung. Da es sich um eine gesetzliche Übermittlungsbefugnis im Sinne des § 4 Absatz 1 BDSG han-

delt, kommt es weder auf ein Einverständnis noch auf einen Widerspruch gegen die Datenübermittlung an.

Vorliegend wurde die Nichtanstellung wohl aufgrund des Gesamteindrucks des Vorstellungsgesprächs begründet. Ob dies letztlich eine Nichtanstellung bzw. eine Verhinderung der Anbahnung eines Arbeitsverhältnisses rechtfertigt, entzieht sich meiner Prüfung, da es sich hierbei nicht um eine datenschutzrechtliche, sondern um eine rein materiell-rechtliche Frage, nämlich ob die Voraussetzungen des § 31 Absatz 1 Nummer 2 SGB II erfüllt sind, handelt.

2.7.3.2 Versand elektronischer Lohnbescheinigungen

Nachdem ich darüber informiert worden war, dass ein Arbeitgeber beabsichtigte, die Gehaltsabrechnungen seiner Mitarbeiter unverschlüsselt an deren private E-Mail-Adresse zu versenden, habe ich mich sogleich an diesen gewandt und auf die erheblichen datenschutzrechtlichen Risiken einer unverschlüsselten E-Mail-Übertragung hingewiesen. Eine unverschlüsselte E-Mail ist weder gegen eine Kenntnisnahme durch Unbefugte noch gegen eine inhaltliche Veränderung geschützt. Das bedeutet, dass es unbefugten Personen ohne großen Aufwand möglich ist, eine unverschlüsselte E-Mail zu lesen und inhaltlich nach Belieben abzuändern. Eine unverschlüsselte E-Mail ist letztlich einer mit Bleistift geschriebenen Postkarte vergleichbar. Bei Lohn- und Gehaltsdaten der Mitarbeiter handelt es sich um besonders sensible Daten. Arbeitgeber haben eine besondere Sorgfaltspflicht, diese persönlichen Daten der Arbeitnehmer vor unberechtigten Zugriffen zu schützen.

Ich habe daher folgende Empfehlungen gegeben und auf deren Umsetzung gedrungen:

- Allen Mitarbeitern sollten private, auf Firmenservern gehostete E-Mail-Postfächer zur Verfügung gestellt werden, denn eine Datenerhebung und Datenverarbeitung (hier der privaten E-Mail-Adressen der Mitarbeiter) ist nur zulässig, wenn diese zur Durchführung des Arbeitsverhältnisses erforderlich ist (§ 32 Absatz 1 Satz 1 BDSG). Zunächst ist schon nicht davon auszugehen, dass alle Mitarbeiter eine (eigene) private E-Mail-Adresse besitzen. Selbst wenn dies der Fall wäre, sind die Mitarbeiter nicht verpflichtet, ihrem Arbeitgeber diese mitzuteilen. Aufgrund des im Arbeitsverhältnis bestehenden Über-/Unterordnungsverhältnisses ist grundsätzlich davon auszugehen, dass eine freiwillige Preisgabe der privaten E-Mail-Adressen im Sinne einer Einwilligung gemäß § 4a Absatz 1 BDSG ausscheidet. Zudem kann eine Einwilligung jederzeit widerrufen werden. Deshalb sind Arbeitgeber rechtlich auf der sicheren Seite, wenn sie den Arbeitnehmern private E-Mail-Postfächer zum Empfang der Lohnbescheinigungen einrichten. Denn auf diese Weise vermeiden sie auch, dass ggf.

Dritte Zugriff auf die Lohnbescheinigungen haben. Das bedeutet aber auch, dass der Zugriff auf das private E-Mail-Postfach durch ein Passwort geschützt sein muss, das ausschließlich der jeweilige Mitarbeiter kennt.

- Die Verschlüsselung der PDF-Dokumente muss dem Stand der Technik entsprechen, der in den Technischen Richtlinien des BSI, insbesondere der TR-02102-1, niedergelegt ist.
- Für die Verschlüsselung sind individuelle Passwörter mit ausreichender Komplexität zu verwenden. Die Passwörter müssen in regelmäßigen Abständen geändert werden und sind geheim zu halten. Arbeitgeber können sich hierzu an den Vorgaben des BSI, M 2.11 Regelung des Passwortgebrauchs, orientieren und sollten ihre Mitarbeiter entsprechend schriftlich informieren und anweisen.

2.7.3.3 Veröffentlichung des Namens und eines Gebühr einer Mitarbeiterin auf Ärztehomepage

Die Mitarbeiterin einer Arztpraxis wandte sich an mich mit dem Anliegen, dass ihr Name ohne vorherige Information auf der Homepage der Arztpraxis veröffentlicht worden war und darüber hinaus beabsichtigt sei, nunmehr auch ein Bildnis auf der Homepage zu veröffentlichen. Die Mitarbeiterin bat mich um Information über die rechtliche Zulässigkeit.

Nach Prüfung des Anliegens teilte ich der Betroffenen bzgl. der Veröffentlichung ihres Namens als Praxismitarbeiterin auf der Homepage mit, dass die datenschutzrechtliche Zulässigkeit maßgeblich davon abhängt, inwieweit dies für einen geregelten, branchenüblichen Geschäftsbetrieb zwingend erforderlich und verhältnismäßig sei oder jedenfalls ein berechtigtes Interesse des Arbeitgebers an der Veröffentlichung ihres Mitarbeiternamens auf der Praxishomepage bestehe und dem gegenüber keine schutzwürdigen Interessen der betroffenen Mitarbeiterin vorrangig seien. Dies sei stets eine Frage des konkreten Einzelfalles und kann nur unter Berücksichtigung aller Umstände beantwortet werden. Sollten die vorgenannten Voraussetzungen zu Gunsten des Arbeitgebers vorliegen und seitens der betroffenen Mitarbeiterin kein überwiegendes schutzwürdiges Interesse bestehen, wäre die Veröffentlichung ihres Namens auch ohne ihre Einwilligung zulässig. Gleichwohl muss der Arbeitgeber sie jedoch über die Veröffentlichung informieren.

Hinsichtlich der beabsichtigten Veröffentlichung eines Fotos habe ich der betroffenen Mitarbeiterin mitgeteilt, dass die datenschutzrechtliche Zulässigkeit zunächst einmal davon abhänge, ob sie im Fokus der Aufnahme stehe, sozusagen einen „Fotoschwerpunkt“ bilde, oder im rechtstechnischen Sinne lediglich „Beiwerk“ sei. Im ersten Fall wäre eine Veröffentlichung nur mit schriftlichen Einwilligung nach § 22 KunstUrhG

zulässig. Es empfiehlt sich im Übrigen, die Einwilligung, die freiwillig ist, befristet für das Bestehen des Beschäftigungsverhältnisses zu erteilen, damit es keine Streitigkeiten für den Fall des Ausscheidens aus dem Beschäftigungsverhältnis gibt. Andernfalls könnte die einmal erteilte Einwilligung gegebenenfalls fortwirken. Im zweiten Fall, in dem die Veröffentlichung lediglich als „Beiwerk“ zu bewerten ist, wäre eine Veröffentlichung einwilligungsfrei möglich (§ 23 KunstUrhG). Es ist daher stets zu klären, wie die Fotoaufnahmen aussehen/veröffentlicht werden sollen.

Über eine vergleichbare Thematik hatte ich bereits in meinem 7. Tätigkeitsbericht unter Punkt 8.3.5 berichtet.

2.7.3.4 Herausgabe von Personalunterlagen an ausgeschiedene Mitarbeiter

Nach Beendigung seines Arbeitsvertrages wollte ein Arbeitnehmer seine persönlichen Unterlagen einfordern. Dabei ging es ihm um Urlaubsunterlagen, Krankschreibungen und weitere persönliche Daten. Er meinte, dies sei sein gutes Recht. Allerdings weigerte sich das Unternehmen, diesen Forderungen nachzukommen.

Meines Erachtens weigerte sich das Unternehmen zu Recht. Die Auffassung des Petenten, wonach ein Arbeitgeber Personalunterlagen nach Ende der Beschäftigung unverzüglich herauszugeben hätte, teile ich aus folgenden Gründen nicht:

Das Datenschutzrecht kennt keinen Herausgabeanspruch, sondern nur den Anspruch auf Löschung (Vernichtung) oder Sperrung, also eine besonders geschützte und zweckbegrenzte Form der Aufbewahrung (§ 35 Absatz 2 Satz 1 bzw. § 35 Absatz 3 BDSG).

Ein arbeitsrechtlicher oder allgemein zivilrechtlicher Herausgabeanspruch mag allenfalls bei Unterlagen in Betracht kommen, die dem Arbeitgeber vom Beschäftigten überlassen wurden und deren Verbleib vom Arbeitgeber über das Beschäftigungsende hinaus nicht länger beansprucht werden kann. Dies trifft auf Unterlagen, die im Rahmen ordnungsgemäßer Personalaktenführung rechtmäßig zur Personalakte genommen wurden, regelmäßig nicht zu.

Vielmehr gilt – auch datenschutzrechtlich – der Grundsatz, dass Personalunterlagen so lange aufbewahrt werden dürfen, wie noch mit Ansprüchen des Beschäftigten zu rechnen ist. Da nach § 195 BGB die regelmäßige Verjährungsfrist von Ansprüchen ehemaliger Beschäftigter erst nach drei Jahren endet, können Personalakten dementsprechend gleichermaßen lange aufbewahrt werden. Zudem beginnt wegen § 199 BGB die Verjährungsfrist erst am Jahresende des Jahres, in dem der Beschäftigte das Unternehmen verlässt.

Ferner ist die Aufbewahrung von Personalunterlagen auch über diesen Zeitraum hinaus vielfach aus anderem Recht geboten und damit gestattet: So gibt es diverse gesetzliche Aufzeichnungs- und Aufbewahrungspflichten, teils mit Fristen bis zu 10 Jahren, um Steuerbehörden und den Sozialversicherungsträgern Prüfungen zu ermöglichen. Eine Darstellung aller hier möglicherweise einschlägigen Bestimmungen und Sachverhalte ist mir an dieser Stelle nicht möglich. Nur beispielhaft möchte ich das für Krankschreibungen relevante Aufwendungsausgleichsgesetz benennen. Nach § 6 Absatz 1 AAG besteht ein Erstattungsanspruch bis zu vier Jahren nach Ablauf des Kalenderjahrs, in dem er entstanden ist. Somit können Arbeitsunfähigkeitsbescheinigungen erst fünf Jahre nach Ablauf des Kalenderjahrs, in dem der Erstattungsanspruch entstanden ist, vernichtet werden.

2.7.3.5 Mailingaktionen einer Gewerkschaft an die gesamte Belegschaft

Eine Gewerkschaft führte zur Information der Beschäftigten und damit auch zu Werbezwecken für ihre Ziele nach Artikel 9 Absatz 3 GG regelmäßig Mailing-Aktionen an alle Beschäftigten eines Unternehmens durch, mithin auch an Nicht-Mitglieder. Sie bezog sich dabei auf das Grundsatzurteil des BAG vom 20.01.2009 (1 AZR 515/08, juris), wonach Arbeitgeber von einer tarifzuständigen Gewerkschaft grundsätzlich nicht verlangen könnten, es zu unterlassen, sich zu Werbe- und Informationszwecken per E-Mail an die Beschäftigten über deren betriebliche E-Mail-Adressen zu wenden.

Anders als die Gewerkschaft kann ich dem Grundsatzurteil des BAG keine pauschale Erlaubnis für eine tarifzuständige Gewerkschaft entnehmen, alle Beschäftigten der betreffenden Arbeitgeber per betrieblicher E-Mail anzusprechen. Das BAG hat insoweit nur in Bezug auf die gewerkschaftsangehörigen Beschäftigten keine Bedenken geäußert und dies auf § 28 Absatz 1 Satz 1 Nummer 1 BDSG gestützt (vgl. Rz. 53 des Urteils).

In Bezug auf Nichtmitglieder hat das BAG offen gelassen, ob in der Nutzung derer betrieblichen Mail-Adressen eine Verletzung ihres Selbstbestimmungsrechtes liegt. Darauf ist es in dem konkreten Streitfall wegen des von der Klägerin gestellten Globalantrages nicht angekommen (vgl. wiederum Rz. 53 des Urteils). § 28 Absatz 1 Satz 1 Nummer 1 BDSG wäre insoweit als Rechtsgrundlage jedenfalls nicht heranzuziehen gewesen. Das BAG hat diesbezüglich lediglich darauf hingewiesen, dass es im Schrifttum umstritten ist, ob Gewerkschaften zum Zweck der Mitgliederwerbung und -information E-Mails an die betrieblichen E-Mail-Adressen der Arbeitnehmer senden dürfen (Rz. 32 des Urteils).

Die bei Nichtmitgliedern als Rechtsgrundlage in Betracht kommende Interessenabwägung nach § 28 Absatz 1 Satz 1 Nummer 2 BDSG wird die Zulässigkeit solcher Mailingaktionen meiner Auffassung nach nicht begründen können. Eine rechtssichere Lösung bietet daher insoweit nur eine Einwilligung gemäß § 4a BDSG.

2.7.4 Gesundheitswesen

2.7.4.1 Einsichtnahme in die Patientenakte: Fremdbefunde

"Briefe oder Befunde anderer Einrichtungen oder Krankenhäuser dürfen wir nicht an Sie weitergeben, diese müssen direkt an den jeweiligen Stellen angefordert werden." – Dies erhielt eine Petentin als Auskunft bei einer Akteneinsicht und fragte mich nach meiner Rechtsauffassung.

Ich nahm hierzu wie folgt Stellung:

Patienten haben ein Recht auf Einsichtnahme in ihre Patientenakte, und zwar in die Originalakte. Das ist in § 630g BGB festgehalten. Das Begehren des Patienten auf Einsicht muss der Arzt bzw. der Behandelnde unverzüglich erfüllen.

Der Arzt bzw. Behandelnde kann die Einsichtnahme verweigern (ganz oder teilweise), wenn erhebliche therapeutische Gründe dagegen sprechen.

Nach § 630 g Absatz 1 Satz 2 BGB ist § 811 BGB entsprechend anwendbar. Die Einsichtnahme in die Patientenakte muss an dem Ort erfolgen, an dem sich die einzusehenden Unterlagen oder Dokumente befinden. Lediglich, wenn ein wichtiger Grund vorliegt, kann der Patient die Einsichtnahme an einem anderen Ort fordern.

Einen Anspruch auf Zusendung der Original-Patientenakte für einen bestimmten Zeitraum erkenne ich nicht.

Nach § 630g Absatz 2 BGB hat der Patient das Recht, Abschriften von der Patientenakte zu verlangen. Abschriften können von einem Text, von elektronischen Dokumenten oder auch in Form von Dateien in elektronischer Form angefertigt werden. Die Kosten für die Abschriften bzw. Kopien hat entsprechend § 811 Absatz 2 Satz 1 BGB der Patient zu tragen.

Werden Arztbriefe oder Befunde anderer Einrichtungen/Krankenhäuser/Behörden in die Patientenakte des Arztes eingefügt – soweit diese z. B. aufgrund der Überweisung zu einem Facharzt anfallen und der Facharzt sodann eine fachärztliche Stellungnahme erstellt und dem Hausarzt übermittelt –, also Bestandteil der Patientenakte des Hausarztes werden, dann umfasst das Einsichtsrecht meiner Auffassung nach auch diese Briefe oder Befunde. Denn die Patientenakte erstreckt sich über alle Behandlungszusammenhänge bei einem konkreten Arzt.

Ansonsten ist der jeweilige behandelnde Arzt verantwortliche Stelle im datenschutzrechtlichen Sinne und muss das Einsichtsrecht selbständig sicherstellen.

2.7.4.2 Aufbewahrungsfristen für Patientenakten

Ein Petent fragte mich Mitte 2017 nach Aufbewahrungsfristen bei Ärzten. Er hatte bei der Vorsprache in einer Facharztpraxis – nach Angabe seines Namens und Geburtsdatums – den Hinweis erhalten, dass er bereits acht Jahre zuvor schon einmal in der Facharztpraxis behandelt worden war. Der Petent war über dieses langjährige Vorhalten seiner Daten beunruhigt.

Ärzte sind verpflichtet, die Behandlung ihrer Patienten korrekt zu dokumentieren. Die Aufbewahrungsfrist der ärztlichen Dokumentation – dazu zählen natürlich die Adress- wie auch Geburtsdaten – ist im Bürgerlichen Gesetzbuch geregelt. Dazu heißt es in § 630f BGB, dass der Arzt die Patientenakte für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren hat, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen gelten. Ebenso schreiben der Bundesmantelvertrag-Ärzte und die Berufsordnung eine zehnjährige Aufbewahrungsfrist vor.

Der Arzt kann also davon ausgehen, dass er im Zweifel grundsätzlich alle Unterlagen mindestens zehn Jahre lang aufbewahren muss. Sofern die Aufzeichnungen elektronisch dokumentiert worden sind, muss der Vertragsarzt dafür sorgen, dass sie innerhalb der Aufbewahrungszeit zur Verfügung gestellt werden können. Er muss die Daten also entsprechend sichern.

Die Unterlagen von Patienten mit chronischen Erkrankungen sollte der Arzt ggf. länger als zehn Jahre aufbewahren, sofern sich der Patient noch in Behandlung befindet. Weiterhin können sich längere Aufbewahrungszeiten ergeben, sofern während der Behandlung Komplikationen auftreten oder ein Rechtsstreit anhängig gemacht wird.

Kommt es beispielsweise zu einem Gerichtsverfahren, in dem Schadensersatzansprüche geltend gemacht werden, sollte die Dokumentation wegen der geltenden Verjährungsfristen 30 Jahre lang aufbewahrt werden. Bewahren Ärzte die Dokumentation in diesem Fall nicht auf, legen die Gerichte dies den Ärzten zum Teil negativ aus. Die Gerichte gehen dann davon aus, dass die Dokumentation und damit auch die Behandlung nicht ordnungsgemäß erfolgt sind. Bei den Vorschriften, aus denen sich längere Aufbewahrungsfristen ergeben, ist insbesondere auf die Röntgenverordnung hinzuweisen. Nach § 28 RöV ist vorgeschrieben, dass der Betreiber einer Röntgeneinrichtung Aufzeichnungen über diese Behandlung für 30 Jahre nach der letzten Behandlung aufzubewahren hat. Röntgenbilder muss er zehn Jahre lang nach der letzten Untersuchung aufbewahren. Röntgenbilder und die Aufzeichnungen der Röntgenuntersuchung einer Person, die noch keine 18 Jahre alt ist, sind bis zum Alter von 28 Jahren aufzubewahren.

Die Strahlenschutzverordnung regelt, dass Aufzeichnungen über die Untersuchung zehn Jahre lang und über die Behandlung 30 Jahre lang nach der letzten Untersuchung oder Behandlung aufzubewahren sind. Wenn ein Arzt einen Patienten mit radioaktiven Stoffen oder ionisierender Strahlung untersucht oder behandelt hat, hat er einem später behandelnden Kollegen auf dessen Verlangen Auskunft über die Aufzeichnungen zu erteilen und diesem die Unterlagen vorübergehend zu überlassen.

Auch im Transfusionsgesetz sind längere Aufbewahrungsfristen vorgesehen. Je nach Art der Unterlagen betragen die Aufbewahrungsfristen 15, 20 oder 30 Jahre. Die Dokumentation der Blutprodukte und Plasmaproteine ist 30 Jahre lang aufzubewahren, Aufzeichnungen über Spenderdaten 15 Jahre. Dokumentationen über die Spenderimmunisierung muss der Arzt hingegen 20 Jahre lang aufbewahren. Zu beachten ist, dass der Arzt diese Daten vernichten oder löschen muss, wenn die Aufbewahrung nicht mehr erforderlich ist. Werden Aufzeichnungen länger als 30 Jahre aufbewahrt, sind sie zu anonymisieren.

Aufbewahrungszeiten sind zudem auch in den Richtlinien für die Bestellung von Durchgangsärzten geregelt.

2.7.4.3 Übergabe betriebsärztlicher Befunde an den Arbeitgeber

Ein Arbeitnehmer war auf Veranlassung seines Arbeitgebers zu einer betriebsärztlichen Untersuchung gewesen, wo er mit dem Arzt ausdrücklich vereinbart hatte, dass die Untersuchungsergebnisse, insbesondere seine Blutwerte, ausschließlich an ihn übersandt werden. Dennoch erhielt der Arbeitnehmer wenig später auf seiner Arbeitsstelle einen – seiner Darstellung nach – mehr oder weniger unverschlossenen Umschlag überreicht, in dem sich die – insoweit unkritische – ärztliche Bescheinigung für die arbeitsmedizinische Vorsorgeuntersuchung, aber eben auch die konkreten Untersuchungsergebnisse befanden. Der Betroffene war mit der Übersendung dieser Daten an den Arbeitgeber in keiner Weise einverstanden und bat mich, den Vorgang zu bewerten.

Nach § 8 Absatz 1 ASiG haben Betriebsärzte – wie jeder andere „normale“ Arzt auch – die Regeln der ärztlichen Schweigepflicht zu beachten und sind ohne Einwilligung nicht befugt, Arbeitnehmer betreffende Befunde dem Arbeitgeber mitzuteilen; andernfalls machen sie sich strafbar (§ 203 StGB). Vorliegend vermochte ich aber nicht zu erkennen, dass der Betriebsarzt seine Befunde dem Arbeitgeber bzw. einem Betriebsangehörigen vorsätzlich zur Kenntnis gebracht hätte, so dass ihm ein strafrechtlicher Vorwurf insoweit wohl nicht gemacht werden konnte; der fahrlässige Bruch des Patientengeheimnisses ist jedenfalls nicht strafbar.

Indem der Betriebsarzt jedoch die Befunde – entgegen der Absprache mit dem Betroffenen – nicht an dessen Privatanschrift, sondern an seine betriebliche Adresse gesandt hatte, könnte er allerdings fahrlässig unbefugt (besondere) personenbezogene Daten übermittelt haben. Indes scheiterte auch ein solcher Fahrlässigkeitsvorwurf bereits dann, wenn der Brief so – z. B. mit dem Zusatz „persönlich/vertraulich“ – gekennzeichnet gewesen ist, dass eine fremde Kenntnisnahme nur unter Verstoß gegen das Briefgeheimnis möglich gewesen wäre. Auf die besondere Absprache mit dem Betroffenen kommt es dabei solange nicht an, wie der Betriebsarzt nicht auch der Verkehrssitte nach fahrlässig gehandelt hätte.

Eine konkrete(re) Aufklärung des Sachverhalts war mir an dieser Stelle leider nicht möglich, da der Betroffene mich gebeten hatte, seine Identität seinem Arbeitgeber gegenüber nicht offenzulegen.

2.7.4.4 Schweigepflicht bei Praxisübergang auf Erben

Was geschieht beim Tod des Praxisinhabers mit der Patientenakte? Mit dieser Frage wandte sich eine betroffene Patientin an mich.

Ist Ursache für die Praxisaufgabe der Tod des Praxisinhabers, so geht die Praxis im Ganzen mit allen Rechten und Pflichten auf die Erben über (§ 1922 BGB). Die Schweigepflicht, an die der Arzt gemäß § 203 StGB und § 9 der Berufsordnung der Sächsischen Landesärztekammer gebunden war, geht auf die Erben nicht über, wenn sie nicht selbst Ärzte sind. Da die Schweigepflicht des Arztes aber wie die Dokumentations- und Aufbewahrungspflicht ebenfalls eine Nebenpflicht aus den früher geschlossenen Behandlungsverträgen darstellt, geht diese Nebenpflicht auf diejenigen Personen über, welche als Erben die Patientenkartei aus dem Nachlass erlangen. Von ihnen ist zu verlangen, dass sie – wie ein Arzt – alle zumutbaren Maßnahmen ergreifen, um eine ordnungsgemäße Aufbewahrung der Patientenkartei zu ermöglichen.

Konkretere Regelungen bestehen nicht. Anders ist dies zum Beispiel im Heilberufe-Kammergesetz Baden-Württemberg geregelt: Die Kammern haben dort nach § 4 HBKG bei der Wahrnehmung ihrer Aufgaben die Interessen des Gemeinwohls und die Rechte der Patienten zu beachten. Sie haben Patientenunterlagen für die Dauer der Aufbewahrungspflicht in Obhut zu nehmen und den Patienten Einsicht zu gestatten, sofern dies nicht durch das verpflichtete Kammermitglied oder dessen Rechtsnachfolgerin oder -nachfolger gewährleistet ist. Gegenüber den Verpflichteten besteht in diesem Fall ein Anspruch auf Erstattung der Kosten, welche im Zusammenhang mit der Aufbewahrung der Patientenakten entstehen. Die Kammern können andere Kammermitglieder oder Dritte mit der Erfüllung dieser Aufgabe betrauen, des Weiteren können die Kammern gemeinsame Einrichtungen zur Erfüllung dieser Aufgabe errichten oder nutzen.

2.7.4.5 Apothekenübernahmen

Eine Versandapotheke hatte im Berichtszeitraum eine Reihe ehemaliger Konkurrenten aus anderen Bundesländern übernommen. Im Zusammenhang mit dem dadurch bedingten erheblichen Unternehmenswachstum erreichten mich zahlreiche Eingaben zur Newsletter-Problematik, zur Account-Löschung sowie zu Auskünften nach § 34 BDSG, die sich im Wesentlichen auch rasch und unbürokratisch klären ließen. Ich stand dazu in ständigem – auch beratenden – Kontakt mit dem Unternehmen, insbesondere dessen Datenschutzbeauftragten.

Praktisch erfolgte die Übernahme der Versandapotheken dabei so, dass der jeweilige Altbetreiber seine Kunden über die Möglichkeit informiert hatte, ihr Kundenkonto per ausdrücklicher Zustimmung auf den Neubetreiber zu übertragen. Wer davon keinen Gebrauch machte, dessen Daten verblieben ausschließlich auf dem Server des Altbetreibers. Soweit war diese Verfahrensweise vom Grundsatz her auch nicht zu beanstanden.

In der Praxis gab es dann aber doch einen ganzen „Strauß“ von Problemen. Da der Neubetreiber die Website häufig auch auf sein eigenes Design umgestellt und die Altbetreiber auch weiterhin im eigenen Namen Newsletter, deren Zulässigkeit hier einmal dahingestellt, versandt hatten, war für die Kunden nicht immer klar ersichtlich, wer denn nun ihre Daten tatsächlich verarbeitet und wo sie ihre Löschungs- oder andere Rechte geltend machen müssen. Dadurch sowie infolge der verschiedenen Arten der Betriebsübernahme (nur Online-Geschäft oder Komplettübernahme) wie auch durch Fehlhandlungen der Betroffenen entstanden verschiedenste Fallkonstellationen, in denen die zahlreichen Kundenanliegen nicht immer schnell genug und so zufriedenstellend durch den Neubetreiber verarbeitet werden konnten, wie das wünschenswert gewesen wäre. So wurden beispielsweise auch Löschungsbegehren an den Neubetreiber gerichtet, obwohl dieser (mangels Zustimmung) gar keine Kundendaten hatte; es gab aber auch Fälle, in denen die Kunden der Übertragung ihrer Daten an den Neubetreiber (zu Testzwecken) mehrfach zugestimmt hatten, womit Löschungen beim Neubetreiber immer wieder rückgängig gemacht wurden bzw. erneut durchgeführt werden mussten.

Um die durch die Übernahmen entstandenen teilweise komplizierten Gemengelagen für die Kunden der Altbetreiber unbürokratisch aufzulösen, hat sich der Neubetreiber generell bereit erklärt, auch (fehlerhaft adressierte) Löschungswünsche solcher Personen, die ihr Kundenkonto nicht auf ihn migriert hatten, an den Altbetreiber bzw. dessen IT-Dienstleister weiterzuleiten. Insoweit musste auch ich die betreffenden Kunden nicht aus Zuständigkeitsgründen ab- und an die stattdessen zuständigen Aufsichtsbehörden anderer Bundesländer verweisen.

In einem (und erfreulicherweise tatsächlich singulären) Einzelfall hatte ein Betroffener allerdings bereits starken Unmut an der Sinnhaftigkeit meines Tätigwerdens kundgetan, weil die von ihm begehrte Löschung seines (nicht auf den Neubetreiber migrierten) Kundenkontos offenbar zum wiederholten Male nicht korrekt umgesetzt worden war.

Jedes Mal hatte der Petent dabei Bestätigungen erhalten, das Konto sei nunmehr gelöscht. Bei dem von ihm daraufhin durchgeführten Test konnte er jedoch weiterhin mit seinen alten Login-Daten vollen Zugang auf das Konto erhalten. Mehrfach wiederholte Löschungen seitens der Altbetreiber brachten kein anderes Ergebnis. Der Fall stand mithin kurz davor, eine aufsichtsrechtliche Anordnung auszulösen. Erst durch eine aufwendige Recherche in der Kauf-Historie des Betroffenen konnte das Unternehmen ermitteln, dass seinerzeit zum Login nicht nur die (ausschließlich von ihm angegebene) E-Mail-Adresse geeignet war, sondern auch ein selbst gewählter Nickname. Mit diesem hatte er sich Mal um Mal wieder eingeloggt und das Konto damit wieder reaktiviert. Die Löschung des Datenbestandes selbst durfte aufgrund von Aufbewahrungsfristen noch nicht erfolgen.

Das Kundenkonto konnte schließlich also doch noch unwiderruflich gelöscht und die buchungsrelevanten Inhalte mit den vorgesehenen Aufbewahrungspflichten gesperrt werden.

2.7.4.6 Apotheken: Was tun bei Verdacht auf Rezeptbetrug?

Ein Apothekenleiter wollte Ärzte in der Umgebung seiner Apotheke anschreiben, nachdem ihm aufgefallen war, dass eine Kundin große Mengen eines verschreibungspflichtigen Medikaments erworben hatte, wobei die erforderlichen Verordnungen nach Angaben des Apothekers von einer Vielzahl von Ärzten im Landkreis ausgestellt worden waren.

Bei einem solchen Vorhaben ist jedoch die apothekerliche Schweigepflicht maßgeblich zu beachten. Der Apothekenleiter und das Apothekenpersonal sind zur Verschwiegenheit über das, was in Ausübung des Berufs bekannt geworden ist, verpflichtet. Insoweit verweise ich auch auf § 16 SächsHKaG und auf § 4 der BO der Sächsischen Landesapothekerkammer.

Sinn und Zweck der apothekerlichen Schweigepflicht ist einerseits der Schutz des Einzelnen vor Beeinträchtigung seiner Privatheit/Verhaltensfreiheit, andererseits aber auch der Schutz des Vertrauens der Allgemeinheit in die Verschwiegenheit und Funktionsfähigkeit bestimmter Berufe, eben z. B. der Ärzte oder der Apotheker, und damit der verfassungsmäßigen Ordnung.

Von der apothekerlichen Schweigepflicht umfasst sind dabei bereits der bloße Umstand, dass sich jemand in die Apotheke begibt und auch die Begleitumstände; selbstverständlich fallen unter die Schweigepflicht Angaben zur Art und Häufigkeit der Abgabe eines Medikaments oder Hilfsmittels, oder Diagnosen, auf die mittels des Medikaments geschlossen werden kann (z. B. Suchtneigung).

Die Schweigepflicht gilt dabei gegenüber jedermann, z. B. auch gegenüber Angehörigen eines Kunden (Ehefrau, Großeltern), auch wenn es sich dabei um minderjährige Patienten handelt, wobei hier Alter und Einsichtsfähigkeit zu berücksichtigen sind.

Die Pflicht zur Verschwiegenheit gilt insbesondere auch gegenüber Berufskollegen und Vorgesetzten, soweit diese nicht selbst mit der Bearbeitung des konkreten Falles befasst sind.

Die Verletzung der apothekerlichen Schweigepflicht ist nach § 203 StGB strafbar. Dies bedeutet, dass eine Offenbarung von personenbezogenen Daten nur zulässig ist, wenn eine Offenbarungsbefugnis zur Durchbrechung der Schweigepflicht vorhanden ist, das heißt eine gesetzliche Grundlage oder eine Einwilligung des Betroffenen.

Insoweit besteht bei einer erkannten Rezeptfälschung – was eine Urkundenfälschung bzw. ein versuchter Betrug, bei einem Betäubungsmittelrezept zusätzlich evtl. ein versuchtes Delikt nach § 29 ff. BtmG darstellen kann – zwar die Möglichkeit des Apothekers, die Abgabe zu verweigern (siehe § 17 Absatz 4 ApBetrO), indes ist zu beachten, dass das einfache Strafverfolgungsinteresse des Staates den grundgesetzlich geschützten Anspruch des Betroffenen auf informationelle Selbstbestimmung in besonderen Vertrauensverhältnissen normalerweise nicht überwiegt. Daher ist ein Bruch der Schweigepflicht nicht ohne Weiteres gerechtfertigt, wenn ein Patient beispielsweise Apotheken oder Krankenkassen betrügt, obwohl auch hier eine Straftat vorliegt (§ 263 StGB), bei der sogar von Amts wegen ermittelt wird (Offizialdelikt). Einen Fall des rechtfertigenden Notstands nach § 34 StGB kann ich an dieser Stelle ebenso wenig erkennen wie ich sonstige gesetzliche Offenbarungsbefugnisse für nicht einschlägig halte.

Insoweit ist meiner Auffassung nach eine gesetzliche Befugnis, die Patientin gegenüber Dritten zu offenbaren, nicht ersichtlich. Eine Einwilligung ist hierzu offensichtlich nicht erteilt und wird auch nicht erteilt werden. Mithin besteht keine Befugnis zur Durchbrechung der Schweigepflicht.

Als zulässig erachte ich indes einen Hinweis an die Apotheker- bzw. Ärztekammer, in der auf den Verdacht zu Bestellungen/Käufen nicht therapiekonformer Mengen spezieller Arzneimittel hingewiesen wird, sodass die Kammern ggf. dazu aufrufen können, bei

bestimmten Bestellungen/Verkäufen mehr Achtsamkeit walten zu lassen. Eine namentliche Nennung der Patientin ist dabei aber nicht zulässig.

Es dürfen zudem dabei auch schon keine Angaben zu der Patientin, z. B. in Form biografischer Daten, erfolgen, die den Kollegen eine Personenbeziehbarkeit ermöglichen, etwa weil das Präparat erst für den Kunden bestellt werden muss.

Insoweit habe ich den Apotheker von seinem Vorhaben abgeraten, Ärzte in seinem Umkreis anzuschreiben und über seinen Verdacht in Kenntnis zu setzen.

2.7.5 Handel, Gewerbe, Dienstleistungen

2.7.5.1 Übermittlung von Schuldnerdaten an Arbeitgeber

Ein Gläubiger, der bereits einen Vollstreckungsbescheid gegen einen Schuldner besaß, war unter Mitteilung konkreter Informationen über dessen Vermögens- und Verschuldenslage an dessen Arbeitgeber herangetreten und hatte angefragt, ob dieser seinen Arbeitnehmer zur Vermeidung kostenträchtiger Pfändungsmaßnahmen zu freiwilligen Ratenzahlungen bewegen könne. Dazu hatte er eine entsprechende E-Mail an die allgemeine E-Mail-Adresse des Arbeitgebers gesandt. Dies bedauerte der Gläubiger mir gegenüber zwar ausdrücklich, gab dann aber – was die Sache nicht viel besser machte – an, dass er sich eigentlich direkt an die Personalabteilung hatte wenden wollen.

Ohne Einwilligung des Betroffenen, die hier natürlich nicht vorlag, gestattet § 4 Absatz 1 BDSG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet. Daran fehlte es aber im konkreten Fall. Erst ein richterlicher Pfändungs- und Überweisungsbeschluss berechtigt zur Lohnpfändung und damit zum Herantreten an den Arbeitgeber des Schuldners. Liegt ein solcher Beschluss nicht vor, überwiegen schutzwürdige Interessen des Beschäftigten, dass seine Vermögens- und Verschuldungslage seinem Arbeitgeber und seinem beruflichen Umfeld, insbesondere seinen Kollegen, nicht zur Kenntnis gelangt. Derartige Informationen sind regelmäßig geeignet, die Reputation des Betroffenen zu beschädigen. Dies gilt auch bzw. gerade gegenüber der Personalabteilung, für die geordnete finanzielle Verhältnisse eines Beschäftigten gemeinhin auch eine Compliance-relevante Frage sind. Der mit der E-Mail verfolgte Zweck, der Arbeitgeber möge seinen Beschäftigten zu einer freiwilligen Begleichung seiner Schulden „bewegen“, verfolgte im Übrigen schon keine berechtigte Interessen im Sinne von § 28 Absatz 1 Nummer 2 BDSG, da mit einem solchen Vorgehen offenbar sozialer Druck jenseits gesetzlich erlaubter Instrumente zur Beitreibung finanzieller Forderungen aufgebaut bzw. genutzt werden sollte.

Dass eine außergerichtliche Lösung zur Begleichung seiner Schulden möglicherweise auch im wirtschaftlichen Interesse des Betroffenen lag, legitimiert die Übermittlung an seinen Arbeitgeber nicht, denn Offerten dieser Art hätten dem Betroffenen auch unmittelbar unterbreitet werden können.

2.7.5.2 Anonyme Kundenbefragung

Ein Kunde eines Einkaufszentrums hatte sich wegen einer Kundenbefragung an mich gewandt. Er schilderte die Situation der Befragung als sehr aufdringlich und aggressiv. Die Fragesteller hätten sich nicht vorgestellt und auch nicht den Grund der Befragung erläutert. Der Kunde hatte das Gefühl, es sollte eine Situation der Überrumpelung ausgenutzt werden. Befragt worden sei der Kunde zunächst nach seiner Anschrift (Ort, Postleitzahl und Straße). Ausdrücklich nicht erfragt worden wären allerdings der Name des Kunden und die Hausnummer. Darüber hinaus seien Auskünfte zu Anzahl und finanzieller Höhe der Einkäufe in dem konkreten Einkaufszentrum sowie von Einkäufen in Konkurrenzeinkaufszentren erbeten worden. Sämtliche Informationen seien durch die Fragesteller in einem Smartphone gespeichert worden. Aufgrund der Art und Weise der Befragung habe der Kunde die Befragung abgebrochen. Mir gegenüber hatte er anschließend die datenschutzrechtliche Zulässigkeit der Befragung in Frage gestellt.

Ich habe dem Kunden zunächst einmal mitgeteilt, dass auch ich die geschilderte Kundenbefragung als sehr kundenunfreundliches Vorgehen bewerte und seinen Unmut nachvollziehen könne. Hinsichtlich der datenschutzrechtlichen Zulässigkeit der Befragung musste ich dem Kunden jedoch mitteilen, dass vorliegend keine personenbezogenen Daten im Rahmen der Kundenbefragung verarbeitet worden sind, da eine Zuordnung zu einer konkreten Person allein mit den erhobenen Daten nicht möglich ist. Die im Rahmen der Befragung erhobenen Daten beziehen sich lediglich auf eine Personengruppe, sodass die Befragung in Bezug auf den konkret betroffenen Kunden anonym erfolgt ist. Die Kundenbefragung unterfiel somit nicht dem Datenschutzrecht.

2.7.5.3 Begrüßungstafel im Hotel

Nach dem Hinweis eines Hotelgastes hatte ich die Praxis des Hotelbetreibers, neu ankommende Hotelgäste namentlich auf einer Begrüßungstafel in der Lobby zu begrüßen, zu überprüfen und zu bewerten.

Mit einer namentlichen Begrüßungstafel werden nicht nur ankommende Gäste empfangen, sondern zugleich auch alle anderen Gäste sowie alle sonstigen die Hotellobby betretenden Personen darüber unterrichtet, welche (Name und ggf. Vorname und Wohnort) Personen am jeweiligen Tag anreisen. Datenschutzrechtlich stellt dies eine Übermittlung personenbezogener Daten dar.

Nach § 28 Absatz 1 Satz 1 Nummer 1 BDSG ist das Übermitteln personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke nur zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Für den Hotelbetrieb als solchen bzw. für die Vertragserfüllung gegenüber den Hotelgästen ist eine namentliche Begrüßung, die von jedermann zur Kenntnis genommen werden kann, nicht erforderlich.

Auch aus § 28 Absatz 1 Satz 1 Nummer 2 BDSG, wonach eine Übermittlung (Bekanntgabe) personenbezogener Daten dann zulässig wäre, wenn es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung überwiegt, ergibt sich keine Zulässigkeit einer derartigen Verfahrensweise. Zur Verwirklichung des Servicegedankens sind andere individuelle Begrüßungsdienste (z. B. Begrüßungskärtchen auf dem Hotelzimmer oder namentliche Begrüßung auf dem TV-Hotel-Kanal) in gleicher Weise geeignet, zugleich aber weniger in das informationelle Selbstbestimmungsrecht eingreifend als eine öffentliche Bekanntgabe in der Lobby. Zudem ist zu berücksichtigen, dass es durchaus eine Reihe von Hotelgästen gibt, die – aus den verschiedensten privaten oder dienstlichen Gründen – gerade nicht wollen, dass allgemein bekannt wird, dass sie sich in diesem Hotel aufhalten. Insoweit besteht also durchaus auch Grund zu der Annahme, dass schutzwürdige Interessen der Betroffenen das – in diesem Fall als von eher geringfügiger Bedeutung einzustufende – Interesse an einer öffentlichen Begrüßung neuer Hotelgäste überwiegen.

Ebenso wie Dritten – von Ausnahmen abgesehen – keine Auskünfte über Hotelgäste gegeben werden dürfen, besteht auch keine Befugnis, diese Informationen im Rahmen einer Begrüßungstafel öffentlich bekanntzugeben.

2.7.5.4 Begrüßungsmonitor im Autohaus

Nicht nur – wie unter dem vorangegangen Punkt geschildert – in Hotels greift man offensichtlich gern auf Begrüßungstafeln zurück, sondern auch in Autohäusern.

Eine Kunde, der sich gerade ein neues Fahrzeug zugelegt hatte, war in dem betreffenden Autohaus von einem großen Monitor im Eingangsbereich empfangen worden. Auf diesem war zu lesen: „Wir begrüßen heute:“, gefolgt von einer Reihe von Vornamen, Namen und Fahrzeugkennzeichen. Auf seine Bitte hin, dass er nicht in diesem Benachrichtigungssystem auftauchen möchte, wurde ihm mitgeteilt, dass dies Teil des Qualitätsmanagements wäre und er über so viel Kundenfreundlichkeit doch froh sein sollte!

Auch hier gilt aber nichts anderes als in der Hotelbranche. Der Betrieb eines solchen Begrüßungsmonitors stellt eine Veröffentlichung von Kundendaten und damit eine Übermittlung personenbezogener Daten an Dritte dar und ist daher gemäß § 4 Absatz 1 BDSG nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der betroffene Kunde gemäß § 4a Absatz 1 BDSG ausdrücklich eingewilligt hat. So scheidet etwa § 28 Absatz 1 Satz 1 Nummer 1 BDSG aus, da eine solche Veröffentlichung für die Durchführung des Werkstatttermins nicht erforderlich ist. Auch die Heranziehung des § 28 Absatz 1 Satz 1 Nummer 2 BDSG scheitert daran, dass Kunden überwiegend schutzwürdige Interessen haben, dass ihre personenbezogenen Daten nicht auf dem Terminal beliebigen Dritten zugänglich gemacht werden. Im Gegensatz zu Hotels kann man bei Autohäusern wegen des hohen Stammkundenanteils zwar überlegen, ob man den Betrieb eines Begrüßungsmonitors über individuelle Einwilligungen rechtfertigt, gleichwohl dürfte eine im Ergebnis sicherlich nur partielle Kundenbegrüßung kaum im Interesse eines derart auf Qualitätsmanagement bedachten Autohauses liegen und daher gleichfalls ausscheiden.

2.7.6 Vereine / Verbände

2.7.6.1 Datenübermittlung an Behindertenverband in Verfahren nach RL Wohnraumanpassung

Ein Bürger beabsichtigte, die Förderung einer Rollstuhlgarage unter Anwendung der Richtlinie des Sächsischen Staatsministeriums des Innern zur Förderung der Anpassung von Wohnraum an Belange von Menschen mit Mobilitätseinschränkungen (RL Wohnraumanpassung – RL WRA) zu beantragen. Er rügte mir gegenüber, dass im Vorfeld des Genehmigungsverfahrens der regionale Behindertenverband einbezogen werden müsse und ihm dazu die entsprechenden personenbezogenen Daten zu übermitteln seien, ohne dass der Antragsteller in einem Mitgliedschaftsverhältnis zu dem Verein stehe.

Nach Prüfung des Sachverhaltes teilte ich dem betroffenen Bürger mit, dass das Förderverfahren gesetzlich in der RL Wohnraumanpassung geregelt sei. Gemäß Ziffer VII Nummer 2 RL WRA (SächsABl. 2017 Nummer 23, S. 758) ist einem Antrag auf Förderung eine Bestätigung einer hierfür vom Staatsministerium des Innern beauftragten Stelle beizufügen. Die Liste der regional zuständigen Stellen wird im Internet unter www.bauen-wohnen.sachsen.de bekannt gegeben. Der betreffende Behindertenverband war unter dieser Internetadresse als für den Landkreis des Bürgers zuständige Beratungsstelle genannt. Somit war der Behindertenverband für entsprechende Beantragungen zuständig und folglich legitimiert, die erforderlichen personenbezogenen Daten zu verarbeiten. Aufgrund dieser gesetzlichen Regelung stellte die Einbeziehung des Behindertenverbandes und die damit erforderliche Datenübermittlung und -verarbeitung keinen Datenschutzverstoß dar.

2.7.6.2 Häuserchronik

Ein Heimatverein arbeitete an einer Häuserchronik und hatte schon viele Informationen aus Archiven und alten Dokumenten gesammelt. Gleichwohl war er auch auf die Mitarbeit der aktuellen Hauseigentümer angewiesen, an die er sich mit einem Anschreiben, einem Befragungsformular und einer Einverständniserklärung gewandt hatte. Nicht alle Eigentümer waren jedoch bereit, diese ortsgeschichtliche Arbeit zu unterstützen; einige untersagten gar die Veröffentlichung jedweder Informationen zu den aktuell in ihrem Eigentum befindlichen Gebäuden. Die mir dazu übersandte Anfrage habe ich wie folgt beantwortet:

Angaben zu Gebäuden und Grundstücken sind immer auch personenbezogene Daten zu deren Eigentümern. Damit sind auch bei der Erstellung einer Häuserchronik die datenschutzrechtlichen Vorschriften zu beachten.

Dies bedeutet, dass die Datenerhebungen bei den Eigentümern grundsätzlich nur auf freiwilliger Basis erfolgen dürfen. Die spätere Veröffentlichung dieser personenbezogenen Daten ist von der schriftlichen Einwilligung der (noch) lebenden Betroffenen abhängig (§§ 4, 4a BDSG). Soweit Einwohner schriftlich oder auch nur mündlich jegliche Information bzw. Veröffentlichung untersagen, muss sich der Verein grundsätzlich auch daran halten. Allerdings kann dies mit Blick auf die Gebäude- und Grundstücksgeschichte nicht schrankenlos gelten – vielmehr findet dieses Einwilligungserfordernis seine Grenze im Zeitpunkt des Eigentumserwerbs bzw. bei früheren Eigentümern im Zeitraum des Eigentums.

Dies bedeutet, dass Informationen, die aus öffentlich zugänglichen Quellen, z. B. dörflichen Erzählungen, gewonnen oder von früheren Eigentümern (mit deren Einverständnis) bezogen worden, auch dann für die Häuserchronik verwendet werden dürfen, wenn dem der aktuelle Eigentümer widersprochen hat. Zwar weisen auch diese vergangenheitsbezogenen Informationen eine Verbindung zu den aktuellen Eigentümern auf und sind damit prinzipiell auch personenbezogene Daten der aktuellen Eigentümer, jedoch ist diese Verbindung – da es sich ja um die Geschichte des Gebäudes vor dem Erwerb durch die Betroffenen handelt –, sehr schwach, die Betroffenheit der aktuellen Eigentümer also nur marginal, sodass etwaige entgegenstehende Interessen der aktuellen Eigentümer gegenüber dem vom Verein verfolgten Interesse an der Erarbeitung einer ortsgeschichtlichen Dokumentation insoweit zurücktreten müssen (§ 28 Absatz 1 Satz 1 Nummer 2 BDSG).

2.7.7 Wohnungswirtschaft

2.7.7.1 WEG-Verwaltung: Weitergabe der Telefonnummer eines Mieters an den neuen Eigentümer

Nachdem ein Mietshaus verkauft worden war, wurde ein Mieter unvermittelt vom neuen Eigentümer auf seinem Mobiltelefon angerufen. Auf die Frage, woher er diese Nummer habe, teilte er dem Mieter mit, dass er diese von der vorherigen Hausverwaltung erhalten habe.

Grundsätzlich sehe ich den Vermieter einer Mietwohnung auf Grundlage von § 28 Absatz 1 Satz 1 Nummer 1 bzw. 2 BDSG befugt, zur kurzfristigen Erreichbarkeit des Mieters dessen Mobilfunkrufnummer zu erheben. Die Durchführung eines Mietverhältnisses sowie ein berechtigtes Interesse des Vermieters, gerade in Notfällen (z. B. unverzüglicher Zugang zur Wohnung bei Havarien) seinen Vertragspartner und gleichzeitig Verfügungsberechtigten seines Eigentums schnell zu erreichen, begründen das entsprechende datenschutzrechtliche Erfordernis.

Insoweit sah ich den bisherigen Verwalter auf Grundlage von § 28 Absatz 2 Nummer 2 Buchstabe a BDSG auch befugt, nach einem Eigentümerwechsel ebenso dem neuen Vermieter jene Rufnummer weiterzugeben, die der Mieter seinerzeit dem Voreigentümer für entsprechende Zwecke überlassen hatte.

Anders verhielte es sich allein dann, wenn er dem neuen Eigentümer eine andere gleichwertige Erreichbarkeit (sprich andere Rufnummer) angeboten und dem alten Verwalter die Weitergabe explizit untersagt hätte, etwa weil er diese Rufnummer anderen Erreichbarkeiten exklusiv vorbehalten wollte.

2.7.8 Energie- und Versorgungswirtschaft

2.7.8.1 Smart Meter

Nach der Schilderung eines Kunden wollte dessen örtlicher Netzbetreiber bei ihm den Einbau eines elektronischen Energiezählers – Smart Meter – durchsetzen. Dieser hatte sich bisher dem Einbau verweigert, da er erhebliche Bedenken gegen die Datengenauigkeit, -verarbeitung und -weitergabe hatte und der Auffassung war, dass Energieverbrauchsdaten aus seinem Haushalt über das zur Abrechnung erforderliche Maß (jährliche Ablesung) allein ihm zur Verfügung stehen dürfen. Er wollte damit auch verhindern, dass jetzt oder in Zukunft sein Verbrauchsprofil ausgelesen werden könne oder ihm tariflich oder anderweitig vorgeschrieben werde, wann er welche elektrischen Geräte nutzen dürfe.

Bei Einhaltung der bestehenden gesetzlichen Vorgaben habe ich trotz der sensiblen Datenverarbeitungen und besonderen Profilbildungsrisiken allerdings keine grundlegenden datenschutzrechtlichen Bedenken gegen den Einbau von Smart Metern:

So der Kunde nicht in eine weitergehende Datenverarbeitung einwilligt, dürfen seine Daten ausschließlich in den Fällen bzw. im Umfang des § 50 Messstellenbetriebsgesetz (MsbG) und zudem ausschließlich von den in § 49 Absatz 2 MsbG genannten Stellen erhoben, verarbeitet und genutzt werden. Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften – etwa durch Polizei bzw. Staatsanwaltschaften zur Strafverfolgung oder im Rahmen allgemein zivilrechtlicher Auseinandersetzungen beispielsweise zwischen Mieter und Vermieter – ist grundsätzlich unzulässig (§ 49 Absatz 1 Satz 2 MsbG). Das Ausmaß der Datenverarbeitung beschränkt sich also allein auf das vom Gesetzgeber definierte energiewirtschaftlich zwingende Maß und richtet sich primär nach dem jeweiligen Vertrag. So kein Tarif gewählt worden ist, der besondere Verarbeitungen erfordert, bleibt das betreffende Verarbeitungsmaß folglich (weiterhin) äußerst limitiert, zumal bis zu einem Jahresverbrauch bis 10.000 kWh die abrechnungsrelevanten Daten lediglich einmal pro Jahr an den Netzbetreiber und den Energielieferanten übermittelt werden (§ 60 Absatz 3 MsbG). Mithin trifft das Gesetz erhebliche Vorsorge, dass die eingesetzten Geräte auch sicherheitstechnisch hohen Anforderungen genügen.

Inwieweit der Kunde aktuell (schon) zur Duldung eines Einbaus verpflichtet ist, habe ich nicht zu beurteilen, da dies keine datenschutzrechtliche Frage ist.

2.7.9 Rechte Betroffener

2.7.9.1 Pflicht zur Erteilung von Negativauskünften?

Ein Betroffener wollte wissen, ob er Selbstauskünfte nach § 34 BDSG nur bei solchen Unternehmen einfordern dürfe, bei denen er wisse, dass er mit diesen eine vertragliche Beziehung eingegangen ist, oder ob er auch "blind" Anfragen stellen dürfe.

Nach § 34 Absatz 1 Satz 1 BDSG ist eine verantwortliche Stelle jedenfalls dann verpflichtet, dem Betroffenen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen, wenn sie solche auch tatsächlich verarbeitet. Eine Verpflichtung zu einer Negativauskunft ist weder im Gesetz enthalten, noch ist es in diesem Fall überhaupt anwendbar. Zudem regelt § 34 Absatz 1 Satz 2 BDSG, dass der Betroffene die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen soll, d. h. er sollte schon gewisse Anhaltspunkte dafür haben, dass die verantwortliche Stelle tatsächlich Daten über ihn speichert. Solche Anhaltspunkte können sich nicht nur aus bestehenden vertraglichen Beziehungen ergeben, sondern beispielsweise auch aus einer werblichen Ansprache oder aus Geschäftsbeziehungen mit anderen Unternehmen, von

denen bekannt ist, dass sie personenbezogene Daten unter konkreten Voraussetzungen weitergeben. Natürlich besteht das Recht auf Selbstauskunft nach § 34 BDSG auch gegenüber Adresshändlern oder Wirtschaftsauskunfteien, mit denen Betroffene im Allgemeinen keine vertraglichen Beziehungen pflegen.

Mit anderen Worten: Sicherlich können auch „blind“ Anfragen nach § 34 BDSG gestellt werden, jedoch darf dann nicht erwartet werden, dass in jedem Fall auch eine entsprechende Negativauskunft erteilt wird.

Allerdings zeichneten sich im Berichtszeitraum bereits diesbezügliche Änderungen im Interesse der Betroffenen ab. Ab 25. Mai 2018 schreibt Artikel 15 Absatz 1 DSGVO konkret vor, dass die betroffene Person das Recht hat, von dem Verantwortlichen eine Bestätigung darüber zu erlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ab dann muss also auch auf „blinde“ Anfragen in jedem Fall eine (Negativ-) Auskunft erteilt werden.

2.7.9.2 Selbstauskünfte

Im Berichtszeitraum haben mich wieder zahlreiche Eingaben wegen nicht oder unvollständig erteilter Auskunft (§ 34 BDSG) erreicht, denen auf verschiedene Weise aufsichtsrechtlich nachzugehen war und denen überwiegend auch abgeholfen werden konnte.

Darüber, dass ein Auskunftsverlangen überhaupt gestellt worden und in die Sphäre der verantwortlichen Stelle gelangt ist, ist im Zweifel der Betroffene beweisbelastet. Es ist daher stets anzuraten, den Versand eines Auskunftsverlangens angemessen zu dokumentieren. Zugleich erleichtert der – einer etwaigen Beschwerde stets beizufügende – Nachweis den Aufwand der behördlichen Sachverhaltsfeststellung und ermöglicht damit eine beschleunigte Bearbeitung. Betroffene sollten daher sicherstellen, dass zumindest eine Kopie des Verlangens vorliegt und Zeit sowie Art der Übermittlung dokumentiert worden sind.

Ein Auskunftsverlangen muss für den Empfänger als solches erkennbar, aber nicht zwingend so benannt werden. Außer Frage steht dabei die Pflicht des Auskunftsbegehrenden, sich eindeutig (oder durch rechtswirksame Vollmacht über einen Vertreter) als berechtigt auszuweisen.

Der Auskunftsanspruch nach § 34 BDSG entsteht mit dem eingehenden Verlangen des Betroffenen und umfasst sodann die Verpflichtung der verantwortlichen Stelle, die zur Person des Betroffenen gespeicherten Daten zu recherchieren, zusammenzustellen und diesem mitzuteilen – und zwar grundsätzlich vollständig. Normierte Ausnahmen hiervon bestehen gemäß § 34 Absatz 1 Satz 4 und Absatz 7 BDSG. Die Vorschrift des § 34

Absatz 1 Satz 2 BDSG, wonach der Betroffene die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen soll, kann dabei nicht in der Weise ausgelegt werden, dass ihm im Ergebnis all jene Auskunftsinhalte vorenthalten werden, von denen er keine Kenntnis hat. Die Auskunft hat insoweit stets in dem Sinne vollständig zu erfolgen, dass über alle objektiv vorliegenden Daten informiert wird.

Ein Immobilienunternehmen hatte zu einer potentiellen Hausverkäuferin (ausweislich der dem Auskunftsverlangen beigefügten E-Mail) eine Geschäftsbeziehung angebahnt und dafür einen vollständigen Namen, eine E-Mail-Adresse sowie eine Telefonnummer gespeichert. Jedoch hatte die Betroffene in ihrem Verlangen nach Auskunft nicht ausdrücklich mitgeteilt, dass sie – inzwischen einen anderen Nachnamen führend – mit der in der E-Mail angesprochenen Person identisch war. Das Unternehmen hat das Auskunftsverlangen daraufhin behandelt, als würde es keinerlei Kenntnisse über den Vorgang besitzen und der Betroffenen stattdessen u. a. mitgeteilt, dass eine erneute Kontaktaufnahme durch sie nicht gewünscht sei. Gegen eine knappe Rückfrage bezüglich des abweichenden Nachnamens hätte hier selbstverständlich nichts gesprochen.

Soweit ein externer Datenschutzbeauftragter die gegenüber der verantwortlichen Stelle geforderte Auskunft erstellt und verschickt, handelt dieser nicht als „weitere Firma“, an die Daten des Betroffenen übermittelt worden sind. Derlei betriebsinterne Verarbeitungen sind daher nicht auskunftspflichtig und bedürfen keiner Aufschlüsselung oder Erwähnung.

Ein Unternehmen hatte über E-Mails, die mit Daten des Betroffenen an Dritte versandt worden waren, unzutreffend keine Auskunft geben wollen. Der Auskunft zugänglich sind jedoch sämtliche elektronisch gespeicherte oder als Akten strukturierte Dokumente. Speicherinhalte eines E-Mail-Servers fallen selbstverständlich unter diesen Tatbestand.

Hinzuweisen hatte ich verantwortliche Stellen bei Beschwerden auch darauf, dass der Auskunftsanspruch grundsätzlich nicht nur die Kategorien von Daten (z. B. Telefonnummer, Bankverbindung), sondern auch die tatsächlichen Inhalte umfasst. Der Betroffene muss im Hinblick auf seine Berichtigungs- und Löschungsrechte die Möglichkeit erhalten, die Auskunft auch in Hinblick auf ihre Validität prüfen zu können.

2.7.9.3 Ordnungswidrigkeitenanzeigen unter Nachbarn

Es passiert recht häufig, dass ich bei Nachbarschaftsstreitigkeiten konsultiert werde. Selten geht es dabei noch um das eigentliche, ursprünglich streitauslösende Problem; vielmehr handelt es sich um Folgestreitigkeiten infolge gegenseitiger Überwachung und der Dokumentation tatsächlicher oder vermeintlicher Gesetzesverstöße. Dabei stellt sich dann regelmäßig auch die Frage, inwieweit jemand, der seinem Nachbar einen Geset-

zesverstoß vorwirft, berechtigt ist, diesen Verstoß zu dokumentieren und die so erzeugten Beweismittel den zur Ahndung der vorgeworfenen Handlungen zuständigen Behörden vorzulegen.

Soweit ein Nachbar personenbezogene Daten unter dem erklärten Ziel erhebt und verarbeitet, Beweismittel in Ordnungswidrigkeitenverfahren zu beschaffen und diese im Bedarfsfall bei Behörden vorzulegen, handelt er nicht aus rein persönlichen bzw. privaten Motiven, sondern als Sachwalter eigener oder öffentlicher Interessen im Rechtsverkehr. Demgemäß muss sein Handeln den Vorgaben des BDSG genügen (§ 1 Absatz 2 Nummer 3 BDSG). § 28 Absatz 1 Satz 1 Nummer 2 bzw. § 28 Absatz 2 Nummer 2 Buchstabe a bzw. Buchstabe b BDSG gestattet dabei dem redlichen Anzeigeerstatter – als insoweit legitimes Interesse – (auch nur vermeintliche) Rechtsverstöße zu dokumentieren und Behörden wahrheitsgemäß zur Kenntnis zu bringen. Dies gilt für Personen mit schützenswerten Eigeninteressen – insbesondere im Status des von einer Rechtsverletzung (Mit-)Betroffenen – uneingeschränkt, für den „Nichtverletzten“, der sich zum Sachwalter allein öffentlicher Interessen in der Rolle eines – denunziatorisch veranlagten – permanenten „Hilfsscheriffs“ aufschwingt, jedoch nur in den Grenzen sozialadäquaten Verhaltens (vgl. hierzu OVG Lüneburg, Beschluss vom 23. September 2013 – 13 LA 144/12 –, juris).

Wenn die von einem Nachbarn gerügten Verstöße offenbar seine diesbezügliche Sphäre als Eigentümer des Nachbargrundstücks betreffen, mag selbst bei unterstellter querulatorischer Neigung bei ihm ein hinreichendes Eigeninteresse vorliegen, das ihm datenschutzrechtlich sein Handeln insoweit gestattet. Schutz vor einem Übermaß bietet der Opportunitätsgrundsatz im Ordnungswidrigkeitenverfahren, wonach es allein der Behörde obliegt, in welchem Umfang sie zur Wahrung öffentlicher Interessen Ressourcen zur Aufklärung und Verfolgung von Ordnungswidrigkeiten aufwendet, oder – auch zur Wahrung des sozialen Friedens – fragwürdige Anzeigen unbearbeitet lässt (vgl. OVG Lüneburg, aaO). Zudem sind gegenüber Behörden wider besseren Wissens erhobene, also falsche, Tatsachenbehauptungen, die geeignet sind, ein Ordnungswidrigkeitenverfahren herbeizuführen, als falsche Verdächtigung strafbar (§ 164 Absatz 2 StGB). Betroffenen steht es frei, sich bei entsprechendem Verdacht an die zuständigen Strafverfolgungsbehörden zu wenden.

2.7.10 Verkehrs- und Beförderungswesen

2.7.10.1 Fahrausweiskontrollen: Übermittlung von Ticketdaten an den Verkehrsverbund

Ein ÖPNV-Nutzer war in eine Fahrkartenkontrolle geraten. Soweit kein Problem, denn er hatte eine Abo-Monatskarte in seinem Besitz. Ein vom Zugbegleiter eher lapidar hergesagter Satz ließ ihn jedoch aufhorchen und mit mir Kontakt aufnehmen. Auf Nachfra-

ge hatte ihm der Kontrolleur mitgeteilt, dass die elektronische Chipkarte nicht nur im Rahmen der aktuellen Fahrausweisprüfung ausgelesen werde, sondern die auf der Karte gespeicherten Daten würden auch an den Verkehrsverbund zur Auswertung weitergeleitet. Daraus erwuchs für ihn – nachvollziehbar – unmittelbar die Befürchtung der Bildung eines ihn betreffenden Bewegungsprofils.

Der Verkehrsverbund hat die Auskunft des Zugbegleiters als falsch zurückgewiesen. Zwar werden bei einer Kontrolle derartiger elektronischer Fahrscheine (Chipkarten) tatsächlich (Transaktions-)Daten an den Verkehrsverbund übermittelt, allerdings handelt es sich dabei nicht um Informationen zur Identifizierung des Karteninhabers, sondern um ticketbezogene Daten. Zweck der Übermittlung sei es, manipulierte Tickets festzustellen und – im Falle einer festgestellten Manipulation – die betreffenden Tickets auf der Chipkarte sperren zu können. Einzig die Ticket-Nummer lasse Rückschlüsse auf einen konkreten Kunden anhand von Kundendaten zu, allerdings ausschließlich durch das Ticket ausgebende Unternehmen, nicht durch den Verkehrsverbund. Im deutschlandweit gültigen Standard der VDV-Kernapplikation ist – nach Prüfung und Bestätigung durch die Datenschutzaufsichtsbehörden des Bundes und der Länder – geregelt, wie mit Transaktionsdaten und Kundendaten umzugehen ist. Der Verkehrsverbund verfügte insoweit über gar keine Kundendaten.

2.7.10.2 Zusätzliches Kontrollmedium bei HandyTickets

Mich erreichte die Anfrage eines Kunden von HandyTicket Deutschland, einer Smartphone-App zur Buchung eines Fahrscheins für verschiedene Verkehrsverbünde. Zur Nutzung dieser App ist eine vorherige Registrierung einschließlich der Erteilung einer Lastschrifteinzugsermächtigung erforderlich. Nachdem der Kunde über zwei Jahre lang mit dieser App problemlos Fahrscheine erworben und genutzt hatte, war er nunmehr durch einen Kontrolleur eines hiesigen Verkehrsunternehmens aufgefordert worden, zusätzlich zum ordnungsgemäß auf seinem Smartphone abgelegten Fahrschein auch den Personalausweis vorzuzeigen.

HandyTickets sind ebenso wie Online-Tickets nicht übertragbar. Den für diese Tickets genutzten Medien ist es allerdings immanent, dass – im Gegensatz zu konventionellen Tickets – eine Vervielfältigung problemlos möglich ist. Das HandyTicket kann problemlos elektronisch vervielfältigt und weitergegeben, auch das Online-Ticket kann ohne Weiteres kopiert werden. Vor diesem Hintergrund bedarf es einer Kontrolle, ob das Ticket auch tatsächlich durch die Person genutzt wird, durch die (bzw. im Fall eines Online-Tickets ggf. auch für die) es erworben worden ist.

Die Allgemeinen Geschäftsbedingungen HandyTicket Deutschland sehen daher ebenso wie die Beförderungsbedingungen des betreffenden Verkehrsverbundes vor, dass Han-

dyTickets nur in Verbindung mit einem entsprechenden, bei der Registrierung angegebenen Kontrollmedium gültig sind. Die für den Datenabgleich durch das Kontrollpersonal erforderlichen Informationen sind im QR-Code des HandyTickets hinterlegt. Den Schilderungen des Petenten habe ich entnommen, dass er sich bei der Registrierung für das HandyTicket für den Personalausweis als Kontrollmedium entschieden hatte. Alternative Kontrollmedien sind der Reisepass, die Bank- oder Maestrokarte und die Kreditkarte.

Datenschutzrechtliche Bedenken gegen diese Verfahrensweise bestehen nicht; die Zulässigkeit ergibt sich aus § 28 Absatz 1 Satz 1 Nummer 1 BDSG.

Auch wenn für weitere Personen zusätzliche HandyTickets gelöst werden, erfolgt eine Kontrolle bzw. ein Datenabgleich ausschließlich mit dem vom Kunden angegebenen (eigenen) Kontrollmedium.

Soweit in der Vergangenheit durch die jeweiligen Kontrolleure in anderen Verkehrsmitteln eine solche Identitätsprüfung nicht vorgenommen worden ist, kann daraus nicht der Schluss gezogen werden, dass diese nicht erforderlich oder nicht zulässig ist. Ich gehe insoweit davon aus, dass das Kontrollpersonal in Bezug auf die Intensität der Fahrausweiskontrolle einen gewissen Spielraum hat. Man kennt dies von elektronischen Zeitfahrausweisen (Chipkarten) oder auch der Bahncard.

2.7.10.3 Auslaufmodell: anonym erwerbbare Jahreskarte

Beim Barkauf einer Jahreskarte für 2018 wurde ein ÖPNV-Kunde im Dezember 2017 darauf hingewiesen, dass es diese Möglichkeit zukünftig nicht mehr geben werde. Als Alternative wurde ihm der Abschluss eines Abo-Vertrags angeboten.

Er bedauerte dies, weil ihm damit die Möglichkeit einer vollständig anonymen Nahverkehrsnutzung genommen schien. Die bis dahin angebotene Jahreskarte sei in Verbindung mit der Barzahlungsmöglichkeit ein gutes Beispiel für die Verwirklichung des Prinzips der Datenvermeidung (§ 3a BDSG) gewesen. Zukünftig sei bei gelegentlichen Fahrausweiskontrollen bzw. bei der Nutzung von Bussen im Regionalverkehr und im Stadtverkehr ab 20 Uhr (regelmäßige Fahrausweisprüfung beim Einstieg) jedenfalls theoretisch über die Abo-Daten ein Bezug zum Fahrkarteninhaber herstellbar und damit die Erstellung von Bewegungsprofilen vorstellbar.

Ich teile die Einschätzung des Kunden, dass das Auslaufen der bis dahin auch vollständig anonym käuflichen Jahreskarte bei dem betreffenden Verkehrsunternehmen datenschutzunfreundlich ist. Datenschutzunfreundlich ist jedoch nicht gleichzusetzen mit datenschutzrechtlich unzulässig. Letzteres wäre nur dann anzunehmen, wenn es einen Anspruch auf ein bestimmtes bzw. jedes Ticket auch in anonymer Form gäbe, solange dies

prinzipiell möglich ist. Soweit geht das Datenschutzrecht jedoch nicht. Die Prinzipien der Datensparsamkeit und Erforderlichkeit gebieten allenfalls, überhaupt eine anonyme Zahlung und Nutzung von Verkehrsmitteln zu ermöglichen. Letzteres steht aber solange nicht infrage, wie zumindest einige gängige Fahrscheine weiterhin zu vergleichbaren Preisen anonym erworben und genutzt werden können, es also keinen allgemeinen mittelbaren Zwang zur Verarbeitung personenbezogener Daten gibt. Angesichts der weiterhin bestehenden Automatenverkäufe mit der Möglichkeit des Barerwerbs üblicher Fahrkarten (auch Monatskarten), sehe ich die Grenze des Zulässigen in diesem Fall noch nicht überschritten.

Hinzuzufügen ist, dass es sich vorliegend um eine Änderung der Fahrschein- und Preismodelle im gesamten Verkehrsverbund gehandelt hatte. Es war nicht etwa nur die Barzahlungsmöglichkeit bei Jahreskarten abgeschafft worden, sondern vielmehr die Jahreskarte insgesamt. Abo-Monatskarten erfordern schon wegen der monatlichen Zahlungsweise regelmäßig die Verarbeitung von Kundendaten. Im Übrigen handelt es sich bei der vermuteten Erstellung von Bewegungsprofilen nur um eine theoretische Möglichkeit. Die Datenschutzgrundsätze der Verkehrsunternehmen bzw. der Verkehrsverbünde erlauben eine solche Datennutzung nicht. Zudem erforderte dies die regelmäßige Erfassung der Nahverkehrsmittelnutzung inkl. des Ein- und Ausstiegs. Bekanntermaßen ist aber – mit Ausnahme der o. g. Kontrollen beim Einstieg – gerade keine An- und Abmeldung beim Ein- und Ausstieg notwendig. In Straßenbahnen, den Nahverkehrszügen, insbesondere der S-Bahn, und den Bussen im Großstadtverkehr erfolgt die Kontrolle der Fahrausweise unverändert durch mobile Kontrolleure und daher nur zufällig.

2.7.10.4 SMS-Aufforderung zur Bewertung von Taxifahrten

Mir war mitgeteilt worden, dass eine Taxigenossenschaft Mobiltelefonnummern, über die bei ihr Taxibestellungen getätigt worden waren, nachfolgend auch dazu verwendete, um den betreffenden Bestellern SMS zuzusenden, etwa um das unmittelbar bevorstehende Eintreffen des Taxis anzukündigen oder nach der Fahrt zur Abgabe einer Bewertung aufzufordern. Darüber hinaus war mir geschildert worden, dass die Mobiltelefonnummern auch an die beauftragten Taxifahrer weitergegeben würden. Eine Unterrichtung der Kunden bzw. Besteller über diese Datennutzungen bzw. die Datenweitergabe sollte nicht erfolgt sein.

Soweit Kunden eines Taxis per SMS über das baldige Eintreffen des bestellten Taxis unterrichtet werden, ist aus § 28 Absatz 1 Satz 1 Nummer 1 BDSG mangels Erforderlichkeit zur Vertragserfüllung keine Zulässigkeit herzuleiten. Jedoch kann an dieser Stelle alternativ auch § 28 Absatz 1 Satz 1 Nummer 2 BDSG, mithin eine Interessenabwägung, die Zulässigkeit einer solchen Datennutzung begründen. Die Benachrichtigung über das baldige Eintreffen des bestellten Taxis ist eine Serviceleistung der Genossen-

schaft für den Kunden; entgegenstehende Interessen der Kunden sollten also nicht anzunehmen sein. Allerdings muss auf geeignete Weise sichergestellt werden, dass Besteller und Kunde auch identisch sind.

Diese Einschätzung gilt jedoch nicht mehr in Bezug auf die nachträgliche Aufforderung zur Bewertung der Fahrt. Einer diesbezüglichen Datennutzung steht § 28 Absatz 3 Satz 6 BDSG i. V. m. § 7 UWG entgegen, d. h. die Genossenschaft benötigte dafür die vorherige Einwilligung des Betroffenen (vgl. z. B. OLG Köln, Urteil vom 30.03.2012, Az. 6 U 191/11). Die Bekanntgabe der Handy-Nummer im Rahmen der Taxi-Bestellung stellt insoweit keine wirksame Einwilligung dar. Ich habe die Genossenschaft daher aufgefordert, diese Praxis einzustellen, oder aber alternativ die vorherige Einwilligung der betreffenden Kunden einzuholen. Die bloße Dokumentation einer telefonisch erteilten Einwilligung dürfte hierfür angesichts der die Genossenschaft treffenden Beweislast im Streitfall nicht ausreichend sein. Die Genossenschaft hat daraufhin das Verfahren so umgestellt, dass mit der Benachrichtigungs-SMS zugleich das Einverständnis zur Übersendung des Bewertungslinks erbeten wird.

Hinsichtlich der Weitergabe der Telefonnummer des Kunden an den jeweils beauftragten Taxifahrer hat mich die Taxigenossenschaft informiert, dass eine solche Weitergabe nur im Ausnahmefall und nur nach telefonischer Einwilligung des Kunden erfolge. Einen Automatismus gebe es insoweit nicht, vielmehr bedürfe es einer zusätzlichen ausdrücklichen Eingabe im Vermittlungssystem (Vermerk im Fahrauftrag).

2.7.11 Betrieblicher Datenschutzbeauftragter

2.7.11.1 Information der Belegschaft über bestellten Datenschutzbeauftragten

Aus der Belegschaft eines Unternehmens war mir mitgeteilt worden, dass dort nicht bekannt und auch nicht in Erfahrung zu bringen sei, wer aktuell als betrieblicher Datenschutzbeauftragter bestellt und wie er zu erreichen ist. Noch nicht einmal der Betriebsrat sei in der Lage, diese Person zu benennen.

Nach § 4f Absatz 5 Satz 2 BDSG können sich Betroffene – und dazu gehören auch und vor allem die Mitarbeiter – jederzeit an den betrieblichen Datenschutzbeauftragten wenden. Wenn der Belegschaft allerdings keinerlei Informationen über die Person des betrieblichen Datenschutzbeauftragten zur Verfügung gestellt werden, wird dieses Anrufungsrecht untergraben. Den Betroffenen ist auch nicht zuzumuten, sich über die Geschäftsführung oder andere Leitungspersonen an den betrieblichen Datenschutzbeauftragten zu wenden, denn dies wiederum läuft den nach § 4f Absatz 4 BDSG bestehenden Verschwiegenheitspflichten des betrieblichen Datenschutzbeauftragten zuwider. § 4f Absatz 5 Satz 2 BDSG gewährleistet also nicht nur den Zugang zum Beauftragten, sondern schließt auch Umwege aus, die den Betroffenen die Möglichkeit nehmen könn-

ten, den Beauftragten ebenso schnell wie vertraulich anzurufen (vgl. Simitis, BDSG 8. Aufl., Rdnr. 161 zu § 4f). Nicht zuletzt nährt eine mangelnde Kommunikation der Kontaktdetails des betrieblichen Datenschutzbeauftragten auch Zweifel an dessen Zuverlässigkeit, denn sie suggeriert, dass dieser nicht wirklich gewillt ist, seinen diesbezüglichen Aufgaben nachzukommen.

Ich habe die verantwortliche Stelle aufgefordert, umgehend dafür zu sorgen, dass deren Mitarbeitern aktiv bekanntgemacht wird, wer als betrieblicher Datenschutzbeauftragter bestellt worden und wie er erreichbar ist. Die verantwortliche Stelle hat auch dafür zu sorgen, dass diese Information allen Mitarbeitern, insbesondere auch Neueinstellungen, jederzeit zur Verfügung steht, beispielsweise durch Veröffentlichung im Intranet, (dauerhafter Aushang) am Schwarzen Brett oder im innerbetrieblichen Telefonbuch. Eine einmalige Information aller Mitarbeiter würde insoweit also nicht genügen.

2.7.11.2 Mindestbestelldauer für externe betriebliche Datenschutzbeauftragte

Ein externer betrieblicher Datenschutzbeauftragter hatte sich zur Thematik Mindestbestelldauer an mich gewandt und um einen Hinweis gebeten, welche Zeiträume bei der Bestellung eines externen betrieblichen Datenschutzbeauftragten zu beachten seien.

Ich habe dem Datenschutzbeauftragten mitgeteilt, dass die Mindestbestelldauer eines externen betrieblichen Datenschutzbeauftragten vier Jahre umfassen sollte. Bei der Erstbestellung ist ein kürzerer Zeitraum möglich, allerdings sollte er grundsätzlich zwei Jahre nicht unterschreiten.

Die Festlegung einer solchen Mindestbestelldauer ist in den auf einen längeren Zeitraum angelegten Aufgaben des Datenschutzbeauftragten begründet. Die vorgenannte Mindestbestelldauer entspricht dem Beschluss des Düsseldorfer Kreises vom 24./25. November 2010 zu den Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Absatz 2 und 3 BDSG (vgl. 5. TB, Punkt 13.6.3). In diesem Zusammenhang verweise ich auch auf meine Ausführungen zu Kündigungsfristen bei externen Datenschutzbeauftragten in meinem 7. TB unter Punkt 8.11.2.

2.7.12 Technische und organisatorische Maßnahmen

2.7.12.1 Löschung der Sendehistorie bei Faxgeräten

Müssen in Multifunktionsgeräten (Drucker, Scanner, Fax) gespeicherte Faxprotokolle gelöscht werden, wenn diese weiterverkauft werden? Die Faxprotokolle enthalten folgende Daten: Datum, Uhrzeit, Zielnummer, Übertragungsdauer, Seitenanzahl, Übermittlungsergebnis. Nach Mitteilung eines insoweit um Beratung ersuchenden betrieblichen Datenschutzbeauftragten sei das Löschen bzw. Überschreiben der Sendehistorie nur

möglich, indem man von dem Gerät genauso viele Faxe verschickt, wie es Einträge in der Sendehistorie gibt. Eine solche Vorgehensweise sei weder verhältnismäßig noch wirtschaftlich. Zudem stellten die Faxprotokolle seiner Ansicht nach keine personenbezogenen Daten dar, da sich diese weder unmittelbar noch mittelbar einer Person zuordnen lassen würden.

Sollten sich Zielfaxrufnummern in der Sendehistorie der zum Verkauf stehenden Geräte befinden, die einer natürlichen Person als Anschlussinhaber zugeordnet sind, handelt es sich bei den insoweit gespeicherten Informationen stets um personenbezogene Daten. Da für diese keine Übermittlungsbefugnis besteht, wären diese Daten also vor einer Weiterveräußerung zu löschen. Eine geräteseitig fehlende – einfache – Löschroutine bzw. der zur Löschung notwendige (wirtschaftliche) Aufwand befreien nicht von dieser Verpflichtung. Das Gesetz (§ 35 Absatz 2 Nummer 1, Absatz 3 Nummer 3 BDSG) befreit von der Verpflichtung zur Löschung aus Gründen der Verhältnismäßigkeit nur, wenn stattdessen zumindest eine Sperrung der Daten erfolgt. Hier ist aber nicht ersichtlich, wie diese erfolgen könnte, so dass es bei der Löschverpflichtung verbleibt. Dies mag angesichts des damit verbundenen Aufwands – auch für mich – eine äußerst unbefriedigende Antwort sein, ist aber nach der Rechtslage alternativlos. Die Erfahrung lehrt, dass sich in vielen Geräten zumindest verborgene Löschroutinen verbergen, die eine schnelle und damit vertretbare Bereinigung der Sendehistorie erlauben. Insofern habe ich die Anregung gegeben, nochmals beim Hersteller, im Fachhandel oder in einschlägigen Internetforen Rat zu suchen.

2.8 Informationspflichten bei Datenpannen

Nach § 42a BDSG sind die verantwortlichen Stellen verpflichtet, festgestellte Fälle unrechtmäßiger Datenübermittlung oder sonstiger unrechtmäßiger Kenntniserlangung durch Dritte der Aufsichtsbehörde unter bestimmten Voraussetzungen – namentlich wenn die in § 42a Satz 1 BDSG aufgezählten Datenarten betroffen sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen – mitzuteilen.

Im Berichtszeitraum sind bei mir 37 solcher Meldungen eingegangen. Im Vergleich zum vorherigen – zweijährigen – Berichtszeitraum mit 46 Meldungen ist daher erneut eine (relative) Erhöhung der Anzahl eingegangener Meldungen festzustellen. Lediglich in einem Fall konnte die Meldepflicht verneint werden, da keine nach § 42a BDSG maßgeblichen Daten betroffen waren.

In 36 Fällen hat eine Meldepflicht bestanden:

- Fehlversand von Entgeltbelegen infolge einer Fehlkuvertierung eines Personaldienstleisters (fünf Meldungen) (Bankdaten)
- Fehlversand von Unterlagen infolge einer Adressverwechselung durch eine Versicherung (zwei Meldungen) (Daten, die einem Berufsgeheimnis unterliegen)
- Fehlversand von Unterlagen infolge einer Adressverwechselung durch einen Finanzdienstleister (Bankdaten)
- Fehlversand von Unterlagen infolge einer Adressverwechselung durch ein Kreditinstitut (Bankdaten)
- Fehlversand einer SEPA-Lastschrift-Vorabinformation (Pre-Notification) infolge einer Adressverwechselung durch ein Unternehmen (Bankdaten)
- Fehlversand von Unterlagen infolge einer Adressverwechselung durch eine medizinische Einrichtung (Gesundheitsdaten)
- Entwendung von Beratungsprotokollen in einer Bankfiliale (Bankdaten)
- Verlust eines Datenträgers auf dem Postweg bei einer medizinischen Einrichtung (zwei Meldungen) (Gesundheitsdaten)
- Diebstahl eines Speichermediums in einer Arztpraxis (Gesundheitsdaten)
- Hackerangriff auf die Datenbank eines Webbetreibers (besondere Arten personenbezogener Daten)
- Datenleck eines Internetdiensteanbieters für medizinische Produkte (Gesundheitsdaten)
- unberechtigte Zugriffsmöglichkeit auf ein Online-Banking-Konto bei einem Kreditinstitut (zwei Meldungen) (Bankdaten)
- Diebstahl eines Speichermediums bei einem Verein (besondere Arten von personenbezogenen Daten, Gesundheitsdaten)
- gewaltsames Öffnen von Überweisungsbriefkästen in Bankfilialen (sechs Meldungen) (Bankdaten)
- Hackerangriff auf den PC einer Arztpraxis (Gesundheitsdaten)
- unberechtigtes Filmen einer Patientin durch einen Pfleger in einem Krankenhaus (Gesundheitsdaten)
- Entwendung von Überweisungsbelegen in einem Kreditinstitut (Bankdaten)
- unberechtigte Zugriffsmöglichkeit auf ein Online-Kundenkonto bei einem Unternehmen (Bankdaten)
- Falschbuchung eines Kreditinstituts (Bankdaten)

- falsche Separierung eines Pfändungsbetrages durch einen Finanzdienstleister (Daten, die einem Berufsgeheimnis unterliegen)
- Telefongesprächsaufzeichnung einschließlich externer Zugriffsmöglichkeit infolge der Fehlkonfiguration einer TKA (Daten nicht näher spezifiziert)
- Hackerangriff auf den Server eines Unternehmens (drei Meldungen)

In Bezug auf die betroffenen Daten liegt – wie in den Berichtszeiträumen zuvor – der Schwerpunkt der Meldungen auf Bank- und Gesundheitsdaten. Dabei traf die Meldepflicht vor allem Kreditinstitute sowie Unternehmen der Gesundheitsbranche. Wie bereits im vorherigen Berichtszeitraum führte der Fehlversand von Unterlagen besonders häufig zu einer Meldepflicht. Ursachen waren einerseits subjektive Fehlleistungen der jeweiligen Bearbeiter (Adressverwechselungen) und andererseits technisch begründete Fehlkuvertierungen. Insoweit bedarf es also insbesondere einer verstärkten Sensibilisierung der betreffenden Personenkreise im Hinblick auf diese Fehlerquellen sowie der Implementierung verbesserter technischer Verfahren.

Erstmals aufgetreten sind Meldungen infolge gewaltsamen Öffnens von Nachtbriefkästen in Bankfilialen. Ziel war es hier, darin enthaltene Überweisungsbelege zu entwenden.

Nach wie vor aufgetreten sind Fälle des physischen Datenträgerverlustes, sei es durch Verlust auf dem Postweg, sei es durch Einbrüche oder Diebstähle. Der Einsatz wirksamer Verschlüsselungsverfahrenen könnte die mit solchen Vorfällen verbundenen Risiken für die Persönlichkeitsrechte der Betroffenen maßgeblich mindern.

2.9 Stellungnahmen zu Unterlassungsklagen

Nach § 12a UKlaG hat das Gericht vor einer Entscheidung in einem Verfahren über einen Anspruch nach § 2 UKlaG, das eine Zuwiderhandlung gegen ein Verbraucherschutzgesetz nach § 2 Absatz 2 Satz 1 Nummer 11 UKlaG zum Gegenstand hat, die zuständige inländische Datenschutzbehörde zu hören.

Im Berichtszeitraum gingen im Rahmen von Verbandsklagen nach dem Unterlassungsklagengesetz zwei gerichtliche Anhörungen bei mir ein.

Gegenstand beider Klagen war die datenschutzrechtliche Bewertung der Übertragung von Kundendatenbanken im Wege eines Asset-Deals. Da ich mich bereits im letzten Berichtszeitraum mit dieser Thematik umfassend beschäftigt und hierzu ausgeführt hatte, wiederholte ich gegenüber dem Gericht meine Ausführungen aus dem 8. Tätigkeitsbericht unter Punkt 8.14.1, auf welche ich auch hier vollumfänglich verweise.

2.10 Öffentlichkeitsarbeit

Die Aufsichtsbehörden für den nicht-öffentlichen Bereich haben regelmäßig, spätestens jedoch alle zwei Jahre, einen Tätigkeitsbericht zu veröffentlichen (§ 38 Absatz 1 Satz 7 BDSG).

Der nunmehr neunte Tätigkeitsbericht zum Datenschutz im nicht-öffentlichen Bereich ist zugleich auch der insoweit letzte, ausschließlich den nicht-öffentlichen Bereich betreffende Bericht. Er deckt lediglich einen Zeitraum von knapp 14 Monaten ab, denn mit dem 24. Mai 2018 endet die Geltung des Bundesdatenschutzgesetzes in seiner bisher bekannten Form und damit entfällt zu diesem Zeitpunkt auch die diesbezügliche Berichtspflicht. Gleichwohl werde ich auch zukünftig über meine Tätigkeit berichten, nur entfällt dabei die bisherige Trennung zwischen öffentlichem und nicht-öffentlichem Bereich. Zukünftig wird es jährlich einen einheitlichen Tätigkeitsbericht geben (Artikel 59 DSGVO).

Der vorliegende Bericht kann – ebenso wie alle vorangegangenen Tätigkeitsberichte – per Download von meinem Internetauftritt (http://www.datenschutz.sachsen.de) bezogen bzw. als Druckexemplar bei mir abgerufen werden. Darüber hinaus halte ich im Internet weitere Informationen, z. B. bundesweit abgestimmte Orientierungshilfen und Anwendungshinweise, zu aktuellen Themen insbesondere der Datenschutz-Grundverordnung zum Abruf bereit. Besonderes Augenmerk möchte ich auf die immerhin 20 Kurzpapiere zur Datenschutz-Grundverordnung lenken, aus denen eine insoweit zwischen den Aufsichtsbehörden des Bundes und der Länder abgestimmte einheitliche Auffassung zu den drängendsten Fragen der Datenschutz-Grundverordnung entnommen werden kann. Zur Vermeidung von Missverständnissen habe ich – ausgenommen meine Tätigkeitberichte – die sich noch auf die alte Rechtslage (Bundesdatenschutzgesetz) beziehenden Fachbeiträge von meiner Website entfernt. Diese werden schrittweise überarbeitet, d. h. an die Datenschutz-Grundverordnung angepasst, und anschließend wieder online gestellt. Parallel dazu beabsichtige ich auch eine komplette Neugestaltung meiner Webpräsenz.

Den im Berichtszeitraum erwartungsgemäß besondere zahlreich an mich gerichteten Anfragen wegen einer Referententätigkeit bei verschiedenen Fach- und Fortbildungsveranstaltungen konnte ich wegen der unverändert äußerst angespannten Personalsituation leider nur in sehr geringem Umfang entsprechen. Ich bedauere dies ausdrücklich, musste mir aber eingestehen, dass die mir im Berichtszeitraum zur Verfügung gestandenen personellen Ressourcen die Wahrnehmung derartiger Aufgaben einfach nicht in größerem Umfang zugelassen haben, zumal ich auch zahlreiche Aufgaben in Vorbereitung meiner zum 25. Mai 2018 erreichten vollumfänglichen Selbständigkeit als oberste Staatsbehörde zu erledigen hatte.

Auch in Bezug auf die vierteljährlich stattfindenden Erfa-Kreise der GDD musste ich mein Engagement aus diesem Grund wiederum einschränken und konnte nur noch vereinzelt an dessen Tagungen teilnehmen. Das ist sehr bedauerlich, da der Austausch mit den auf diesen Veranstaltungen anwesenden betrieblichen Datenschutzbeauftragten für beide Seiten immer sehr gewinnbringend gewesen ist und gerade in Bezug auf die kommende Datenschutz-Grundverordnung ein erhöhter Informationsbedarf bestanden hat.

2.11 Durchsetzung der Rechte und Befugnisse der Aufsichtsbehörde

2.11.1 Förmliche Heranziehung zur Auskunft

Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen (§ 38 Absatz 3 Satz 1 BDSG).

Förmliche Auskunftsheranziehungsbescheide waren für mich schon immer ein adäquates und wirksames Mittel, um von verantwortlichen Stellen, die zuvor im Regelfall mindestens zwei aufsichtsbehördliche Schreiben ignoriert oder die Auskunftserteilung aktiv verweigert hatten, die zur Aufgabenerfüllung erforderlichen Auskünfte zu erhalten. Der Erlass eines solchen Bescheides ist regelmäßig mit einer Gebühr von mindestens 150 € (bis max. 1.500 €, vgl. Nummer 2 der Anlage zu § 40 SächsDSG) verbunden gewesen. Die Anzahl der insoweit notwendig gewordenen Heranziehungsbescheide bewegte sich in etwa auf dem Vorjahresniveau (hochgerechnet auf einen vergleichbaren Zweijahreszeitraum):

Berichtszeitraum		01.01.09 31.12.10	01.01.11 31.03.13	01.04.13 31.03.15	01.04.15 31.03.17	**01.04.17 24.05.18**
Förmliche Heranziehungen		7	31	20	18	**11**
davon	mit einmaliger Zwangsgeld-festsetzung	4	6	9	4	**3**
	mit zweimaliger Zwangsgeld-festsetzung	0	0	3	0	**0**
	Klage gegen den Heranziehungs-bescheid	0	2	1	4	**0**

In allen Fällen ist die Auskunftserteilung nach Erlass des Heranziehungsbescheides bzw. spätestens nach der erstmaligen Festsetzung eines Zwangsgeldes schließlich doch

noch erfolgt; Rechtsmittel gegen meine Bescheide wurden nicht eingelegt. Auch das noch offene Klageverfahren aus dem letzten Berichtszeitraum ist inzwischen zu meinen Gunsten (Klageabweisung) entschieden worden. Die Gesamtsumme der im Berichtszeitraum festgesetzten drei Zwangsgelder beträgt 3.200 €.

Auch mit der Zahlung eines Zwangsgeldes erlischt die Auskunftspflicht der verantwortlichen Stelle nicht. Zwangsmittel können nach § 19 Absatz 5 SächsVwVG wiederholt und so lange angedroht werden, bis die verantwortliche Stelle ihrer Verpflichtung nachgekommen ist. Das Zwangsverfahren wird aber eingestellt, sobald die geforderten Auskünfte erteilt worden sind. Allerdings müssen verantwortliche Stellen in solchen Fällen regelmäßig mit der Einleitung eines Bußgeldverfahrens rechnen.

2.11.2 Anordnungen

Zur Gewährleistung der Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden (§ 38 Absatz 5 Sätze 1 und 2 BDSG).

Die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Absatz 2 Satz 1 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. Der Auskunftspflichtige hat diese Maßnahmen zu dulden (§ 38 Absatz 4 Sätze 1, 2 und 4 BDSG).

Im Berichtszeitraum habe ich drei Anordnungen erlassen müssen, zwei davon betrafen Maßnahmen zur Beseitigung festgestellter Datenschutzverstöße (§ 38 Absatz 5 BDSG), die dritte bezog sich auf die Duldung einer aufsichtsbehördlichen Kontrollmaßnahme (§ 38 Absatz 4 BDSG). Alle Anordnungen sind bestandskräftig geworden; Zwangsgeldfestsetzungen sind insoweit nicht notwendig geworden.

Die beiden Anordnungen zur Beseitigung von Datenschutzmängeln betrafen jeweils die veränderte Ausrichtung von (auch) öffentliche Verkehrsbereiche erfassenden Videoüberwachungskameras.

Mit der Duldungsanordnung habe ich einer verantwortlichen Stelle zur Sicherstellung eines ordnungsgemäßen und erfolgreichen Ablaufs einer von mir angekündigten örtlichen Kontrolle aufgegeben,

- das Betreten der geschäftlich genutzten Räumlichkeiten während der Öffnungszeiten durch Bedienstete meiner Behörde zu dulden sowie
- Prüfungsmaßnahmen meiner Bediensteten betreffend die inner- und außerhalb der Geschäftsräume betriebene Videoüberwachungsanlage zu unterstützen, indem sie die Einsichtnahme in diesbezügliche Datenverarbeitungsprogramme und Datenverarbeitungsanlagen, auch soweit diese durch Passwörter gesichert sind, ermöglicht und insbesondere auch die Funktionalitäten der Videoüberwachungsanlage selbst demonstriert oder durch fachkundige Personen demonstrieren lässt.

Für Anordnungen werden – in gleicher Weise wie für Heranziehungsbescheide (vgl. Punkt 2.11.1) – gemäß Nummer 3 der Anlage zu § 40 SächsDSG Gebühren in Höhe von 150 bis 1.500 € fällig.

2.11.3 Kostenerhebung

Ich kann für Amtshandlungen und sonstige öffentlich-rechtliche Leistungen nach dem Bundesdatenschutzgesetz Kosten (Gebühren und Auslagen) erheben (§ 40 Absatz 1 SächsDSG).

Nach § 40 SächsDSG durfte ich von nicht-öffentlichen Stellen insbesondere dann einen Kostenausgleich verlangen, wenn ich bei meiner Prüfung Datenschutzverstöße festgestellt habe. Auch datenschutzrechtliche Beratungen nicht-öffentlicher Stellen waren im Regelfall kostenpflichtig. Lediglich Kontrollen und Beratungen einfacher Art sowie die Beratung von Stellen ohne Gewinnerzielungsabsicht blieben kostenfrei. Für Anordnungen, Untersagungen, Abberufungen von Datenschutzbeauftragten sowie bestimmte Prüfungen, Verfahren oder Genehmigungen waren in der Anlage zu § 40 SächsDSG spezielle Kostensätze festgelegt.

Auf der Grundlage dieser Gebührenregelung habe ich im Berichtszeitraum bzw. infolge der im Berichtszeitraum erlassenen Bescheide tatsächliche Einnahmen in Höhe von mehr als 21.000 € erzielen können. Dies liegt zwar absolut unter der Summe des letzten Berichtszeitraums (ca. 27.000 €), hochgerechnet auf den üblichen Zweijahreszeitraum

würde dies aber einer Summe von ca. 37.000 € (+37 %), mithin einer deutlichen Steigerung entsprechen. Diese Einnahmen stammen aus:

- 42 Mängelfeststellungen bei Datenschutzkontrollen (§ 38 Absatz 1 Satz 1 BDSG),
- 12 Heranziehungsbescheiden (§ 38 Absatz 3 Satz 1 BDSG),
- 5 Anordnungen (§ 38 Absatz 4, 5 BDSG),
- 4 Beratungen (§ 38 Absatz 1 Satz 2 BDSG) sowie
- Registervorgängen (§ 38 Absatz 2 Satz 1 BDSG).

Die Akzeptanz meiner Kostenbescheide ist deutlich höher als die meiner Bußgeldbescheide. In lediglich zwei Fällen haben verantwortliche Stellen in Bezug auf die Kostenerhebung Klage erhoben. In einem Fall ist die Klage in der Hauptverhandlung wieder zurückgenommen worden; im andern Fall steht eine gerichtliche Entscheidung noch aus.

Auch die beiden Klageverfahren aus dem letzten Berichtszeitraum sind zu meinen Gunsten entschieden worden: Einmal wurde die Klage abgewiesen, einmal zurückgenommen.

2.12 Ordnungswidrigkeitenverfahren

Als Verwaltungsbehörde nach § 36 Absatz 2 OWiG (§ 15 OWiZuVO) bin ich für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 43 BDSG, § 16 Absatz 2 Nummer 2 bis 5 TMG sowie § 130 OWiG zuständig.

Im Berichtszeitraum sind insgesamt 69 Bußgeldverfahren bei mir anhängig gewesen; drei davon stammten noch aus den Vorjahren (vgl. 8. TB, Punkt 13.1). Rechnet man die neu eingeleiteten Verfahren auf den bisher üblichen Zweijahreszeitraum hoch, kommt man auf 113 Verfahren, was den bislang höchsten Wert darstellt.

In 17 Fällen habe ich die vorgeworfenen Datenschutzverstöße mit einem Bußgeldbescheid geahndet; in sieben weiteren Fällen habe ich lediglich eine Verwarnung ausgesprochen und dies – von einer Ausnahme abgesehen – mit einem Verwarnungsgeld in der maximal möglichen Höhe von 55 Euro verbunden. 31 Verfahren habe ich wieder eingestellt und zwei Verfahren zur weiteren Verfolgung als Straftat an die Staatsanwaltschaft abgegeben.

Berichtszeitraum		01.01.09 31.12.10	01.01.11 31.03.13	01.04.13 31.03.15	01.04.15 31.03.17	**01.04.17 24.05.18**
Einleitung		24	79	88	102	**66**
zzgl. Übernahme Vorjahr		2	3	29	22	**3**
anhängig gesamt		26	82	117	124	**69**
davon	Bußgelder	14	36	49	47	**17**
	Verwarnungen	0	1	0	2	**7**
	eingestellt	9	16	41	63	**31**
	unzuständig	0	0	5	9	**2**
	noch in Bearbeitung	3	29	22	3	**12**
Bußgeldsumme in Euro		24.800	54.095	353.572	174.226	**40.855**

Die Anzahl der nach Abschluss des Berichtszeitraums noch offenen Verfahren ist wegen der im Verhältnis erneut gestiegenen Anzahl neuer Verfahren einerseits sowie der zum Ende des Berichtszeitraums erfolgten Konzentration der personellen Ressourcen auf die Vorbereitung der Umstellung auf die Datenschutz-Grundverordnung wieder deutlich angewachsen.

Da es im Berichtszeitraum in meinem Zuständigkeitsbereich (glücklicherweise) an gravierenden Datenschutzverstößen gefehlt hat, ist die Gesamtsumme der festgesetzten Bußgelder wesentlich geringer ausgefallen.

Die im Berichtszeitraum nichtsdestoweniger herausragenden Bußgelder betrafen zum einen die

- Missachtung der Pflicht zur Bestellung eines Datenschutzbeauftragten (3.200 €, 3.600 € und 4.500 €),

und zum anderen

- unzulässige Videoüberwachungen öffentlicher Verkehrs- sowie gastronomisch genutzter Bereiche (4-mal 3.000 € und 2-mal 4.000 €).

Mit 16 mit einem Bußgeld oder einer Verwarnung abgeschlossenen Verfahren bildete die Ahndung des unzulässigen Einsatzes von Dashcams einen besonderen Schwerpunkt (vgl. dazu auch Punkt 2.7.1.1). Ausgangspunkt waren jeweils entsprechende polizeiliche Feststellungen bei Verkehrskontrollen oder im Rahmen der Streifentätigkeit, in deren

weiteren Verlauf dann die Speichermedien der Dashcams sichergestellt oder beschlagnahmt worden waren. Bei den Beschlagnahmen ist in allen Fällen eine nachträgliche richterliche Bestätigung eingeholt worden. Die höchste diesbezüglich festgesetzte Geldbuße hat 1.500 Euro betragen; im Durchschnitt müssen Betroffene je nach Umfang der festgestellten Videosequenzen mit einem dreistelligen Bußgeld im mittleren oder oberen Bereich rechnen. Soweit mittels der Dashcams auch Audioaufnahmen im Fahrzeuginnenraum erfolgt sind, ist dies bei der Bußgeldbemessung verschärfend berücksichtigt worden.

Die konsequente Ahndung des unzulässigen Dashcameinsatzes gründet sich auf die diesbezügliche verwaltungsgerichtliche Rechtsprechung (z. B. VG Göttingen, Beschluss vom 12.10.2016, Az. 1 B 171/16, und VG Ansbach, Urteil vom 12.08.2014, Az. AN 4 K 13.01634), die klar bestätigt, dass der (anlasslose) Einsatz von Dashcams durch Private im öffentlichen Straßenverkehr datenschutzwidrig ist. In diesem Sinne ist auch das Urteil des BGH vom 15.05.2018 (VI ZR 233/17) zu verstehen. Einerseits hat der BGH zwar entschieden, dass Dashcam-Aufnahmen unter gewissen Voraussetzungen als Beweismittel bei Unfall-Prozessen verwertbar sind. Andererseits hat der BGH aber auch unmissverständlich festgestellt, dass die permanente und anlasslose Aufzeichnung des Verkehrsgeschehens mit den datenschutzrechtlichen Regelungen des Bundesdatenschutzgesetzes nicht vereinbar ist, und in diesem Zusammenhang zugleich darauf hingewiesen, dass Verstöße gegen (diese) datenschutzrechtlichen Bestimmungen mit hohen Geldbußen geahndet werden könnten.

2.13 Strafanträge

Nach § 44 Absatz 2 BDSG haben die Datenschutzaufsichtsbehörden ein eigenständiges Strafantragsrecht bei Straftatbeständen nach dem Bundesdatenschutzgesetz.

Als Straftat nach dem Bundesdatenschutzgesetz verfolgbar waren die in § 43 Absatz 2 BDSG genannten materiellen Datenschutzverstöße und dies aber auch nur dann, wenn die Tat vorsätzlich in Bereicherungs- oder Schädigungsabsicht oder gegen Entgelt begangen worden ist (vgl. § 44 Absatz 1 BDSG).

Im Berichtszeitraum hatte ich keine Veranlassung, einen Strafantrag zu stellen.

2.14 Zusammenarbeit mit anderen Aufsichtsbehörden

Die Zusammenarbeit mit den Datenschutzaufsichtsbehörden der anderen Bundesländer sowie mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit spielte sich im Wesentlichen im Rahmen der Datenschutzkonferenz (vgl. dazu meinen

im gleichen Heft erscheinenden Tätigkeitsbericht für den öffentlichen Bereich), dem Düsseldorfer Kreis sowie den diesbezüglichen Arbeitsgruppen und Arbeitskreisen ab.

Der Düsseldorfer Kreis selbst tagte zweimal im Jahr; auf diesen Tagungen stimmten die Aufsichtsbehörden ihre Rechtsauffassungen in grundsätzlichen oder sonst besonders wichtigen datenschutzrechtlichen, ausschließlich den nicht-öffentlichen Bereich betreffenden Fragen sowie in diesbezüglichen länderübergreifenden Sachverhalten untereinander ab. Ich bin regelmäßiger Teilnehmer dieses Gremiums gewesen; die (letzten) im Berichtszeitraum gefassten und durch die DSK bestätigten und veröffentlichten Beschlüsse sind unter Punkt 16 dieses Berichts abgedruckt. Mit Ende dieses Berichtszeitraums endet allerdings auch die Tätigkeit des Düsseldorfer Kreises in seiner bisher bekannten Form und Funktion. Agierte er zuletzt schon nur noch als Gremium unterhalb der Datenschutzkonferenz ohne eigene Entscheidungskompetenz – seit 2017 veröffentlicht der Düsseldorfer Kreis selbst keine Beschlüsse mit Außenwirkung mehr, stattdessen obliegt dies seither vollumfänglich der DSK – wird er zukünftig nur noch als einfacher Arbeitskreis Wirtschaft fungieren und auf diese Weise die Arbeit der anderen Arbeitsgruppen, zukünftig Arbeitskreise, ergänzen.

Diese Arbeitskreise sind nichts anderes als spezialisierte Arbeitsgruppen, in denen auf Arbeitsebene Erfahrungen aus der Aufsichts- und Sanktionspraxis ausgetauscht, allgemein interessierende datenschutzrechtliche Fragestellungen untereinander sowie entweder regelmäßig oder auf besondere Einladung hin auch mit Vertretern der Wirtschaft, insbesondere mit Wirtschaftsverbänden, diskutiert und Beschlüsse für die Datenschutzkonferenz vorbereitet werden. Grundsätzlich ist meine Behörde in allen den nicht-öffentlichen Bereich (bzw. ehemals dem Düsseldorfer Kreis) zuzuordnenden Arbeitsgruppen

- Auskunfteien
- Internationaler Datenverkehr
- Kreditwirtschaft
- Sanktionen
- Versicherungswirtschaft
- Videoüberwachung
- Werbung und Adresshandel (Ad-hoc AG)

sowie auch in den sich mit Querschnittsthemen zwischen öffentlichem und nicht-öffentlichem Bereich befassenden Arbeitskreisen der Datenschutzkonferenz

- Beschäftigtendatenschutz

- (Tele-) Medien
- Technik
- Verkehr
- Zertifizierung (Ad-hoc AG)

vertreten, jedoch habe ich im Berichtszeitraum wegen des bekannten und bereits vielfach thematisierten akuten Personalmangels leider nicht an allen Arbeitskreisen bzw. jedenfalls nicht an allen Arbeitskreissitzungen teilnehmen können.

Ebenso wenig war mir (erstmals) auch keine Teilnahme am jährlichen Workshop der Datenschutzaufsichtsbehörden, der dieses Mal von der Berliner Beauftragten für Datenschutz und Informationsfreiheit ausgerichtet worden war, möglich. Ich schätze diesen Workshop sehr, da dieser regelmäßig Themen aufgreift, die keiner der fachspezifischen Arbeitsgruppen bzw. Arbeitskreise zuzuordnen sind, und auch weil diese Treffen sehr praxisorientiert sind, insbesondere dem Austausch praktischer Kontrollerfahrungen dienen, und bedauere es daher umso mehr, dass ich 2017 keinen Vertreter meiner Behörde dafür abstellen konnte.

Der zwar noch im (absehbar endenden) Geltungsbereich des Bundesdatenschutzgesetzes befindliche Berichtszeitraum des vorliegenden Tätigkeitsberichts war bereits umfangreich von dem bevorstehenden Übergang zur Datenschutz-Grundverordnung geprägt. Nicht nur die Aufsichtsbehörden selbst mussten sich – parallel zur aktuellen Aufsichtstätigkeit – auf den neuen Rechtsrahmen vorbereiten, sondern natürlich auch die Wirtschaft, die insoweit vielfältige Beratungswünsche an die Aufsichtsbehörden herangetragen hat (vgl. dazu auch Punkt 2.4). Um diesem Informations- und Beratungsbedarf möglichst effektiv und vor allem einheitlich zu entsprechen, haben sich zehn Aufsichtsbehörden zusammengefunden und insgesamt 20 Kurzpapiere zur Datenschutz-Grundverordnung entwickelt, unter allen Aufsichtsbehörden einschließlich der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit abgestimmt und anschließend veröffentlicht. Auch ich habe mich an der Erarbeitung dieser Kurzpapiere aktiv beteiligt und dabei insbesondere auch bei zwei Kurzpapieren die Koordination und Federführung übernommen. Alle Kurzpapiere habe ich auch auf meiner Website veröffentlicht.

2.15 Beschlüsse des AK Wirtschaft (vormals „Düsseldorfer Kreis“)

Die nachstehend aufgeführten Beschlüsse unter dem 23.3.2018 und die benannte Orientierungshilfe wurden seitens des AK Wirtschaft vorbereitet und als Materialien durch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder verabschiedet:

- Orientierungshilfe zur "Einholung von Selbstauskünften bei Mietinteressenten"
- Übermittlung von E-Mail-Adressen durch Onlineversandhändler an Postdienstleister
- Aufzeichnung von Telefongesprächen
- Mahnung durch Computeranruf
- Keine fortlaufenden Bonitätsauskünfte an den Versandhandel
- Kontaktloses Bezahlen
- Einmeldung offener und unbestrittener Forderungen in eine Wirtschaftsauskunftei unter Geltung der DSGVO

Die Dokumente sind unter dem Abschnitt 3 nachzulesen.

3 Materialien

3.1 Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 23.03.2018: 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.

3.2 Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 23.03.2018: 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 DSGVO 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.

3.3 Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 23.03.2018: Einmeldung offener und unbestrittener Forderungen in eine Wirtschaftsauskunftei unter Geltung der DSGVO

Die Zulässigkeit einer Einmeldung beurteilt sich künftig nach Artikel 6 Absatz 1 Satz 1 lit. f DSGVO.

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 Artikel 6 Absatz 4 DSGVO 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 DSGVO).

3.4 Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 23.03.2018: Keine fortlaufenden Bonitätsauskünfte an den Versandhandel

Auskunfteien dürfen Bonitätsauskünfte gemäß Artikel 6 Absatz 1 Satz 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 Artikels 6 Absatz 1 Satz 1 lit. f DSGVO 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. Artikel 6 Absatz 1 Satz 1 lit. f DSGVO 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.

3.5 Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 23.03.2018: 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 Artikel 4 Nummer 11 DSGVO 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) eindeutig 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 DSGVO dar. Da der datenschutzrechtlich Verantwortliche nachweisen können muss, dass die betroffene Person eine wirksame Einwilligung erteilt hat (Artikel 7

Absatz 1 DSGVO), muss er auch nachweisen können, dass die betroffene Person die Einwilligung „in informierter Weise“ abgegeben hat (vgl. Artikel 4 Nummer 11 DSGVO).

Die Aufzeichnung betrifft regelmäßig auch Beschäftigte. Insoweit gelten besondere Anforderungen. Sie sind nicht Gegenstand dieses Beschlusses.

3.6 Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26. April 2018 in Düsseldorf: 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:

<u>Zuverlässigkeitsüberprüfungen nur aufgrund einer spezifischen Rechtsgrundlage</u>

Die Gesetzgeber werden aufgefordert, bereichsspezifische Rechtsgrundlagen zu schaffen, die den Grundsatz der Verhältnismäßigkeit beachten und aus denen sich die Vo-

raussetzungen 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.

3.7 Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26. April 2018 in Düsseldorf: 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 gesellschaftlichen 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 (DSGVO) 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 digi-

taler 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.

Redaktionelle Anmerkung: Die Entschließung ist auf der Internetpräsenz der Datenschutzkonferenz auch in englischer Fassung verfügbar.

3.8 Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26. April 2018 in Düsseldorf: Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Absatz 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 Artikel 37 Absatz 1 lit. c DSGVO 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 Praxisgemeinschaften), die ohnehin nach Artikel 37 Absatz 1 lit. c DSGVO 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 Absatz 1 StGB auszulegen und umfasst die in § 203 Absatz 1 Nummer 1, 2, 4 und 5 StGB aufgezählten Berufsbilder.

3.9 Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 23.03.2018: 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 Absatz 1 Satz 1 Nummer 2 BDSG bzw. Artikel 6 Absatz 1 Satz 1 lit. f DSGVO verneint.

3.10 Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 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 Artikel 5 Grundgesetz (GG) und Artikel 11 EU-Grundrechtecharta (GRCh) für die freiheitliche demokratische Grundordnung ebenso Rechnung getragen werden wie dem Recht auf Informationelle Selbstbestimmung gemäß Artikel 1 i.V.m. Artikel 2 GG und dem Recht

auf Schutz personenbezogener Daten gemäß Artikel 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 Artikel 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 Artikel 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 Artikel 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 (Artikel 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 Interventionsmöglichkeiten 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 Rundfunk-Staatsverträgen, Presse- und Mediengesetzen:

- Die gesetzlichen Anpassungen i. S. d. Artikel 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.

3.11 Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 9. November 2017: 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 konkreten 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 visa-befreiten 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.

3.12 Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressentinnen“

Stand: Version 0.6; [aktualisiert auf der Sitzung der Sonder-AG „OH Mietauskünfte“ am 30.01.2018]

Einleitung

Vor der Vermietung von Wohnraum erheben Vermieterinnen[3] bei Mietinteressentinnen persönliche Angaben, auf deren Basis eine Entscheidung über den Vertragsabschluss getroffen werden soll. An der Beantwortung der Fragen müssen Vermieterinnen ein berechtigtes Interesse haben bzw. es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Auf Basis einer Interessenabwägung muss das Recht der Mietinteressentinnen auf informationelle Selbstbestimmung Beachtung finden.

Bezüglich der Datenerhebung kann zwischen bis zu drei Zeitpunkten differenziert werden:

- dem Besichtigungstermin (A.),
- der vorvertraglichen Phase, in welcher die Mietinteressentinnen den künftigen Vermieterinnen mitteilen, eine konkrete Wohnung anmieten zu wollen (B.) und
- der Entscheidung der künftigen Vermieterinnen für bestimmte Mietinteressentinnen (C.).

Die Zulässigkeit der Erhebung personenbezogener Daten der Mietinteressentinnen richtet sich im Besichtigungstermin regelmäßig nach Artikel 6 Absatz 1 lit. f) der Datenschutz-Grundverordnung (DSGVO). Spätestens nach der Erklärung der Mietinteressentinnen, eine konkrete Wohnung anmieten zu wollen, entsteht ein vorvertragliches Schuldverhältnis zu den künftigen Vermieterinnen, so dass dann Artikel 6 Absatz 1 lit. b) DSGVO maßgebend ist. Stehen Vermieterinnen für die Datenerhebung eine gesetzliche Grundlage nach Artikel 6 Absatz 1 lit. b) oder lit. f) DSGVO zur Verfügung, so ist ein Rückgriff auf das Konstrukt der Einwilligung unzulässig, denn für die Mietinteressentinnen würde der Eindruck entstehen, dass die Offenbarung und weitere Verarbeitung der Informationen ihrem Wahlrecht unterläge. Bei der Anwendung von Artikel 6 Absatz 1 lit. b) oder lit. f) DSGVO kommt es dann im Rahmen der Erforderlichkeitsprüfung darauf an, ob von Seiten der Interessentinnen Offenbarungspflichten bestehen bzw. ob von Vermieterinnenseite aus zulässige Fragen gestellt werden. Unzulässige Fragen

[3] Es sind stets Personen aller Geschlechter gleichermaßen gemeint. Aus Gründen der einfacheren Lesbarkeit wird im Folgenden nur die weibliche Form verwendet.

müssen demnach nicht beantwortet werden (Blank, in: Schmidt-Futterer, Kommentar zum Mietrecht, 13. Auflage 2017, § 543, Rn. 204). Maßgebend für die Beurteilung des Fragerechts der Vermieterinnen ist, inwieweit die begehrten Angaben mit dem Mietverhältnis über Wohnraum in einem objektiven Zusammenhang stehen und ob schutzwürdige Interessen der Mietinteressentinnen am Ausschluss der Datenerhebung bestehen.

Die Verwendung von Einwilligungserklärungen gegenüber Mietinteressentinnen in Formularen zur Selbstauskunft ist nicht das richtige Mittel zur Datenerhebung. Abgesehen davon, dass das Vorliegen einer gesetzlichen Grundlage eine Einwilligung für dieselbe Datenverarbeitung ausschließt, erfordert eine wirksame Einwilligung nach Artikel 4 Nummer 11, Artikel 7 Absatz 4 der DSGVO eine freie Entscheidung der betroffenen Person. Wird der Abschluss des Mietvertrags von der Erhebung bestimmter Angaben bei Mietinteressentinnen abhängig gemacht, entsteht eine Zwangslage, in welcher keine freiwillige und damit wirksame Einwilligungserklärung zustande kommen kann.

Die folgende Darstellung zu den verschiedenen Phasen der Datenverarbeitung ist nicht im Sinne einer abschließenden Aufzählung zu verstehen:

A. Besichtigungstermin

Streben Mietinteressentinnen zunächst nur eine Besichtigung der Räumlichkeiten an, so ist es in aller Regel nicht erforderlich, Angaben zu den wirtschaftlichen Verhältnissen zu erfragen. Erfragt werden dürfen:

1. Angaben zur Identifikation

Hierzu zählen Name, Vorname und Anschrift. Vermieterinnen sind auch befugt, im Falle der Besichtigung allein durch die Mietinteressentinnen die Angaben durch Vorzeigen eines Personalausweises zu überprüfen und den Umstand der Überprüfung zu dokumentieren. Die Anfertigung einer Ausweiskopie ist nicht erforderlich und damit unzulässig.

2. Angaben aus Wohnberechtigungsschein

Künftige Vermieterinnen dürfen nach § 27 Absatz 1 Wohnraumförderungsgesetz (WoFG) eine Wohnung, die im Rahmen eines Programms zur sozialen Wohnraumförderung errichtet wurde, nur Wohnungssuchenden zum Gebrauch überlassen, wenn diese ihnen vorher ihre Wohnberechtigung durch Übergabe eines Wohnberechtigungsscheins nachweisen. Möchten Mietinteressentinnen eine solche Wohnung besichtigen, sind Angaben zum Vorliegen eines Wohnberechtigungsscheins sowie zur genehmigten Wohnfläche und Anzahl der Wohnräume erforderlich, da nur in diesem Fall ein Besichtigungstermin sinnvoll ist. Eine Kopie des Wohnberechtigungsscheins darf erst nach der Erklärung der Mietinteressentinnen, eine Wohnung anmieten zu wollen, erfolgen, da die

in dem Formular aufgeführten Angaben zu den Namen und Vornamen der im Haushalt der Mietinteressentinnen befindlichen Personen im Besichtigungstermin nicht erforderlich sind.

B. Erklärung der Mietinteressentinnen, eine Wohnung anmieten zu wollen

1. Familienstand und Angaben zu den im Haushalt lebenden Personen

Angaben zum Familienstand der Mietinteressentinnen werden oft im Hinblick auf die gesamtschuldnerische Haftung von Ehegatten gefordert. Allein aus dieser Zwecksetzung heraus ist kein berechtigtes Interesse der Vermieterinnen gegeben, da Ehegatten nicht zwangsläufig gemeinsam Mietvertragsparteien sein müssen. Soweit nur ein Ehegatte den Wohnraummietvertrag unterzeichnen möchte und im Hinblick auf die äußere Gestaltung des Mietvertrags und die mündlichen Absprachen nicht davon ausgegangen werden kann, dass auch der andere Ehegatte Mietvertragspartei wird, greift keine gesamtschuldnerische Haftung ein. Schließlich ginge auch das Argument ins Leere, von Vermieterinnenseite aus einer möglichen Gebrauchsüberlassung an Dritte zuvor zu kommen, denn nach § 553 Absatz 1 BGB hätten Mieterinnen im Regelfall ein berechtigtes Interesse daran, Ehegatten den Wohnraum zur Nutzung zu überlassen.

Die Anzahl der einziehenden Personen und Informationen darüber, ob es sich um Kinder und/oder Erwachsene handelt, dürfen erfragt werden, da dies für die Beurteilung der Wohnungsnutzung erforderlich ist. Weitere Angaben dürfen zu diesen Personen nicht eingeholt werden, es sei denn, diese möchten Mietvertragspartnerinnen sein.

2. Eröffnetes Insolvenzverfahren, Angabe einer Vermögensauskunft, Räumungstitel wegen Mietzinsrückständen

Die Frage nach einem eröffneten und noch nicht abgeschlossenen Verbraucherinsolvenzverfahren ist zulässig, da Mietinteressentinnen diesbezüglich eine Offenbarungspflicht trifft. Ein Insolvenzverfahren führt dazu, dass das gesamte pfändbare Vermögen zur Insolvenzmasse gehört und davon betroffenen Mietinteressentinnen nur die nicht pfändbaren Vermögensteile zur Verfügung stehen (AG Bonn, Urteil v. 22.09.2005, Az.: 6 C 411/05; LG Bonn, Beschluss v. 16.11.2005, Az.: 6 T 312/05 und 6 S 226/05).

Ob in begründeten Fällen ein Fragerecht nach abgegebenen Vermögensauskünften besteht, hängt u.a. davon ab, nach welchem Zeitraum (in der Regel 2 Jahre) gefragt wird. Bei der Abgabe einer Versicherung an Eides statt im Rahmen einer Vermögensauskunft (§ 802c Absatz 3 ZPO) sind Mietzinsansprüche der Vermieterinnen nicht in gleicher Weise gefährdet (LG Bonn, Beschluss v. 16.11.2005, Az.: 6 T 312/05 und 6 S 226/05). Ferner ist zu berücksichtigen, dass gemäß § 882f Satz 1 Nummer 4 ZPO eine Einsicht in das Schuldnerverzeichnis unter bestimmten Voraussetzungen möglich ist und zum

Inhalt eines solchen Verzeichnisses auch Eintragungsanordnungen nach § 882c ZPO zählen. Nach § 882f Satz 1 Nummer 4 ZPO ist die Einsicht in das Schuldnerverzeichnis jedem gestattet, der darlegt, Angaben nach § 882b ZPO zu benötigen, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldnerinnen ihren Zahlungsverpflichtungen nicht nachkommen. Im Hinblick auf den erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung der Mietinteressentinnen ist bei der Anwendung von § 882f Satz 1 Nummer 4 ZPO vor allem der Verhältnismäßigkeitsgrundsatz zu beachten. Ferner muss den wirtschaftlichen Nachteilen bedeutsames Gewicht zukommen (Utermark/Fleck, in: Vorwerk/Wolf, Beck`scher Online-Kommentar ZPO, 2017, § 882f, Rn 8). An die Zulässigkeit einer Datenerhebung beim Vollstreckungsgericht nach § 882f Satz 1 Nummer 4 ZPO sind ähnlich hohe Anforderungen zu stellen, wie im Rahmen einer Datenerhebung nach Artikel 6 Absatz 1 lit. b) DSGVO bei Mietinteressentinnen.

Fragen nach Räumungstiteln wegen Mietzinsrückständen sind dann zulässig, wenn diese aufgrund der zeitlichen Nähe noch Auskunft darüber geben können, ob künftige Mietzinsansprüche gefährdet wären. Dies kann der Fall sein, wenn bezüglich eines bestehenden Wohnraummietverhältnisses mit anderen Vermieterinnen die Zwangsräumung wegen Mietzinsrückständen droht (AG Wolfsburg, Urteil v. 09.08.2000, Az.: 22 C 498/99). Fragen danach, ob in den letzten fünf Jahren Räumungsklagen wegen Mietzinsrückständen eingeleitet oder durchgeführt wurden, in welchen das Verfahren mit einem Räumungstitel abgeschlossen wurde, werden als zulässig angesehen (LG Wuppertal, Urteil v. 17.11.1998, Az.: 16 S 149/98).

3. Religion, Rasse, ethnische Herkunft bzw. Staatsangehörigkeit

Eine pauschale Abfrage dieser Angaben ist unzulässig. Dies ergibt sich auch aus dem Verbot der unterschiedlichen Behandlung von Personen anhand dieser Merkmale aus § 19 Absatz 1 AGG. Nach § 19 Absatz 3 AGG ist bezüglich der Rasse, der ethnischen Herkunft und der Religion bei der Vermietung von Wohnraum eine unterschiedliche Behandlung ausnahmsweise zulässig, wenn dies im Hinblick auf die Schaffung und Erhaltung sozial stabiler Bewohnerstrukturen und ausgewogener Siedlungsstrukturen sowie ausgeglichener wirtschaftlicher, sozialer und kultureller Verhältnisse notwendig ist. Zwingende Voraussetzung hierfür ist, dass zunächst ein schlüssiges wohnungspolitisches Konzept vorliegt. Dieses Konzept muss auch zur Prüfung sachlicher Gründe (vgl. etwa § 20 Absatz 1 Nummer 4 AGG) Auskunft geben, die eine Ungleichbehandlung rechtfertigen und folglich zur Entschärfung von Konflikten beitragen können.

Die Frage nach der Staatsangehörigkeit ist nicht erforderlich (i. S. d. Artikel 6 Absatz 1 DSGVO) und damit nicht zulässig.

4. Vorstrafen und strafrechtliche Ermittlungsverfahren

Die Erhebung von Angaben zu Vorstrafen ist grundsätzlich nicht erforderlich und damit unzulässig. Berücksichtigt werden muss zum einen, dass bestimmte Strafen nicht in ein polizeiliches Führungszeugnis aufzunehmen sind, § 32 Absatz 2 BZRG, und sich schon deshalb keine darüber hinaus gehenden Mitteilungspflichten gegenüber einem Vermieter ergeben können.

Eine Offenbarung von Vorstrafen wird bisher nur im Zusammenhang mit der Begründung von Arbeitsverhältnissen und bei Vorliegen weiterer Voraussetzungen als zulässig angesehen. Bei der Anbahnung von Mietverhältnissen besteht keine vergleichbare Gefährdungslage, da hier ausschließlich die Frage nach der Bonität der Mietinteressentinnen von Bedeutung ist.

Auch die Erhebung von Informationen zu laufenden strafrechtlichen Ermittlungsverfahren ist unzulässig.

5. Heiratsabsichten, Schwangerschaften, Kinderwünsche

Angaben zu Heiratsabsichten, bestehenden Schwangerschaften und Kinderwünschen zählen zum Kernbereich privater Lebensgestaltung. Fragen hierzu sind unzulässig. Eine Aufnahme von Kindern und Ehegatten in der Wohnung wäre für zukünftige Mieterinnen schon nicht erlaubnispflichtig im Sinne von § 553 Absatz 1 Satz 1 BGB, denn diese Personen sind in Anwendung von Artikel 6 Absatz 1 GG bereits keine Dritten (§ 553 Absatz 1 BGB), sondern nahe Familienangehörige. Die Aufnahme von Familienangehörigen muss nur angezeigt werden. Einer Aufnahmeerlaubnis durch die Vermieterinnen bedarf es nicht.

6. Mitgliedschaften in Parteien und Mietvereinen

Die Frage nach einer evtl. bestehenden Zugehörigkeit zu Parteien oder Mietervereinen ist unzulässig. Mit den Angaben wird nämlich keine Aussage zur Bonität der Mietinteressentinnen bzw. zu deren Zahlungsfähigkeit und Zahlungswilligkeit getroffen.

7. Angaben zu Arbeitgebern, zum Beschäftigungsverhältnis und zum Beruf

Für die Entscheidung über den Abschluss eines Mietvertrags darf nach dem Beruf und den Arbeitgeberinnen als Kriterium zur Beurteilung der Bonität der Mietinteressentinnen gefragt werden. Die Dauer einer Beschäftigung bietet in einer mobilen Gesellschaft hingegen keine Gewissheit über die Fortdauer und Beständigkeit des Beschäftigungsverhältnisses und ist daher ungeeignet, das Sicherungsbedürfnis der Vermieterinnen zu erfüllen. Fragen nach der Dauer der Beschäftigung sind damit unzulässig.

8. Einkommensverhältnisse

Die Erfragung der Höhe des Nettoeinkommens und desjenigen Betrags, der nach Abzug der laufenden monatlichen Belastungen für die Tilgung des Mietzinses zur Verfügung steht, ist regelmäßig erforderlich. Bezüglich der Höhe des Nettoeinkommens wäre jedoch auch die Angabe einer bestimmten Betragsgrenze durch Mietinteressentinnen ausreichend, verbunden mit dem Hinweis, dass diese Grenze überschritten wird. Im Hinblick auf die monatlichen Belastungen ist die Erfragung der Forderungsgründe (Unterhaltsverpflichtungen, Darlehensverbindlichkeiten etc.) unzulässig, da dies für die Beurteilung der Bonität nicht erforderlich ist.

Fragen nach den Einkommensverhältnissen sind unzulässig, wenn die Mietzahlungen vollständig von einer öffentlichen Stelle übernommen und direkt an die Vermieterinnen geleistet werden sollen.

9. Angaben zu Haustieren

Fragen der Vermieterinnen nach der beabsichtigten Haltung von Haustieren sind zulässig, soweit die Tierhaltung nicht zum vertragsgemäßen Gebrauch der Mietsache zählt und folglich zustimmungsbedürftig ist. Dies gilt nicht für Kleintiere.

C. Entscheidung der künftigen Vermieterinnen für bestimmte Mietinteressentinnen

Haben sich zwei oder mehrere Mietinteressentinnen für eine konkrete Wohnung entschieden, so trifft die künftige Vermieterin die Entscheidung für bestimmte Mietinteressentinnen (Erstplatzierte). Nach dieser Entscheidung kann die Einholung weiterer Informationen bei der Erstplatzierten erforderlich sein.

1. Angaben zum Vormietverhältnis

Fragen nach den Kontaktinformationen aktueller oder früherer Vermieterinnen der Mietinteressentinnen (z.B. Name, Anschrift, Telefonnummer, E-Mail-Adresse) sind unzulässig. Denn solche Angaben sind für die Entscheidung über die Begründung eines Mietverhältnisses nicht erforderlich.

Erfragt werden dürfen Angaben zur Erfüllung mietvertraglicher Pflichten, sofern diese Aufschluss über die Zahlungsfähigkeit der Mietinteressentinnen geben. Angaben, die zur Zahlungsfähigkeit Auskunft geben, sind etwa die Zahlung der vereinbarten Miete und der Nebenkosten.

Fragen nach Pflichtverletzungen können zulässig sein. Voraussetzung ist aber, dass die Pflichtverletzung eine Kündigung rechtfertigt und solche Pflichtverletzungen auch noch

in Zukunft zu erwarten sind. Die Kündigung muss dazu rechtskräftig oder die Pflichtverletzung in tatsächlicher Hinsicht unbestritten sein und auch aus Sicht der Mietinteressentinnen eine Kündigung in rechtlicher Hinsicht rechtfertigen.

Im Rahmen der Anforderung einer Selbstauskunft der Mietinteressentinnen ist zu beachten, dass bisherige Vermieterinnen diesen gegenüber nicht verpflichtet sind, eine Mietschuldenfreiheitsbescheinigung zu erstellen (BGH, Urteil v. 30.09.2009, Az.: VIII ZR 238/08). Folglich kann eine solche Bescheinigung vom Mietinteressentinnen bei der beabsichtigten Neuanmietung von Wohnraum nicht verlangt werden. Zulässig wäre es aber, vom Mietinteressentinnen wahlweise entweder nach § 368 BGB von Vorvermieterinnen geschuldete Quittungen über empfangene Zahlungen oder geschwärzte Kontoauszüge und Mietverträge als Beleg zu geleisteten Mietzahlungen an Vorvermieterinnen sowie zur Höhe des Mietzinses und damit zum Nachweis einer bestehenden Bonität zu erbitten.

2. Nachweise zu den Einkommensverhältnissen

Künftige Vermieterinnen können bereits bei der Erfragung der Höhe des Nettoeinkommens und der Höhe der monatlichen Belastungen darauf hinweisen, dass für den Fall einer positiven Entscheidung für die Mietinteressentin, quasi unmittelbar vor Unterzeichnung des Vertrags, noch Nachweise zu den Einkommensverhältnissen vorgelegt werden müssen, z.B. eine Lohn- oder Gehaltsabrechnung, ein Kontoauszug oder ein Einkommensteuerbescheid in Kopie – jeweils unter Schwärzung der nicht erforderlichen Angaben.

3. Vorlage der Selbstauskunft nach Anfrage bei einer Auskunftei

Von den Mietinteressentinnen dürfen nur solche Auskünfte angefordert werden, die zum Nachweis ihrer Bonität für den spezifischen Fall der Eingehung eines Mietverhältnisses durch Mietinteressentinnen z.B. bei Auskunfteien eingeholt werden können und ausschließlich die hierfür erforderlichen Angaben enthalten.

Nicht angefordert werden dürfen Selbstauskünfte im Sinne des Artikels 15 DSGVO, die betroffene Personen bei Auskunfteien einholen können. Denn diese enthalten häufig wesentlich mehr Angaben über die wirtschaftlichen Verhältnisse der betroffenen Personen, als für eine Beurteilung der Bonität im Rahmen des Mietverhältnisses erforderlich ist.

4. Abfrage von Bonitätsauskünften über die Mietinteressentinnen durch Vermieterinnen

Die Abfrage von Bonitätsauskünften über Mietinteressentinnen bei Auskunfteien ist nur dann zulässig, wenn die Voraussetzungen einer gesetzlichen Vorschrift (Artikel 6 Ab-

satz 1 lit. b) oder lit. f) DSGVO) erfüllt sind. Liegen bereits ausreichende Informationen über die Bonität der Mietinteressentinnen vor, z. B. durch spezielle Bonitätsnachweise im Sinne von C. 3. (1. Absatz), ist eine Abfrage bei Auskunfteien nicht zulässig.

Da die Verwendung von Einwilligungserklärungen gegenüber Mietinteressentinnen in Formularen zur Selbstauskunft nicht als das richtige Mittel zur Datenerhebung anzusehen ist, wäre auch das Verlangen des künftigen Vermieters, eine Einwilligungserklärung für die Einholung einer Bonitätsauskunft abzugeben, nicht rechtmäßig. Dabei ist auch Artikel 4 Nummer 11 DSGVO i. V. m. Artikel 7 Absatz 4 DSGVO zu beachten, nach dessen Vorgaben keine freiwillige und damit eine unwirksame Einwilligungserklärung vorliegen würde, wenn der Abschluss des Mietvertrags von der Einwilligung in die Erhebung nicht erforderlicher Angaben abhängig gemacht wird.

3.13 Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 26. April 2018 in Düsseldorf: Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht

Stand: 26.04.2018

1 Zielsetzung

Immer mehr Bildungsinstitutionen setzen auf die webgestützte Wissensvermittlung und die elektronischen Kommunikationsmöglichkeiten zwischen Lehrenden und Lernenden. Zu diesen Zwecken werden auch an Schulen zunehmend Online-Lernplattformen für den Unterricht eingesetzt. Diese Online-Lernplattformen werden von Schulaufsichtsbehörden, Schulbuchverlagen, Computer- und Softwareherstellern und sonstigen Anbietern bereitgestellt. Die Vorteile werden in der orts- und zeitunabhängigen Nutzung dieser Verfahren gesehen. Allerdings werden dabei zahlreiche Schüler[4]- und Lehrerdaten webbasiert verarbeitet. Die vorliegende Orientierungshilfe richtet sich insbesondere an Schulen, die Online-Lernplattformen als Lernmittel einsetzen wollen. Sie sollen sich einen Überblick darüber verschaffen können, welche datenschutzrechtlichen (Mindest-)Kriterien Online-Lernplattformen erfüllen müssen. Diese Orientierungshilfe gibt auch den Anbietern von Online-Lernplattformen die Möglichkeit, ihr jeweiliges Produkt so zu gestalten oder anzupassen, dass eine Nutzung durch Schulen zulässig ist.

Online-Lernplattformen sollen den Bildungs- und Erziehungsauftrag der Schule unterstützen, beispielsweise

[4] Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die gewählte männliche Form schließt eine adäquate weibliche Form gleichberechtigt ein.

- Kompetenzorientierung
- Integration fachlicher, methodischer und sozialer Lernziele
- Prozesshaftigkeit des Lerngeschehens
- Unterstützung von Schülern in Kleingruppen
- Begabungsgerechte Förderung
- Erkennen individueller Lernfortschritte und Lernschwierigkeiten
- Beratung und Lernförderung einzelner Schüler

Ergänzend wird auf die Orientierungshilfe „Cloud Computing“ der Arbeitskreise Technik und Medien der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises in der aktuellen Fassung verwiesen, weil diese besondere Anforderungen für webbasierte Anwendungen bzw. „Datenverarbeitung in der Wolke“ aufzeigt.

Soweit die Online-Lernplattformen für andere als schulische Zwecke über das Internet zur Nutzung zur Verfügung stehen, sind sie nicht Gegenstand dieser Orientierungshilfe.

2 Begriffsbestimmungen

Online-Lernplattformen im Sinne dieser Orientierungshilfe sind Softwaresysteme, die den Lehr- und Unterrichtsbetrieb durch die Bereitstellung und Organisation von Lerninhalten ergänzen oder sogar ersetzen. Schulsoftwaresysteme, die für Aufgaben der Schulverwaltung genutzt werden, sind davon systemtechnisch zu trennen.

Die virtuelle Lernumgebung einer Online-Lernplattform kann von der Schule so gestaltet werden, dass Kommunikation, Gruppenarbeit, Aufgabenbearbeitung und Lernkontrollen eingerichtet werden. Der Zugriff auf die Software erfolgt ortsunabhängig mittels eines Endgerätes (PC, Tablet etc.) über einen Web-Browser. Die faktische Teilhabe der Schüler ist durch die Schule zu gewährleisten. Jeder Teilnehmer muss zunächst als Benutzer angelegt werden. Das System stellt dann jedem Nutzer ein personalisiertes Benutzerkonto zur Verfügung. Darüber hinaus muss die Schule bzw. die verantwortliche Lehrkraft die Zugriffsrechte für die einzelnen Nutzer festlegen und die Funktionalitäten auswählen, die die Online-Lernplattform bietet (Bereitstellung von Lerninhalten, Diskussionsforen, Übungsaufgaben etc.). Für die Teilnahme an einem bestimmten Kurs müssen sich z. B. die Schüler einer Klasse oder eines Jahrgangs dann in einem bestimmten Schulfach vor einer Nutzung zunächst im Onlineverfahren auf der Lernplattform anmelden

3 Datenschutzrechtliche Problematik

In aller Regel melden sich die Benutzer solcher Plattformen personalisiert an und ihre Nutzungsbewegungen werden regelmäßig gespeichert. So wird beispielsweise festgehalten, welcher Nutzer wann auf welche Seite zugegriffen hat, sowie ob und mit welchem Ergebnis er sich an welchem Test beteiligt hat. Dadurch können Persönlichkeitsprofile über Schüler erstellt werden.

Die schulrechtlichen Regelungen für die Verarbeitung und Nutzung von personenbezogenen Daten durch die Schule setzen voraus, dass die erhobenen Daten für die Aufgabenwahrnehmung durch die Schule erforderlich sein müssen. Viele Online-Lernplattformen stellen erheblich mehr Möglichkeiten zur Datenauswertung zur Verfügung, als dies für die Aufgabenwahrnehmung erforderlich ist und sind daher entsprechend anzupassen.

Auch beim Einsatz von Online-Lernplattformen benötigen Lehrkräfte die Möglichkeit, den Lernfortschritt einzelner Schüler zu beobachten, um im individuellen Beratungsgespräch
oder bei der Planung und Umsetzung von lernförderlichen Interventionen gezielt den Schüler in seiner Lernsituation zu unterstützen. Weitergehende Angaben, z. B. wie oft und zu welchen Zeiten ein Schüler sich in der Online-Lernplattform an bestimmten Aufgaben beteiligt hat, dürfen in diesem Zusammenhang nicht eingesehen werden. Die Schüler und - falls erforderlich - auch die Erziehungsberechtigten sind vor der Nutzung der Online-Lernplattform darüber zu informieren, welche Auswertungsmöglichkeiten die Anwendung bietet und welche Konsequenzen das Nutzerverhalten haben kann.

Fazit:

- Die Online-Lernplattform ist so zu konfigurieren, dass ausschließlich die zur pädagogischen Aufgabenerfüllung der Schule erforderlichen Daten erhoben und verarbeitet werden.
- Es bietet sich die Nutzung von Online-Lernplattformen an, die je nach vorgesehenem Einsatzszenario modular angepasst werden können.

Die Betroffenen sind vor der Nutzung der Online-Lernplattform über mögliche Auswertungen umfassend zu informieren.

4 Rechtsgrundlagen

Rechtsgrundlage für die Verarbeitung personenbezogener Schülerdaten auch in Online-Lernplattformen ist zunächst die Verordnung (EU) 2016/679 des Europäischen Parlament und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO). Über die Öffnungsklausel in Artikel 6 Absatz 1 Buchstabe e) DSGVO in Verbindung mit Artikel 6 Absatz 3 Satz 1 Buchstabe b DSGVO sind dann die jeweiligen Schulgesetze, Schuldatenschutzgesetze und dazu erlassene Rechtsverordnungen anzuwenden, sofern sie mit der DSGVO, die seit dem 25. Mai 2018 unmittelbar gilt, in Einklang zu bringen sind[5]. Ergänzend können – je nach Bundesland und Schultyp – die Landesdatenschutzgesetze sowie das Bundesdatenschutzgesetz zur Anwendung kommen.

Die verpflichtende Verwendung einer Lernplattform kann nur durch oder aufgrund eines Gesetzes vorgeschrieben werden. Denkbar ist beispielsweise die Bestimmung als Lehrmittel durch entsprechende Verordnung aufgrund gesetzlicher Ermächtigung. Andernfalls kann es nur auf Basis einer freiwillig erteilten Einwilligung[6] zum Einsatz einer derartigen Plattform kommen. Dabei sind die Anforderungen an eine rechtmäßige Einwilligung nach Artikel 7 DSGVO zu beachten[7].

Fazit:

Vor dem Einsatz der Online-Lernplattform ist zu prüfen, ob deren Einsatz rechtlich zulässig ist und ob die Schüler und ggf. die Erziehungsberechtigten in die Nutzung der Plattform einwilligen müssen.

5 Verantwortlicher

Verantwortlicher ist nach Artikel 4 Nummer 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung der personenbezo-

[5] Hiervon ist grundsätzlich auszugehen. Bei Zweifeln wird empfohlen sich an die zuständige Datenschutzaufsichtsbehörde zu wenden.

[6] Gem. Artikel 8 Absatz 1 bedarf es für Dienste der Informationsgesellschaft, die dem Kind direkt angeboten werden, der Einwilligung des Kindes, wenn es das 16. Lebensjahr vollendet hat. Im Übrigen ist die Einwilligung im Hinblick auf Erwägungsgrund 32 und 43 nicht unproblematisch. Einwilligungslösungen sind danach im Über- Unterordnungsverhältnis eingeschränkt möglich, da die zwingende Voraussetzung der Freiwilligkeit nicht zweifelsfrei sichergestellt ist. In jedem Einzelfall ist zuverlässig zu prüfen und zu gewährleisten, dass die betroffenen Personen auch tatsächlich frei von Druck oder Zwang ihre Entscheidungen getroffen haben. Wenn personenbezogene Daten zu Unterrichtszwecken oder in Verbindung mit der Durchführung und Bewertung von pädagogischen Aufgaben im Unterricht verarbeitet werden, ist die Beurteilung der Freiwilligkeit äußerst schwierig.

7 siehe hierzu auch Guidelines on Consent under Regulation 2016/679, WP 259, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849

genen Daten entscheidet. Maßgeblich ist, welche Stelle über den grundsätzlichen Einsatz der Online-Lernplattform und die näheren Umstände der Umsetzung verantwortlich entscheidet. Unerheblich ist für diese Frage, wo die Daten verarbeitet werden. Der Verantwortliche muss über die Art und Weise der Datenverarbeitung maßgeblich bestimmen können, also „Herr der Daten“ bleiben. Lehrende dürfen im Rahmen der Freiheit der Gestaltung des Unterrichts nur insoweit Online-Lernplattformen im Unterricht einsetzen, als die Schule oder die Schulaufsicht über den Einsatz der jeweiligen Online-Lernplattform entschieden hat.

6 Umfang der Datenverarbeitung

6.1 Erforderliche Daten

Die Schule/Schulaufsichtsbehörde muss festlegen, welche Daten für die Nutzung der Online-Lernplattform zwingend benötigt werden.

6.1.1 Zwingend erforderliche Stammdaten

- Name und Anschrift der jeweiligen Schule und des Verantwortlichen, die, wenn die Schulaufsichtsbehörde diese Aufgaben wahrnimmt, differieren können.
- Stammdaten zur Anlage von Benutzerkonten, die sowohl zur Identifikation des Nutzers im System als auch zum Zwecke der Vergabe von Rollen und Berechtigungen dienen. Es gibt die Möglichkeit, dass der Nutzer selbst die Daten eingibt und anlegt oder dass die Daten durch die Schule erfasst oder geändert werden. Wichtig ist, dass nur Daten eingegeben werden können, die für die sinnvolle Nutzung der pädagogischen Aufgabenerfüllung der Schule erforderlich sind.
- Bei der Benutzerverwaltung durch den Administrator ist zwischen dem Benutzernamen und dem Anmeldenamen zu unterscheiden. Der Benutzername muss den realen Namen (Klarname) des Benutzers enthalten. Der Klarname ist zur Identifikation des Schülers durch betreuende Lehrer erforderlich und muss nicht dem Anmeldenamen entsprechen. Der Anmeldename wird bei der Anmeldung im System verwendet und sollte nicht mit dem Benutzernamen identisch sein. Im Gegenteil: nach Artikel 25 Absatz 1 Datenschutz-Grundverordnung sollen geeignete technische und organisatorische Maßnahmen wie etwa die Pseudonymisierung, getroffen werden, die die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen. Der Anmeldename kann frei gewählt werden. Die Anmeldung mit Pseudonymen ist geboten, um den Missbrauch des Kontos durch Dritte maßgeblich zu erschweren.
- Die Angabe einer E-Mail-Adresse ist je nach System optional oder zwingend erforderlich. Sie dient insbesondere der Zusendung von Benachrichtigungen aus

den belegten Kursen sowie der Abfrage eines neuen Passworts bei dessen Verlust. Ein Passwort-Rücksetz-Mechanismus darf aus Sicherheitsgründen grundsätzlich nicht allein auf E-Mail-Zusendungen basieren. Die Vergabe einer internen E-Mail-Adresse ist in aller Regel geboten, weil ansonsten die Gefahr besteht, dass personenbezogene Daten aus dem kontrollierten Bereich der Lernplattform über Benachrichtigungen an Unbefugte gelangen können.

Ein Benutzerkonto kann weitere Informationen enthalten, die die Kommunikation innerhalb des Systems erleichtern, beispielsweise Klassenstufe, Bezeichnung der Lerngruppe, Ausbildungsgang (beispielsweise an berufsbildenden Schulen).

Fazit:

- Bei der Auswahl der Online-Lernplattform ist darauf zu achten, dass die Grundsätze der Datensparsamkeit und Datenvermeidung (z. B. nicht zu viele Stammdaten, Freitextfelder, Kommentarfunktionen) gewährleistet werden.
- Es ist eine pseudonymisierte Nutzerverwaltung der Lernplattform geboten.

6.1.2 Optionale Daten

Weitere optionale Daten können im Nutzerprofil auf freiwilliger Basis durch den Benutzer selbst erfasst werden. Felder wie "Beschreibung“, „Nutzerbild" und “Interessenfelder" verdienen in diesem Zusammenhang besonderes Augenmerk.

Optionale Datenfelder können bei den gängigen Online-Lernplattformen sein:

- Zeitzone: Dieses Feld wird im Regelfall deaktiviert oder mit einem Standardwert belegt, da alle Nutzer in der Regel in der gleichen Zeitzone leben,
- Beschreibung: Hier können Nutzer Angaben zur eigenen Person eintragen. Diese sind innerhalb der Lernplattform, nicht aber öffentlich sichtbar. Dieses Feld ist nicht erforderlich und sollte deaktiviert werden.
- Nutzerbild: Der Nutzer kann eine Grafikdatei (beispielsweise ein Porträtfoto) hochladen, für die er die Urheberrechte besitzt. Dieses Feld ist nicht erforderlich, birgt die Gefahr von Rechtsverstößen und sollte deaktiviert werden.
- Interessenfelder: Hier können Schlagworte zur eigenen Person angegeben werden (beispielsweise Hobbys). Dieses Feld ist nicht erforderlich und sollte deaktiviert werden.
- Webseite: Teilnehmer können hier die URL zu einer eigenen Internetpräsenz angeben. Dieses Feld ist zu deaktivieren.

- Bevorzugte Sprache: Die Einstellung ermöglicht, dass Benutzeroberflächen in anderen Sprachen als Deutsch zur Verfügung stehen. Dieses Feld ist in aller Regel nicht erforderlich und sollte deaktiviert werden.
- Institution, Abteilung: Diese Information wird in der Regel in der Schule nicht verwandt.

Für organisatorische Zwecke können zusätzliche optionale Datenfelder angelegt und gepflegt werden. Dies ist nur zulässig, soweit es für die Aufgabenerfüllung erforderlich ist. Zu denken ist hier beispielsweise an die Angabe, an welchen Kursen ein Schüler teilnimmt, damit er Zugang zu den zugehörigen Dokumenten erhält. Nicht hierunter fallen persönliche Angaben wie Hobbies oder private Telefonnummern.

6.1.3 Nutzungsdaten

Bei der Nutzung einer Lernplattform werden automatisch Daten über den Nutzer und seine Aktivitäten erfasst und gespeichert. Diese Logdaten werden auf dem Server abgelegt, sie dürfen ausschließlich für die Überwachung der Funktionsfähigkeit und Sicherheit dieser Systeme sowie bei rechtswidrigem Missbrauch verwendet werden. Ergänzend wird auf die Orientierungshilfe „Protokollierung“ des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder in der aktuellen Fassung verwiesen. Näheres sollte in der Nutzungsordnung konkret festgelegt werden.

Nutzungsdaten sind in aller Regel für die Wahrnehmung schulischer Aufgaben nicht erforderlich und sollten daher nur unter klar definierten Voraussetzungen für eindeutig bestimmte Personengruppen zu festgelegten Zwecken einsehbar sein. Nutzungsdaten sind beispielsweise

- Anmeldestatus: Erstlogin im System, letzter Login, Zeitpunkt der Abmeldung
- Protokollierung von Eingaben oder Änderungen
- IP-Adressen, genutzte Dienste (z. B. Dateidownloads, Chat)

6.1.4 Pädagogische Prozessdaten

Als pädagogische Prozessdaten werden Informationen bezeichnet, die dem Lehrer die Möglichkeit geben, den individuellen und kollektiven Lernprozess nachzuvollziehen, um didaktische Interventionen zu planen, Unterricht zu reflektieren, zu evaluieren und weiterzuentwickeln sowie individuelle Lernberatung für einzelne Schüler oder kleine Gruppen zu gestalten. In den verschiedenen Modulen einer Online-Lernplattform werden Prozessdaten generiert, die jeweils für unterschiedliche Personenkreise sichtbar sind. Solche Module sind:

- Forendiskussion: Die Beiträge können den Verfassern zugeordnet und in zeitlicher Struktur geordnet werden. Zudem zeigt die Darstellungsstruktur an, zu welchem Beitrag eine Antwort abgegeben wurde. Diese Informationen sind für alle Nutzer sichtbar. Eine Anzeige noch nicht gelesener Beiträge hingegen ist nur für den jeweiligen Einzelnutzer sichtbar.
- Wiki-Einträge: Ein Wiki ist ein mehrseitiges Dokument, an dem von verschiedenen Verfassern in einem Kurs gearbeitet wird. Durch die Speicherung der Historie ist erkennbar, wer welche Teile an einem Dokument bearbeitet hat. Die Lehrkraft kann dadurch die Beteiligung und die Beiträge Einzelner erkennen. Dies ist für Rückmeldungen und die Bewertung sowie die Förderung sozialer und kommunikativer Aspekte des Lernens wichtig.
- Glossar (Datenbank): Das Glossar stellt eine Sammlung von Informationen in strukturierter Form dar. Es enthält einzelne Texteinträge mit Angaben zum Erstellungszeitpunkt und dem Verfasser. Diese Details sind für alle Nutzer sichtbar.
- Lernobjekte (Aufgaben, Tests): Je nach Art des Objekts sind unterschiedliche Daten nur für Lehrkräfte oder auch für einzelne Schüler sichtbar. Eine Überwachung der außerunterrichtlichen Aktivitäten von Schülern durch Lehrende darf nicht stattfinden. Die Sichtbarkeit der Daten für Lehrende, ist pädagogisch zu begründen und von der Schulleitung bzw. der Schulkonferenz festzulegen.
- SCORM-Module, LTI-Module, Live Classroom, Plagiatsüberprüfung etc.: Bei der Nutzung derartiger Module werden unter Umständen personenbezogene Daten an externe Dienstleister weitergegeben. Dies ist nur im Rahmen von bestehenden Auftragsverarbeitungsverträgen zwischen Schule/Schulträger und Anbieter zulässig und ist datenschutzrechtlich gesondert zu prüfen. Prozessdaten von Lernenden dürfen nur dann für andere Teilnehmer sichtbar sein, wenn dies methodisch oder didaktisch erforderlich ist. Als Beispiel sei die Bewertungsfunktion in einem Diskussionsforum angeführt. Je nach Implementierung erlaubt sie eine schnelle, unter Umständen nonverbale Rückmeldung zu Beiträgen. Da auf diese Weise von Schülern auch unsachgemäße und verletzende Kritik gegenüber Mitschülern geäußert werden kann, ohne dass von Seiten der Lehrenden rechtzeitig eingegriffen werden kann, ist eine solche Funktion nur mit Bedacht zu aktivieren.

6.1.5 Statistische Daten

Die Lernplattformen erlauben die Auswertung statistischer Daten beispielsweise über Art und Umfang der Nutzung. Echte statistische Daten haben aber keinen Personenbezug und sind daher aus datenschutzrechtlicher Sicht unproblematisch. Sollte es sich nicht um echte statistische Daten in diesem Sinne handeln, gelten für sie die jeweiligen

Schulgesetze, Schuldatenschutzgesetze und dazu erlassene Rechtsverordnungen der Länder.

6.2 Schriftliche Festlegungen

Vor dem Einsatz der Online-Lernplattform hat die Schule / die Schulaufsichtsbehörde schriftliche Festlegungen zur zulässigen Datennutzung und zum Rollen- und Berechtigungskonzept zu treffen. Die zum Verfahren notwendigen Angaben sind im Verzeichnis über die Verarbeitungstätigkeit zu machen, Artikel 30 Datenschutz-Grundverordnung[8].

Die Vorgaben zur Konfiguration und Anwendung der Online-Lernplattform durch die Administratoren, Lehrer und Lehrerinnen kann beispielsweise in Form einer Nutzerordnung geschehen, in der klar geregelt wird, wie die Vertraulichkeit, Integrität, Authentizität, die Nichtverkettbarkeit der Daten und die Intervenierbarkeit des Nutzers entsprechend dem jeweils geltenden Landesrecht vor Ort konkret umzusetzen ist. Hierzu gehören ein Löschkonzept (9.9) sowie die Frage, welche E-Mailadressen verwendet werden (9.2).

Fazit:

Die Grundlagen der Datenverarbeitungprozesse sind vor dem Einsatz der Online-Lernplattform abschließend in einer Nutzerordnung festzulegen.

7 Notwendige Prüfungen

7.1 Allgemeine Bewertung des Schutzbedarfes der zu verarbeitenden Daten

Werden durch den Verantwortlichen Daten (siehe Nummer 6) verarbeitet, ist es notwendig den Schutzbedarf der Daten festzulegen. Aus dieser Festlegung heraus ist es dann möglich, die erforderlichen Schutzmaßnahmen (dazu nicht abschließend Nummer 9) zu ergreifen, um die Rechte der Betroffenen zu wahren. Für die Festlegung des Schutzbedarfes und der Maßnahmen zum Schutz der Rechte der betroffenen Personen haben die Datenschutzaufsichtbehörden das Standard-Datenschutzmodell (SDM)[9] als Hilfe für die Praxis entwickelt. Dieses steht auf den Internetseiten der Datenschutzaufsichtbehörden bereit zum Download. Die Methodik des SDM kann auch als Hilfsmittel für die Datenschutz-Folgeabschätzung aus Nummer 7.2 genutzt werden.

[8] Hierzu wird auf das Kurzpapier Nummer 1 der Dsk verwiesen, https://www.tlfdi.de/mam/tlfdi/gesetze/dsk_kpnr_1_verzeichnis_verarbeitungstatigkeiten.pdf.
[9] Hierzu „Das Standard-Datenschutzmodell“ in der Version 1.0 – Erprobungsfassung, https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/sdm-methode_v_1_1.pdf.

7.2 Datenschutz-Folgenabschätzung

Vor dem Einsatz von Online-Lernplattformen hat der Verantwortliche (Schule oder Schulaufsichtsbehörde) im Zusammenwirken mit seinem Datenschutzbeauftragten zu prüfen, ob die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen (Schüler, Lehrer, Eltern) zur Folge hat. Hiervon ist aufgrund der Art, der Umstände und der Zwecke der Verarbeitung bei einer Online-Lernplattform in aller Regel auszugehen[10]. Es ist dann durch den Verantwortlichen vorab eine Datenschutz-Folgenabschätzung nach Artikel 35 Datenschutz-Grundverordnung durchzuführen. Der Verantwortliche hat hierbei den Rat seines Datenschutzbeauftragten einzuholen, bleibt aber für die Durchführung allein verantwortlich. Bei der Datenschutz-Folgenabschätzung sind insbesondere folgende Aspekte zu beachten:

- Einhaltung der ggf. bestehenden landesrechtlichen Regelungen zum Einsatz von Online-Lernplattformen
- Bei der Anschaffung einer Online-Lernplattform eines externen Dienstleisters ist zu prüfen, ob dieser die datenschutzrechtlichen und schulischen Anforderungen erfüllen kann.
- Gestaltung und Auswahl von Datenverarbeitungssystemen nach den Grundsätzen der Datenvermeidung und Datensparsamkeit

7.3 Auftragsverarbeitung

Beim Einsatz von externen Dienstleistern sind die gesetzlichen Voraussetzungen der Auftragsverarbeitung nach Artikel 28 DSGVO zu beachten. Dabei gelten folgende allgemeine Anforderungen:

- Die Schule/Schulaufsichtsbehörde muss „Herrin der Daten“ bleiben. Sie bestimmt, wer die Daten auf welche Weise verarbeitet und nutzt. Sie muss gegenüber dem Auftragsverarbeiter ein Weisungsrecht in Bezug auf die Datenverarbeitung und -nutzung haben und sich vertraglich Kontrollrechte einräumen lassen.
- Die Allgemeinen Geschäftsbedingungen externer Dienstleister sind unter Beachtung der hier dargestellten Grundsätze zu überprüfen und ggf. vertraglich abzuändern.

[10] siehe hierzu Kurzpapier Nummer 5 der DSK unter https://www.tlfdi.de/mam/tlfdi/gesetze/dsk_kpnr_5_datenschutz-folgenabschatzung.pdf

- Mit dem Auftragsverarbeiter ist ein Vertrag zu schließen, der den datenschutzrechtlichen Anforderungen an die Auftragsverarbeitung nach Artikel 28 DSGVO genügt[11].

7.4 Sonstige Anforderungen

- Es gilt der Grundsatz der Zweckbindung. Danach ist insbesondere zu gewährleisten, dass die Daten der Schüler, Lehrer und Eltern nicht zu Werbezwecken genutzt werden.
- Die von der Schule/Schulaufsichtsbehörde zu erstellenden Nutzungsbedingungen, das Verzeichnis von Verarbeitungstätigkeiten (Artikel 30 DS-GVO) und die sonstigen getroffenen technischen und organisatorischen Maßnahmen sind einer datenschutzrechtlichen Prüfung zu unterziehen.

8 Unterrichtungs-, Benachrichtigung-, Schulungs- und Unterweisungspflichten

Schüler, Eltern[12] und Lehrkräfte sind vor dem Einsatz von Online-Lernplattformen ausführlich über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung ihrer Daten zu unterrichten. Hierbei sind die Anforderungen an die Informationen der betroffenen Personen nach Artikel 13 und 14 DSGVO zu beachten.

Sofern die Einwilligung für die Nutzung bestimmter Module erforderlich ist, sind sie ausdrücklich auf deren Freiwilligkeit und das bestehende Widerrufsrecht und dessen Rechtsfolgen zu informieren (Satz hierzu auch Nummer 4). Die Einwilligung ist in einer Weise einzuholen, die dem Verantwortlichen den Nachweis über die Einhaltung der gesetzlichen Voraussetzungen ermöglicht (z. B. schriftlich). Aus der Einwilligung hat hervorzugehen, welche Daten, in welcher Form und zu welchem Zweck verarbeitet werden sollen. Darüber hinaus sind die Nutzer darüber zu informieren, ob und an wen Daten übermittelt werden. Die Einwilligungserklärung muss vom Verantwortlichen in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden, vgl. Erwägungsgrund 42 DSGVO.

Außerdem sind die Lehrkräfte und Administratoren entsprechend zu schulen und die Schüler entsprechend zu unterweisen.

[11] siehe hierzu Kurzpaier Nummer 13 der DSK unter https://www.tlfdi.de/mam/tlfdi/gesetze/dsk_kpnr_13_auftragsverarbeitung.pdf

[12] Hier ist zu beachten, dass die Eltern möglicherweise bei volljährigen Schülern nach dem geltenden Landesrecht nicht immer eine Zugriffsberechtigung haben dürfen.

9 Hinweise zur technischen und organisatorischen Umsetzung

9.1 Passwörter

Die Nutzung einer Online-Plattform erfordert einen passwortgeschützten Zugriff. Passwörter müssen kryptographisch sicher gespeichert werden, z.B. mittels Schlüsselableitungsfunktionen. Bereiche mit besonderen Kategorien von personenbezogenen Daten nach Artikel 9 Absatz 1 DSGVO sollten mit einer 2-Faktor-Authentifizierung abgesichert werden. Es muss gewährleistet sein, dass niemand innerhalb der Lernplattform Passwörter im Klartext einsehen kann. Dies gilt auch für Administratoren.

Bei der Vergabe von Passwörtern durch die Schule ist zu gewährleisten, dass bei der ersten Nutzung des Logins der Nutzer sein Passwort ändern muss. Von dieser Regel kann im begründeten Einzelfall abgewichen werden (beispielsweise bei Grundschülern oder Schülern mit speziellem Förderbedarf). Nutzer mit der administrativen Berechtigung zur Bearbeitung der Benutzerkonten im System können für andere Nutzer Passwörter zurücksetzen. Von der Vergabe neuer Passwörter wird abgeraten, da dann der Administrator Kenntnis vom neuen Passwort erlangt. Bei der Passwortgenerierung, dem Passwortgebrauch und der Passwortverwaltung sollte die Maßnahme „M 2.11 - Regelung des Passwortgebrauchs“ der vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichten IT-Grundschutz-Kataloge beachtet werden. Dies betrifft insbesondere die Komplexität des Passwortes und die Geheimhaltungspflicht. Ein vorgegebener regelmäßiger Passwortwechsel kann sinnvoll sein. Dies ist von den individuellen Rahmenbedingungen abhängig.

Für die Verwendung von Passwörtern muss eine Vorgabe erfolgen, die die Mindestzahl an Zeichen und deren Zusammensetzung (Zahl der Großbuchstaben, Zahl der Kleinbuchstaben, Zahl der Ziffern und Zahl der Sonderzeichen) festlegt. Bei der Festlegung dieser Vorgaben ist das Alter der Schüler zu beachten, um keine Zugangsprobleme zu schaffen. Ein Passwort soll aber in keinem Falle kürzer als acht Zeichen sein.

9.2 E-Mail-Adresse

Die E-Mail-Adresse ist ein eindeutiger Wert. Soll eine E-Mail-Adresse innerhalb der Lernplattform zur Verfügung gestellt werden, dann ist sicherzustellen, dass diese E-Mailadresse nicht für mehrere Benutzerkonten verwendet werden kann. Die Verwendung der E-Mail-Adressen ist schriftlich zu regeln.

9.3 Erfassung der Daten des Benutzerkontos und Änderbarkeit

Benutzerkonten können durch Import, manuelle Eingabe oder Anbindung an eine bestehende Datenbank nach Maßgabe der in der Schule verwandten Systeme angelegt werden. Bei einem Import oder einer Anbindung an eine bestehende Datenbank sollte nur der Anmeldename, wie er im bestehenden Datenbestand gespeichert ist, an die Lernplattform übermittelt werden (unidirektionaler Informationsfluss). Dass Passwort muss den Richtlinien aus 9.1 entsprechen und daher evtl. neu vergeben werden. Die Schule oder die Schulaufsichtsbehörde legt die Vorgehensweise in Form von einer Nutzerordnung fest.

9.4 Öffentliche Bereiche

Es ist grundsätzlich möglich, bestimmte Bereiche einer Online-Lernplattform öffentlich zugänglich zu machen. Für diese Bereiche gelten dieselben datenschutzrechtlichen Regelungen wie für andere Internetpräsenzen von Schulen, insbesondere im Hinblick auf die Nennung von Namen oder die Abbildung von Schülern oder Lehrkräften; darüber hinaus gelten das Telemediengesetz und das Telekommunikationsgesetz. Unter Beachtung der einschlägigen Vorschriften muss eine allgemeine Zugänglichkeit immer unterbleiben, sobald dadurch personenbezogene Daten sichtbar werden.

9.5 Suchmaschinen

Bereiche, in denen nutzerspezifische Daten gespeichert werden, dürfen nicht öffentlich angeboten werden. Es ist dafür Sorge zu tragen, dass öffentliche Suchmaschinen (Google, Bing, etc.) keinen Zugriff auf diese Bereiche haben.

9.6 Rollenkonzept

Folgende Rollen sind in einer Online-Lernplattform in der Regel vorgegeben:

- Administrator: Der Administrator hat alle Berechtigungen für sämtliche Bereiche und Inhalte, er kann Benutzerkonten-Einstellungen ändern und systemweite Einstellungen vornehmen.
- Kursverwalter: Der Kursverwalter kann Bereiche anlegen und Berechtigungen vergeben. Das Recht kann auf Teilbereiche (Kurskategorien, beispielsweise Ausbildungsgänge, Fächer, Jahrgangsstufen) beschränkt werden.
- Lehrkraft: Die Lehrkraft kann in bestimmten Bereichen Inhalte pflegen, Teilnehmer zulassen, Lernfortschritte und Lernergebnisse einsehen.

- Teilnehmer: Teilnehmer können in den Bereichen arbeiten, zu denen sie eine Zugangsberechtigung haben, Lerninhalte nutzen und Eingaben tätigen.

In Übereinstimmung mit dem Rollen- und Berechtigungskonzept der Schule können weitere Rollen definiert werden.

Folgende Grundsätze sind bei der Vergabe von Rechten und Rollen zu beachten:

Ein **Administrator** kann auf alle Bereiche zugreifen. Personen mit Administrationsberechtigungen können daher alle Kurse sowie alle Beiträge der Schüler und Lehrer einsehen. Dies schließt Bewertungen mit ein. Bei der Vergabe von Administrationsrechten muss daher mit besonderer Sorgfalt vorgegangen werden und zwar:

- Jedem Administrator ist ein eigener personenbezogener Benutzeraccount zuzuweisen, d.h. es ist nicht zulässig, dass mehrere Administratoren das gleiche Benutzerkonto (= Gruppenadministratorkonto) nutzen. Der Anmeldename des Administrators muss pseudonym sein, um so eine missbräuchliche Kontosperrung zu verhindern. Das Pseudonym muss so gewählt werden, dass es nicht auf einfachem Weg herauszufinden ist.
- Administratoren, die gleichzeitig noch andere Tätigkeiten wahrnehmen, wie z.B. auch Lehraufgaben, müssen über ein separates Benutzerkonto für diese Zwecke verfügen. Es muss also die Möglichkeit bestehen, einer Person entsprechend ihrer verschiedenen Rollen mehrere Benutzerkonten zuweisen zu können.
- Die Anzahl der Administratorenkonten ist so gering wie möglich zu halten, um das Missbrauchsrisiko zu minimieren (z.B. unbefugte Kenntnisnahme, unkontrollierbare Rechtevergaben, etc.). Eine Vertretungsregelung muss aber gewährleistet sein.
- Administratorenrechte darf nur erhalten, wer innerhalb des Systems entsprechende Aufgaben tatsächlich wahrnehmen muss.
- Alle Aktivitäten der Administratoren sind ausschließlich zu Zwecken der Datenschutzkontrolle für einen Zeitraum von in der Regel minimal sechs Monaten und maximal einem Jahr zu protokollieren. Eine regelmäßige Kontrolle der Protokolle sollte im 4-Augen-Prinzip stattfinden.

9.7 Zugriffsrechte

9.7.1 Zugriff durch schulinterne Stellen oder Personen

Welche Zugriffsrechte Lehrkräfte, die Schüler, die Schulleitung und der Administrator auf das System erhalten, ist in einem Rollen- und Berechtigungskonzept vorab schrift-

lich festzulegen. Dabei sind u. a. auch personalvertretungsrechtliche Vorgaben zu beachten.

Mitglieder der Schulleitung und gegebenenfalls Funktionsträger haben das Recht zur Durchführung von Unterrichtshospitationen. Dieses Recht dient der Wahrnehmung der Führungsaufgabe, der Beschaffung von Informationen und Eindrücken zur Unterrichts- und Schulkonzeptentwicklung. In vielen Schulen werden Klassenarbeiten exemplarisch nach der Bewertung und vor der Rückgabe an die Schüler der Schulleitung zur Information und Kenntnisnahme vorgelegt. Gleichwohl dürfen diese Zugriffe nur erfolgen, soweit es für die jeweilige Aufgabe erforderlich ist.

Werden Online-Lernplattformen eingesetzt, so werden sie automatisch zu einem Bestandteil der Unterrichtsarbeit. Damit gelten die schulinternen Vereinbarungen, die im Hinblick auf Hospitationen getroffen wurden, auch hier.

Die Art der Einsichtnahme der Schulleitung in die Arbeit mit einer Online-Lernplattform muss den schulinternen Vereinbarungen entsprechen, wie sie für Unterrichtshospitationen im Klassenraum gelten. Die Nutzer der Lernplattform sind über diese Vorgehensweisen und Vereinbarungen vor Beginn der Nutzung zu informieren. Jede Einsichtnahme wird in derselben Weise dokumentiert, wie dies für Hospitationen im regulären Unterrichtsbetrieb erforderlich und festgelegt ist.

Eine Überwachung der Arbeit mit der Lernplattform durch die Schulleitung oder andere Stellen und Personen ist nicht zulässig. Insbesondere darf auch eine Überwachung der Aktivitäten von Schülern durch Lehrende nicht stattfinden. Etwas anderes gilt, wenn die Plattform für pädagogische Aufgaben, wie organisierte Chats zu bestimmten Themen, Gruppenarbeiten usw. genutzt wird, die einer Benotung unterfallen. In diesem Fall darf die für die Benotung notwendig zu beobachtende Aktivität durch die Lehrkraft überwacht werden. Der Umfang der Daten, die für Lehrende sichtbar sein soll, ist daher pädagogisch zu begründen und von der Schulkonferenz festzulegen. Ebenso wenig dürfen die Aktivitäten von Lehrenden durch Vorgesetzte auf der Online-Lernplattform überwacht werden. Die entsprechenden Regelungen sind in der Nutzerordnung festzulegen.

9.7.2 Zugriff auf die Daten durch schulexterne Stellen oder Personen

Schulexterne haben grundsätzlich keinen Zugriff auf geschützte Bereiche der Online-Lernplattform. Sollte es in begründeten Ausnahmefällen nötig sein, so ist jeder Zugriff dieser Art zuvor durch den Verantwortlichen auf seine Rechtmäßigkeit zu prüfen. Die Teilnehmer sind über diesen Zugriff frühzeitig zu informieren. Es ist im Rahmen der datenschutzrechtlichen Vorschriften zulässig, externen Personen, die nicht als Lehrer, Schüler oder Mitarbeiter in der Schulverwaltung tätig sind, einen temporären und be-

grenzten Zugriff auch auf geschützte Bereiche der Lernplattform zu geben, sofern dies für die Gewährleistung der Funktion des Systems erforderlich ist, beispielsweise bei einer Fernwartung. Hierbei muss mit dem jeweiligen Auftragsverarbeiter ein Vertrag über die Auftragsverarbeitung abgeschlossen werden.

9.8 Datenlöschung

Soweit die Speicherung personenbezogener Daten einer Einwilligung bedarf, werden die gespeicherten Daten der Lehrer und Schüler gelöscht, wenn die Einwilligung widerrufen wird. Die Daten der Schüler in Kursen (letzte Bearbeitung, bearbeitete Lektionen, Fehler, Korrekturanmerkungen u. Ä.) werden jeweils am Ende des laufenden Schuljahres gelöscht. Aufbewahrungsfristen aus den Landesschulgesetzen bzw. zugehörigen Rechtsverordnungen sind ebenfalls zu beachten. Es ist schriftlich festzulegen, wie die Aufbewahrungsfristen eingehalten werden. Ausnahmen sind zulässig beispielsweise bei schuljahresübergreifenden Projekten zur Vorbereitung auf Nachprüfungen, bei abiturrelevanten Kursen und aufgrund von Dokumentationspflichten der Schule. Auch E-Portfolios der Schüler können im Sinne einer Sicherheitskopie während der Zeit des kompletten Schulbesuchs hinterlegt werden. Die übrigen Daten der Schüler und Lehrer werden spätestens am Ende des Schuljahres gelöscht, in dem die Lehrkraft von der Schule abgegangen ist oder der Schüler ausgetreten ist.

Benutzerkonten von Schülern und Lehrern sind nach deren Ausscheiden aus der Schule zu löschen oder wenn diese ihre Einwilligung widerrufen.

Die unter 6.1.3 genannten Log-Daten (z.B. wann welcher Nutzer auf welche Daten zugegriffen hat oder wann welche Funktionen genutzt wurden) fallen auf Serverseite an und ermöglichen es, Probleme beim technischen Betrieb und beim Zugriff der Nutzer im Bedarfsfall zu untersuchen und zu lösen. Die Speicherdauer sollte maximal zehn Tage betragen. Eine längere Speicherdauer ist nur in begründeten Ausnahmefällen zulässig. Für weitergehende Regelungen zur Protokollierung wird auf die o.g. Orientierungshilfe „Protokollierung“ [13] verwiesen.

Die entsprechenden Regelungen sind in der Nutzerordnung festzulegen.

9.9 Trennung der Datenbanken

Jede Schule wird als eigenständige Organisationseinheit verstanden. Die Daten verschiedener Schulen sind logisch getrennt zu halten und zu verwalten. Es muss mindestens gewährleistet sein, dass Schulen nur auf ihre eigenen Daten zugreifen können. Hierzu wird auf die OH Mandantenfähigkeit des Arbeitskreises Technische und organi-

[13] siehe unter 6.1.3

satorische Datenschutzfragen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in der jeweils aktuellen Fassung verwiesen.

9.10 Sonstige technische Maßnahmen

Es sollten konkrete Maßnahmen vorgeschlagen werden, die insbesondere den Zugriff externer Stellen auf die Daten verhindern und gewährleisten, dass die Datenübertragung auf den häuslichen Rechner der Lehrkräfte und Schüler sowie je nach Rollenkonzept ggf. der Eltern sicher vor unbefugtem Zugriff erfolgt. Die jeweils zu treffenden Maßnahmen richten sich dabei nach den konkreten Umständen des Einzelfalls. Je nach der Art der betroffenen Daten, dem Personenkreis, der auf sie Zugriff haben soll, dem Ort, an dem die Daten gespeichert werden, differiert das Maß der erforderlichen Sicherheit. Wenn es sich lediglich um eine reine Lernplattform handelt, die nur Informationen für die Schüler zur Verfügung stellt, sind nicht die gleichen hohen Schutzmaßnahmen erforderlich wie bei einer Plattform, auf der Noten abgespeichert werden und auf die in bestimmen Bereichen auch Dritte Zugriff haben.

Die Sicherheitsmaßnahmen betreffen insbesondere drei Punkte: die Datensicherheit auf dem Server, den Schutz des Administratorzugangs und den Schutz der Datenübertragung hin zum Nutzer.

1. Für die Nutzung der Lernplattform ist auf dem Server ein umfassendes Rechte- und Rollenkonzept vorzuhalten, das jedem Nutzer nur den Zugang zu den Programmteilen ermöglicht, für die er vorgesehen ist.

2. Der Administratorzugriff ist innerhalb der Lernplattform ein sehr kritischer Punkt. Das Passwort sollte gängigen Sicherheitsvorkehrungen genügen. Es wird hierbei auf die jeweils aktuelle BSI Richtlinie zur Erstellung von Passwörtern verwiesen. In Anbetracht der sehr experimentierfreudigen Natur der Schüler sollte außerdem die Administration nur über für Schüler unzugängliche Rechner erfolgen, da dann ausgeschlossen werden kann, dass Schüler unbemerkt Schadsoftware installieren können, die dann das Administratorpasswort ausspähen könnte. Außerdem ist der Einsatz einer Firewall und aktueller Anti-Viren Software auf dem Server unerlässlich. Eine Zweifaktor- Authentifizierung, wie sie bei vielen webbasierten Anwendungen Standard ist, wird abhängig vom Ergebnis der Datenschutz-Folgenabschätzung für administrative Zugriffe bei Anwendungen mit erhöhtem Funktionsumfang unerlässlich

sein, ebenso ggf. auch für die Rollen „Kursverwalter“ und „Lehrkraft“ (Abschnitt 9.6).

3. Die Datenübertragung zwischen Server und Nutzer ist zu verschlüsseln. Je nach Lernplattform ist dabei der Einsatz der Verschlüsselungstechnologie einzeln zu prüfen.

Schutz des Persönlichkeitsrechts

Tätigkeitsbericht
des
Sächsischen Datenschutzbeauftragten

Teil 2

Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten 2018

Datenschutz-Grundverordnung (EU) 2016/679
Richtlinie (EU) 2016/680 und sonstige Bereiche

- Berichtszeitraum: 25. Mai bis 31. Dezember 2018 -

Inhaltsverzeichnis Teil 2

Sachgebietsregister

Berichtszeitraum: 25. Mai 2018 bis 31. Dezember 2018

* | *ausschließlich öffentlicher Bereich – öB*
nicht markiert| *nicht-öffentlicher Bereich – nöB bzw. ggfs. auch öffentlicher Bereich - öB/nöB*

Datenschutz-Grundverordnung (EU) 2016/697	**Fundstelle** (Ziffern der Gliederung)
Archivwesen*	
Auftragsverarbeitung	2.1.2, 4.3, 4.9.1
Beliehene*	4.8.5
Beschäftigtendatenschutz (incl. Personalvertretungen*, Betriebsräte, sonstige Vertretungen und Beauftragte)	2.1.1, 4.3.3, 4.9.8, 7.2.10, 9.2, 9.6
Betrieblicher Datenschutzbeauftragter, s. *Datenschutzbeauftragter*	4.8, 6.2.5
Betroffenenrechte (Information, Auskunft, Löschung etc.)	3
Bildung und Wissenschaft	
· Hochschulen, Forschungseinrichtungen	4.1.6
· Schulen, Schulbehörden*, Bildungseinrichtungen	2.3.3
· Sonstiges, Allgemeines	
Datenschutzbeauftragter	4.8
Datenschutz-Folgenabschätzung	4.7, VI 2.6
Dashcam, s. Videografie	
E-Government*	
Einwilligung	2.3
Freie Berufe	
· Rechtsanwälte	4.5.1
· Notare	2.3.4
· Steuerberater, Wirtschaftsprüfer	4.3.3
· Architekten, Ingenieure	
· Sonstiges, Allgemeines	
Gemeinsam Verantwortliche	4.2, 8.1
Gesundheitswesen	
· Behördliche Aufsicht und Überwachung*	
· Krankenhäuser	3.2.3, 7.2.5

Richtlinie (EU) 2016/680 (Strafverfolgung, Polizei, Justiz)	
Polizei*	8
Ordnungswidrigkeitenbehörden*	
Strafverfolgung*	8
Strafvollzug*	

Sonstige Bereiche außerhalb Verordnung 2016/697 und Richtlinie EU 2016/680	
Sächsischer Landtag als Parlament	1.3, 7.2.6, 8.2
Verfassungsschutz	8.2
Weitere datenverarbeitende Stellen	

1 Datenschutz im Freistaat Sachsen

1.1 Gesetzgeberische Anpassung an EU-Recht in Sachsen*

Mit dem Wirksamwerden der Datenschutz-Grundverordnung waren landesgesetzlich zahlreiche Anpassungen an die europarechtliche Verordnung vorzunehmen. Das entsprechende Artikelgesetz, das *Gesetz zur Anpassung landesrechtlicher Vorschriften an die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG* enthielt allein 46 einzelne Gesetze und Rechtsverordnungen betreffende Änderungen, Drucksache 6/10918.

Hervorzuheben ist hierbei Artikel 1, Sächsisches Datenschutzdurchführungsgesetz, SächsDSDG, das für die Datenverarbeitung der Behörden und sonstigen öffentliche Stellen des Freistaates Sachsen, der Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Freistaates Sachsen unterstehenden juristischen Personen des öffentlichen Rechts und fortan ergänzend zur Datenschutz-Grundverordnung Anwendung findet.

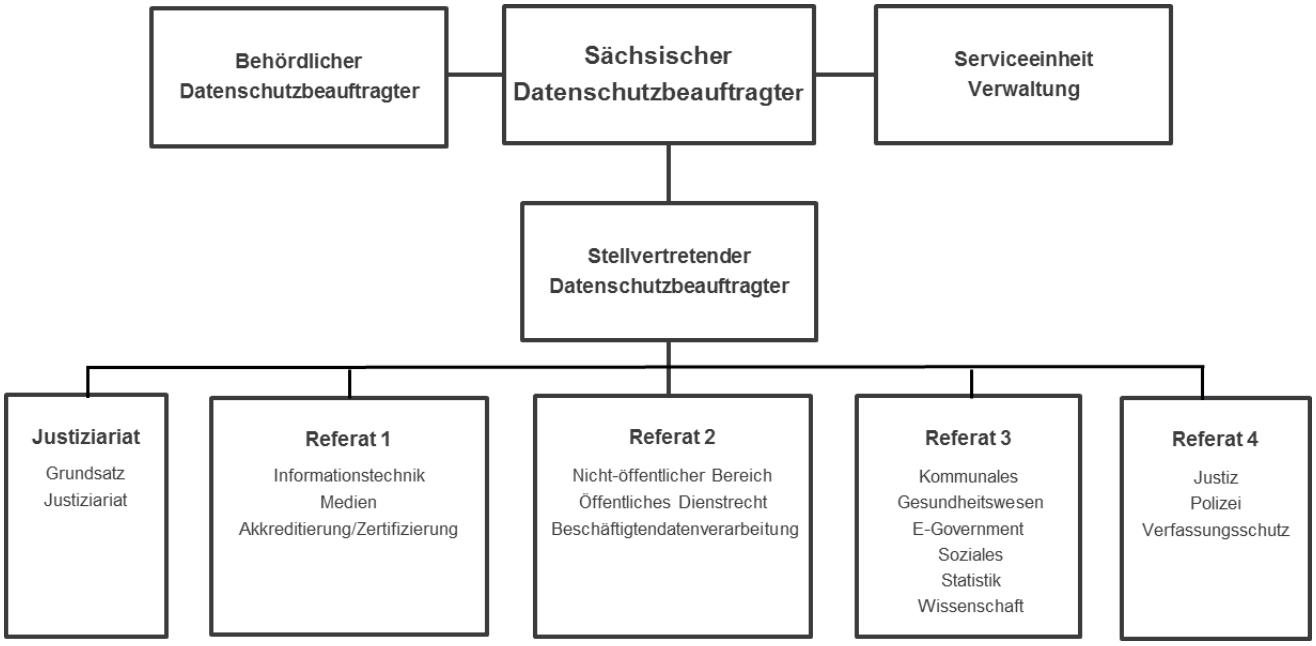
Das Sächsische Datenschutzgesetz – SächsDSG – wurde hingegen mit Artikel 46 für den Bereich der *Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates* – Amtsblatt der Europäischen Union vom 4.5.2016, L 119/89 – angepasst. Es gilt mithin für den Polizei- und Justizbereich der Strafverfolgung, Strafvollstreckung und der Gefahrenabwehr. Auch die Datenverarbeitungstätigkeit der Ordnungswidrigkeitenbehörden unterfällt dem Richtlinienbereich.

Zu erwähnen bleibt noch die *Änderung des Staatsvertrags über den Mitteldeutschen Rundfunk zum Zwecke der Umsetzung der Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/G (MDR-Datenschutz-StV)*. Der Bereich des Mitteldeutschen Rundfunks unterliegt weiterhin einer sektoralen Datenschutzaufsicht durch den Datenschutzbeauftragten des Mitteldeutschen Rundfunks. Ich hätte eine deutlichere Ausgestaltung der Unabhängigkeit der Datenschutzaufsicht befürwortet.

1.2 Die personelle Ausstattung des Sächsischen Datenschutzbeauftragten

War die sachliche Ausstattung meiner Behörde bisher im Wesentlichen in zurückliegenden Haushaltsjahren als hinreichend zu betrachten gewesen, machte ich aufgrund des Inkrafttretens der Datenschutz-Grundverordnung und der Richtlinie für den Polizei- und Strafjustizbereich, angesichts zusätzlicher Aufgaben und Befugnisse sowie des sich abzeichnenden stetig steigenden Geschäftsanfalls wegen Artikel 52 Absatz 4 DSGVO frühzeitig gegenüber der Staatsregierung einen erhöhten Stellenbedarf mit insgesamt 30 Vollzeitstellen geltend, woraufhin mir zunächst allerdings kein adäquater Stellenaufwuchs in Aussicht gestellt wurde. Zusätzlich zu den bei Wirksamwerden der Datenschutz-Grundverordnung im Mai bestehenden 22 Vollzeitstellen ist allerdings zwischenzeitlich haushaltsgesetzlich der Personalaufwuchs auf 31 Personalstellen nachgebessert worden. Der so vorgesehene Stellenplan ist eine deutliche Verbesserung, perpetuiert aber immer noch eine fortwährende Unterbesetzung. Beratungsanfragen können mit dem Personalbestand häufig nur verzögert bearbeitet, Vortragswünsche oft nicht positiv beantwortet werden und notwendige Vor-Ort-Kontrollen werden verschoben. Verfahren und Vorgänge dauern zum Nachteil betroffener Personen und ratsuchender Unternehmen länger als es notwendig wäre. Das ist nicht zuletzt auch für die Bediensteten meiner Behörde nicht zufriedenstellend. Beschäftigte in Schlüsselfunktionen meiner Behörde zeigen mir gegenwärtig regelmäßig ihre Überlastung an.

Die Struktur der Dienststelle soll sich auf der haushaltsgesetzlichen Grundlage wie folgt darstellen:



Zur weiteren Information:

Mit der Umsetzung der Datenschutz-Grundverordnung erhielt meine Behörde den Status einer obersten Staatsbehörde.

Der gesamte Sach- und Stellen-Haushalt ist daher gesondert im Einzelplan 13 aufgeführt, https://www.finanzen.sachsen.de/download/EP13_DHH_2019_2020.pdf.

1.3 Datenschutz im Sächsischen Landtag bei der Wahrnehmung parlamentarischer Aufgaben*

Das „Gesetz zur Anpassung landesrechtlicher Vorschriften an die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“, mit dem landesrechtliche Vorschriften zum Datenschutz an die Verordnung (EU) 2016/679 (Europäische Datenschutz-Grundverordnung – DSGVO) angepasst wurden, trat am 25. Mai 2018 in Kraft, an dem Tag also, ab dem die Vorschriften der DSGVO in dem von ihr erfassten Bereich unmittelbar anzuwenden waren. Damit änderte sich – zumindest in Teilen – auch die Datenschutzrechtslage im Sächsischen Landtag.

Während es bis zu diesem Zeitpunkt in den allgemeinen Datenschutzgesetzen (BDSG a. F. und SächsDSG a. F.) keine speziell auf die Mitglieder und Gremien des Landtags zugeschnittenen Vorschriften gab und die allgemeinen datenschutzrechtlichen Vorschriften der Datenschutzgesetze zur (beschränkten) Anwendung kamen – je nach Einordnung der Handelnden als öffentliche oder nicht-öffentliche Stellen und unter Berücksichtigung der besonderen verfassungsrechtlichen Stellung des Parlaments und seiner Mitglieder –, ist nun ausdrücklich gesetzlich geregelt, welche datenschutzrechtlichen Bestimmungen gelten.

Für Verarbeitungen personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben durch den Landtag, seine Gremien, seine Mitglieder, die Fraktionen und deren Beschäftigte sowie die Landtagsverwaltung ist der Anwendungsbereich der DSGVO nicht eröffnet. Nach Artikel 2 Absatz 2 Buchstabe a DSGVO gilt die DSGVO nicht für „Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen“. Die Tätigkeit der mitgliedsstaatlichen Parlamente in Ausübung der klassischen Parlamentsfunktionen unterfällt diesem Ausschluss und somit auch die Verarbeitung personenbezogener Daten, die der einzelne Abgeordnete im Rahmen der Ausübung seines Mandats und die anderen genannten Stellen bei der Wahrnehmung originärer parlamentarischer Aufgaben vornehmen.

Soweit bei der Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeitet werden, gilt seit dem 25. Mai 2018 übergangsweise das Sächsische Datenschutzgesetz für einen Zeitraum von ca. anderthalb Jahren bis zum 31. Dezember 2019 (§ 2 Absatz 2 SächsDSG i. V. m. § 42 Satz 1 SächsDSG). Bis zu diesem Zeitpunkt wird sich das Parlament eine Datenschutzordnung geben (Verpflichtung aus § 2 Absatz 1 Satz 4 SächsDSDG).

Was (mehr oder weniger) genau die „parlamentarischen Aufgaben“ in diesem Sinne sind, ergibt sich aus der Sächsischen Verfassung, aus der Geschäftsordnung des 6. Sächsischen Landtags (GO) und aus gesetzlichen Vorschriften. Von herausgehobener Bedeutung sind hierbei Artikel 39 Absatz 2, 3 der Sächsischen Verfassung (SächsVerf): „Der Landtag übt die gesetzgebende Gewalt aus, überwacht die Ausübung der vollziehenden Gewalt nach Maßgabe dieser Verfassung und ist Stätte der politischen Willensbildung. Die Abgeordneten vertreten das ganze Volk. Sie sind nur ihrem Gewissen unterworfen und an Aufträge und Weisungen nicht gebunden.“, Artikel 52 Absatz 1 SächsVerf i. V. m. §§ 21 Absatz 1, 39 Absatz 1 GO: „Der Landtag bildet ständige Ausschüsse. Die Geschäftsordnung bestimmt Aufgaben, Zusammensetzung und Arbeitsweise.“, „…Als vorbereitende Beschlussorgane des Landtags haben sie die Pflicht, dem Landtag bestimmte Beschlüsse zu empfehlen, die sich nur auf die ihnen überwiesenen Vorlagen oder mit diesen im unmittelbaren Sachzusammenhang stehenden Fragen beziehen dürfen. Sie können sich jedoch auch mit anderen Fragen aus ihrem Geschäftsbereich befassen, wenn es der Ausschuss beschließt.“, „Beratungsgegenstände sind die dem Ausschuss überwiesenen Vorlagen, die mit diesen unmittelbar im Zusammenhang stehenden Fragen und andere Fragen aus dem Geschäftsbereich des Ausschusses.“ und § 1 Absatz 4 des Fraktionsrechtsstellungsgesetzes: „Die Fraktionen dienen der politischen Willensbildung im Sächsischen Landtag nach den Grundsätzen der parlamentarischen Demokratie. Sie koordinieren die Kontrolle der Staatsregierung, unterstützen die politisch-parlamentarische Tätigkeit ihrer Mitglieder nach innen und außen einschließlich darauf bezogener spezifischer Schulungsmaßnahmen im Einzelfall und ermöglichen ein aufeinander abgestimmtes Verfolgen gemeinsamer politischer Ziele. Sie können insbesondere mit anderen Fraktionen zusammenarbeiten, regionale und überregionale sowie internationale Kontakte pflegen. Die Fraktionen dürfen die Öffentlichkeit über ihre Ziele und Tätigkeit informieren; sie dürfen sich dabei auch mit gesellschaftspolitischen Fragen befassen, die mit ihrer Tätigkeit in unmittelbarem Zusammenhang stehen“.

Danach kann eine klare Abgrenzung des Aufgabenbereichs, wie sie bei Verwaltungsbehörden und Gerichten anhand genauer gesetzlicher Aufgabenzuweisungen und Zuständigkeitsvorschriften möglich ist, im parlamentarischen Bereich nicht gelingen. Wie etwa politische Willensbildung oder die Befassung mit gesellschaftspolitischen Mitteln

inhaltlich gestaltet wird, kann mit Blick auf das freie Mandat des Abgeordneten nicht einfachgesetzlich eindeutig definiert werden.

Allerdings – und insoweit ist eine Grenzziehung durchaus möglich – unterfallen rein administrative Tätigkeiten des Abgeordneten, der Fraktionen und der Landtagsverwaltung, die die Mandatsausübung sowie Fraktions- und Ausschussarbeit lediglich unterstützen, nicht dem Bereich der Wahrnehmung parlamentarischer Aufgaben; das Schaffen von Rahmenbedingungen also, unter denen die Abgeordneten und die Fraktion sowie die Ausschüsse ihre „klassischen“ parlamentarischen Aufgaben optimal wahrnehmen können. Hierzu zählen etwa die Beschäftigung von Mitarbeitern, der technische Betrieb einer Homepage, die Beschaffung von Materialien, Räumlichkeiten usw. Werden in diesen Zusammenhängen personenbezogene Daten verarbeitet, gelten die allgemeinen Vorschriften; Abgeordnete, Fraktionen und Landtagsverwaltung können sich hier nicht auf ein „Sonderrecht“ berufen.

Soweit der Landtag, seine Gremien, seine Mitglieder, die Fraktionen und deren Beschäftigte sowie die Landtagsverwaltung bei der Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten, gelten, wie oben erwähnt, gemäß § 2 Absatz 2 SächsDSG die Vorschriften des Sächsischen Datenschutzgesetzes. Die Verarbeitung personenbezogener Daten ist danach nur zulässig, wenn das Sächsische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat (§ 4 Absatz 1 SächsDSG). Die maßgeblichen Verarbeitungsvorschriften des Sächsisches Datenschutzgesetzes finden sich in §§ 12 ff. SächsDSG; personenbezogene Daten dürfen unter den dort normierten Voraussetzungen erhoben, gespeichert, verändert und genutzt sowie übermittelt werden. Wesentliches Kriterium ist dabei die Erforderlichkeit der Verarbeitung für die Wahrnehmung (= Erfüllung) der parlamentarischen Aufgaben. Nach einer strengen, auf behördliches Handeln der Exekutive zielenden Auslegung ist die Erforderlichkeit im datenschutzrechtlichen Sinn (nur) zu bejahen, wenn die verantwortliche Stelle ihre (in aller Regel gesetzlich klar umrissenen und zugewiesenen) Aufgaben ohne Verarbeitung der konkreten Daten nicht oder nur mit unverhältnismäßig großem Aufwand erfüllen könnte.

Angesichts der Stellung des Parlaments im Gefüge der Staatsgewalten, unter Berücksichtigung des freien Mandats des Abgeordneten und mit Blick auf die naturgemäß wenig konturierte Aufgabenbeschreibung (s.o.) kann für die Erforderlichkeit der Datenverarbeitung bei der Wahrnehmung parlamentarischer Aufgaben nicht derselbe (strenge) Maßstab gelten, der bei Exekutivbehörden heranzuziehen ist. Im Ergebnis dürfen keine allzu hohen Anforderungen an die Erforderlichkeit gestellt werden; die Breite der parlamentarischen Aufgaben und die für die politische Willensbildung, die Kontaktpflege und die Befassung mit gesellschaftspolitischen Fragen notwendigen Informationsbezie-

hungen müssen zu einer weiten Auslegung des Begriffs der Erforderlichkeit führen, wobei gleichwohl stets kritisch hinterfragt werden sollte, ob – insbesondere bei Übermittlungen an Dritte oder bei Veröffentlichungen – die Verwendung von Namen oder anderen Angaben mit eindeutigem Personenbezug für die Wahrnehmung der betreffenden parlamentarischen Aufgabe wirklich notwendig sind.

Eine – neben der „weiten Erforderlichkeit“ – weitere Besonderheit bei der Anwendung des SächsDSG bei der Verarbeitung personenbezogener Daten zur Wahrnehmung parlamentarischer Aufgaben betrifft die Frage der datenschutzrechtlichen Kontrolle. Zwar kontrolliere ich gemäß § 27 Absatz 1 SächsDSG die Einhaltung des SächsDSG und anderer Vorschriften über den Datenschutz. Tatsächlich kontrolliere ich nicht, soweit die oben genannten Stellen in Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten. Aus Gründen der Gewaltenteilung und der verfassungsrechtlichen Stellung des Landtags erstreckt sich meine Kontrollzuständigkeit – insoweit bin ich eine Stelle der Exekutive – nicht auf Tätigkeiten des Parlaments. § 27 SächsDSG ist insoweit verfassungskonform einschränkend auszulegen. Damit wird einerseits eine seit Bestehen des Sächsischen Datenschutzgesetzes geübte Praxis fortgeführt und andererseits der Rechtslage entsprochen, die ab dem Jahr 2020 hinsichtlich des Schutzes personenbezogener Daten bei der Verarbeitung in Wahrnehmung parlamentarischer Aufgaben bestehen wird. Dann wird – wie oben erwähnt – das SächsDSG außer Kraft treten und der Sächsische Landtag sich eine Datenschutzordnung geben (§ 2 Absatz 1 Satz 4 SächsDSDG); eine Datenschutzkontrolle wird dann auch formal nur parlamentsintern erfolgen.

1.4 Ergänzende Rechtssetzung der EU zur Datenschutz-Grundverordnung

Bis zum Wirksamwerden der Datenschutz-Grundverordnung konnte ein bedeutendes und langdauerndes Gesetzgebungsverfahren der EU noch nicht abgeschlossen werden. Die e-Privacy-Verordnung soll die Datenschutz-Grundverordnung im Bereich der elektronischen und Internet-Kommunikation als unmittelbar geltendes Recht in den EU-Mitgliedsstaaten ergänzen und dem Schutz personenbezogener elektronischer Kommunikationsdaten und Kommunikationsinformationen juristischer Personen dienen. Gegenwärtig wird noch eine EU-Richtlinie mit dem nationalen Telekommunikationsgesetz und dem Telemediengesetz realisiert. Die Verordnung, die im Entwurfsstadium vorliegt, wird voraussichtlich die elektronische Kommunikationsvorgänge von Messengerdiensten, internetbasierten E-Mail-Diensten, Internettelefonie und den Bereich Social Media betreffen. Über die Inhalte besteht noch keine endgültige Einigkeit. Betroffen sind Dienstleister, die elektronische Kommunikationsleistungen an Nutzer in der Europäi-

schen Union richten. Gegenwärtig wird ein Inkrafttreten der Verordnung erst im Jahre 2022 erwartet.

Die zu erwartenden Vorschriften erstrecken sich auch auf den Umgang mit sogenannten Cookies sowie Werbung mittels elektronischer Kommunikation einschließlich E-Mail- und Telefonwerbung. Aktueller Streitpunkt des Entwurfs sind insbesondere noch die Voraussetzungen der Zulässigkeit von Cookies, Dateien, welche von einer Internetseite in den Browserverlauf der Nutzer gespeichert wird und die die Nutzung der Internetpräsenz, etwa Häufigkeit des Seitenaufrufs durch den Besucher für den Seitenbetreiber nachvollziehbar machen. Nach dem Entwurf sollen Seitenanbieter zum einen nur noch für die Funktionsweise der Internetpräsenz notwendige und damit weniger Informationen erfassen dürfen und keine Informationen aus den Endgeräten der Seitenbesucher. Ohne Einwilligungen sollen nur noch Cookies eingesetzt werden können, die keine persönlichkeitsrechtlichen Auswirkungen auf die betroffenen Personen haben.

Zum verordnungskonformen Betrieb einer Internetpräsenz und für Hinweise in der Übergangszeit auf Grundlage des bestehenden Rechts vergleiche auch den Tätigkeitsberichtsbeitrag unter 4.1.3.

2 Grundsätze der Datenverarbeitung

2.1 Datenverarbeitungsgrundsätze, Begriffsbestimmungen

2.1.1 Betriebsräte und Personalvertretungen als Verantwortliche

Mehrfach wurde die Frage an meine Dienststelle gerichtet, ob Betriebsräte und Personalvertretungen eigene Verantwortliche im Sinne der Datenschutz-Grundverordnung seien, vergleiche Artikel 4 Nummer 7 DSGVO.

Ich gehe davon aus, dass der Betriebsrat eine zum Unternehmen gehörende Einheit darstellt und dass Personalvertretungen unselbständiger Teil einer öffentlichen Stelle sind. Damit besteht auch eine Benennungspflicht für einen Datenschutzbeauftragten nur für das Unternehmen selbst bzw. die Behörde, nicht aber für die jeweiligen Beschäftigtenvertretungen. Diese Auffassung steht im Einklang mit der Rechtsprechung des Bundesarbeitsgerichts, so unter anderem zuletzt mit Beschluss vom 7. Februar 2012,1 ABR 46/10. In Bezug auf diese Frage besteht allerdings bisher Uneinigkeit zwischen den deutschen Datenschutzaufsichtsbehörden.

Von der Frage zu trennen ist, inwieweit der Datenschutzbeauftragte befugt ist, die personenbezogene Datenverarbeitung des Betriebsrats bzw. der Personalvertretung zu überwachen. Hierzu vergleiche 4.8.8 unten.

2.1.2 Datenschutzrechtliche Einordnung der Immobilienverwaltung als Verantwortlicher

Zu der Frage, ob für Wohnungseigentümergemeinschaften tätige Hausverwaltungen im Rahmen einer Auftragsverarbeitung handeln oder selbst Verantwortliche sind, erreichten mich mehrere Anfragen.

Seitens einiger Hausverwaltungen wurde diesbezüglich die Auffassung vertreten, dass sie lediglich als ausführendes Organ der Wohnungseigentümergemeinschaft handelten und daher ein entsprechender Auftragsverarbeitungsvertrag (Artikel 28 Absatz 3 DSGVO) abzuschließen sei. Verantwortlicher für alle datenschutzrechtlichen Belange im Sinne der DSGVO sei nicht der Verwalter, sondern die Wohnungseigentümergemeinschaft. Dies ergebe sich im Umkehrschluss aus § 27 WEG, der eine Verpflichtung des Verwalters für datenschutzrechtlich relevante Vorgänge wie beispielsweise die Verbrauchsdatenerhebung oder Abrechnungsangelegenheiten nicht statuiere. In diesem Zusammenhang wurden der jeweiligen Wohnungseigentümergemeinschaft dann – natürlich gegen Kostenerstattung – die Erstellung des Verarbeitungsverzeichnisses und die Bearbeitung von Auskunftsersuchen nach Artikel 15 DSGVO angeboten.

Diese Auffassung teile ich nicht. Unter allen deutschen Aufsichtsbehörden (DSK) besteht Einigkeit dahingehend, dass zwischen der Wohnungseigentümergemeinschaft und dem Verwalter kein Auftragsverarbeitungsverhältnis vorliegt. Auch der Dachverband Deutscher Immobilienverwalter e. V. vertritt diese Auffassung.

Die Wohnungseigentümergemeinschaft hat mit der Hausverwaltung einen Hausverwaltungsvertrag abgeschlossen. In dessen Rahmen verarbeitet die Hausverwaltung zur Erfüllung der ihr nach §§ 27 f. WEG obliegenden Aufgaben personenbezogene Daten (in erster Linie der Mitglieder der Wohnungseigentümergemeinschaft) in eigener Verantwortung und ist damit Verantwortlicher im Sinne der DSGVO; ein Auftragsverarbeitungsverhältnis liegt hier nicht vor. Verantwortlicher ist nach Artikel 4 Nummer 7 DSGVO u. a. die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die Hausverwaltung entscheidet im Wesentlichen autark, welche Daten sie zur Erfüllung der ihr gesetzlich obliegenden Aufgaben verarbeitet und in welcher Weise sie das realisiert. Sie kann daher jedenfalls insoweit kein weisungsgebundener Auftragsverarbeiter sein.

Würde die Eigentümergemeinschaft beschließen, über den Aufgabenkatalog der §§ 27 f. WEG hinaus personenbezogene Daten zu verarbeiten, wäre sie für diesen Bereich ggf. als Verantwortlicher und die Hausverwaltung als Auftragsverarbeiter anzusehen. Eine solche Konstellation bestünde beispielsweise dann, wenn die WOHNUNGSEIGENTÜMERGEMEINSCHAFT eine Videoüberwachung einführen wollte.

2.2 Rechtmäßigkeitsvoraussetzungen der Datenverarbeitung

2.2.1 Zum berechtigten Interesse beim Einsatz von Dashcams

Auf die Dashcam-Problematik ist in diesem Bericht – wenn auch unter alter Rechtslage – bereits ausführlich eingegangen worden (vgl. dazu Pkt. 2.7.1.1 meines 9. TB im nichtöffentlichen Bereich). Auf diese Ausführungen wird hier ausdrücklich verwiesen.

Auch nach Maßgabe der DSGVO sowie des ergänzend heranzuziehenden, insoweit im Wesentlichen mit der alten Rechtslage (§ 6b BDSG-alt) übereinstimmenden § 4 BDSG ist der Einsatz solcher Kameras datenschutzrechtlich nur unter sehr engen Voraussetzungen zulässig; praktisch hat sich die Rechtslage dabei nicht verändert.

Soweit mit den Dashcams in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck der Aufnahmen die Verwendung von Filmaufnahmen zur Dokumentation eines etwaigen Unfallhergangs angegeben wird, ist der Einsatz – auch wenn die Kameras von Privatpersonen eingesetzt werden – an Artikel 6 Absatz 1 Satz 1 Buchstabe f DSGVO zu messen. Danach ist die Verarbeitung personenbezogener Daten nur zuläs-

sig, soweit dies zur Wahrung berechtigter Interessen von Verantwortlichen oder Dritten erforderlich ist und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei den betroffenen Personen um Kinder handelt. Das bedeutet, dass die Interessen des eine Dashcam einsetzenden Verantwortlichen mit den Interessen der davon Betroffenen abzuwägen sind. Eine entscheidende Rolle spielt dabei jeweils der Einsatzzweck, der konkrete Betriebsmodus (permanente Daueraufzeichnung / anlassbezogene Kurzaufzeichnung) und auch das örtliche Einsatzumfeld, d. h. wo konkret die Dashcam eingesetzt worden ist. Soweit dabei zunehmend behauptet wird, die Kamera zur Erfassung reizvoller Landschaftsformationen, mithin für persönliche Zwecke zu nutzen, sie dann aber in erster Linie für Fahrten zur Arbeitsstätte, zum Einkaufen, auf Supermarktparkplätzen (während des Parkens!) oder sonst in Innenstadtbereichen (ohne irgendeine Chance auf Landschaftsaufnahmen) betrieben wird, überführen sich die Betreiber regelmäßig selbst der Unwahrheit.

Die oben genannten Voraussetzungen sind jedenfalls bei einer permanenten anlasslosen Aufzeichnung des Verkehrsgeschehens regelmäßig nicht erfüllt, da diese Betriebsform zur Wahrung der Beweissicherungsinteressen nicht erforderlich ist und die schutzwürdigen Interessen betroffener Personen, zumeist unbeteiligter Verkehrsteilnehmer, überwiegen. Letztere können sich insbesondere auf ihr Grundrecht aus Artikel 8 der Charta der Grundrechte der Europäischen Union berufen. Danach hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Dies umfasst das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Dauerhaft aufzeichnende Dashcams erheben permanent und ohne Anlass personenbezogene Daten, wie Kennzeichen der anderen Verkehrsteilnehmer sowie Bewegtbilder von Personen, die sich in der Nähe einer Straße aufhalten, so dass eine Vielzahl von Verkehrsteilnehmern von der Verarbeitung personenbezogener Daten betroffen ist, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können. Das Interesse des Autofahrers als datenschutzrechtlich Verantwortlicher, für den Fall eines Verkehrsunfalls Videoaufnahmen als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Recht auf Schutz der personenbezogenen Daten der anderen Verkehrsteilnehmer nicht rechtfertigen.

2.2.2 Die Meldebehörde als „Datendealer“ – oder zulässige Datenübermittlung von Melderegisterdaten an den Beitragsservice?

Auch in diesem Berichtszeitraum insbesondere nach Inkrafttreten der Datenschutz-Grundverordnung erhielt ich wieder vermehrt Anfragen von Bürgern, die Post vom Beitragsservice des Mitteldeutschen Rundfunks (GEZ) erhalten haben und vermuteten, dass

die Meldebehörden ihrer Gemeinden sich als „Datendealer“ profilieren würden. Ich nehme diese Anfragen zum Anlass, um noch einmal auf die zulässige regelmäßige Übermittlung von Melderegisterdaten durch die Meldebehörden an den Beitragsservice hinzuweisen.

Jede Landesrundfunkanstalt nimmt gemäß § 10 Absatz 7 Rundfunkbeitragsstaatsvertrag (RBStV) in Verbindung mit § 2 der Satzung über das Verfahren zur Leistung der Rundfunkbeiträge die ihr nach diesem Staatsvertrag zugewiesenen Aufgaben und die damit verbundenen Rechte und Pflichten ganz oder teilweise durch die im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebene Stelle der öffentlich-rechtlichen Landesrundfunkanstalten selbst wahr. Diese betriebene gemeinsame Stelle aller Landesrundfunkanstalten ist der ARD ZDF Deutschlandradio Beitragsservice. Er führt namens und im Auftrag der jeweiligen Landesrundfunkanstalt den Einzug der Rundfunkbeiträge durch.

Der Beitragsservice verarbeitet personenbezogene Daten, die er im Rahmen des Rundfunkbeitragseinzugs von der betroffenen Person erhält. Darüber hinaus kann er Daten von öffentlichen und nicht öffentlichen Stellen erhalten: z. B. Meldebehörden, Handelsregister, Gewerberegister, Vollstreckungsorgane, Gerichte, etc.

Das Bundesmeldegesetz (BMG) sieht verschiedene Auskunfts- und Datenübermittlungsbefugnisse aus dem Melderegister durch die Meldebehörden an öffentliche sowie nicht-öffentliche Stellen vor. Hierzu zählen u. a. die einfache Melderegisterauskunft nach § 44 und die erweiterte Melderegisterauskunft nach § 55 BMG.

In Sachsen sind nach § 1 Sächsisches Gesetz zur Ausführung des Bundesmeldegesetzes (SächsAGBMG) die Gemeinden und die Sächsische Anstalt für kommunale Datenverarbeitung (SAKD) Meldebehörden,

Die Rechtsgrundlage für die Weitergabe bzw. Übermittlung von Melderegisterdaten durch Meldebehörden an den Mitteldeutschen Rundfunk (MDR) und den Beitragsservice findet sich in § 6 SächsAGBMG. Danach darf die SAKD als Meldebehörde im Fall der An- oder Abmeldung oder einem Todesfall folgende Daten übermitteln: Familienname, Vorname unter Kennzeichnung des gebräuchlichen Vornamens, Doktorgrad, Familienstand, Tag der Geburt, gegenwärtige und jeweils letzte Anschrift von Haupt- und Nebenwohnungen, ggf. Wohnungsnummer sowie weitere vorhandene Angaben zur Lage der Wohnung, Tag des Wohnungseinzugs und Wohnungsauszugs, Sterbetag.

Die von den Meldebehörden übermittelten Daten dürfen nur für Zwecke der Beitragserhebung sowie zur Feststellung, ob eine Beitragspflicht nach dem Rundfunkbeitragsstaatsvertrag besteht, erhoben, verarbeitet oder genutzt werden. Der MDR und die von

ihm beauftragte Stelle – hier der Beitragsservice – haben durch organisatorische und technische Maßnahmen sicherzustellen, dass die Kenntnisnahme nur durch berechtigte Bedienstete zur Aufgabenerfüllung erfolgt. Die erhobenen Daten sind unverzüglich zu löschen, wenn feststeht, dass sie nicht mehr benötigt werden oder eine Beitragspflicht dem Grunde nach nicht besteht. Nicht überprüfte Daten sind spätestens nach zwölf Monaten zu löschen (§ 6 Absatz 2 SächsAGBMG).

2.2.3 Übermittlung der Daten von Geburtstags- und Ehejubilaren an Seniorenbeauftragte

Wie bereits in meinem letzten Tätigkeitsbericht (vgl. 18. TB unter Kapitel 5.3.1) ausführlich berichtet, sieht das Bundesmeldegesetz vor, dass Mandatsträger Daten von Geburtstags- und Ehejubilaren zu beziehen berechtigt sind. Den Gemeinden ist anzuempfehlen, sich auf die nach § 50 Absatz 2 Bundesmeldegesetz benannten Jubiläen zu beschränken. Für den Empfang der Daten und ihre weitere Verarbeitung im Wege einer Korrespondenz oder direkten Ansprache der betreffenden Einwohner kann gemeinderechtlich eine Befugnis begründet werden, z. B. seitens des Bürgermeisters.

Eine Übermittlung der Daten von Geburtstags- und Ehejubilaren an ehrenamtliche Beauftragte der Gemeinde, wie bspw. Seniorenbeauftragte, sieht das Bundesmeldegesetz jedoch nicht vor. Auch kann eine solche Datenweitergabe nicht auf eine Erforderlichkeit zur Wahrung eines berechtigten Interesses des Verantwortlichen oder eines Dritten nach Artikel 6 Absatz 1 Buchstabe f DSGVO gestützt werden, da diese Rechtsgrundlage nicht für die Verarbeitung durch Behörden gelten soll (siehe Erwägungsgrund 47 zur DSGVO).

Die Weitergabe personenbezogener Daten ist ein intensiver Eingriff in die Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern.

Ich empfehle, gemäß Artikel 6 Absatz 1 Buchstabe a DSGVO die Einwilligung der betroffenen Jubilare zur Datenweitergabe an die Seniorenbeauftrage einzuholen. Hierbei sind die Bedingungen für eine Einwilligung nach Artikel 7 DSGVO zu beachten.

2.2.4 Bekanntgabe der Wohnanschrift von Kandidaten bei Kommunalwahlen

Ein Kandidat für die 2019 anstehende Kommunalwahl fragte mich nach der Vereinbarkeit der öffentlichen Bekanntmachung der Wohnanschrift der Bewerber mit den Regeln der neuen DSGVO: Gerade bei Wahlen gehe es ja auch um politische Einstellungen, woraus sich wiederum ein gewisses Schutzbedürfnis des Privatbereichs eines Kandidaten ergebe.

Die öffentliche Bekanntmachung von Namensangaben und der Wohnanschrift ist materiell-rechtlich in der Kommunalwahlordnung festgelegt (§§ 20, 16 KomWO).

Im Hinblick auf die Datenschutz-Grundverordnung erkenne ich keinen Verstoß gegen datenschutzrechtliche Grundsätze. Die Wahlbewerber begeben sich mit ihrer Kandidatur für ein öffentliches Amt selbst in die Öffentlichkeit, die einen Anspruch darauf hat, zu erfahren, um welche Personen es sich bei der anstehenden Wahl tatsächlich handelt.

Gemäß Artikel 6 Absatz 1e) Datenschutz-Grundverordnung ist eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, eine rechtmäßige personenbezogene Datenverarbeitung.

Aufgrund der in der KomWO festgelegten Veröffentlichungspflicht bedarf es daher für die Veröffentlichung keiner Zustimmung der Bewerber.

2.2.5 Veröffentlichung einer Vorschlagsliste für Schöffen

Ein Hinweisgeber machte mich darauf aufmerksam, dass in der öffentlichen Bekanntgabe einer Gemeinderatssitzung die Liste der 19 Bewerber für die Schöffenwahl mit allen persönlichen Daten im Internet für jedermann frei zugänglich gewesen war. Hierbei wurden der Name, ggf. Geburtsname, Familienstand, Geburtsort, Geburtstag, Beruf, Adresse und Staatsangehörigkeit jedes einzelnen Bewerbers veröffentlicht.

Ich informierte den Hinweisgeber darüber, dass in der Spruchpraxis einiger Datenschutzaufsichtsbehörden in der Vergangenheit zum Teil die Auffassung vertreten wurde, dass die gemäß § 36 Gerichtsverfassungsgesetz verarbeiteten Vorschlagslisten nicht in öffentlicher Ratssitzung beraten und beschlossen werden sollen. Da es möglich sei, dass es auch Ablehnungen und Ausschlüsse von Bewerbern geben kann, etwa wenn Personen bspw. aus gesundheitlichen Gründen nicht zu dem Amt geeignet oder in Vermögensverfall geraten sind.

In dem mir geschilderten Sachverhalt war ein solcher Ausschluss für den interessierten Leser erkennbar, da nur 18 Personen von den ursprünglich 19 Bewerbern als Schöffen bestätigt wurden.

Gegen eine Bekanntmachung der für die Liste gewählten Schöffen ist nach meiner Überzeugung jedoch in jedem Fall nichts einzuwenden. Ich erkenne gemäß dem kommunalverfassungsrechtlichen Öffentlichkeitsgrundsatz der Sächsischen Gemeindeordnung einen Anspruch der Gemeindeöffentlichkeit an, zu erfahren, welcher Einwohner zum Richter berufen werden soll und wie die Entscheidung zustande gekommen ist. Entsprechend verwies ich auf § 36 Absatz 3 Gerichtsverfassungsgesetz. Demnach ist die

Vorschlagsliste in der Gemeinde eine Woche lang zu jedermanns Einsicht auszulegen. Der Zeitpunkt der Auslegung ist vorher öffentlich bekanntzumachen.

Seitens der zuständigen Gemeinde wurde mir gemäß Artikel 33 Datenschutz-Grundverordnung ein datenschutzrechtlicher Verstoß gleichen Inhalts mitgeteilt. Nach Kenntnis des möglichen Verstoßes wurden die Informationen durch die Gemeinde unverzüglich aus dem Ratsinformationssystem genommen.

2.2.6 Zulässigkeit der Datenverarbeitung mittels elektronischer Wasserzähler

Im Berichtszeitraum haben sich zum einen zahlreiche Bürger bei mir darüber beschwert, dass bisherige "analoge" Wasserzähler durch "intelligente" Wasserzähler – auch gegen ihren Willen – ersetzt werden sollen. Auf der anderen Seite haben sich aber auch Stadtwerke und Zweckverbände mit der Bitte um Beratung an mich gewandt.

Elektronische Wasserzählern speichern nach den mir bisher vorliegenden Informationen zumindest den jeweiligen Wasserdurchfluss und -verbrauch in bestimmten Zeitabschnitten und Informationen zum Höchst- und Mindestdurchfluss, mit der Folge, dass bei atypischen Abweichungen das Gerät eine Fehlermeldung generieren kann (beispielsweise "Verdacht auf Rohrbruch").

Diese gespeicherten Daten sind jedenfalls über ein Lesegerät vor Ort am Wasserzähler auslesbar. Ferner senden die "intelligenten" Wasserzähler innerhalb eines festgelegten Zeitraums Signale aus, die von außerhalb des Gebäudes erfasst und ausgewertet werden können.

Die Auslesung von außen findet durch den Wasserversorger zum einem jeweils zum Zwecke der Jahresabrechnung statt, zum anderen, wenn er in konkreten Verdachtsfällen Wasserlecks aufspüren möchte.

Grundsätzlich ist dazu anzumerken, dass die vorgenannten umfangreichen Verarbeitungen der personenbezogenen Daten wegen des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung nicht allein auf §§ 18, 20, 24 AVBWasserV gestützt werden können. Diese müssen vielmehr zumindest mit einer entsprechenden Anpassung der jeweiligen kommunalen Wasserversorgungssatzung eine ausreichende datenschutzrechtliche Verarbeitungsgrundlage erhalten. Der Inhalt kann sich dabei mangels sächsischer gesetzlicher Vorgaben an Artikel 24 Absatz 4 der bayerischen Gemeindeordnung (http://www.gesetze-bayern.de/Content/Document/BayGO-24) orientieren. Vorzusehen sind dementsprechend insbesondere eine ausdrückliche Zweckfestsetzung sowie ein Widerspruchsrecht.

Ich habe gegenüber dem SMI angeregt, ebenfalls entsprechend gesetzgeberisch tätig zu werden und ergänzend und auch kurzfristig einen entsprechenden Mustersatzungsbaustein zur Verfügung zu stellen. Dies wurde leider abgelehnt, da sich derzeit nur schwer einschätzen lasse, „welche konkrete Bedeutung der geschilderte Sachverhalt vor Ort hat“.

Zwischenzeitlich bin ich mit dem SMI wegen einer Lösung im Gespräch.

2.2.7 Öffentliche Veranstaltungen – Fotografieren und Veröffentlichung der Fotos von Teilnehmern

Mit Geltung der Datenschutz-Grundverordnung wurde ich wiederholt von Unternehmen oder Vereinen um Beratung gebeten, was sie aufgrund der neuen Rechtslage beim Fotografieren auf öffentlichen Veranstaltungen und bei der Veröffentlichung dieser Fotos auf ihrer Internetseite zu beachten haben. Insbesondere wurde die Frage aufgeworfen, ob für das Fotografieren und Veröffentlichen der Fotos stets Einwilligungen der abgebildeten Personen gemäß Artikel 7 DSGVO einzuholen sind. Bei öffentlichen Veranstaltungen mit einer großen Teilnehmerzahl würde sich dies naturgemäß schwierig darstellen. Ein besonders interessanter Fall betraf darüber hinaus eine Selbsthilfegruppe, in der sich an einer bestimmten Krankheit erkrankte Personen sowie ihre Angehörigen zusammengeschlossen haben. Hier ging es bei der datenschutzrechtlichen Beurteilung auch um die Frage, ob durch die Art der Aufnahmen und ihre Veröffentlichung, gegebenenfalls auch verbunden mit den Begleittexten, auf gesundheitliche Beeinträchtigungen der Veranstaltungsteilnehmer geschlossen werden kann und daher Gesundheitsdaten verarbeitet werden.

Ich habe zu diesen Fragen folgende Rechtsauffassung vertreten:

Das Anfertigen und Veröffentlichen von Fotografien ist eine Verarbeitung personenbezogener Daten im Sinne der DSGVO. Was personenbezogene Daten sind, ist in Artikel 4 Nummer 1 DSGVO definiert. Hierzu gehören alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Fotos von Veranstaltungen enthalten zu den abgelichteten Personen Informationen, nämlich z. B., dass sie an der Veranstaltung teilgenommen, also zu einer bestimmten Zeit an einem bestimmten Ort waren und ggf. auch welche Aktivitäten sie dort begleitet haben. Die abgelichteten Personen sind auch identifizierbar. Sie können beispielsweise dem Veranstalter oder weiteren Teilnehmern bekannt sein. Werden die Fotos veröffentlicht, dann sind die abgebildeten Personen auch von all den Personen identifizierbar, denen sie ohnehin bekannt sind.

Mit dem Anfertigen der Fotos und der Veröffentlichung im Internet erfolgt überwiegend auch eine Verarbeitung im Sinne der Verordnung, also insbesondere eine automatisierte Verarbeitung. Fotos werden überwiegend digital und damit mittels einer Datenverarbeitungsanlage aufgenommen. Digitalkameras oder Handys nehmen die Fotos dabei nicht nur auf, sondern speichern sie digital. Damit ist ein Verarbeitungsvorgang verbunden. Gleiches gilt, wenn die Fotos über die entsprechenden Verarbeitungen mittels Computer/Tablet oder Ähnlichem im Internet veröffentlicht werden.

Sowohl das Aufnehmen von Fotos als auch deren Veröffentlichung bedürfen einer rechtlichen Grundlage. Ausgangspunkt sind hierfür zum einen die in Artikel 6 Absatz 1 DSGVO aufgezählten Tatbestände, nach denen eine Verarbeitung der personenbezogenen Daten zulässig ist. Zum anderen ist bei einer möglichen Verarbeitung von Gesundheitsdaten Artikel 9 Absatz 1 und 2 DSGVO zu beachten.

1. Das Aufnehmen von Fotos

Werden auf öffentlichen Veranstaltungen durch das Unternehmen oder den Verein bzw. einer entsprechend beauftragten Person Fotos aufgenommen, kommt hierfür als Rechtsgrundlage Artikel 6 Absatz 1 Buchstabe f DSGVO in Betracht. Danach ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn dies zur Wahrung der berechtigten Interessen eines Verantwortlichen erforderlich ist und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Unternehmen oder Vereine haben als Veranstalter öffentlicher Veranstaltungen grundsätzlich ein berechtigtes Interesse daran, die Veranstaltung und die dortigen Aktivitäten auch mittels Fotos zu dokumentieren. Hierfür sind aber nur solche Aufnahmen im Sinne des Artikels 6 Absatz 1 Buchstabe f DSGVO erforderlich, die auch einen Veranstaltungsbezug aufweisen. Daher sind von dieser Vorschrift insbesondere solche Aufnahmen gedeckt, die die Veranstaltung und nicht einzelne Teilnehmer in den Vordergrund stellen.

Dieses berechtigte Interesse und die Erforderlichkeit der Fotos zur Erfüllung dieses Interesses reichen aber noch nicht aus, um die Zulässigkeit der Aufnahmen zu begründen. Vielmehr ist weiterhin eine Interessenabwägung durchzuführen. Dabei sind die Interessen des Veranstalters an der Dokumentation der Veranstaltung gegenüber den Interessen der abzulichtenden Personen am Schutz ihrer personenbezogenen Daten abzuwägen. Die vernünftigen Erwartungen der betroffenen Personen und die Situation, in der die Fotos aufgenommen werden, sind mit einzubeziehen (vgl. Erwägungsgrund 47 der DSGVO). Bei öffentlichen Veranstaltungen wird es regelmäßig der Erwartungshaltung der Teilnehmer entsprechen, dass die Veranstaltung auch fotografisch dokumentiert

wird. Wird dies aus der Veranstaltungssituation heraus deutlich, z. B. bereits in der Bezeichnung als öffentliche Veranstaltung in Einladungen und Flyern, in der Ankündigung, dass fotografiert wird, oder durch offenes Fotografieren, dürften die Interessen des Verantwortlichen an den Aufnahmen im Regelfall überwiegen. Dies kann allerdings dann nicht mehr angenommen werden, wenn die aufzunehmenden Personen das Fotografieren offensichtlich ablehnen, Fotos verdeckt oder heimlich aufgenommen werden, Fotos die aufgenommenen Personen diskreditieren können oder aber die Intimsphäre der fotografierten Personen betroffen ist. In solchen Fällen überwiegt das Interesse der betroffenen Personen am Schutz ihrer personenbezogenen Daten. Auch bei Aufnahmen von Kindern ist die Interessenabwägung wegen ihrer überwiegenden Schutzbedürftigkeit besonders sorgfältig durchzuführen (vgl. Artikel 6 Absatz 1 Buchstabe f DSGVO am Ende).

Ergibt die Prüfung, dass die Fotos auf der Grundlage des Artikels 6 Absatz 1 Buchstabe f DSGVO zulässigerweise aufgenommen werden können, ist das Einholen von Einwilligungserklärungen entbehrlich. Ist dies nicht der Fall, können die Aufnahmen nur erfolgen, wenn die abgelichteten Personen in die Aufnahme eingewilligt haben. Zur Einwilligung gehört dabei auch, die betroffene Person vorab darüber zu informieren, was mit den Fotos geschehen soll. Veranstalter sollten sich daher bereits im Vorfeld Klarheit über die angestrebten Motive verschaffen und die fotografierenden Personen entsprechend instruieren.

2. Die Veröffentlichung von Fotos im Internet

Für die Veröffentlichung von Fotos auf der Internetseite des Veranstalters kommt als Rechtsgrundlage § 23 des „Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie“ (KunstUrhG) in Betracht. Eine Veröffentlichung der Fotos ohne eine Einwilligung ist danach insbesondere dann zulässig, wenn die Personen auf den Bildern nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen. Auch nach § 23 Absatz 2 KunstUrhG müssen jedoch die Interessen der auf den veröffentlichten Fotos abgelichteten Personen Berücksichtigung finden.

Allerdings ist § 23 KunstUrhG nach Inkrafttreten der DSGVO nur ergänzend zu und im Einklang mit der Verordnung anzuwenden. Daher sind auch die oben bereits angegebenen Grundlagen des Artikels 6 Absatz 1 Buchstabe f DSGVO bei der Beurteilung, ob eine Veröffentlichung der Fotos im Internet zulässig ist, zu berücksichtigen.

Auf Seiten des Veranstalters wird ein berechtigtes Interesse anzuerkennen sein, auch mithilfe von Fotos öffentlich über eine Veranstaltung zu berichten oder auf geplante ähnliche Veranstaltungen aufmerksam zu machen. Das Internet ist dafür ein entsprechend genutztes Medium. Voraussetzung ist aber auch insoweit, dass auf den veröffent-

lichten Fotos ein Bezug zu den Veranstaltungen klar zu erkennen ist. Dies ist beispielsweise dann nicht mehr der Fall, wenn eine Person im Mittelpunkt steht oder gezielt nur ein einzelner Teilnehmer auf den Fotos zu sehen ist.

Darüber hinaus ist auch hinsichtlich der Veröffentlichung der Fotos eine Interessenabwägung durchzuführen. Die vernünftigen Erwartungen der betroffenen Personen und die Situation, in der die Fotos aufgenommen werden, sind auch insoweit einzubeziehen. Auch wenn es bei öffentlichen Veranstaltungen oftmals der Erwartungshaltung der Teilnehmer entsprechen wird, dass über die Veranstaltung öffentlich berichtet wird, sollten die Veranstalter besonderes Augenmerk darauf legen, die Veranstaltungsteilnehmer auf eine geplante Veröffentlichung im Internet hinzuweisen. Dies kann beispielsweise über entsprechende Hinweise in Flyern oder auf Hinweistafeln vor Ort erfolgen. Auch bei der Veröffentlichung von Fotos gilt, dass die Interessen der abgelichteten Personen zu berücksichtigen sind. Von deren entgegenstehenden Interesse ist daher dann auszugehen, wenn die aufgenommenen Personen eine Veröffentlichung ausdrücklich ablehnen oder die Fotos die aufgenommene Person diskreditieren können oder deren Intimsphäre betroffen ist. Vor allem bei jungen Kindern kann im Übrigen nicht davon ausgegangen werden, dass sie mit einer Veröffentlichung ihrer Fotos im Internet rechnen und sich der Tragweite der damit verbundenen Verarbeitung bewusst sind. Sind die Kinder auf den Fotos klar erkennbar, sollten die Erziehungsberechtigten vor der Veröffentlichung der Fotos einbezogen und um Einwilligung gebeten werden. Denn auch für die Veröffentlichung von Fotos im Internet gilt: Wenn § 23 KunstUrhG bzw. Artikel 6 Absatz 1 Buchstabe f DSGVO nicht greifen, ist eine Veröffentlichung der Fotos nur mit Einwilligung der abgelichteten Personen zulässig.

3. Gesundheitsdaten

In dem oben geschilderten Fall war darüber hinaus die Frage zu klären, ob mit den Aufnahmen und der Veröffentlichung der Fotos mit entsprechenden Begleittexten im Internet Gesundheitsdaten verarbeitet werden. Gesundheitsdaten sind nach Artikel 9 Absatz 1 DSGVO besonders geschützte Daten, für deren zulässige Verarbeitung strengere Voraussetzungen gelten. Die Verarbeitung ist nur zulässig, wenn eine der in Artikel 9 Absatz 2 DSGVO genannten Ausnahmen greift. Für die hier vorliegenden Fälle des Anfertigens und Veröffentlichens von Fotos käme nur das Einholen einer Einwilligung nach Artikel 9 Absatz 2 Buchstabe a DSGVO in Betracht.

Kann aber das Fotografieren von Personen mit gesundheitlichen Einschränkungen oder das Veröffentlichen dieser Fotos mit einem Begleittext, der auf die Gesundheitsbeeinträchtigung hinweist, ein Verarbeiten von Gesundheitsdaten im Sinne des Artikels 9 DSGVO darstellen? Meiner Ansicht nach ja, wobei die Grenzziehung nicht immer einfach ist.

Was Gesundheitsdaten sind, ist in Artikel 4 Nummer 15 DSGVO definiert. Hierzu gehören alle personenbezogenen Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen, einschließlich der Erbringung von Gesundheitsleistungen, und aus denen Informationen über den früheren, gegenwärtigen oder zukünftigen Gesundheitszustand einer Person hervorgehen. Beließe man es allein bei den Merkmalen dieser Definition, dann wäre bei jedem Foto mit Personen, bei denen aufgrund des gewählten Motivs eindeutig eine gesundheitliche Einschränkung erkennbar ist, von einer Verarbeitung von Gesundheitsdaten auszugehen und immer eine Einwilligung für die Aufnahme und deren Veröffentlichung einzuholen. Die könnte z. B. bereits die Aufnahme von Fotos mit Brillenträgern betreffen. Wendet man die Definition des Artikels 4 Nummer 15 DSGVO in dieser strengen Form an, kommt man meines Erachtens nicht zu sinnvollen und von der DSGVO gewollten Ergebnissen. Daher gehe ich, wie auch ein Teil der Kommentarliteratur zur DSGVO, davon aus, dass bei der Frage, ob Gesundheitsdaten verarbeitet werden, auch auf den Verwendungszusammenhang abzustellen ist. Relevant ist, ob direkt oder indirekt die Angabe Informationen über den Gesundheitszustand der betroffenen Person vermittelt (vgl. z. B. Kühling/Buchner, DSGVO, BDSG, Kommentar, 2. Auflage, Artikel 4 Nummer 15 DSGVO, Rdnr. 7). Mit einem Foto, das eine Vielzahl von Personen und darunter z. B. auch Brillenträger auf einer öffentlichen Veranstaltung zeigt, vermittelt keine Gesundheitsinformationen über diese Personen sondern dokumentiert die Veranstaltung. Wird dagegen ein Foto mit einem Begleittext veröffentlicht, der auf ein bestimmtes Handicap der aufgenommenen Personen hinweist und dient das Foto z. B. dazu, mögliche Therapien aufzuzeigen, kann eine Verarbeitung von Gesundheitsdaten vorliegen. In Zweifelsfällen sollte, da die Gesundheitsdaten zu den sehr sensiblen Daten gehören, eine Einwilligung der betroffenen Personen sowohl in die Aufnahmen als auch in deren Veröffentlichung eingeholt werden.

(Zu Sportveranstaltungen vergleiche auch den Beitrag 2.3.2, zu Schulveranstaltungen 2.3.3, jeweils unten.)

2.2.8 Datenübermittlung aufgrund von Auskunftsersuchen der Polizei oder Staatsanwaltschaft

Zur Befugnis und Pflicht, personenbezogene Daten aufgrund von Auskunftsverlangen der Polizei oder Staatsanwaltschaft in Ermittlungsverfahren preiszugeben, vergleiche den auf die Vorschriften Artikel 6 Absatz 1 Buchstabe c DSGVO, §§ 163, 163 StPO, § 24 BDSG bezugnehmenden Tätigkeitsberichtsbeitrag unter 8.3.

2.2.9 Vermerk von Namen und Adressen von Kunden auf Kassenbelegen

Im zurückliegenden Berichtszeitraum erreichte mich die Beschwerde von Kunden, die mitteilten, dass sie bei der Nachschau des ihnen ausgehändigten Kassenbons eines Händlers Namen und Anschrift einer fremden Person festgestellt hätten. Seitens der Hinweisgeber bestand die Besorgnis, dass auch ihre personenbezogenen Daten in ähnlicher Weise verarbeitet worden sein könnten.

Meine Dienststelle forderte das Unternehmen zur Stellungnahme auf. Nicht verständlich war mir auch der Umstand, warum überhaupt Namen und Anschriften von Kunden auf den Kassenbons aufgedruckt worden waren. Neben der Missbrauchsgefahr durch weggeworfene Kundenbelege erschien meiner Behörde auch die Erforderlichkeit der Verarbeitung zu Vertragszwecken in Frage zu stehen, Artikel 6 Absatz1 Buchstabe b) DSGVO.

In seiner Stellungnahme führte das Unternehmen aus, dass es ein umsatzbezogenes Stammkundenprogramm führe. Um Besuche und Einkaufswert belegen zu können, würde für jeden Stammkunden in der Kasse ein Kundenkonto angelegt, um die Umsätze zu erfassen. Das Unternehmen teilte mit, dass eine entsprechende Erlaubnis der betroffenen Kunden dazu vorgelegen hatte. Die den Hinweis gebenden Kunden wiederum hätten nicht an diesem Stammkundenprogramm teilgenommen und es seien auch keine Daten zu ihnen gespeichert gewesen. Wegen eines Stammkunden habe eine Kassiererin an dem Tag, an dem die Hinweisgeber eingekauft hätten, geprüft, weshalb Informationssendungen nicht hätten zugestellt worden können. Daher sei in diesem Zeitraum durch die Bearbeiterin an der Kasse das Kundenkonto der Stammkunden im Kassensystem aufgerufen worden. Bei dem entsprechenden Kassiervorgang der Hinweisgeber sei der Einkauf auf das Kundenkonto der Stammkundin gebucht und der Kassenbon entsprechend bedruckt worden. Es habe sich um einen Fehler gehandelt. Maßnahmen zur zukünftigen Fehlervermeidung wurden zudem dargestellt.

Den Bedenken meiner Dienststelle zur Praxis des Aufdrucks der Daten auf dem Kassenbon vermochte das Unternehmen nicht zu folgen. Zudem, so die Stellungnahme sei eine Entkoppelung des Kundenkontos von dem Ausdruck technisch nicht umsetzbar. Allerdings sagte der Verantwortliche zu, die Datenschutzinformationen mit einem entsprechenden Warnhinweis zu versehen.

2.3 Einwilligungsfragen

2.3.1 Fortgeltung bestehender Einwilligungen

Ich erhielt zahlreiche Anfragen, wie mit Einwilligungen, die vor Anwendbarkeit der DSGVO nach damaligen Recht wirksam erteilt wurden, umzugehen sei.

Die Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat in ihrem Kurzpapier Nummer 20 zur Einwilligung (vergleiche auch 7.2.11), das in meinem Internetangebot abgerufen werden kann, auch Ausführungen zur Fortgeltung von Einwilligungen gemacht:

Vor Anwendbarkeit der DSGVO erteilte Einwilligungen wirken nach Erwägungsgrund 171 der DSGVO fort, sofern sie der Art nach den Bedingungen der DSGVO entsprechen. Hierzu zählen insbesondere folgende Punkte:

- Die Erteilung einer wirksamen Einwilligung muss gemäß Artikel 7 Absatz 1 DSGVO nachgewiesen werden können, was eine entsprechende Dokumentation voraussetzt.
- Die Einwilligung muss freiwillig abgegeben worden sein (Artikel 4 Nummer 11 DSGVO), wobei die besonderen Anforderungen nach Artikel 7 Absatz 4 DSGVO i. V. m. Erwägungsgrund 43 DSGVO zu beachten sind.
- Erforderlich ist eine Willensbekundung für den bestimmten Fall, in informierter Weise und in unmissverständlicher Form (Artikel 4 Nummer 11 DSGVO), wobei die Anforderungen nach Artikel 7 Absatz 2 DSGVO i. V. m. ErwGr. 32 und 42 DSGVO zu beachten sind.
- Der Verantwortliche muss Mechanismen bereithalten, die den Widerruf der Einwilligung ermöglichen und Informationen bereithalten, wie die Einwilligung widerrufen werden kann.
- Im Falle der Einwilligung durch ein Kind in Bezug auf Dienste der Informationsgesellschaft müssen die Voraussetzungen nach Artikel 8 DSGVO vorliegen.

Die betroffene Person muss darüber hinaus zum Zeitpunkt der Abgabe der Einwilligungserklärung die Informationen zur Verfügung gehabt haben, die zur Abgabe einer informierten Einwilligung notwendig sind. Nach ErwGr. 43 sind dies mindestens Informationen darüber, wer der Verantwortliche ist und für welche Zwecke die personenbezogenen Daten verarbeitet werden.

Diese Informationen sind zum Teil identisch mit den nach Artikel 13 DSGVO vorgesehenen Informationspflichten. Die darüber hinausgehenden Informationspflichten müssen für die Fortgeltung bisher erteilter Einwilligungen hingegen grundsätzlich nicht erfüllt worden sein. Unabhängig von den genannten Bedingungen für erteilte Einwilligungen müssen künftig die Informationspflichten nach Artikel 13 DSGVO beachtet werden.

2.3.2 Datenschutz bei Sportwettkämpfen

Aus Beschwerden von Vereinsmitgliedern einerseits sowie Anfragen von Vereins- bzw. Verbandsvorständen andererseits ist mir bekannt, dass im Zusammenhang mit der Durchführung von Sportwettkämpfen Unsicherheiten bei der Umsetzung der DSGVO bestehen. Praktisch äußert sich dies u. a. darin, dass die meldenden Vereine von Wettkampfteilnehmern eine Reihe von Einwilligungen abverlangen, die ihren Ursprung – meines Wissens – in den jeweiligen Wettkampfausschreibungen haben. Diese Ausschreibungen enthalten häufig Formulierungen wie folgt:

1. Mit der Abgabe der Meldungen erklärt der Verein sein Einverständnis zur Speicherung der vereins- und personenbezogenen Daten der gemeldeten Aktiven und erteilt seine Zustimmung zur Veröffentlichung der Wettkampfdaten (Name, Geburtsjahrgang, Verein, Ergebnisse) in Meldeergebnissen, Protokollen und Bestenlisten.
2. Ebenso erklärt der Verein sein Einverständnis zur unentgeltlichen Nutzung der Daten für Medienberichte und Sponsorenmaßnahmen.
3. Weiterhin erklärt der Verein im Namen der gemeldeten Aktiven bzw. deren gesetzlichen Vertreter die Einwilligung zur Nutzung von Film- oder Fotoaufnahmen, die im Rahmen der Veranstaltung erfolgen und veröffentlicht werden.

Davon ausgehend wollen sich die meldenden Vereine natürlich absichern und fordern ihrerseits von ihren Mitgliedern inhaltsgleiche Einverständniserklärungen ab. Dies wiederum führt dazu, dass einige Vereinsmitglieder bzw. in erster Linie Eltern minderjähriger Vereinsmitglieder ihre Zustimmung verweigern und sich dann darüber beklagen, nunmehr vom Wettkampfbetrieb ausgeschlossen zu werden. Die Ausrichter der Wettkämpfe bzw. die meldenden Vereine sehen sich in solchen Fällen vor die Wahl gestellt, entweder gegen die jeweiligen Wettkampfbestimmungen oder gegen die DSGVO zu verstoßen.

Nach meiner Einschätzung sind in erster Linie Ausschreibungstexte wie oben wiedergegeben für die geschilderten Konflikte ursächlich. Die dort als Voraussetzung vorgegebenen Einverständnisse sind entweder unnötig oder zu unkonkret und vermischen Vereins- und Mitgliedsangelegenheiten. Teilweise werden auch die Verantwortungsbereiche Dritter (z. B. Medien) adressiert.

Soweit ich die Rechts- bzw. Satzungslage im Vereinssport überblicken kann, stellt sich mir diese wie folgt dar:

Sportwettkämpfe werden grundsätzlich auf der Grundlage sportartbezogener Wettkampfbestimmungen durchgeführt. Für die Wettkampfteilnahme ist regelmäßig eine

vorherige Registrierung des jeweiligen Sportlers im Lizenzregister des Sportverbandes notwendig. Die betreffenden Formulare enthalten zumeist bereits eine Erklärung des Sportlers zur (Internet-) Veröffentlichung seiner Wettkampfdaten. Mit der Antragstellung bzw. der auf dieser Grundlage erteilten Lizenz ist der Sportler startberechtigt. Die Wettkampfteilnahme vollzieht sich dann gemäß der jeweiligen Wettkampfbestimmungen; die darin beschriebenen bzw. dafür erforderlichen Datenverarbeitungen sind durch Artikel 6 Absatz 1 Buchstabe b DSGVO legitimiert. Einer nochmaligen Zustimmung des Sportlers zur Veröffentlichung seiner Wettkampfdaten wie in Nummer 1 des eingangs wiedergegebenen Ausschreibungstextes bedarf es daher nicht. Damit ist an dieser Stelle auch keine Verweigerung der Zustimmung zur Veröffentlichung der Wettkampfdaten möglich. Wer mit der Veröffentlichung seiner Wettkampfdaten nicht einverstanden ist, dürfte bereits keine Lizenz und somit keine Startberechtigung besitzen; folglich stellt sich die Frage der Verweigerung der Wettkampfteilnahme wegen fehlender Zustimmung gar nicht. Satz 1 des Ausschreibungstextes ist also entbehrlich und führt nur zu Missverständnissen wie dargestellt. Ich weise an dieser Stelle darauf hin, dass der Verein ohnehin kein Einverständnis zur Verarbeitung von Daten seiner Mitglieder erteilen kann – dieses müssten die Sportler schon selbst erklären.

Die Nummer 2 des Ausschreibungstextes ist in jedem Fall zu unkonkret. Es ist weder klar, gegenüber wem eine Einwilligung erteilt werden soll, noch welche Daten diese umfasst und welche genauen Zwecke (Sponsorenmaßnahmen?) verfolgt werden. Die Medien sind für ihre Berichterstattung grundsätzlich selbst verantwortlich; der Veranstalter kann lediglich darauf hinweisen, dass (bei öffentlichen Wettkämpfen) auch Medien anwesend sein werden bzw. zugelassen sind. Im Hinblick auf die Datenweitergabe an Sponsoren stellt sich wieder das Problem, dass die Sportler selbst einwilligen müssten, nicht etwa der Verein. Eine solche Einwilligung kann aber keinesfalls eine Bedingung für die Wettkampfteilnahme sein kann, da sie die Wettkampfbestimmungen unberührt lässt. Tatsächlich wird dies auf Vereinsebene den Mitgliedern aber dann oftmals fälschlicherweise so kommuniziert.

Zu Nummer 3: Die Veröffentlichung von Film- und Fotoaufnahmen einer Sportveranstaltung richtet sich nach dem KunstUrhG. Soweit von den Wettkämpfen als solchen (Überblicks-) Aufnahmen gefertigt werden sollen, können diese gemäß § 23 Absatz 1 Nummer 3 KunstUrhG ohne Einwilligung veröffentlicht werden. Anders in Fällen, in denen Abbildungen einzelner Personen veröffentlicht werden sollen: Hier ist eine Einwilligung der betroffenen Personen bzw. der Erziehungsberechtigten notwendig (§ 22 Satz 1 KunstUrhG), so etwa bei Mannschafts- oder Porträtaufnahmen, wobei klar zu bezeichnen ist, gegenüber wem diese Einwilligung erteilt wird und welcher Art die Veröffentlichung sein soll. Auch hier gilt, dass diesbezügliche Einwilligungen keine Bedingung für eine Wettkampfteilnahme sein können bzw. dürfen. Dies widerspräche

dem Kopplungsverbot des Artikel 7 Absatz 4 DSGVO. Eine pauschale Einwilligung des Vereins bzw. eine diesbezügliche Zusicherung kann es daher nicht geben.

2.3.3 Veröffentlichung personenbezogener Schülerdaten – Bildaufnahmen

Das SMK hat im Zusammenhang mit der unmittelbaren Anwendbarkeit der DSGVO die VwV Schuldatenschutz umfassend überarbeitet. Danach ist u. a. für die Veröffentlichung von personenbezogenen Daten, Fotos, Videos oder Filmen auf Grund einer Einwilligung (sofern eine solche erforderlich ist, siehe dazu Fotografien bei Schulaufnahmeveranstaltungen) ein in Anlage 2 der VwV enthaltenes Muster zu verwenden. In diesem ist durch die Schule anzugeben, welche Daten wo veröffentlicht werden sollen. Dieses Formular ist gemäß Nummer 5 VwV Schuldatenschutz zu unterschreiben, wobei nicht gewünschte Datenverarbeitungen gestrichen werden können.

An mich wurde dazu die Frage herangetragen, ob hierfür bei getrennt lebenden Eltern die Unterschrift des Elternteils, bei dem sich das Kind mit Einwilligung des anderen Elternteils oder auf Grund einer gerichtlichen Entscheidung gewöhnlich aufhält, ausreicht. Dies ist nach meiner Auffassung der Fall, da in diesem Fall gemäß § 1687 BGB die Befugnis zur alleinigen Entscheidung in Angelegenheiten des täglichen Lebens besteht. Dies gilt jedoch nach der Auffassung des OLG Oldenburg (Beschluss vom 24.05.2018, Az: 13 W 10/18) nicht für kommerziellen Zwecken dienende Internetseiten.

Aufgrund einer häufig zu vernehmenden Fehleinschätzung sehe ich mich weiterhin zu einem klarstellenden Hinweis veranlasst: Fotoaufnahmen von Schülern sind zwar geeignet, personenbezogene Daten im Sinne der Datenschutz-Grundverordnung darzustellen. Der Anwendungsbereich der DSGVO ist allerdings gerade in dem häufigen Fall nicht eröffnet, dass natürliche Personen, zumeist Anverwandte der Schüler, Fotografien allein zu persönlichen oder familiären Zwecken anfertigen. Die Verarbeitung personenbezogener Daten in Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten wird als Vorgang nämlich gemäß Artikel 2 Absatz 2c) DSGVO gerade nicht von der Verordnung erfasst.

Der Anwendungsbereich der DSGVO ist hingegen dann eröffnet, wenn die Schule selbst oder gewerbliche Fotografen (auf Einwilligungsgrundlage) Abbildungen der Schüler erstellen und verwenden. In diesen Fällen sind seitens der Verantwortlichen regelmäßig auch die Informationspflichten nach der DSGVO gegenüber den betroffenen Schülern bzw. den sorgeberechtigten Personen einzuhalten.

Für die Zulässigkeit der Verbreitung und Veröffentlichung personenbezogener Abbildungen gelten weiterhin unverändert die bundesgesetzlichen Vorschriften des Kunsturheberrechtsgesetzes.

Zur Zulässigkeit der Verarbeitung von Bildaufnahmen und Einwilligungsfragen vergleiche auch den Beitrag 2.2.7.

2.3.4 Nicht erforderliche Einwilligungen bei vertraglichen oder vertragsähnlichen Verhältnissen

Im Berichtszeitraum erhielt ich immer wieder Anfragen zur Notwendigkeit einer Einwilligung zur personenbezogenen Verarbeitung der Daten von Auftraggebern, Vertragspartnern und Mitgliedern. Unter anderem ging die Anfrage ein, ob für die Verwaltung der Daten der Mitglieder einer als Verein organisierten Garagengemeinschaft eine Einwilligung erforderlich sei. Ich verwies hierzu auf die maßgebliche Rechtsgrundlage, nämlich Artikel 6 Absatz 1 Buchstabe b) DSGVO. Eine Einwilligung oder Genehmigung der Mitglieder der Garagengemeinschaft zur Verwaltung deren Daten war hingegen nicht einzuholen gewesen. In einem anderen Fall erhielt ich den Hinweis, dass Notariate zum Teil Einwilligungserklärungen zur Speicherung personenbezogener Daten im Rahmen von so genannten „allgemeinen Mandatsbedingungen“ oder separat abverlangen. Auch an dieser zum Teil eingeführten Praxis habe ich Zweifel. Es handelt sich jedenfalls zunächst überhaupt nicht um eine Einwilligungssituation, wenn sich Vertragsparteien oder natürliche Personen zu einem Notar begeben, um z. B. eine Beurkundung zu beauftragen. Aufgrund der besonderen Fragestellung machte ich zudem deutlich, dass es sich bei der Tätigkeit des Notars und dessen Status nach meiner Überzeugung auch nicht um eine Auftragsverarbeitung handeln könne (vergleiche auch das Kurzpapier Nummer 13 der unabhängigen Datenschutzbehörden des Bundes und der Länder samt Anlage, abrufbar auf der Internetpräsenz des Sächsischen Datenschutzbeauftragten. Zu den herausgegebenen Kurzpapieren der Datenschutzkonferenz siehe auch den Berichtsbeitrag 7.2.11.)

Ein Problem bei erfolgten, aber nicht erforderlichen Einwilligungen erkenne ich im Rechtsverkehr auch darin, dass mit der Einwilligung als Grundlage, die weitergehende Datenverarbeitung der Einwendung bzw. des Vorbehalts eines Widerrufs ausgesetzt sein könnten, was aber in den Rechtsfolgen seitens der Vertragsparteien, Vereinigungen und sonstigen Stellen gar nicht gewünscht sein kann.

2.4 Sensible Daten, besondere Kategorien personenbezogener Daten

2.4.1 Heilpraktiker – Einwilligungserfordernis bei Behandlung

Den Aufsichtsbehörden stellte sich die grundsätzliche Frage der Rechtsgrundlage der Verarbeitung von Gesundheitsdaten i. S. d. Artikel 9 Absatz 1 DSGVO durch Heilpraktiker, da diesen hierzu verschiedene Anfragen z. B. vom Verband der Osteopathen Deutschland e. V. vorlagen.

Im Gesundheitsbereich wird in der Regel die Datenverarbeitung auf Artikel 9 Absatz 2 Buchstabe h DSGVO i. V. m. Artikel 6 Absatz 1 Buchstabe b DSGVO gestützt. Danach ist die Verarbeitung von Gesundheitsdaten i. S. d. Artikel 9 Absatz 1 DSGVO zulässig, wenn sie auf Grund eines Vertrages mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Artikel 9 Absatz 3 genannten Bedingungen und Garantien erforderlich ist.

Nach Artikel 9 Absatz 3 DSGVO dürfen die Gesundheitsdaten zu den in Absatz 2 Buchstabe h DSGVO genannten Zwecken vom Fachpersonal oder unter deren Verantwortung verarbeitet werden, wenn dieses nach dem Unionsrecht oder dem Recht eines Mitgliedstaates oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt. § 22 Absatz 1 Buchstabe b BDSG fordert, dass die Gesundheitsdaten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden.

Die Aufsichtsbehörden der Länder haben sich über diese Fragen ausgetauscht. Der von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder eingerichtete Arbeitskreis Gesundheit und Soziales hat sich bei seiner Beratung am 18. Oktober 2018 mit der Frage der Anwendbarkeit des Artikels 9 Absatz 2 Buchstabe h DSGVO auf Heilpraktiker befasst. Der Arbeitskreis Gesundheit und Soziales vertritt bei einer Enthaltung die Auffassung, dass Artikel 9 Absatz 2 Buchstabe h DSGVO keine Anwendung auf Heilpraktiker finden kann, da die Voraussetzungen des Artikels 9 Absatz 3 DSGVO nicht erfüllt sind. Insbesondere werden vertraglich vereinbarte Geheimhaltungspflichten nicht als ausreichend im Sinne des Artikels 9 Absatz 3 DSGVO und § 22 BDSG bzw. § 203 StGB als für Heilpraktiker nicht einschlägig erachtet. Insoweit müsste der Gesetzgeber klarstellend tätig werden. Die Verarbeitung von Gesundheitsdaten durch Heilpraktiker wäre damit derzeit nur auf der Grundlage einer Einwilligung möglich (Artikel 9 Absatz 2 Buchstabe a DSGVO). Der Verband der Osteopathen Deutschland e. V. wurde mit Schreiben des Hessischen Beauftragten für Datenschutz und Informationsfreiheit vom 9. November 2018 über die abgestimmte Auffassung der Aufsichtsbehörden informiert.

3 Betroffenenrechte

3.1 Spezifische Pflichten des Verantwortlichen (inklusive Informationspflichten)

3.1.1 Ablehnung der Behandlung durch Ärzte bei Weigerung des Patienten, die Kenntnisnahme der Informationen nach Artikel 13 DSGVO durch Unterschrift zu bestätigen

Seit dem Inkrafttreten der DSGVO erhielt ich zahlreiche Beschwerden von Patientinnen und Patienten, denen bei einem Besuch einer Arztpraxis eine Information nach Artikel 13 DSGVO zur Unterschrift vorgelegt wurde. Bei Verweigerung der Unterschrift, wurde der Patientin oder dem Patienten zumeist erklärt, man werde sie ohne die Unterschrift nicht behandeln.

Die Sonderkonferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat anlässlich der Tagung am 5. September 2018 zu dieser Problematik folgenden Beschluss gefasst:

„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 Artikel 13 DSGVO nicht mit ihrer oder seiner Unterschrift versieht. Eine solche Praxis ist mit der DSGVO nicht vereinbar.

Die Informationspflicht nach Artikel 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.“

Im Anschluss an den Beschluss habe ich die Sächsische Landesärztekammer, die Kassenärztliche Vereinigung Sachsen und die Landeszahnärztekammer Sachsen mit Schreiben vom 6. September 2018 hierüber informiert. Es wurde erläutert, dass eine Pflicht zur aktiven Kenntnisnahme, also eine Annahmepflicht des Betroffenen Artikel 13 DSGVO nicht zu entnehmen ist. Allerdings belegt die DSGVO die Nichterfüllung der Informationspflicht mit einem Bußgeld. Zumindest gegenüber der Aufsichtsbehörde muss die Ärztin bzw. der Arzt in der Lage sein, nachzuweisen, dass der Patientin bzw.

der Patient die Möglichkeit hatte, die Information zur Kenntnis zu nehmen. Das Aushändigen der Information kann praxisintern vermerkt werden. Ausreichend ist es aber auch, wenn ein konkreter Verfahrensablauf betreffend die Umsetzung der Informationspflicht festgehalten und dokumentiert wird, aus dem hervorgeht, in welcher Weise die Patientin bzw. der Patient die Information im Regelfall erhält (z. B. Übergabe mit Anamnesebogen am Empfang oder Ähnliches). Diese Dokumentation ist der Aufsichtsbehörde auf Verlangen vorzuzeigen. Im Ärzteblatt Sachsen (11/2018, S. 510/511) wurde meine Information veröffentlicht.

3.1.2 Abmahnungen wegen Verstoßes gegen Informationspflichten

Im unmittelbaren zeitlichen Zusammenhang mit dem Beginn der Anwendbarkeit der DSGVO hatten einige Unternehmer Abmahnungen wegen (angeblicher) datenschutzrechtlicher Verstöße, beispielsweise einer fehlenden oder nicht „an geeigneter Stelle“ einer Website befindlichen Datenschutzerklärung, erhalten. Natürlich waren diese Abmahnungen mit entsprechenden Kostennoten versehen; außerdem sollte eine strafbewehrte Unterlassungserklärung (kein Weiterbetrieb der Website ohne korrekt platzierte Datenschutzhinweise, andernfalls Vertragsstrafe) abgegeben werden. Die weithin befürchtete Abmahnwelle indes ist bislang ausgeblieben.

Derartige Abmahnungen leiten ihre Berechtigung aus dem UWG ab. Bislang ist unklar, ob Unternehmer ihre Konkurrenten wegen Verstößen gegen die DSGVO aus wettbewerbsrechtlichen Gründen abmahnen oder verklagen dürfen. In Deutschland gab es hierzu auch vor der Anwendbarkeit der DSGVO keine einheitliche Rechtsprechung. Dies setzt sich nun auch in Bezug auf die DSGVO entsprechend fort:

Das LG Bochum hat mit Urteil vom 07.08.18 (I-12 O 85/18, juris) entschieden, dass eine grundsätzliche wettbewerbsrechtliche Abmahnbarkeit von Verstößen gegen die DSGVO nicht besteht, weil in den Artikeln 77 bis 84 DSGVO eine die Ansprüche von Mitbewerbern ausschließende, abschließende Regelung getroffen worden sei. Dafür spreche insbesondere, dass die DSGVO eine detaillierte Regelung des anspruchsberechtigten Personenkreises enthält. Danach steht nicht jedem Verband ein Recht zur Wahrnehmung der Rechte einer betroffenen Person zu, sondern nur bestimmten Einrichtungen, Organisationen und Vereinigungen ohne Gewinnerzielungsabsicht unter weiteren Voraussetzungen. Hieraus sei zu schließen, dass der Unionsgesetzgeber eine Erstreckung auf Mitbewerber des Verletzers nicht zulassen wollte.

Das LG Würzburg (Beschluss vom 13.09.18, 11 O 1741/18, juris) hingegen schätzt den Sachverhalt der Abmahnfähigkeit anders ein. Nach dessen Auffassung liegt beim Betrieb einer geschäftlichen Website ohne eine der DSGVO genügenden Datenschutzerklärung und der Verwendung eines Kontaktformulars ohne Verschlüsselung ein Verstoß

gegen Marktverhaltensregelungen im Sinne von § 3a UWG vor. Ebenso hat das OLG Hamburg (Urt. vom 25.10.18, 3 U 66/17, juris) geurteilt: Die DSGVO enthalte kein abgeschlossenes Sanktionssystem und stehe deshalb der Klagbefugnis von Wettbewerbern nach § 8 Absatz 3 Nummer 1 UWG wegen Verstoßes gegen datenschutzrechtliche Bestimmungen nicht entgegen. Allerdings habe nicht jegliche datenschutzrechtliche Norm marktverhaltensregelnden Charakter i. S. des § 3a UWG. Vielmehr müsse die jeweilige Norm konkret darauf überprüft werden, ob gerade jene Norm eine Regelung des Marktverhaltens zum Gegenstand hat.

Um auf den Ausgangsfall zurückzukommen: Grundsätzlich ist es richtig, dass eine fehlende, unvollständige oder nur schwer aufzufindende Datenschutzerklärung auf einer Website einen Verstoß gegen die Artikel 12, 13 DSGVO darstellt. Ob dies aber tatsächlich die Möglichkeit einer wettbewerbsrechtlichen Abmahnung eröffnet, ist höchstrichterlich noch nicht geklärt. Einstweilen kann ich betroffenen Unternehmern nur dringend raten, anwaltliche Hilfe zur Abklärung ihrer Handlungsmöglichkeiten, insbesondere ob es ratsam ist, die geforderte Unterlassungserklärung tatsächlich abzugeben und die geltend gemachten Kosten zu erstatten, in Anspruch zu nehmen. Dies gilt umso mehr, als dass der von den abmahnenden Kanzleien zumeist auch angeführte § 13 TMG seit dem 25. Mai 2018 wegen des Anwendungsvorrangs der DSGVO nach einhelliger Auffassung der Datenschutzaufsichtsbehörden gar nicht mehr anwendbar ist. Ich muss an dieser Stelle allerdings regelmäßig auch um Verständnis dafür bitten, dass ich in dieser wettbewerbsrechtlichen Frage mangels Zuständigkeit darüber hinaus keine weitere Unterstützung geben bzw. Beratung leisten kann.

3.1.3 Auslegung des Artikel 13 DSGVO zur Informationspflicht der betroffenen Personen bei Direkterhebungen

Im Berichtszeitraum wurden durch anfragende Verantwortliche und Behörden Auslegungsfragen zu den Informationspflichten gemäß Artikel 13 DSGVO problematisiert.

Insbesondere im nicht-öffentlichen Bereich führt eine strenge Auslegung der Vorschriften des Artikels 13 DSGVO regelmäßig zu unpraktikablen Vorgaben, insbesondere für privatwirtschaftliche Unternehmen.

Meine Behörde hat sich um entsprechende Hilfestellung bemüht und verweist hierbei auf ihre Hausmeinung mit nachstehendem Inhalt:

Bei der Anbahnung eines Geschäftskontaktes bis möglicherweise hin zu einem beabsichtigten Vertragsabschluss kann es über einen längeren Zeitraum mehrere Erhebungen mit unterschiedlichen spezifischen Erhebungszweck und -umfang geben (bspw.: Terminabsprache beim Arzt als neuer Patient; der Vertrag wird beim Erstbesuch in der Pra-

xis geschlossen). Der Umfang der Informationen richtet sich nach der Adäquanz des jeweiligen Erhebungsschritts.

Das „Mitteilen“ der Information setzt nicht ein aktives Herantreten an den Betroffenen voraus, sondern ist mit der englischen Fassung „provide“ als ein „Zur-Verfügung-Stellen“ zu verstehen. Dies kann „durch geeignete Maßnahmen“ des Verantwortlichen erfolgen (Artikel 12 Absatz 1 DSGVO), die sich gegenseitig ergänzen können (Aushang, Info-Blatt, Erklärung auf Webseite, Textteil im Vertrag, mündlicher Hinweis, …). Entscheidend ist, dass die Information des Betroffenen durch ihn zumutbar erlangt werden kann.

Bei einem aktiven Herantreten des Betroffenen an den Verantwortlichen (Telefonanruf, E-Mail, …) ist regelmäßig damit zu rechnen, dass ihm die Kontaktdaten des Verantwortlichen bekannt sind (Artikel 13 Absatz 1 Buchstabe a) sowie der (von ihm intendierte) Zweck - Artikel 13 Absatz 1 Buchstabe c) DSGVO).

Sofern Informationen bei diesem ersten Erhebungsschritt fehlen (z. B. die Kontaktdaten des Datenschutzbeauftragten, Artikel 13 Absatz 1 Buchstabe b) DSGVO, oder die Benennung der Rechtsgrundlage, Artikel 13 Absatz 1 Buchstabe c) DSGVO), kann dies nach Auffassung der Aufsichtsbehörde bei einem späteren Erhebungs- oder Verarbeitungsschritt erfolgen (z. B. als Link in der Signatur einer E-Mail-Antwort). Entscheidend ist dabei, ob die Umstände der ersten Erhebung „geeignet“ (bzw. nicht „geeignet“) sind, diese Information sachgerecht zu ermöglichen.

Besteht kein Erfordernis für eine dauerhafte Verarbeitung der Daten (z. B. wird der vereinbarte Arzttermin nicht wahrgenommen), sind die Daten zu löschen, es sei denn, es liegt eine Voraussetzung für eine zweckändernde Verarbeitung vor (Artikel 6 Absatz 4 DSGVO). In diesem Fall hat eine entsprechende (diesen Fall betreffende) Information des Betroffenen zu erfolgen, sofern dies nicht schon beim ersten Erhebungsschritt erfolgt ist.

3.1.4 Informationspflichten von Behörden bei Erhebungen personenbezogener Daten bei Dritten*

Seitens öffentlicher Stellen wird die Frage gestellt, ob eine Behörde, die personenbezogene Daten bei Dritten erhebt oder durch Dritte erlangt, den Informationspflichten nach Artikel 14 Absatz 1 bis 3 DSGVO nachkommen müsse.

Behörden beziehen personenbezogene Daten ausschließlich auf gesetzlicher Grundlage, entweder im Wege des zielgerichteten Beschaffens oder indem sie sie unangefordert erlangen. In beiden Fällen kommt regelmäßig die Ausnahmevorschrift des Artikels 14 Absatz 5 Buchstabe c) DSGVO zum Tragen. Die Informationspflichten nach Artikel 14

Absatz 1 bis 3 DSGVO finden keine Anwendung, wenn die Erlangung der Daten durch EU-, deutsche oder sächsische Rechtsvorschriften ausdrücklich geregelt ist und diese Rechtsvorschriften geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen. Das ist bei Rechtsvorschriften, die die Tätigkeit von Behörden regeln, regelmäßig der Fall. Daher ist eine Behörde, abgesehen von eintretenden Ausnahmen, in denen keine Schutzmaßnahmen zugunsten betroffener Personen vorgesehen sind, nicht pflichtig, Informationspflichten nach Artikel 14 Absatz 1 bis 3 DSGVO zu erfüllen.

Ein Beispiel: Der Sächsische Rechnungshof erhebt zu Kontrollzwecken – manchmal als bloßen „Beifang“, manchmal zielgerichtet – viele personenbezogene Daten bei anderen Behörden oder sogar nicht-öffentlichen Stellen. Seine Rechtsgrundlage hierfür sind die §§ 88 ff. SäHO, die ihm die Erhebung solcher Daten zu Prüfungszwecken erlaubt. In diesem Fall kommt die Ausnahmeregelung des Artikel 14 Absatz 5 Buchstabe c) DSGVO zur Anwendung: Die Erlangung der personenbezogenen Daten durch den Rechnungshof ist durch Rechtsvorschrift, hier insbesondere durch die §§ 88 ff. SäHO, ausdrücklich geregelt; diese Rechtsvorschriften sehen auch geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vor, hier u. a. § 12 RechnungshofG (Beratungsgeheimnis).

3.2 Auskunftsrecht

3.2.1 Der Auskunftsanspruch in der Praxis

Ich erhielt zahlreiche Anfragen zu dem in Artikel 15 DSGVO neu geregelten Auskunftsanspruch.

Dies betraf zunächst die Kostenfreiheit nach Artikel 12 Absatz 5 DSGVO. Diese gilt wie der gesamte Anspruch nur für personenbezogene Daten des Antragstellers. Dabei sind gemäß Artikel 4 Nummer 1 DSGVO personenbezogene Daten alle Informationen, die sich auf ihn beziehen. Gemäß Artikel 15 Absatz 4 DSGVO ist aber ohnehin sicherzustellen, dass Rechte Dritter durch die Auskunft nicht beeinträchtigt werden. Sollten Verantwortliche zu dem Ergebnis kommen, dass eine derartige Beeinträchtigung vorliegt, wären beispielsweise entsprechende Schwärzungen vorzunehmen.

Ich konnte auf Anfrage auch bestätigen, dass der Anspruch aus Artikel 15 DSGVO jederzeit und neben anderen Ansprüchen beispielsweise auch unabhängig von einem eventuellen Verwaltungsverfahren besteht.

Weiterhin wurde ich um Auskunft gebeten, wie einem „globalen Auskunftsersuchen“ beispielsweise gegenüber Kommunen zu entsprechen ist. Ein Antragsteller hat zunächst Anspruch auf Mitteilung, ob überhaupt Daten zu seiner Person verarbeitet werden, Arti-

kel 15 Absatz 1 Satz 1, 1. Variante DSGVO. Verarbeitet ein Verantwortlicher Daten zu ihm, hat er einen Anspruch auf Mitteilung des Katalogs nach Artikel 15 Absatz 1 Satz 1, 2. Halbsatz Buchstabe a bis h DSGVO. Außerdem hat der Antragsteller einen Anspruch auf Mitteilung der Daten selbst (Wie sonst sollte der Antragsteller überprüfen können, ob die zu ihm gespeicherten Daten richtig sind?).

Einer Mitwirkungspflicht unterliegt der Antragsteller dabei nur bedingt. Artikel 15 DSGVO enthält keine Aussage dazu, ob und in welcher Weise die betroffene Person durch eigene Informationen gegenüber dem Verantwortlichen dazu beitragen muss, ihm die Erfüllung der Auskunftspflicht zu erleichtern. Lediglich für den Fall, dass der Verantwortliche eine große Menge von Informationen über die betroffene Person verarbeitet, soll er gemäß dem Erwägungsgrund 63 Satz 7 von ihr verlangen können, dass sie präzisiert, auf welche Informationen oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht. Verantwortlichen ist also unbenommen, den „globale Auskunft“ beantragenden Antragsteller im Hinblick auf den Aufwand und die Dauer solch einer Auskunft zu bitten, seinen Antrag zu präzisieren. Falls er dies jedoch nicht kann oder will, müssen sie die einzelnen Ämter abfragen (dem Antragsteller die Ausübung seines Rechts erleichtern, wie Artikel 12 Absatz 2 DSGVO es vorsieht).

Ich empfehle Kommunen hierzu, entsprechende Anfragen zunächst an Stellen, die mit höherer Wahrscheinlichkeit personenbezogene Daten gespeichert haben, wie das Meldeamt, das Standesamt, das Ordnungsamt, das Steueramt und das Stadtkassenamt mit der Bitte um entsprechende Auskunft weiterzuleiten. Darüber sollte der Auskunftssuchende informiert werden. Dabei kann nachgefragt werden, ob ihm diese Auskünfte ausreichen. Auch kann er gebeten werden, dass er andernfalls präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich das Auskunftsersuchen bezieht und gegebenenfalls auf die Verlängerung der Beantwortungsfrist auf drei Monate gemäß Artikel 12 Absatz 3 Satz DSGVO hingewiesen werden. Für die Antwort sollte eine angemessene Frist eingeräumt werden. Sollte innerhalb dieser Frist keine entsprechende Antwort eintreffen, sind die übrigen Ämter einzubeziehen. In jedem Fall sollte die Antwort wegen einer fehlenden Rechtsgrundlage für die Übermittlung an eine zentrale Stelle durch die jeweiligen Ämter erfolgen. Es ist auch nicht ersichtlich, dass eine entsprechende Beantwortung zu den Aufgaben des gemeindlichen Datenschutzbeauftragten gehört.

Schließlich besteht die Möglichkeit, nach Artikel 12 Absatz 5 DSGVO bei (von den Verantwortlichen nachzuweisenden) offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anträgen einer betroffenen Person entweder ein angemessenes Entgelt zu verlangen oder sich zu weigern, aufgrund des Antrags tätig zu werden. Gemäß Artikel 12 Absatz 6 DSGVO können bei begründeten

Zweifeln an der Identität des Antragstellers zusätzliche Informationen angefordert werden, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

3.2.2 Vermieter – Auskunft nach Artikel 15 DSGVO – Einsicht in die gesamte Mieterakte

Es erreichten mich mehrere Anfragen bzw. Beschwerden von Mietern, die von ihrem Vermieter auf der Grundlage von Artikel 15 DSGVO Einsicht in die gesamte Mieterakte gefordert hatten. Die Einsichtnahme bzw. Übermittlung einer Datenkopie wurde vom Vermieter abgelehnt. Teilweise wurde die Ablehnung mit dem Fehlen des berechtigten Interesses des Mieters begründet.

Die betroffene Person hat nach Artikel 15 Absatz 1 DSGVO das Recht vom Verantwortlichen Auskunft über die personenbezogenen Daten, die von diesem verarbeitet werden, zu verlangen. Daneben besteht nach Artikel 15 Absatz 3 DSGVO das Recht vom Verantwortlichen eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zu verlangen. Weder der Auskunftsanspruch nach Artikel 15 Absatz 1 DSGVO noch das Recht auf eine Datenkopie nach Artikel 15 Absatz 3 DSGVO setzen ein berechtigtes Interesse voraus. Dem Betroffenen ist nach Artikel 15 Absatz 3 DSGVO eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen. Die erste Kopie ist nach Artikel 15 Absatz 3 DSGVO kostenfrei.

Die Mieterakte besteht aus Daten, die sich auf den Mieter beziehen. Sie stellt daher in ihrer Gesamtheit personenbezogene Daten des Mieters dar. D. h., sie ist in Gänze zu kopieren und dem Mieter zur Verfügung zu stellen, wenn dieser nach Artikel 15 Absatz 3 DSGVO eine Kopie seiner personenbezogenen Daten verlangt. Das Auskunftsrecht nach Artikel 15 Absatz 1 DSGVO und das Recht nach Artikel 15 Absatz 3 DSGVO erstrecken sich damit auf die gesamte Mieterakte.

Nach Artikel 15 Absatz 4 DSGVO darf das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Das Recht sollte etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen (beispielhafte Aufzählung im Erwägungsgrund 63). Dies darf im Ergebnis aber nicht dazu führen, dass jegliche Auskunft verweigert wird.

Auskunftsbegehren sind nach Artikel 12 Absatz 3 DSGVO unverzüglich, in jedem Fall aber innerhalb eines Monats zu beantworten.

3.2.3 Kostenlose Kopie der personenbezogenen Daten nach Artikel 15 Absatz 3 DSGVO, Verhältnis zu § 630g BGB

Im Berichtszeitraum hatte sich eine Familie an mich gewandt, die ihren behandelnden Arzt um eine kostenlose Kopie ihrer personenbezogenen Daten der jeweiligen Patientenakte nach Artikel 15 Absatz 3 DSGVO gebeten hatte. Der behandelnde Arzt habe dies abgelehnt und sei nur gegen Zahlung einer Gebühr bereit eine Kopie der Patientenakte zur Verfügung zu stellen. Er berufe sich dabei auf § 630g Absatz 2 BGB.

Nach Artikel 15 Absatz 3 DSGVO kann die betroffene Person vom Verantwortlichen eine Kopie der personenbezogenen Daten verlangen, die er über sie verarbeitet. Die erste Kopie ist nach Artikel 15 Absatz 3 DSGVO kostenfrei. § 630g BGB trifft eine davon abweichende Regelung. Der Patient kann nach § 630g Absatz 2 BGB auch elektronische Abschriften von der Patientenakte verlangen. Der Patient hat dem Behandelnden die entstandenen Kosten zu erstatten.

Derzeit ist noch nicht abschließend geklärt, in welchem Verhältnis die beiden Ansprüche - der Anspruch aus Artikel 15 Absatz 3 sowie der Anspruch aus § 630g BGB - zueinander stehen. Nach einer Auffassung handelt es sich um zwei unterschiedliche Ansprüche, die nebeneinander bestehen. Andererseits wird § 630g BGB als Sonderregelung im Sinne des Artikels 23 Absatz 1 Buchstabe i DSGVO gesehen. Die Pflicht zur Kostenerstattung nach § 630g BGB würde fortbestehen, weil insoweit von einem überwiegenden Interesse der zur Gewährung der Einsichtnahme verpflichteten Person im Sinne von Artikel 23 Absatz 1 Buchstabe i DSGVO auszugehen wäre. Rechtsprechung zum Verhältnis der beiden Ansprüche liegt noch nicht vor.

Ich habe erhebliche Zweifel, dass hier von einem Vorliegen des Artikels 23 Absatz 1 Buchstabe i DSGVO ausgegangen werden kann, da bei der Interessenabwägung auf Seiten des Arztes lediglich wirtschaftliche Interessen (Kostenerstattung) vorliegen. Artikel 15 DSGVO sieht die kostenfreie Bereitstellung einer Datenkopie vor. Nach meiner Auffassung kann deshalb bei einem Auskunftsanspruch, der sich auf Artikel 15 Absatz 3 DSGVO stützt, keine Kostenerstattung gefordert werden.

Da sich der Arzt, laut Angaben der Beschwerdeführer, auf eine entsprechende Beratung durch die Sächsische Landesärztekammer berufen habe, wurde diese von mir mit Schreiben vom 29. November 2018 über das Problem und meine Rechtsauffassung informiert. In Bezug auf die Beschwerde hat der Arzt inzwischen der Familie die Kopien der personenbezogenen Daten der Patientenakte kostenlos zur Verfügung gestellt.

3.2.4 Auskunftserteilung durch Gerichtsvollzieher

Nach Geltungsbeginn der DSGVO erreichten mich einige Beschwerden von Petenten, die sich mit der Bitte um Auskunft über die zu ihrer Person verarbeiteten Daten (Artikel 15 DSGVO) an Gerichtsvollzieher gewandt und keine Antwort erhalten hatten.

Das Recht betroffener Personen auf Auskunft nach Artikel 15 DSGVO ist ein zentrales Betroffenenrecht, ermöglicht das Wissen um Verarbeitung und deren Hintergrund im Einzelfall dem Betroffenen doch erst, die Rechtmäßigkeit der Verarbeitung nachvollziehen zu können oder – bei vermuteter Rechtswidrigkeit – Beschwerde bei der Aufsichtsbehörde zu erheben oder weitergehende Ansprüche (z. B. auf Berichtigung oder Löschung) geltend zu machen. Das Recht auf Auskunft steht jeder betroffenen Person zu; die Verpflichtung, Auskunft zu erteilen, trifft jeden Verantwortlichen. Dass – im Vergleich zur Lage vor dem 25. Mai 2018 – ein gesteigertes Auskunftsinteresse gegenüber Gerichtsvollziehern zu verzeichnen ist, liegt vermutlich an der medialen Beachtung der Datenschutz-Grundverordnung.

Gerichtsvollzieher sind Verantwortliche im Sinne der Datenschutz-Grundverordnung (Artikel 4 Nummer 7 DSGVO), deren Vorschriften neben spezialgesetzlichen Bestimmungen etwa der ZPO auf die Verarbeitung personenbezogener Daten durch Gerichtsvollzieher Anwendung finden. Maßgeblich für die Behandlung von Anträgen, mit denen betroffene Personen ihre datenschutzrechtlichen Ansprüche geltend machen, ist Artikel 12 DSGVO. In den Petitionsvorgängen, in denen Auskunftsanträge Betroffener tatsächlich über Wochen ohne Reaktion geblieben waren, habe ich die Gerichtsvollzieher auf die Rechtslage und bestehende Verpflichtungen aufmerksam gemacht.

Artikel 12 Absatz 3 DSGVO bestimmt, dass die erbetenen Informationen unverzüglich, jedenfalls aber innerhalb eines Monats nach Antragstellung zu erteilen sind. Die Frist kann u.U. um zwei Monate verlängert werden; hierüber ist der Antragsteller aber wiederum innerhalb eines Monats nach Antragstellung unter Angabe der Gründe zu informieren. Nach Artikel 12 Absatz 4 DSGVO ist der Antragsteller auch über ein Nicht-Tätigwerden (d.h. eine Ablehnung des Ersuchens) innerhalb eines Monats zu unterrichten. Diese Bestimmungen sind zwingend und gelten unmittelbar; der klare Wortlaut steht einer Auslegung zu Lasten Betroffener entgegen. Reagiert ein Verantwortlicher einen Monat lang überhaupt nicht auf ein Ersuchen einer betroffenen Person – weder durch Erfüllung des Anspruchs, noch durch Unterrichtung über Fristverlängerung oder durch begründete Ablehnung des Antrags – verstößt er auf jeden Fall gegen seine Pflichten aus der DSGVO.

In einem der Petitionsvorgänge machte mich der betroffene Gerichtsvollzieher darauf aufmerksam, dass das für ihn zuständige Amtsgericht Dresden zwischenzeitlich für die

Gerichtsvollzieher des Gerichtsbezirks ein Musterdatenblatt für die Beantwortung von Auskunftsersuchen nach Artikel 15 DSGVO erarbeitet hatte, das er dann auch für die Auskunftserteilung an den Petenten verwendete. Das Musterdatenblatt entspricht m. E. den Anforderungen an eine Auskunftserteilung nach Artikel 15 Absatz 1 DSGVO, es entlastet die Gerichtsvollzieher und beschleunigt das Verfahren, wodurch letztendlich auch betroffene Personen zügig zu ihrem Recht kommen. Die Initiative des Amtsgerichts Dresden begrüße ich daher ausdrücklich.

3.3 Recht auf Löschung

3.3.1 Das Recht auf Löschung und gesetzliche Aufbewahrungsfristen

Immer wieder wandten sich im letzten Berichtszeitraum betroffene Personen an meine Behörde und verlangten die Löschung ihrer Daten, zumeist bei Unternehmen, aber auch bei Behörden. In vielen Fällen stellte sich heraus, dass die Betroffenen sich in einem Vertragsverhältnis mit der nicht-öffentlichen Stelle befunden hatten. Hintergrund der Forderungen auf Löschung, die seitens der Unternehmen verweigert wurden, waren zumeist Kaufverträge, bei denen es zu Streitigkeiten zwischen den Vertragsparteien gekommen war. Soweit zum Beispiel ein Kaufvertrag zustande gekommen ist, also ein Geschäftsvorfall bzw. Kostenvorgang auf Seiten des Händlers aufgetreten ist, sind durch den Händler gemäß § 147 AO bzw. gemäß § 257 Absatz 1 HGB Geschäftsbriefe und Buchungsbelege als Geschäftsunterlagen bis zu 10 Jahren aufzubewahren. In derartigen Fällen besteht kein Löschungsanspruch der betroffenen Person auf ihre in den aufzubewahrenden Unterlagen vorhandenen personenbezogenen Daten der Betroffenen.

Auch Behörden verfügen über eine allgemeine Pflicht zur vollständigen Aktenführung und nicht selten bereichsspezifisch über konkrete Aufbewahrungspflichten, so dass nicht wenige der mir gegenüber geltend gemachten Löschungsbegehren gegenüber öffentlichen Stellen ebenfalls rechtlich nicht umgesetzt werden konnten.

Festzuhalten bleibt generell, dass gesetzliche Aufbewahrungsfristen datenschutzrechtlichen Löschpflichten vorgehen. Soweit solche Aufbewahrungsfristen bestehen, dürfen personenbezogene Daten also nicht gelöscht werden, Artikel 17 Absatz 3 Buchstabe b) DSGVO.

3.4 Recht auf Datenübertragbarkeit, Widerspruchsrecht, Sonstiges

3.4.1 Widerspruchsrecht im Bauplanungsrecht bei Veröffentlichungen

Ein Petent fragte mich an, da für sein Grundstück ein Enteignungsverfahren eingeleitet worden war. Für den Petenten problematisch war dabei der an ihn erfolgte Hinweis, dass die ortsübliche Bekanntmachung hierüber zwingend den Namen des Eigentümers enthalten müsse.

Der Petent wollte indes nur die Offenlegung des entsprechenden Flurstücks erreichen und insoweit von seinem Widerspruchsrecht zum Schutz seiner Interessen als natürliche Person Gebrauch machen.

Gemäß § 108 Absatz 5 Satz 1 Baugesetzbuch ist in der Tat das betroffene Grundstück, aber auch der im Grundbuch als Eigentümer eingetragene ortsüblich bekanntzumachen. Zutreffend ist daher die dem Petenten gegenüber erfolgte Auskunft gewesen, dass die ortsübliche Bekanntmachung auch den Namen des Eigentümers, Vornamen und Zunamen, mit dem Zusatz „Eigentümer und Betroffener“ enthalten muss. Hierbei handelt es sich aus meiner Sicht um eine Frage der Transparenz. Die Öffentlichkeit soll nachvollziehen können und teilhaben, wen die enteignungsbegünstigte Gemeinde heranzieht.

Die ortsübliche Bekanntmachung erfolgt regelmäßig durch das amtliche Mitteilungsblatt der Gemeinde. Ob seitens der Gemeinde allerdings per Bekanntmachungssatzung festgelegt ist, dass das Mitteilungsblatt auch online publiziert wird, konnte ich nicht überprüfen, da ich keine Kenntnis davon hatte, um welche Gemeinde es sich handelte.

§ 4 Absatz 1 Sächsisches E-Government-Gesetz ist aus meiner Sicht nicht anwendbar, da es sich bei der baugesetzlichen (Bundes-)Vorschrift um keine Rechtsvorschrift des Freistaates Sachsen handelt.

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die wie hier aufgrund von Artikel 6 Absatz 1 Buchstabe e DSGVO erfolgt, Widerspruch gemäß Artikel 21 DSGVO einzulegen.

Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Hier wurde allerdings seitens des Petenten bereits eine solche besondere Situation nicht dargetan, die eine Abweichung von dem Grundsatz der Bekanntmachung rechtfertigen könnte.

3.4.2 Widerspruchsrecht bei Direktwerbung

Gemäß Artikel 21 Absatz 2 DSGVO haben betroffene Personen das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zweck der Direktwerbung gegenüber dem Verantwortlichen – der datenverarbeitenden Stelle – zu erheben. Im Falle des Widerspruchs dürfen verarbeitete Daten der betroffe-

nen Person dann nicht mehr für Zwecke der Direktwerbung Verwendung finden, Artikel 21 Absatz 3 DSGVO.

Im zurückliegenden Berichtszeitraum erhielt ich zahlreiche Beschwerden betroffener Personen, insbesondere wegen zugegangener E-Mail-Werbung. In sehr vielen Fällen handelte es sich hierbei um Bestandskunden von Händlern, die über das Internet an die Kunden Waren verkauft hatten. Überwiegend hatten die Internethändler auch über die Zusendung von Werbezuschriften nach der Datenschutz-Grundverordnung ordnungsgemäß informiert, Artikel 13 DSGVO, und die Betroffenen hatten entweder eingewilligt oder die Nutzung der Daten zu Zwecken der Direktwerbung konnte im Sinne von Artikel 6 Absatz 1 Satz 1 Buchstabe f DSGVO als vertretbar angesehen werden, so dass nicht von einem Datenschutzverstoß auszugehen war. So waren die betroffenen Personen in nicht wenigen Fällen seitens meiner Behörde auf ihr selbst auszuübendes Widerspruchsrecht gemäß Artikel 21 Absatz 2, Absatz 3 DSGVO zu verweisen, was sie nicht genutzt hatten. Häufig war die Beschwerde bei meiner Behörde auch mit dem Wunsch auf Datenlöschung verbunden, das ebenfalls selbstständig gegenüber dem Verantwortlichen geltend zu machen gewesen wäre. Die Löschung wiederum kann sich allerdings nur auf die Kundeninformationen beziehen, die nicht gemäß den steuerrechtlichen und handelsrechtlichen Vorschriften als Geschäftsunterlagen aufzubewahren gewesen sind, worauf meine Dienststelle ebenfalls mehrfach aufmerksam machte, vergleiche auch den Tätigkeitsberichtsbeitrag oben unter 3.3.1.

Artikel 21 Absatz 4 DSGVO bestimmt auch, dass die betroffenen Personen über ihr Widerspruchsrecht gegen eine Verarbeitung zu Zwecken der Direktwerbung hinzuweisen sind. Überwiegend konnte bei den durch meine Behörde geprüften Vorgängen kein Verstoß gegen die einzuhaltenden Informationspflichten festgestellt werden. In vielen Fällen war es augenscheinlich so, dass die betroffenen Personen ihnen übersandte Datenschutzinformationen der Händler nicht zur Kenntnis genommen hatten.

Weitere Informationen enthält der Text der Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DSGVO), Tätigkeitsberichtsbeitrag 7.2.9 unten.

4 Pflichten Verantwortlicher und Auftragsverarbeiter

4.1 Verantwortung für die Verarbeitung, Technikgestaltung

4.1.1 Standard-Datenschutzmodell

Mit dem Standard-Datenschutzmodell (SDM) wird eine Methode zur Verfügung gestellt, mit der Verantwortliche und Aufsichtsbehörden bei der Entwicklung, beim Betrieb und bei der Prüfung von Datenverarbeitungen beurteilen können, ob personenbezogene Daten datenschutzkonform verarbeitet werden. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat empfohlen, dieses Modell anzuwenden.

Im Handbuch zur Methodik des Standard-Datenschutzmodells wird im Kapitel 7 auf einen Katalog mit technischen und organisatorischen Referenzmaßnahmen hingewiesen. Die Datenschutzkonferenz hat im April 2018 beschlossen, dass der in einzelne Bausteine gegliederte Katalog sukzessive zunächst von einzelnen Aufsichtsbehörden veröffentlicht und zum Test durch Anwender freigegeben werden sollen. Die dazu eingerichtete Unterarbeitsgruppe „SDM-Bausteine“ (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Sächsischer Datenschutzbeauftragter, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein und Der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland) hat die folgenden Bausteine erarbeitet und am 10. September 2018 veröffentlicht:

- Datenschutz-Management
- Planung / Spezifikation
- Dokumentation
- Protokollierung
- Trennung
- Löschen
- Aufbewahrung

Zu finden sind die Texte unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

Die Autoren der Unterarbeitsgruppe weisen ausdrücklich darauf hin, dass diese Bausteine noch nicht in der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder abgestimmt sind. Sie empfehlen den Anwendern, ihre Erfahrungen bei

der Erprobung der Bausteine den beteiligten Datenschutzbehörden mitzuteilen, und somit zur Weiterentwicklung von Methode und Maßnahmen beizutragen.

4.1.2 Vorbelegung des Buttons „Angemeldet bleiben“ bei Online-Accounts

Die Service- und Kommunikationsdienstleistungen von Online-Communities stehen üblicherweise nur registrierten Nutzern zur Verfügung. Auf der Anmeldeseite findet sich dann neben den üblichen Eingabemöglichkeiten für Nutzername und Passwort häufig auch ein Ankreuzfeld mit der Bezeichnung „Angemeldet bleiben“. Setzt der Nutzer dort ein Häkchen, muss er sich nicht bei jedem Aufruf der betreffenden Website neu anmelden, vorausgesetzt er nutzt dazu das gleiche Gerät und er hat sich nach der letzten Session nicht explizit abgemeldet. Technisch umgesetzt wird dies durch das Setzen eines Text-Cookies mit eindeutiger Kennung und einer Gültigkeit über die jeweilige Session hinaus.

Das Mitglied einer solchen Community hat mich auf die dort erfolgte Vorbelegung des Buttons „Angemeldet bleiben“ angesprochen und dies als entsprechend risikobehaftet kritisiert.

Ich habe dies entsprechend nachvollziehen können. Was im konkreten Fall als nutzerfreundlich zu betrachten ist (Vorbelegung: ja/nein), hängt zwar vom individuellen Nutzungsverhalten des jeweiligen Mitglieds, d. h. in welchem privaten oder dienstlichen Umfeld er welche Geräte dafür nutzt, ab. Datenschutzfreundlich ist aber in jedem Fall eine Voreinstellung, die mögliche Risiken für alle Nutzergruppen ausschließt, zumal es jedem Nutzer unbenommen ist, diese Voreinstellung entsprechend (einmalig) zu ändern.

Artikel 25 Absatz 1 DSGVO legt den Verantwortlichen solcher Communities die Verpflichtung auf, durch datenschutzfreundliche Voreinstellungen dafür zu sorgen, dass die notwendigen Garantien für die Rechte und Freiheiten ihrer Mitglieder in die Verarbeitung aufgenommen werden. Zudem haben sie nach Absatz 2 dieser Vorschrift geeignete technische Maßnahmen zu treffen, dass durch entsprechende Voreinstellungen gewährleistet ist, dass personenbezogene Daten nicht länger als notwendig verarbeitet werden.

Vor diesem Hintergrund habe ich es als wichtigen und wesentlichen Punkt angesehen, dass die Mitglieder einer solchen Community nur dann deren Dienste ohne erneute Anmeldung nutzen können, wenn sie dies selbst für sich als Vorteil empfinden und dies dem Verantwortlichen gegenüber – nach einer individuellen, u. a. die Zugänglichkeit der jeweiligen Computertechnik für Dritte berücksichtigenden Risikobetrachtung – mit einer ausdrücklichen Handlung auch entsprechend erklären. Die Vorbelegung des betreffenden Buttons zwingt sie allerdings bei jeder Anmeldung jeweils zu einem zusätzlichen Schritt, während bei einer Entscheidung für das „Angemeldet bleiben“ dieser

Schritt nur einmal erforderlich wäre. Dass es sich – jedenfalls in Fällen der Nutzung fremder Computertechnik – bei einem Verzicht auf das „Angemeldet bleiben“ um eine datenschutzfreundliche Voreinstellung handelt, sollte angesichts der zumindest in diesen Fällen wohl unstrittigen Risiken für die Rechte und Freiheiten der Nutzer wohl keiner weiteren Diskussion bedürfen.

Der Community-Betreiber ist meiner Argumentation gefolgt und hat die kritisierte Voreinstellung zurückgenommen. Darüber hinaus hat er in sein Angebot eine Schaltfläche aufgenommen, die es einem (angemeldeten) Mitglied ermöglicht, alle derartigen Freischaltungen auf anderen Geräten, auf denen er sich einmal angemeldet (und nicht wieder abgemeldet) hat, zurückzunehmen. Nach Betätigung dieser Schaltfläche kann das Mitglied davon ausgehen, dass es definitiv auf keinem anderen als dem aktuell genutzten Gerät mehr angemeldet ist.

4.1.3 Verordnungskonformer Betrieb von Webseiten

Beim Betrieb von Webseiten hat sich die Rechtslage seit dem 25. Mai 2018 geändert. Bis zum Inkrafttreten der europäischen e-Privacy-Verordnung – vergleiche hierzu den Tätigkeitsberichtsbeitrag 1.4 – vertritt die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder die Auffassung, dass die DSGVO für die Verarbeitung von Nutzungsdaten der Besucher von Webseiten anzuwenden ist (https://www.saechsdsb.de/images/stories/sdb_inhalt/behoerde/oea/Position-zur-Anwendbarkeit-des-TMG-fr-nicht-ffentliche-Stellen-ab-dem-25.-Mai-2018.pdf). Die bis Mai 2018 angewandte Regelung zur Erstellung von Nutzungsprofilen in § 15 Absatz 3 TMG ist nicht mehr anwendbar. Wenn in diesem Beitrag von Webseiten die Rede ist, sei angemerkt, dass alle Aussagen auch für andere Telemedien, wie z. B. Apps mit Zugang zum Internet, anzuwenden sind.

Wenn pseudonyme Nutzungsdaten von Besuchern durch den Webseitenbetreiber selbst oder durch eine in die Webseite integrierte Technik (Java-Script, Cookies, Videos etc.) durch Dritte verarbeitet werden, ist eine Rechtsgrundlage aus der DSGVO heranzuziehen. In Betracht kommen die Einwilligung (Artikel 6 Absatz 1 Buchstabe a DSGVO) oder ein berechtigtes Interesse eines privaten Webseitenbetreibers (Artikel 6 Absatz 1 Buchstabe f DSGVO) bzw. für öffentliche Stellen ein öffentliches Interesse (Artikel 6 Absatz 1 Buchstabe e DSGVO). Alle Rechtgrundlagen sind gleichberechtigt. In der Praxis ist jedoch zu beobachten, dass eine Einwilligung gern vermieden wird und pauschal ein berechtigtes oder ein öffentliches Interesse geltend gemacht wird. Besucher einer Webseite werden dann stets nur darüber informiert, dass z. B. Cookies eingesetzt werden und können maximal auf „Einverstanden“ klicken. Ein solches Vorgehen ist in aller Regel nicht mit der DSGVO vereinbar. Webseitenbetreiber sind verpflichtet, sich mit den auf ihrer Webseite eingesetzten Technologien auseinanderzusetzen und ange-

messene Maßnahmen zu ergreifen, um die Risiken für Rechte und Freiheiten natürlicher Personen zu gewährleisten.

Wenn ein Interesse des Verantwortlichen, bspw. zur Analyse des Nutzungsverhaltens für Verbesserungen der Webseite oder das Ausspielen von Werbung, geltend gemacht wird, ist dies konkret für jeden Fall mit den Risiken für Rechte und Freiheiten natürlicher Personen abzuwägen. In der Abwägung ist zu berücksichtigen, dass die DSGVO Kinder besonders schützt und dass bei der Verarbeitung sensibler Daten ein erhöhtes Risiko gegeben ist. Fällt die Interessenabwägung aufgrund erhöhter Risiken für Rechte und Freiheiten natürlicher Personen zugunsten des Betroffenen aus, ist eine Einwilligung die verbleibende Rechtsgrundlage. Zu beachten ist, dass diese einer ausreichenden Information des Betroffenen bedarf, was Webseitenbetreiber insbesondere bei der häufig intransparenten Datenverarbeitung durch Dritte, insbesondere große internationale Internetkonzerne, regelmäßig vor Schwierigkeiten stellen wird.

Wie kann eine solche Abwägung im Einzelfall aussehen? Aus der DSGVO lassen sich eine Reihe von Parametern ableiten, welche einzelnen Risiken zu betrachten sind:

a. Vernünftige Erwartung der betroffenen Personen und Vorhersehbarkeit / Transparenz

Hier ist eine Webseite in Gänze zu betrachten. Sicherlich entspricht es der Erwartungshaltung eines durchschnittlichen Internetnutzers, dass auf Webseiten von privat betriebenen Angeboten Werbung zur Finanzierung ausgespielt wird oder sein Verhalten statistisch erfasst wird. Nicht mit einer vernünftigen Erwartungshaltung verbunden sein dürfte, dass beim Besuch einer Webseite bis zu 100 Cookies mit langfristiger Möglichkeit der webseitenübergreifenden Profilbildung gesetzt werden oder ebenso viele Dritt-Webseiten mit IP-Adresse und Browserdaten beim Besuch der einen Webseite kontaktiert werden.

b. Interventionsmöglichkeiten der betroffenen Personen

Für die Interventionsmöglichkeiten sind die effektiv gegebenen Steuerungsmöglichkeiten eines Webseitenbesuchers zu betrachten. Durch den Nutzer eher einfach durch Browsereinstellung zu kontrollierende Text-Cookies sind als weniger risikobehaftet zu betrachten als nicht oder schwer zu kontrollierende Methoden wie Browser- und Canvas-Fingerprinting oder Flash-Cookies.

c. Verkettung von Daten, beteiligte Akteure und Umfang der Datenverarbeitung

Die Möglichkeit der Verkettung von Daten ist insbesondere beim Einsatz von Drittanbietern auf der Webseite zu betrachten. Wie groß sind die Möglichkeiten eines solchen

Dritten die über die Webseite bereitgestellten Datenflüsse Profile von Nutzern anzulegen? Das Risiko ist dann besonders hoch anzusiedeln, wenn das Geschäftsmodell der Drittanbieter aus der Profilbildung besteht. Das Risiko erhöht sich weiter, wenn diese Drittanbieter Profile nicht nur pseudonym erstellen, sondern mit konkreten Personen oder Nutzerkonten verknüpfen können. Als Beispiel kann die Firma Google dienen, welche allein durch die massenhaften Verbreitung von Android-Smartphones, die in aller Regel mit einem Nutzerkonto bei Google verknüpft sind, zahlreiche Möglichkeiten hat und nutzt, das Verhalten realer Personen über lange Zeiträume auszuwerten. Die Bewertung der beteiligten Akteure knüpft unmittelbar daran an. Ein Webseitenbetreiber ist auch für die Datenverarbeitung der von ihm aktiv eingebunden Dritten mitverantwortlich. Er hat daher eine explizite Prüfpflicht. Eine Einbindung einer Reichweitenmessung durch einen Dienstleister, der die gewonnenen Daten auch für eigene Zwecke verarbeitet, ist daher mit einer Berufung auf das berechtigte Interesse des Webseitenbetreibers nicht vereinbar.

d. Dauer der Beobachtung

Die Dauer einer Beobachtung bezeichnet das Risiko, dass ein Betroffener langfristig und eindeutig für einen Verantwortlichen wiedererkennbar ist. Das Risiko steigt, wenn Identifikatoren besonders langfristig angesetzt werden. Ein in der Praxis oft anzutreffender eindeutiger Cookie mit einer Gültigkeit von einem Jahr ist schwer mit dem berechtigten Interesse eines Verantwortlichen zur Erstellung einer Nutzungsstatistik in Einklang zu bringen.

e. Kreis der Betroffenen (bspw. besonders schutzbedürftige Personen) und Datenkategorien

Kinder, Jugendliche und Personen, welche besonders schutzbedürftige Informationen preisgeben, sind durch die DSGVO besonders geschützt. Je nach Zielgruppe oder Art der Webseite ist das Risiko daher gesondert zu betrachten. Polemisch gefragt: Muss Facebook unbedingt erfahren, dass ich eine Webseite über seltene Hautkrankheiten besucht habe?

Im Ergebnis muss der verantwortliche Webseitenbetreiber also für jede Verarbeitung von Nutzungsdaten eine Interessenabwägung durchführen und ggf. Risiken für die Rechte und Freiheiten natürlicher Personen soweit minimieren, dass ein berechtigtes Interesse überwiegt. Anderenfalls muss er auf eine individuelle Einwilligung setzen.

Die nachfolgend aufgeführten Maßnahmen gemäß Artikel 25, 32 DSGVO können die Risiken für die betroffenen Personen minimieren und in Bezug auf die o. g. Kriterien zur Absicherung der Interessen, Grundfreiheiten und Grundrechte der betroffenen Per-

sonen beitragen. Neben den hier aufgeführten Maßnahmen sind auch technische Äquivalente zur Eindämmung der Risiken umsetzbar.

- Kürzung der IP-Adresse zum technisch frühestmöglichen Zeitpunkt, es sei denn der Nutzer hat selbst Inhalte bereitgestellt oder ist beim Dienst registriert
- Vergröberung von Nutzerdaten (Browserversion, Betriebssystem)
- Keine Erhebung von Geräte- oder Sensordaten zur Wiedererkennung (Fingerprinting über Batteriedaten, Geolokation, Canvas, HTML5, Fonts etc.)
- Keine Nutzung des User-Agent (inkl. Browser-Version und Betriebssystem) für das Erkennen eines Nutzers oder für Fingerprinting.
- Setzen von Identifikatoren ausschließlich über Text-Cookies; kein Einsatz von nutzerseitig schwer zu kontrollierenden DOM-Storage-Objekten oder Fingerprinting
- Berücksichtigung von nutzerseitigen Voreinstellungen (z. B. Do Not Track, kein Third-Party-Tracking über First-Party-Cookies)
- Widerspruchsmöglichkeit (Datenschutzerklärungen und Widerspruchsmöglichkeiten sind von jeder Form der Reichweitenanalyse auszunehmen)
- Datenschutzerklärung (Ansprechpartner, Widerspruch, zielgruppenspezifische und zweckgenaue Erklärung der verwendeten Techniken)
- Prüffähige interne Dokumentation
- Prüfung einer Datenschutz-Folgenabschätzung.
- Löschung von übermittelten Rohdaten von Besuchern zum frühestmöglichen Zeitpunkt,
- Zweckorientierte Aufzeichnung von Benutzerinteraktion auf Minimalbasis (Abwägung, welche Funktionen einer eingesetzten Software für die verfolgten Zwecke erforderlich sind)
- Bei Einsatz einer eigenen Lösung: Einsatz der aktuellen Softwareversion
- Bei Einsatz eines Auftragsverarbeiters: Sicherheit der Übertragung, Mandantenfähigkeit, nachgewiesene Zweckbindung

Die oben genannten Kriterien sind keinesfalls abschließend. Sie sollen lediglich eine Hilfestellung und Konkretisierung für die Interessenabwägung gemäß Artikel 6 Absatz

1 Buchstabe f) DSGVO geben und die Sichtweise der Aufsichtsbehörden darstellen. Weitere Hinweise zur Interessenabwägung sind in der „Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG“ (WP 217) enthalten. Das WP 217 kann auch als Orientierung für die Interessenabwägung nach Artikel 6 Absatz 1 Buchstabe f) DSGVO dienen.

4.1.4 Über W-Lan frei zugängliche Kameraaufnahmen

Ein Kunde eines Einzelhandelsgeschäfts hatte die dort tätige Verkäuferin zunächst darauf aufmerksam gemacht, dass am Eingang des Geschäfts der obligatorische Hinweis auf die installierte Videoüberwachung fehlte. Zudem wies er sie darauf hin, dass das WLAN der Kamera frei zugänglich war und er sich mit seinem Smartphone direkt mit der Kamera verbinden konnte. Die Verkäuferin konnte dazu offensichtlich keine Angaben machen, sodass der Kunde sich in dieser Angelegenheit im Nachgang per Facebook-Nachricht an die Geschäftsführung wandte. Als auch darauf keine Reaktion erfolgte und er bei seinem nächsten Besuch sogar feststellen musste, dass die Kamerabilder auch über das Internet einsehbar waren, hat er sich schließlich an mich gewandt.

Der Sachverhalt war für mich vor diesem Hintergrund sehr gut nachvollziehbar. Die betreffende Videokamera lief praktisch rund um die Uhr, ermöglichte so eine fast lückenlose Überwachung der in diesem Geschäft tätigen Verkäuferinnen sowie der dort anwesenden Kunden und war in der Tat für jedermann frei zugänglich. Dass eine solche Form der Überwachung nach Artikel 6 DSGVO bzw. der §§ 4, 26 BDSG (unzulässige Veröffentlichung bzw. Übermittlung der Kamerabilder an einen unbestimmten Personenkreis) rechtswidrig war, muss an dieser Stelle sicher nicht näher ausgeführt werden.

Etwas schwieriger war hingegen die Ermittlung des Verantwortlichen. Da der Petent das konkrete Fachgeschäft nicht näher bezeichnet, sondern nur den Hauptsitz der eine ganze Reihe von Filialen betreibenden Firma benannt hatte, war zunächst nicht klar, ob es sich nur um einen Einzelfall oder eine größere Anzahl offener Überwachungskameras handelte. Schließlich stellte sich dann heraus, dass das betreffende Geschäft von einer rechtlich selbstständig agierenden Einheit, die allerdings noch unter der gemeinsamen Firmenmarke auftrat, betrieben wurde. Dies bedeutete, dass also tatsächlich nur ein Einzelfall zu betrachten war.

Die Inhaberin des betreffenden Geschäfts fiel praktisch „aus allen Wolken“, als sie noch vor mir durch die Geschäftsführung der Firmenkette mit dieser Problematik konfrontiert wurde. Tatsächlich war die offene Kamera also weder gewollt noch der Inhaberin überhaupt bewusst. Da sie lediglich eine Mitarbeiterin beschäftigte und daher zumeist mit in dem überwachten Geschäftsraum tätig war, war auch sie selbst in erheblichem Maß von

diesem Vorfall betroffen. Zweck des Kamerabetriebs war zum einen die Diebstahlsprävention, zum anderen die Signalisierung eintreffender Kunden über Tablet für den Fall, dass beide Verkäuferinnen im hinteren Bereich der Geschäftsräume (Werkstatt) zugange waren. Aufzeichnungen erfolgten nicht.

Die Kamera wurde durch die Inhaberin sofort nach Bekanntwerden des Sachverhalts außer Betrieb genommen und anschließend die nach Artikel 32 DSGVO notwendigen Zugriffsschutzmaßnahmen beauftragt.

4.1.5 Einsatz von WhatsApp bei Kundenkontakten

Viele Anfragen aus den nicht-öffentlichen Bereich betrafen die Nutzung des Kommunikationsverfahrens WhatsApp.

Der Einsatz von WhatsApp im geschäftlichen Umfeld bleibt auch nach dem Wirksamwerden der Datenschutz-Grundverordnung Problem behaftet. Aufgrund des standardmäßigen Zugriffs auf Kontaktdaten ist bereits der in Artikel 25 DSGVO verankerte Grundsatz „Privacy by Design“ nicht erfüllt. Automatisierte Verfahren und so genannte Containerlösungen, die den Zugriff auf die Kontaktdaten unterbinden, sind aufwendig und werden in der Praxis nur von größeren Unternehmen genutzt. Schon dem Umstand, dass eine permanente Beobachtung des Programms erforderlich ist und es bei Fehlern oder Unachtsamkeit beim nächsten Update des Verfahrens doch zu einem Abgleich der Kontakte mit WhatsApp kommen kann, halte ich für einen Ausschlussgrund.

Allerdings wird die Nutzung von WhatsApp im geschäftlichen Umfeld als Kommunikationskanal mit Kunden, wenn auf die datenschutzrechtliche Problematik hingewiesen wird und ein alternativer sicherer Kommunikationskanal (verschlüsselte E-Mail, Post) für den Kunden bereitsteht, nicht beanstandet. Darüber hinaus sind Kundendaten dadurch zu schützen, dass WhatsApp keinen Zugriff auf Kontakte von Kunden erhält, welche nicht über WhatsApp kommunizieren. Dies kann dadurch erfolgen, dass keine solchen Kundendaten auf dem Gerät in den Kontakten verarbeitet werden oder indem ein bestimmtes Verfahren oder eine Container-Lösung für WhatsApp mit eigener Kontaktverwaltung implementiert wird. Auch darf der Erstkontakt nur ausschließlich von der Kundenseite her stattfinden.

Im öffentlichen Bereich ist das Verfahren als Kommunikationsmittel zum Teil untersagt.

4.1.6 Einführung eines gemeinsamen ERP-Verbundprojektes an den sächsischen Hochschulen nach Datenschutz-Grundverordnung

Die Hochschulen in Sachsen (ausgenommen die TU Dresden) beabsichtigen in einem gemeinsamen Verbundprojekt ein Enterprise-Resource-Planning-Systems (ERP-Systems) zur Planung, Verwaltung und Steuerung der Ressourcen der Hochschulen einzuführen. Ich berate die Projektverantwortlichen des SMWK und der Hochschulen. Seit Projektbeginn werden bei der Planung und Umsetzung die erforderlichen Datenschutzmaßnahmen entsprechend der neuen Datenschutz-Grundverordnung berücksichtigt.

Der Betrieb des Test- und Produktivsystemen war für das Jahr 2018 geplant. Deshalb wurde durch die Lenkungsgruppe Neue Hochschulsteuerung-IT (NHS-IT) beschlossen, die Datenschutzanforderungen für das Projekt bereits gemäß der ab dem 25. Mai 2018 geltenden neuen Datenschutz-Grundverordnung (DSGVO) zu konzipieren.

Im Ergebnis wurde zwischen dem Sächsischen Staatsministerium für Wissenschaft und Kunst (SMWK) und dem Hauptpersonalrat beim SMWK (HPR) eine „Musterdienstvereinbarung zum Umgang mit dem Datenschutz und zum Umgang mit personenbezogenen Daten bei dem Einsatz eines Enterprise-Resource -Planning-Systems (ERP-Systems) in den sächsischen Hochschulen (außer der TU Dresden) “ abgeschlossen. Das SMWK hat diese Musterdienstvereinbarung erarbeitet und mit dem HPR und den behördlichen Datenschutzbeauftragten der Hochschulen sowie dem Sächsischen Datenschutzbeauftragten abgestimmt.

Bestandteile dieser Musterdienstvereinbarung sind insbesondere die Regelungen zum Datenschutz nach der neuen DSGVO, wie beispielsweise das Verzeichnis der Verarbeitungstätigkeiten gemäß Artikel 30 DSGVO, die Anlage zur Datenschutz-Folgeabschätzung nach Artikel 35 DSGVO und die Regelungen der Rechte der Beschäftigten gemäß DSGVO. Aber auch die Informationssicherheit wie die Gewährleistung der Sicherheit der personenbezogenen Daten durch organisatorische und technische Maßnahmen ist Bestandteil dieser Musterdienstvereinbarung. Sie können von den Hochschulen als Vorlage verwendet werden und an die spezifischen Gegebenheiten der Hochschule angepasst werden. Diese Dienstvereinbarungen zum Datenschutz müssen durch die jeweiligen Hochschulen und die örtlichen Personalräte abgeschlossen werden, bevor personenbezogene Daten mit dem ERP-System verarbeitet werden.

In diesem Rahmen muss auch vor dem Produktivstart des ERP-Systems an der jeweiligen Hochschule eine Datenschutz-Folgenabschätzung gemäß Artikel 35 DSGVO durchgeführt werden. Bei der Durchführung ist der Datenschutzbeauftragte zu beteiligen. Ferner hat jede Hochschule gemäß Artikel 30 DSGVO ein Verzeichnis der Verarbeitungstätigkeiten für das ERP-System zu führen. Der vollständige Text der Vereinba-

rung kann dem folgenden Link entnommen werden: http://www.smwk.sachsen.de/download/HPR_MDV_Datenschutz_ERP.pdf

Die Projektleitung des SMWK und die Hochschulen haben die Datenschutzbeauftragten frühzeitig informiert und konstruktiv in die Planung des ERP-Systems einbezogen. Sie werden weiterhin gemeinsam darauf hinwirken, dass diese Musterdienstvereinbarung und die Regelungen zum Datenschutz an den Hochschulen bis zum Start des Roll-Out umgesetzt und berücksichtigt werden.

4.2 Gemeinsame Verantwortliche

4.2.1 Vorgänge im Berichtszeitraum

Gemeinsam Verantwortliche sind in Artikel 26 der Datenschutz-Grundverordnung geregelt worden. Artikel 4 Nummer 7 DSGVO enthält die Definition des „Verantwortlichen“ und legt gleichzeitig fest, dass die datenschutzrechtliche Verantwortung auch mehreren Verantwortlichen übertragen sein kann. Abzugrenzen ist das Rechtsinstitut von der Auftragsverarbeitung.

Im Bereich Social Media, dem Betreiben einer Facebook-Fanpage, hatte der Europäische Gerichtshof im Berichtszeitraum entschieden, dass Facebook und die Fanpage-Betreiber gemeinsam Verantwortliche sind, vergleiche auch den Tätigkeitsberichtsbeitrag unter 9.1. Auch wird die Vorschrift des Artikels 26 DSGVO in einer zunehmend vernetzten Informationsgesellschaft und häufiger werdenden informationstechnischen Zusammenarbeit zwischen Verantwortlichen im nicht-öffentlichen Bereich, aber auch im Verwaltungssektor an Bedeutung gewinnen, selbst wenn damit regelmäßig auch eine (nicht gewollte) gesamtschuldnerische Rechtslage verbunden sein wird.

Im letzten Berichtszeitraum gingen bei meiner Behörde allerdings bisher noch wenige Anfragen zu gemeinsam Verantwortlichen und damit zusammenhängenden Rechtsvorgängen ein. Ein allein berichtenswerter Vorgang betraf die Videoüberwachung in Innenstadtbereichen von Chemnitz, bei dem die Einrichtung einer gemeinsamen Infrastruktur zur Videoüberwachung unter Beteiligung von drei Verantwortlichen erfolgte, die gemessen an ihren Aufgaben und divergierenden Zwecken der Verarbeitung jeweils erforderliche und unterschiedliche Zugriffe auf die durch die Chemnitzer Verkehrsbetriebe AG mittels eines Auftragsverarbeiters bereitgestellten Videobilddaten bekommen sollten. Beteiligt an dem Verfahren sind die Stadt Chemnitz, die C³ Chemnitzer Veranstaltungszentren GmbH der Stadt Chemnitz und die Chemnitzer Verkehrsbetriebe AG (CVAG). Darüber hinaus erfolgt auch zusätzlich eine Verarbeitung der Videodaten durch die Polizei als einer dem Richtlinienbereich und nicht der Datenschutz-Grundverordnung unterliegenden Stelle auf selbstständiger Rechtsgrundlage, vergleiche hierzu den ausführlichen Tätigkeitsberichtsbeitrag unter 8.1. Zum Ende des Berichts-

zeitraums war der datenschutzaufsichtliche Vorgang noch nicht abgeschlossen. Im nächsten Tätigkeitsbericht wird die Darstellung zu der gemeinsamen Videoüberwachung mit einer weitergehenden Betrachtung und Bewertung fortgesetzt.

4.3 Auftragsverarbeitung

4.3.1 Wann handelt es sich bei der technischen Wartung einer Videoüberwachungsanlage nicht um eine Auftragsverarbeitung?

Es wurde die Anfrage an mich herangetragen, ob es sich bei einer rein technischen Wartung der Videoüberwachungsanlage ohne Zugriff auf personenbezogene Daten, d. h. kein Zugriff auf den Server, kein Auslesen von Daten, um eine Auftragsverarbeitung handeln würde.

Eine Auftragsverarbeitung liegt vor, wenn eine Stelle im Auftrag des Verantwortlichen personenbezogene Daten verarbeitet (nach Artikel 4 Nummer 8 DSGVO).

Nach meiner Auffassung sind Wartungs- und Fernwartungsdienstleistungen vor genauso wie nach Inkrafttreten der DSGVO grundsätzlich als Auftragsverarbeitung anzusehen.

In der Beantwortung solcher Anfragen verweise ich auch auf das Kurzpapier Nummer 13 „Auftragsverarbeitung, Artikel 28 DSGVO“ der Datenschutzkonferenz.

Demnach handelt es sich im Hinblick auf die weite Definition einer Verarbeitung in Artikel 4 Nummer 2 DSGVO (z. B. Auslesen, Abfragen, Verwenden) bei einem Vertrag zwischen Verantwortlichem und Auftragsverarbeiter, in dem die IT-Wartung oder Fernwartung (z. B. Fehleranalysen, Support-Arbeiten in Systemen des Auftraggebers) Vertragsgegenstand ist und in dessen Rahmen für den Auftragsverarbeiter die Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten besteht, ebenfalls um eine Form oder Teiltätigkeit einer Auftragsverarbeitung und die Anforderungen des Artikel 28 DSGVO – wie etwa der Abschluss eines Vertrages zur Auftragsverarbeitung – sind umzusetzen.

Das Kurzpapier sieht aber hierfür auch eine Einschränkung vor – demzufolge liegt keine Auftragsverarbeitung und somit eine Anwendung von Artikel 28 DSGVO vor, wenn es sich rein um eine technische Wartung der Infrastruktur einer IT durch Dienstleister handelt (z. B. Arbeiten an Stromzufuhr, Kühlung, Heizung), die nicht zu einer Qualifikation des Dienstleisters als Auftragsverarbeiter führt.

Da es sich nach den Ausführungen in der Anfrage bei der Wartung der Videoüberwachungsanlage um eine reine Betreuungs- und Reparaturtätigkeit handelte und personenbezogene Daten nur „beiläufig“ zur Kenntnis genommen werden konnten, lag aus mei-

ner Sicht keine Auftragsverarbeitung vor (vgl. Gola, DSGVO, Kommentar 2017, S. 178, Artikel 4 Rn. 60).

4.3.2 Übersetzungsdienstleistungen

Mehrere Anfragen bezogen sich auf Übersetzungsdienstleistungen und die Fragestellung, ob diese als Auftragsverarbeitung nach Artikel 28 DSGVO zu bewerten sind. Die Frage kann nicht pauschal beantwortet werden. Die Einordnung hängt einerseits vom Inhalt der zu übersetzenden Texte, also der Frage, ob es sich dabei (auch bzw. vor allem) um personenbezogene Daten handelt, ab. Andererseits ist zu berücksichtigen, welche Freiräume der Übersetzer bei seiner Tätigkeit hat, er sich also - wie etwa bei der Übersetzung amtlicher Dokumente - streng und wortgetreu am Original halten muss oder ob es letztendlich nur um eine sinngemäße Übertragung geht, bei der dem Übersetzer entsprechende Spielräume zugestanden werden. Auch wenn eine Privatperson ausschließlich sie selbst betreffende Dokumente oder Texte zur Übersetzung vorlegt, wird man nicht von einer Auftragsverarbeitung ausgehen können, soweit dieser nicht als Verantwortlicher der Datenschutz-Grundverordnung unterfällt, vergleiche Artikel 2 Absatz 2 Buchstabe c) DSGVO.

Für den ggf. erforderlichen Abschluss eines Auftragsverarbeitungsvertrages ist grundsätzlich der jeweilige Auftraggeber verantwortlich. Dieser muss auch die Einbeziehung entsprechender Sub-Auftragnehmer genehmigen, Artikel 28 Absatz 2 DSGVO. In Bezug auf die insoweit abzuschließenden Vereinbarungen verweist meine Dienststelle auf Artikel 28 Absatz 4 DSGVO. Handelt es sich um Subauftragnehmer in Ländern außerhalb der EU bzw. des EWR sind dabei die Vorschriften des Kapitels V der Datenschutz-Grundverordnung, insbesondere Artikel 45, 46 und 49 DSGVO, zu beachten.

4.3.3 Lohn und Gehaltsabrechnung durch Steuerberater - Frage der Auftragsverarbeitung

Mehrere Anfragen betrafen die Problematik der Lohn und Gehaltsabrechnung durch Steuerberater und die Frage, ob diese Tätigkeit eine Auftragsverarbeitung darstellt.

Nach der Spruchpraxis des Sächsischen Datenschutzbeauftragten ist die Lohn- und Gehaltsabrechnung, soweit sie durch Steuerberater erfolgt, kein Gegenstand einer Auftragsverarbeitung. Eine gemeinsame explizite Position der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu der Thematik steht zwar aus. Zu verweisen ist dennoch auf das schon bestehende Kurzpapier Nummer 13 zur Auftragsverarbeitung, das seitens der Datenschutzkonferenz abgestimmt worden ist: In Anhang B wird dargestellt, dass keine Auftragsverarbeitung vorliegt, soweit die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen, für die

bei der Verarbeitung personenbezogener Daten eine Rechtsgrundlage gemäß Artikel 6 DSGVO gegeben sein muss, vorliegt. Beispielhaft genannt werden hierbei Berufsgeheimnisträger und auch Steuerberater.

Ausschlaggebend ist aus Sicht meiner Behörde, dass der Steuerberater nach seinem Berufsrecht eigene und damit originäre Verantwortung für den Inhalt der Lohn- und Gehaltsabrechnung zu leisten hat. Der Steuerberater haftet und attestiert für die inhaltlichen Ergebnisse seiner Leistung weitergehender, auch wenn andere Dienstleister, denen berufsrechtlich nicht versagt ist, sich auf Weisungen ihrer Mandantschaft zu berufen, über die Möglichkeit verfügen mögen, im Wege der Auftragsverarbeitung die Lohn- und Gehaltsabrechnung zu betreiben. Es besteht Gestaltungsfreiheit im Privatrecht. Soweit der Steuerberater zum Beispiel ein Unternehmen oder eine Lohn- und Gehaltsabrechnungsstelle ausgliedert, in der Steuerberater nicht berufsständisch auftreten, ist das Geschäftsmodell auch im Wege der Auftragsbearbeitung umsetzbar.

Bei der Lohn- und Gehaltsabrechnung, da diese einkommenssteuergesetzlich die Einbehaltung vom Bruttolohn einschließt, werden allerdings steuerrechtliche Tatbestände offengelegt und übermittelt. Aufgrund der Rechtslage in Deutschland zählen dazu also neben möglichen Gesundheitsinformationen auch die Informationen zur Veranlagung und Abführung der Kirchensteuer, die nach meiner Einschätzung als besondere Kategorien personenbezogener Daten im Sinne von Artikel 9 Absatz 1 DSGVO anzusehen sind.

Aufgrund der Notwendigkeit der einheitlichen und gleichmäßigen Datenverarbeitung im Bereich der Lohn- und Gehaltsabrechnung durch den Arbeitgeber scheidet in der Praxis eine ausdrückliche Einwilligung der Arbeitnehmer in Datenübermittlungen und Bearbeitungen durch einen externen Dienstleister aus. Es besteht also die Erforderlichkeit einer belastbaren gesetzlichen Übermittlungsgrundlage. Die Frage der zulässigen Datenübermittlung ist dabei aufgrund der Verschränkungen der relevanten Vorschriften mit Artikel 9 DSGVO nicht einfach zu beantworten. Umgekehrt führt aber dieses Problem nicht zu einer Anwendbarkeit der Auftragsverarbeitungsregeln, siehe oben.

Eine Anwendbarkeit von § 26 Absatz 3 BDSG halte ich für durchführbar. Zunächst kann nach meiner Überzeugung aufgrund der Vorschrift eine Übermittlung seitens des Arbeitgebers an den empfangenden Verantwortlichen, der die ausgelagerte Lohn- und Gehaltsabrechnung durchführen soll, gerechtfertigt werden. Das betrifft dabei zunächst die Phase der Datenübermittlung. Auch wenn die Lohn- und Gehaltsabrechnung seitens der Steuerberater zu eigenen Geschäftszwecken erfolgt und nicht zu den Zwecken des Arbeitgebers, dient die Leistung, die Verarbeitung der bereitgestellten Daten, eben gerade auch der Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, die arbeitgeberseitig

zu erfüllen sind. Ob die Anwendbarkeit des Artikels 26 DSGVO zu bejahen ist, kann zunächst offen bleiben.

Auch für den Fall, dass die Lohn- und Gehaltsabrechnung nicht im Wege der Auftragsbearbeitung sondern als steuerberaterische Leistung erfolgt, wären daher nach sämtlichen oben gemachten Überlegungen vertragliche Vereinbarungen erforderlich, die sicherstellen, dass die Grundsätze der Verarbeitung personenbezogener Daten gemäß Artikel 5 DSGVO durch den beauftragten Steuerberater eingehalten werden. Insbesondere ist die Zweckbestimmung der Datenübermittlung bzw. des Datenempfangs vertraglich eindeutig zu regeln. Die Beschäftigten der beauftragenden Unternehmen sind im Wege der Informationspflicht gemäß Artikel 13 DSGVO über die zum Teil ausgelagerte Personalverwaltung in Form der Lohn- und Gehaltsabrechnung zu unterrichten. Zertifizierungen im Sinne von Artikel 42 Datenschutz-Grundverordnung werden meinerseits in Bezug auf tätige Steuerberater nicht verlangt.

4.3.4 Frage der rechtlichen Einordnung als Auftragsverarbeitung bei Sicherheitstests

Meiner Behörde ist die Frage gestellt werden worden, ob sogenannte „Penetrationstests“ als Auftragsverarbeitung zu werten sind.

Nach der Rechtslage sind geeignete technische und organisatorische Maßnahmen zum Schutz der Daten seitens Verantwortlicher zu ergreifen und diese auch zu dokumentieren. Meine Behörde bezieht sich hierbei auch ausdrücklich auf die Vorschrift des Artikels 5 Absatz 1, Absatz 2 DSGVO. Die Vorschrift korrespondiert mit Artikel 32 DSGVO und auch mit dem betroffene Personen schützenden Artikel 25 der Datenschutz-Grundverordnung. Artikel 25 legt Prinzipien fest, wie personenbezogene Datenverarbeitung zum Schutz des Einzelnen gestaltet sein muss und welche Voreinstellungen vorzunehmen sind. Die Vorschrift des Artikels 32, die nicht auf den Schutz des Einzelnen, sondern die Systemsicherheit bezogen ist, präzisiert zu ergreifende Maßnahmen. Artikel 32 Absatz 1 Buchstabe d) Datenschutz-Grundverordnung sieht neben der Implementierung und Durchführung technischer und organisatorischer Maßnahmen in Bezug auf die Verfügbarkeit, Vertraulichkeit und Integrität der Systeme vor, dass die tatsächliche Wirksamkeit der Maßnahmen durch geeignete Verfahren nachzuweisen sind.

Somit wäre als Zwischenergebnis festzuhalten, dass sogenannte „Penetrationstests“, also Verfahren mit denen gezielt ein Angriff auf IT-Systeme und Anwendungen zum Zweck der Identifizierung von Schwachstellen der Systeminfrastruktur erfolgt, ausdrücklich auf Vorschriften der Datenschutz-Grundverordnung gestützt werden können.

Hinzuzufügen ist, dass neben der bloßen Identifikation von Sicherheitslücken bei komplexen IT-Systemstrukturen gegebenenfalls erst hierdurch Maßnahmen zur Erhöhung der technischen Sicherheit sowie in personeller und organisatorischer Hinsicht entwickelt werden können.

Zusätzlich zu den technischen Eingriffen, internen und externen Zugriffen, die durch Penetrationstests erfolgen, können auch Maßnahmen durchgeführt werden, um die Einhaltung von Sicherheitsrichtlinien und das Sicherheitsbewusstsein der Beschäftigten zu prüfen, sogenannte „Social Engineering-Tests“.

Aufgrund durchgeführter Testmaßnahmen besteht, je nach Auftrag, die Möglichkeit, dass seitens eines Auftragnehmers, der die Tests durchführt, personenbezogene Daten erlangt, ausgelesen oder auf irgendeine Weise verarbeitet werden. Ist dies nicht auszuschließen, rate ich Verantwortlichen, den Auftragnehmer im Wege einer Auftragsverarbeitung zu binden, so dass dieser rechtlich nicht als Dritter handelt und der Auftraggeber Herr der Daten bleibt. Auch wenn Penetrationstests in der Praxis, wie zuvor dargestellt, durchaus gesetzlichen Zwecken dienen, hätte ich in Bezug auf personenbezogene Datenerhebungen durch den Auftragnehmer und Datenübermittlungen an diesen, auch zum Zweck der Durchführung der Analysen, Vorbehalte.

Bei der Auftragsverarbeitung handelt es sich eigentlich um eine vertragliche technische Hilfsdienstleistung, die die Verwahrung, die Pflege, das Einsammeln oder eine sonstige personenbezogene Datenverarbeitung zum Hauptgegenstand hat. Zudem ist der Auftragnehmer weisungsgebunden und der Auftraggeber steuert weiterhin die Datenverarbeitung und bestimmt sie inhaltlich. Bei Wartungsverträgen und Penetrationstests ist die Verarbeitung der personenbezogenen Daten eigentlich nicht Kern des Vertrags. Gleichwohl weiß der Auftraggeber von der Möglichkeit der Offenlegung und beauftragt quasi „mit bedingtem Vorsatz“.

So halte ich es für interessengerecht und erforderlich, den Auftraggeber für den Fall der Kenntnisnahme personenbezogener Daten aus dem Bereich des Auftraggebers zu binden, wie bei einer Auftragsverarbeitung. Ich empfehle praktisch, einen ergänzenden Standard-Auftragsverarbeitungsvertrag zu verwenden, der auf den Hauptvertrag referenzieren kann. Vertraglich sollte darin konkret festgelegt sein, wie mit personenbezogenen Daten, für den erwartbaren oder unerwarteten Fall, dass diese aus der Sphäre des Auftraggebers empfangen oder offengelegt werden, nach Weisung des Auftraggebers umgegangen wird bzw. dass die Informationen nach Abschluss der Testmaßnahmen und Berichterstattung gegenüber dem Verantwortlichen übergeben oder ordnungsgemäß gelöscht werden.

4.4 Verzeichnis von Verarbeitungstätigkeiten, Kooperationspflicht mit der Aufsichtsbehörde

4.4.1 Hilfen zur Anfertigung des Verzeichnisses

Für Verantwortliche und Auftragsverarbeiter hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) Anwendungshinweise herausgegeben, die über die Internetpräsenz der Datenschutzkonferenz beziehbar sind. Darüber hinaus ist auf das Kurzpapier Nummer 1 – Verzeichnis von Verarbeitungstätigkeiten – Artikel 30 DSGVO hinzuweisen.

Zu Datenschutz-Folgenabschätzungen – Artikel 35 DSGVO – vergleiche Beitrag 4.7.1, unten.

4.5 Sicherheit der Verarbeitung

4.5.1 Unverschlüsseltes Kontaktformular auf der Internetseite einer Rechtsanwaltskanzlei

In dem Berichtsbeitrag 4.1.3, vergleiche oben, wurde dargestellt, wie Internetseiten verordnungskonform einzurichten sind. Tatsächlich sind den technisch-organisatorischen Anforderungen und der Sicherheit der Verarbeitung nicht genügende Internetpräsenzen häufiger Anlass meiner Behörde, datenschutzaufsichtlich tätig zu werden.

In einem Fall wurde meine Dienststelle durch einen Hinweis auf die unverschlüsselte Bereitstellung eines Kontaktformulars auf der Webseite einer Rechtsanwaltskanzlei aufmerksam gemacht. Nachdem der Hinweis verifiziert werden konnte, forderte meine Behörde die Anwaltskanzlei daraufhin auf, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Datenschutzrisiko angemessenes Schutzniveau mittels einer Verschlüsselung herzustellen. Artikel 32 Absatz 1 Buchstabe a) DSGVO regelt, dass Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen haben, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem auch die Verschlüsselung personenbezogener Daten ein.

Die Einrichtung einer SSL-Verschlüsselung entspricht dem Stand der Technik und ist ohne besonderen Aufwand umsetzbar. Ein unverschlüsselt bereitgestelltes Kontaktformular auf der Internetseite eines Berufsgeheimnisträgers, das der Erhebung personenbezogener Daten dient, ist hingegen nicht als im Einklang mit Artikel 32 Absatz 1 Buchstabe a) DSGVO zu betrachten, vergleiche auch Artikel 25 Absatz 1 DSGVO.

4.6 Meldung von Datenschutzverletzungen

4.6.1 Meldungen von Datenpannen im Berichtszeitraum – Ein erstes Resümee der Eingänge

Nach Artikel 33 DSGVO sind Verantwortliche verpflichtet, im Falle der Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung diese der Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Eine der Meldepflicht nach Artikel 33 DSGVO entsprechende Pflicht zur Information der Aufsichtsbehörde war im Bundesdatenschutzgesetz alte Fassung (BDSG a. F.) in § 42a geregelt.

Im Berichtszeitraum (25.05. bis 31.12.2018) sind bei mir über 200 solcher Meldungen eingegangen. Im Vergleich zum Zeitraum vor Geltung der Datenschutz-Grundverordnung sind damit die Meldungen um das Zehnfache gestiegen.

Diese massive Erhöhung der Meldungen ist meines Erachtens auf folgende Ursachen zurückzuführen:

- Der meldepflichtige Bereich von Datenpannen wurde mit Geltung der Datenschutz-Grundverordnung im Vergleich zum Bundesdatenschutzgesetz alte Fassung erweitert. Nach § 42a BDSG a. F. war die unrechtmäßige Datenübermittlung oder sonstige unrechtmäßige Kenntniserlangung Dritter meldepflichtig. Artikel 33 DSGVO hat die Meldepflicht nunmehr allgemein auf den Eintritt einer Verletzung des Schutzes personenbezogener Daten erweitert. Was hierunter zu verstehen ist, wird durch die Legaldefinition in Artikel 4 Nummer 12 DSGVO näher konkretisiert. Eine Verletzung des Schutzes personenbezogener Daten umfasst eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Damit ist der meldepflichtige Bereich wesentlicher weiter gefasst.

- Ein weiterer Grund für die Erhöhung der Meldungen liegt darin begründet, dass Artikel 33 DSGVO im Vergleich zu § 42a BDSG a. F. grundsätzlich jede Art von personenbezogenen Daten erfasst und nicht mehr auf besondere Kategorien beschränkt ist. Hierdurch wurde der Anwendungsbereich meldepflichtiger Datenpannen objektiv massiv erweitert.

- Nach § 42a BDSG a. F. musste stets mit einer Datenpanne eine schwerwiegende Beeinträchtigung für die Rechte oder schutzwürdigen Interessen der Betroffenen verbunden sein. Artikel 33 DSGVO sieht nunmehr lediglich noch einen Ausschluss der Meldepflicht vor, wenn die Datenpanne voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Insoweit ist festzuhalten, dass die Tatbestandsvoraussetzung für die Annahme eines Risikos für die Rechte und Freiheiten natürlicher Personen geringere Anforderungen stellt als für eine schwerwiegende Beeinträchtigung für die Rechte oder schutzwürdigen Interessen der Betroffenen, was wiederum eine Ursache für die Zunahme von Meldungen darstellt. Hinsichtlich des Risikobegriffs verweise ich auf die näheren Ausführungen im Kurzpapier Nummer 18 der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz - DSK).

- Die Datenschutz-Grundverordnung richtet sich hinsichtlich des Verantwortlichen sowohl an öffentliche wie auch an nichtöffentliche Stellen. § 42a BDSG a. F. begründete für meinen Geltungsbereich lediglich eine Informationspflicht gegenüber nichtöffentlichen Stellen. Das Sächsische Datenschutzgesetz (SächsDSG) enthielt dagegen keine Meldepflicht gegenüber öffentlichen Stellen, so dass bzgl. öffentlicher Stellen vor Geltung der Datenschutz-Grundverordnung lediglich aufgrund vereinzelter spezialgesetzlicher Informationspflichten (z.B. für Sozialleistungsträger gemäß § 83a SGB X) eine Meldepflicht bestand. Somit ist auch bzgl. des Adressatenkreises festzuhalten, dass die Datenschutz-Grundverordnung den Anwendungsbereich erweitert hat.

- Abschließend sind noch zwei Punkte zu erwähnen, die wohl auch maßgeblich zur Erhöhung der Meldungen beigetragen haben. Dies ist zum einen, dass die mit der Einführung der Datenschutz-Grundverordnung verbundene öffentliche Berichterstattung über das Thema Datenschutz im Allgemeinen und deren (neue) Pflichten im Besonderen zum Teil erstmals das Bewusstsein über das Bestehen einer solchen Meldepflicht hervorgerufen hat, obgleich eine Informationspflicht bereits unter Geltung des Bundesdatenschutzgesetzes alte Fassung schon bestand. Zum anderen wird die Tatsache, dass der Bußgeldrahmen bei Verstößen gegen datenschutzrechtliche Vorgaben (u.a. eben auch Meldepflichten) mit Geltung der Datenschutz-Grundverordnung erheblich erweitert wurde, eine wichtige Rolle spielen, so dass auch hierin eine Ursache für die Zunahme der Meldungen gesehen werden kann.

Hinsichtlich der im Berichtszeitraum eingegangenen Meldungen von Datenpannen gemäß Artikel 33 DSGVO sind folgende Fallgruppen besonders häufig vorgekommen, die sowohl den öffentlichen wie auch den nichtöffentlichen Bereich betreffen:

1. Fehlversand von Unterlagen

Die häufigste Fallgruppe der Meldungen von Datenpannen gemäß Artikel 33 DSGVO ist der Fehlversand von Unterlagen. Die Kategorien der betroffenen personenbezogenen Daten umfasst von einfachen Kontaktdaten, über Daten zu Vertragsbeziehungen bis hin zu Bank- und Gesundheitsdaten jeden Bereich. Auch die Ursachen, die den Fehlversendungen zu Grunde liegen, sind vollkommen vielschichtig und betreffen jede nur denkbare Fehlerquelle sowie jeden Transportweg (Post, Fax oder E-Mail). Eine häufige Ursache ist z.B. die einfache Verwechslung der Empfängerperson bei (Nach-) Namensgleichheit. Eine weitere Ursache sind fehlerhaft hinterlegte Kontaktdaten, was bei Verwendung von Fax und E-Mail regelmäßig und bei Post gelegentlich (in der Regel kommt es hier zu Rückläufern) zu einer falschen Zustellung an einen unberechtigten Dritten führt. Ebenfalls eine häufige Fehlerquelle ist die automatisierte Kuvertierung, bei der mehrere Briefbögen lediglich einem Briefumschlag beigefügt werden und somit zu einer fehlerhaften Zustellung führen. Auch die nichtautomatisierte, händische Kuvertierung von „Massenpost“ ist eine häufige Fehlerquelle, bei der es zur gleichen Fehlzustellung wie zuvor beschrieben kommen kann.

2. Verwendung eines offenen E-Mail-Verteilers

Des Weiteren stellt häufig die Verwendung eines offenen E-Mail-Verteilers eine meldepflichtige Datenschutzverletzung dar. Mindestens dann, wenn sich die E-Mail-Adressen vor der Domain-Angabe aus Vornamen und Nachnamen zusammensetzen, handelt es sich um personenbezogene Daten, für deren Übermittlung regelmäßig gerade keine Rechtsgrundlage gegeben ist. In Abhängigkeit des Adressatenkreises ist hierin dann ein Risiko für die Rechte und Freiheiten natürlicher Personen zu sehen.

3. Einbruch und Diebstahl

Ebenfalls eine häufige Fallgruppe der meldepflichtigen Datenschutzverletzungen geht mit Einbrüchen und/oder Diebstählen einher. Bereits bei einem Einbruch kann es bei nicht ordnungsgemäß verwahrten Unterlagen zu einer unberechtigten Kenntnisnahme von personenbezogenen Daten kommen verbunden mit dem entsprechenden Risiko für die Rechte und Freiheiten natürlicher Personen. Noch wesentlich höher ist dagegen das Risiko zu bewerten, wenn es ggf. in Verbindung mit einem Einbruch zu Diebstählen von Unterlagen oder ungesicherten digitalen Datenträgern kommt, da in diesen Fällen die kriminelle Zielrichtung oftmals unmittelbar auf die personenbezogenen Daten gerichtet ist.

4. Allgemein der Verlust von Unterlagen oder Datenträgern

Neben den Datenschutzverletzungen durch Verlust von Unterlagen oder Datenträgern aufgrund kriminellen Eingriffs (z.B. durch Diebstähle) ist eine häufige Fallgruppe auch der Verlust durch anderweitige Umstände, wie z.B. das Verlieren von USB-Sticks, das Verlorengehen von Unterlagen bei Umzügen oder sogar der Verlust infolge eines Brandes. Das Risiko für die Rechte und Freiheiten natürlicher Personen kann sich hier – ausgenommen der Brand – in einer möglichen Kenntnisnahme der personenbezogenen Daten durch unberechtigte Dritte realisieren, aber auch in einer möglicherweise nicht mehr bestehenden Verfügbarkeit der personenbezogenen Daten, wenn entsprechende Sicherungsmaßnahmen fehlen.

5. Weitere Fallgruppen

Weitere Fallgruppen sind der Verlust von Unterlagen auf dem Postweg oder durch den Eingriff/die Zerstörung von Briefkästen durch Dritte, die fehlerhafte Speicherung von personenbezogenen Daten in einem internen Netzwerk mit der damit verbundenen Möglichkeit des Zugriffs durch unberechtigte Mitarbeiter oder die Fälle von Hackerangriffen im weitesten Sinne, wie z.B. Erpressungstrojaner, Phishingfälle oder allgemein der unberechtigte Zugriff auf Datenbanken oder Onlinedienste.

Zur Vermeidung solcher Meldefälle ist es stets ratsam, sich mit den erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten auseinander zu setzen. Soweit die Meldefälle auf menschliches Versagen zurückzuführen sind, ist es stets erforderlich, die involvierten Personen bzgl. entsprechender Fehlerquellen zu sensibilisieren sowie technische Vorkehrungen zur Vermeidung zu implementieren. Des Weiteren ist die Thematik der Datensicherheit von erheblicher Bedeutung und insbesondere unter Berücksichtigung des Risikos in fachkundige Hände zu geben.

Des Weiteren weise ich abschließend auf die neben der grundsätzlich bestehenden Rechenschaftspflicht gemäß Artikel 5 Absatz 2 DSGVO im Besonderen für die Meldefälle bestehende Dokumentationspflicht nach Artikel 33 Absatz 5 DSGVO sowie auf die mögliche Pflicht der Benachrichtigung der betroffenen Person nach Artikel 34 DSGVO hin.

4.7 Datenschutz-Folgenabschätzung

4.7.1 Liste der Verarbeitungstätigkeiten gemäß Artikel 35 Absatz 4 DSGVO

Gemäß Artikel 35 Absatz 4 Datenschutz-Grundverordnung hat die Datenschutzaufsichtsbehörde eine Liste der Verarbeitungsvorgänge, für die gemäß Artikel 35 Absatz 1

Datenschutz-Grundverordnung eine Datenschutz-Folgenabschätzung durchzuführen ist, zu veröffentlichen. Eine entsprechende Liste mit Erläuterungen wurde auf meiner Internetseite veröffentlicht (https://www.saechsdsb.de/liste-verarbeitungsvorgaenge-dsfa).

Der Inhalt der Liste ist zwischen den Datenschutzaufsichtsbehörden abgestimmt worden. Überarbeitungen und Fortschreibungen der Liste sind vorgesehen.

Zum Verzeichnis der Verarbeitungstätigkeiten, vgl. 4.4.1.

4.8 Datenschutzbeauftragte

4.8.1 Benennungspflicht Datenschutzbeauftragter in Arztpraxen, Mitzählung des Praxisinhabers

Etliche Ärzte und Apotheker baten mich um Stellungnahme, ob nach dem Inkrafttreten der DSGVO für ihre Arztpraxis bzw. Apotheke eine gesetzliche Pflicht besteht, einen Datenschutzbeauftragen (DSB) benennen.

Nach Artikel 37 Absatz 1 Buchstabe c DSGVO benennen der Verantwortliche und der Auftragsverarbeiter auf jeden Fall einen DSB, wenn die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 besteht.

Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c DSGVO ist § 38 BDSG anzuwenden, wonach der Verantwortliche und der Auftragsverarbeiter einen DSB benennen müssen, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Die Verarbeitung personenbezogener Daten muss nicht die Hauptaufgabe der jeweiligen Mitarbeiter sein. Das Tatbestandsmerkmal „ständig“ ist selbst dann erfüllt, wenn die Aufgabe nur gelegentlich (z. B. einmal im Monat) anfällt.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat anlässlich der Tagung am 26. April 2018 in Düsseldorf zur Bestellpflicht nach Artikel 37 Absatz 1 Buchstabe c Datenschutz-Grundverordnung (DSGVO) bei Arztpraxen, Apotheken und sonstigen Gesundheitsberufen folgende Entschließung gefasst:

1. Betreibt ein einzelner Arzt, Apotheker oder sonstiger Angehöriger eines Gesundheitsberufs eine Praxis, Apotheke oder ein Gesundheitsunternehmen 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 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 Artikel 37 Absatz 1 Buchstabe c DSGVO 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 DSB zu benennen. Dies kann neben einer umfangreichen Verarbeitung (z. B. große Praxisgemeinschaften), die ohnehin nach Artikel 37 Absatz 1 Buchstabe c DSGVO zu einer Benennungspflicht führt, beispielsweise beim Einsatz von neuen Technologien, die ein hohes Risiko mit sich bringen, der Fall sein. Der DSB 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 Absatz 1 StGB auszulegen und umfasst die in § 203 Absatz 1 Nummer 1, 2, 4 und 5 StGB aufgezählten Berufsbilder.

4.8.2 Benennung juristischer Personen als Datenschutzbeauftragter

Mehrfach ist meiner Behörde die Frage gestellt worden, ob juristische Personen als Datenschutzbeauftragte gemäß Artikel 37 DSGVO benannt werden können. Zurückliegend hatten die deutschen Datenschutzaufsichtsbehörden dazu einhellig die Auffassung vertreten, dass angesichts der auf eine einzelne geeignete Person abzielenden gesetzlichen Anforderungen an Datenschutzbeauftragte, eine Bestellung juristischer Personen unzulässig sei. Die Artikel 29-Gruppe als Vorgänger des Europäischen Datenschutzausschusses

hingegen ging von der Zulässigkeit der Benennung einer juristischen Person unter der Bedingung aus, dass jedes Mitglied der juristischen Person, dass die Funktion eines Datenschutzbeauftragten wahrnimmt, sämtliche im 4. Abschnitt der Datenschutz-

Grundverordnung genannten Anforderungen zu erfüllen in der Lage ist. Einige deutsche Datenschutzaufsichtsbehörden haben diese Auffassung ausdrücklich geteilt. Der Europäische Datenschutzausschuss hat das zurückliegende Votum nachträglich bestätigt.

Ich akzeptiere allein aus Gründen der Rechtseinheitlichkeit Benennungen von juristischen Personen als Datenschutzbeauftragten Verantwortlicher. Die Benennung geeigneter natürlicher Personen wird nachhaltig empfohlen. Gemessen an der Entscheidung des Europäischen Datenschutzausschusses, dass die für die juristische Person handelnden und die Aufgaben des Datenschutzbeauftragten ausführenden Personen sämtliche Voraussetzungen des 4. Abschnitts der Datenschutz-Grundverordnung zu erfüllen geeignet sein müssen, sind zudem die mit der Aufgabenwahrnehmung betrauten natürlichen Personen intern zu dokumentieren und auf Anforderung der Aufsichtsbehörde vorzulegen, vergleiche Artikel 24 Absatz 1 DSGVO.

Bisher haben nur in wenigen Fällen Verantwortliche meiner Behörde die Benennung einer juristischen Person als Datenschutzbeauftragten angezeigt.

4.8.3 Pflicht zur Veröffentlichung von Namensangaben des Datenschutzbeauftragten nach Artikel 37 Absatz 7 DSGVO

Im letzten Berichtszeitraum wurde meine Dienststelle angefragt, ob die Veröffentlichung von Namensangaben bzw. personenbezogenen Kontaktdaten des benannten Datenschutzbeauftragten im Einklang mit der Datenschutz-Grundverordnung stehe. Zutreffend ist, dass gemäß des Wortlauts des Artikel 37 Absatz 7 DSGVO der Verantwortliche oder der Auftragsverarbeiter die „Kontaktdaten des Datenschutzbeauftragten" zu veröffentlichen hat. Nicht notwendigerweise enthalten die erforderlichen Kontaktdaten die Namensangaben des Datenschutzbeauftragten. Auch in der Praxis verfahren einzelne öffentliche und nicht-öffentliche Verantwortliche in der Weise, dass keine Namensangaben aber zum Beispiel Rufnummern und E-Mail-Funktionsadressen angegeben werden.

Auch wenn die Datenschutz-Grundverordnung die Mindestanforderungen in der vorgenannten Weise festgelegt hat, bedeutet dies nach meiner Überzeugung nicht, dass eine Veröffentlichung der Namensangaben des benannten Datenschutzbeauftragten mangels Erforderlichkeit rechtswidrig wäre. Gegen eine namentliche Nennung des benannten Datenschutzbeauftragten bestehen seitens meiner Behörde keine rechtlichen Bedenken, erst recht nicht in den Fällen, in denen Bedienstete öffentlicher Stellen als Amtsträger mit der Funktion beauftragt worden sind.

4.8.4 Stellvertretender Datenschutzbeauftragter

Im Berichtszeitraum ist an meine Behörde auch die Frage gerichtet worden, ob stellvertretende Datenschutzbeauftragte gemäß Artikel 37 Absatz 7 DSGVO der Datenschutzaufsichtsbehörde mitzuteilen sind. Ich habe dies verneint.

Darüber hinaus ist an meine Dienststelle die Fragestellung herangetragen worden, ob stellvertretende Datenschutzbeauftragte über dieselben Befugnisse verfügen, wie der Datenschutzbeauftragte selbst, vergleiche Artikel 38 und 39 DSGVO. Grundsätzlich habe ich diese Frage bejaht.

4.8.5 Benennungspflicht bei hoheitlicher Tätigkeit – Beliehene*

Aufgrund von Anfragen hatte sich meine Behörde mit der Frage auseinanderzusetzen, ob eine Benennungspflicht von kleineren Unternehmen für Datenschutzbeauftragte bei hoheitlicher Tätigkeit besteht. So hatte meine Dienststelle unter anderem auch der Frage nachzugehen, ob Firmen, die mit Kraftfahrzeugzulassungen betraut sind, bspw. Sicherheitsüberprüfungen gemäß Anlage VIII c Nummer 1.1 StVZO durchführen und damit hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen, einen Datenschutzbeauftragten zu benennen haben. Die Frage wird seitens meiner Behörde dahingehend beantwortet, dass Beliehene, die insoweit als öffentliche Stellen gemäß § 2 Absatz 1 Satz 2 zu gelten haben, gemäß Artikel 37 Absatz 1 Buchstabe a) DSGVO unabhängig von der Beschäftigtenzahl – wie andere öffentliche Stellen auch – einen Datenschutzbeauftragten zu benennen haben. Auch auf den Umfang der öffentlich-rechtlichen Tätigkeit kommt es insoweit nicht an. Die Benennungspflicht besteht allerdings nur für die hoheitliche Tätigkeit. Die Vorschrift des § 38 Absatz 1 Satz 1 BDSG, wonach eine Benennungspflicht dann besteht, wenn in dem Unternehmen in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, kommt dann wieder zur Anwendung, soweit keine hoheitlichen Aufgaben erfüllt werden.

Im Ergebnis sind also Beliehene als öffentliche Stellen pflichtig, einen Datenschutzbeauftragten zu benennen. Dies betrifft sowohl Kfz-Betriebe, wie in dem Beispielsfall, als auch häufig Einzelpersonen, wie öffentlich-rechtlich bestellte Prüfingenieure und Bausachverständige, öffentlich-rechtlich bestellte Vermessungsingenieure oder Bezirksschornsteinfeger. In der Praxis schließen sich die betroffenen Bereiche über Berufsverbände oder berufsständische Körperschaften zusammen, um der Benennungspflicht eines Datenschutzbeauftragten nachzukommen.

4.8.6 Benennungspflicht - Merkmale des § 38 Absatz 1 BDSG „in der Regel“ und „ständig beschäftigt“

§ 38 Absatz 1 BDSG enthält ergänzende Festlegungen zur Benennungspflicht eines Datenschutzbeauftragten. Zu dieser Vorschrift erhielt meine Dienststelle sehr viele Nachfragen.

Zunächst sind bei der maßgeblichen Beschäftigtenzahl ausschließlich die Mitarbeiter oder weitere beim Unternehmen tätige Personen, z. B. Auszubildende, zu berücksichtigen. Unter anderem nicht ausschlaggebend sind Mitarbeiter bei Auftragsverarbeitern des Verantwortlichen.

Mit dem in § 38 Absatz 1 BDSG enthaltenen Merkmal „ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt“ wird nach meiner Überzeugung schlicht bestimmt, dass es sich um eine regelmäßig wiederkehrende Tätigkeit handelt, es aber nicht auf den Anteil der dafür aufgewendeten Arbeitszeit ankommt. Die Verarbeitung personenbezogener Daten muss also nicht Hauptaufgabe der jeweiligen Mitarbeiter sein. Das Tatbestandsmerkmal „ständig“ ist selbst dann erfüllt, wenn die Aufgabe nur gelegentlich, zum Beispiel einmal im Monat, anfällt.

Das weitere Merkmal „in der Regel“ ist an § 1 Betriebsverfassungsgesetz angelehnt und bedeutet, dass es auf kurzfristige Schwankungen des Personalbestandes nicht ankommt, sondern der mittlere tatsächliche Personalbestand über einen Betrachtungszeitraum von einem Jahr maßgeblich ist (vergleiche auch die Kommentierung von Kühling/Sackmann in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG 2. Aufl., Rdnr. 10 zu § 38 BDSG).

4.8.7 Qualifikation des Datenschutzbeauftragten

Mehrere Anfragen an meine Behörde betrafen das Thema der Qualifikation des benannten oder zu benennenden Datenschutzbeauftragten und welche Art von Ausbildung oder Qualifikation der Datenschutzbeauftragte eines Unternehmens aufzuweisen habe, um ordnungsgemäß benannt werden zu können.

Nach Artikel 37 Absatz 5 DSGVO ist ein betrieblicher Datenschutzbeauftragter auf der Grundlage seiner beruflichen Qualifikation und insbesondere seines Fachwissens auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der ihm nach Artikel 39 DSGVO obliegenden Aufgaben zu benennen. Die erforderliche Qualifikation des Datenschutzbeauftragten richtet sich nach Erwägungsgrund 97 in erster Linie nach den von dem Unternehmen durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz der verarbeiteten personenbezogenen Daten.

Darüber hinausgehende dezidierte Vorgaben zum Fachkundeerwerb hat der Verordnungsgeber nicht gemacht, insbesondere hat er auch keine speziellen Ausbildungen und Abschlüsse vorgeschrieben. Vor diesem Hintergrund haben Unternehmer, aber auch andere Verantwortliche bei der Auswahl geeigneter Weiterbildungsveranstaltungen also einen gewissen Spielraum, haben aber sicherzustellen, dass der zu benennende Datenschutzbeauftragte im spezifischen Unternehmensbereich bzw. Kontext der Anforderungen fachlich und persönlich zur Erfüllung seiner Aufgaben in der Lage ist.

Meiner Behörde gegenüber ist auch die Auffassung vertreten worden, dass es sich bei externen Datenschutzbeauftragten um Juristen bzw. kammerangehörige Volljuristen handeln müsse. Eine für Datenschutzbeauftragte erforderliche Sach- und Fachkunde kann nach Überzeugung meiner Behörde aber auch daneben bestehen. Die dahinter immer wieder aufgeworfene Frage, ob es sich bei der Tätigkeit des Datenschutzbeauftragten um Rechtsdienstleistungen handelt, die dieser nicht ohne Zugehörigkeit zu einem Berufsstand auszuüben befugt wäre, ist eine weitergehende und wäre gegebenenfalls durch den Bundesgesetzgeber einer abschließenden Klärung zuzuführen.

4.8.8 Reichweite der Überwachungsbefugnisse des benannten Datenschutzbeauftragten bei Betriebsrat und Personalvertretung

Zurückliegend bestand nach der Rechtsprechung des Bundesarbeitsgerichts – BAG, Beschluss vom 11. November 1997,1 ABR 21/97 – keine Kontrollbefugnis des betrieblichen Datenschutzbeauftragten nach alter Rechtslage bei Betriebsrat oder Personalvertretung. Geschlussfolgert wurde diese rechtliche Einschätzung mit der nach dem Betriebsverfassungsgesetz vorgeschriebenen Unabhängigkeit des Betriebsrats von dem Arbeitgeber und einer Gefährdung der unabhängigen Stellung im Falle der Ausübung von Kontrollrechten des Datenschutzbeauftragten gegenüber dem Betriebsrat. Der Datenschutzbeauftragte nehme insoweit keine „neutrale Stellung“ zwischen Arbeitgeber und Betriebsrat ein, da er vom Arbeitgeber ohne Beteiligungsrecht des Betriebsrats ausgewählt und bestellt werde und eine Pflicht des Datenschutzbeauftragten, aus seinem Amt ergebende Aufgaben zu erfüllen, nur gegenüber dem Arbeitgeber bestehe, nicht aber gegenüber betroffenen Personen. Selbst die Weisungsfreiheit und die Verschwiegenheitspflicht nach der alten bundesdatenschutzgesetzlichen Regelung führten nach Auffassung des Bundesarbeitsgerichts nicht dazu, dass eine Unterwerfung des Betriebsrats unter die Kontrollbefugnis des Datenschutzbeauftragten zu bejahen gewesen wäre. Eine Ausnahme des Betriebsrats von der Kontrollbefugnis nach dem Bundesdatenschutzgesetz ergebe sich, da das Verhältnis zwischen beiden Institutionen nicht gesetzlich geregelt worden sei.

Die Benennung und die Aufgaben und Befugnisse des Datenschutzbeauftragten sind nunmehr in der Datenschutz-Grundverordnung geregelt worden. Weiterhin finden sich

im die Verordnung ergänzenden Bundesdatenschutzgesetz keine Hinweise zur Reichweite der Überwachungsbefugnisse des Datenschutzbeauftragten. Dennoch stellt sich die Frage, ob nicht bereits die Datenschutz-Grundverordnung von einer lückenlosen Kontrolle bei Verantwortlichen ausgeht. Gegenüber der Datenschutz-Grundverordnung – im Gegensatz zum Bundesdatenschutzgesetz a. F. zuletzt – befindet sich auch das Betriebsverfassungsgesetz nicht mehr in einem gleichrangigen Verhältnis. Nach der Kommentierung von Kühling/Buchner zu Artikel 38 der Datenschutz-Grundverordnung sei davon auszugehen, dass gemäß Artikel 38 Absatz 2 Datenschutz-Grundverordnung den Datenschutzbeauftragten Zugang zu (allen) personenbezogenen Daten und Verarbeitungsvorgängen zu gewähren sei und es keine kontrollfreie Datenverarbeitung gebe. Erfasst sei dabei auch selbst die Datenverarbeitung durch Berufsgeheimnisträger, die der Kontrolle durch den Datenschutzbeauftragten unterläge. Ebensolches gelte für den Betriebsrat, vergleiche Kühling/Buchner DSGVO – BDSG – Kommentar, 2. Auflage, Art. 38, Rdnr. 18. Gerichtlich ist die Frage bisher noch nicht entschieden worden.

Ich schließe mich der in der erwähnten Kommentarliteratur dargestellten Auffassung an.

Entsprechendes gilt nach meiner Überzeugung auch für das Verhältnis der Datenschutzbeauftragten gegenüber Personalvertretungen bei Behörden.

Die vollständige Überwachungsbefugnis besteht auch gegenüber anderen weisungsfrei und autonom entscheidenden funktionalen Stellen innerhalb von Verantwortlichen, wie zum Beispiel bei Schwerbehinderten- und Gleichstellungsbeauftragten.

In allen Fällen hat der Datenschutzbeauftragte sich jedoch im Rahmen seiner Geheimhaltungs- und Vertraulichkeitspflicht zu bewegen, Artikel 38 Absatz 5 DSGVO.

4.9 Verhaltensregeln und Zertifizierung

4.9.1 Zertifizierung

Die DSGVO hat mit den Artikeln 42 und 43 die Grundlagen für eine einheitlich geregelte Zertifizierung von Produkten, Prozessen und Dienstleistungen für die Verarbeitung von personenbezogenen Daten geschaffen. Damit will der Unionsgesetzgeber sicherstellen, dass die Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Auch bislang gibt es zahlreiche, zum Teil phantasievolle Siegel und Zertifikate, welche Produkte oder Dienstleistungen als besonders datenschutzfreundlich kennzeichnen. Für den Verbraucher oder auch Verantwortliche war es dennoch schwer, diese Zusagen konkret einzuordnen und den Wert eines solchen Siegels oder Zertifikats zu bemessen.

Die DSGVO schafft nun die Voraussetzungen für ein geregeltes Verfahren unter Mitwirkung der Aufsichtsbehörden. Stellen, welche Zertifikate ausstellen wollen, müssen einen Akkreditierungsprozess durchlaufen, welcher zahlreiche Voraussetzungen an die Fachkunde und Unabhängigkeit der Zertifizierungsstelle überprüft und dauerhaft sicherstellen soll. Die Aufsichtsbehörden genehmigen die Kriterien, welche für eine Zertifizierung maßgeblich sind. Damit soll eine verlässliche Qualität erreicht werden, welche sowohl dem Bürger als auch Verantwortlichen bei der Auswahl geeigneter Produkte oder Dienstleistungen, z. B. im Rahmen der Auftragsverarbeitung, eine sichere Auswahlmöglichkeit eröffnet. Nicht zuletzt kann damit der oftmals bemühte „Datenschutz als Wettbewerbsvorteil“ in eine konkrete Anwendungsmöglichkeit überführt werden.

Um Zertifikate für Produkte, Prozesse und Dienstleistungen, bei denen personenbezogene Daten verarbeitet werden, ausgeben zu dürfen, muss sich die Zertifizierungsstelle akkreditieren lassen und sich in der Folge einem fortlaufenden Überwachungsprozess stellen. Als ersten Schritt muss eine potenzielle Zertifizierungsstelle der zuständigen Aufsichtsbehörde die Kriterien für die Zertifizierung zur Bewertung und Genehmigung vorlegen. Neben diesen Zertifizierungskriterien, welche anhand rechtlicher Maßstäbe geprüft werden, müssen Zertifizierungsstellen eine angemessene Qualifikation ihrer Beschäftigten, Unabhängigkeit und Unparteilichkeit sowie geeignete organisatorische Prozesse und Strukturen nachweisen. Diese formalen Anforderungen richten sich nach der internationalen Norm EN-ISO/IEC 17065/2012, welche Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren, allgemein normiert. Die Aufsichtsbehörden des Bundes und der Länder haben diese Norm um Datenschutz-Spezifika ergänzt. Auch bei weiteren ergänzenden Unterlagen stimmen sich die Aufsichtsbehörden eng ab, um Transparenz und Vergleichbarkeit bundesweit sicherzustellen.

Für den Prozess der Akkreditierung sind die Aufsichtsbehörden gemeinsam mit der Deutschen Akkreditierungsstelle zuständig. Die Deutsche Akkreditierungsstelle ist für die formale Antragsannahme und die Steuerung des Akkreditierungsprozesses zuständig. Die Aufsichtsbehörden prüfen und genehmigen die Zertifizierungskriterien und überprüfen Fachkunde und Unabhängigkeit der Antragsteller. Die zuständige Aufsichtsbehörde entscheidet gemeinsam mit der Deutschen Akkreditierungsstelle, ob alle Anforderungen erfüllt sind und eine Befugnis erteilt werden kann. Der Ablauf des Akkreditierungsprozesses unterteilt sich in mehrere Phasen:

- Antragsphase mit Prüfung der formalen Anforderungen und der Vollständigkeit der Unterlagen,
- Programmprüfung und Genehmigung der Kriterien,

- Akkreditierungsphase mit Begutachtung und Befugniserteilung und
- Überwachungsphase.

Auch nach einer erteilten Akkreditierung soll durch die Überwachung eine dauerhafte Sicherstellung der Qualität der Zertifizierungen aufrechterhalten werden.

5 Internationaler Datenverkehr

5.1 Zulässige Datenübermittlung

5.1.1 Konzernprivileg

Vereinzelt erhält meine Behörde Beratungsanfragen zum (grenzüberschreitenden) Datenaustausch innerhalb einer Unternehmensgruppe.

Die Datenschutz-Grundverordnung kennt, ebenso wie zuvor das Bundesdatenschutzgesetz a. F., kein Konzernprivileg. Jedoch erkennt Erwägungsgrund 48 das Interesse an einem Datenaustausch innerhalb einer Unternehmensgruppe ausdrücklich als berechtigt an. Datenflüsse, z. B. zu Verwaltungszwecken oder im Rahmen der Verarbeitung von Beschäftigten- oder Kundendaten, innerhalb eines Konzerns, d. h. zwischen für die Verarbeitung verantwortlichen Teilen einer Unternehmensgruppe, sind daher letztendlich leichter über eine Interessenabwägung zu rechtfertigen als solche an externe Dritte. „Unternehmensgruppen“, so die Terminologie der Datenschutz-Grundverordnung für Konzerne, haben also - und das wiederum ist der Unterschied zu den früheren Regelungen im Bundesdatenschutzgesetz – nun ein anerkanntes Interesse am (begrenzten) Datenaustausch, müssen aber durch entsprechende Verträge oder interne Regelungen einen ausreichenden Schutz der betroffenen Personen sicherzustellen. In Bezug auf mögliche Anerkennungsverfahren für verbindliche interne Datenschutzvorschriften ist auf Artikel 4 Nummer 20, Artikel 47 DSGVO zu verweisen. Zuständig ist insoweit die Datenschutzaufsichtsbehörde am Hauptsitz der Unternehmensgruppe.

6 Sächsischer Datenschutzbeauftragter – Tätigkeit, Aufgaben, Befugnisse

(Zur personellen Ausstattung des Sächsischen Datenschutzbeauftragten, siehe Beitrag 1.2 oben.)

6.1 Zuständigkeit

6.1.1 Verfahren bei Unzuständigkeit

Immer wieder wenden sich betroffene Personen an meine Dienststelle, obwohl andere deutsche Datenschutzaufsichtsbehörden allein oder federführend zuständig sind. Zu vermuten ist, dass viele betroffene Personen und Beschwerdeführer auch glauben, dass meine Behörde uneingeschränkt für Bürger mit Wohnsitz in Sachsen zuständig ist. Die Zuständigkeit richtet sich allerdings nach dem Sitz der datenverarbeitenden Stelle. Ich bin im Wesentlichen für die personenbezogene Datenverarbeitung der sächsischen Behörden und der in Sachsen belegenen nicht-öffentlichen Stellen zuständig, Artikel 55, 56 DSGVO, § 14 Absatz 1 und 2 SächsDSDG. Verfügen Unternehmen allerdings über mehrere Niederlassungen, ist auch die Aufsichtsbehörde zuständig, in deren Zuständigkeitsbereich die Hauptniederlassung angesiedelt ist. So erhält meine Behörde nicht selten im nicht-öffentlichen Bereich Beschwerden zu Kreditinstituten oder Versicherungsvertretungen, deren Hauptniederlassung sich nicht in Sachsen befindet. Im öffentlichen Bereich gehen hingegen immer wieder Beschwerden oder Petitionen zu Stellen der Bundesagentur bei meiner Dienststelle ein. Überwiegend sind die Vorgänge in dem nicht-öffentlichen Bereich an einen anderen Landesdatenschutzbeauftragten abzugeben. Für die Bundesbehörden ist wiederum der Bundesbeauftragte für Datenschutz und Informationsfreiheit zuständig.

Werden die Beschwerden per Online-Formular oder per E-Mail bei mir eingereicht, machen meine Bediensteten die Absender regelmäßig auf die Unzuständigkeit aufmerksam und teilen die Kontaktdaten der zuständigen Aufsichtsbehörde mit. Regelmäßig ist es den Beschwerdeführern in diesen Fällen möglich und zumutbar, sich selbstständig an die zuständige Behörde zu wenden. Gehen Schreiben auf dem herkömmlichen Briefpostweg ein, wird eine Abgabenachricht erteilt und die Sendung weitergeleitet.

6.1.2 Anbieterkennzeichnungspflicht, sog. „Impressumpflicht“

Zahlreiche Beschwerden und Hinweise beziehen sich allein auf die fehlende Anbieterkennzeichnung von Internetpräsenzen, vgl. § 5 Absatz 1 Telemediengesetz (TMG), ohne eine datenschutzrechtliche Beschwer darzutun.

Für die Frage der Anbieterkennzeichnungspflicht („Impressumpflicht“) nach dem Telemediengesetz ist meine Dienststelle nicht zuständig. Diesbezüglich abzuhelfen, soweit nicht auch die Informationspflichten gemäß Artikel 13, 14 DSGVO hiermit verbunden sind, ist keine meiner Behörde zugewiesene Aufgabe nach Artikel 55, 56 DSGVO.

Beschwerdeführer haben sich an die für die gemäß des Artikels 1 Absatz 2 des *Gesetzes zum Neunten Rundfunkänderungsstaatsvertrag und zur Änderung des Sächsischen Privatrundfunkgesetzes vom 24. Januar 2007 (SächsGVBl. S. 17)* für die nach § 59 Absatz 2 Rundfunkstaatsvertrag für die Einhaltung der Bestimmungen für Telemedien zuständige Landesdirektion Sachsen, Altchemnitzer Straße 41, 09120 Chemnitz, zu wenden. Regelmäßig verweise ich auf die Zuständigkeit der Landesdirektion.

Auch für den Fall einer Ordnungswidrigkeitenanzeige wegen eines Verstoßes gegen die Anbieterkennzeichnungspflicht verweise ich zuständigkeitshalber an die Landesdirektion Sachsen, § 4 Nummer 37 *Ordnungswidrigkeiten-Zuständigkeitsverordnung vom 16. Juni 2014 (SächsGVBl. S. 342), die durch Artikel 2 der Verordnung vom 26. Oktober 2015 (SächsGVBl. S. 627) geändert worden ist, für Ordnungswidrigkeitenverstöße gegen die Anbieterkennzeichnungspflicht in Verbindung mit § 16 Absatz 1 und 2 Nummer 1 des Telemediengesetzes (TMG) vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692) geändert worden ist, in der jeweils geltenden Fassung*. Ob der Bußgeldtatbestand überhaupt erfüllt sein könnte, kann seitens meiner Behörde wegen der Unzuständigkeit nicht geprüft werden.

6.1.3 Kurioses

Meine Dienststelle erreichen unzuständigerweise immer wieder Mitteilungen von Dritten, möglicherweise auch wegen unzureichender oder unvollständiger Informationen, Datenschutzerklärungen oder Kontaktinformationen Verantwortlicher oder weil die Absender die Kontaktdaten von zumeist im Internet verbreiteten Datenschutzinformationen fehlinterpretieren. Wenn Verantwortliche keine oder nur lückenhafte (E-Mail-)Kontaktdaten von sich bzw. des benannten Datenschutzbeauftragten in den für die betroffenen Personen gemäß Artikel 13 und 14 DSGVO vorgesehenen Informationen und Datenschutzerklärungen im Internet anbieten, aber die vollständigen Kontaktdaten des Sächsischen Datenschutzbeauftragten als zuständiger Datenschutzaufsichtsbehörde genannt sind, ergibt es sich wohl, dass sich betroffene Personen mit Inhalten, die eigentlich dem Verantwortlichen zugedacht sind, insbesondere per E-Mail, an meine Dienststelle wenden. In diesen Fällen verweise ich auf meine Unzuständigkeit und den Verantwortlichen. Datenverarbeitende Stellen, darunter befinden sich nicht wenige Freiberufler, möchte ich nachhaltig anraten, ihre Kunden, Patienten und Mandanten nicht zu verärgern und vollständig verordnungskonform bzw. adressatengerecht zu informieren.

Die nachstehende Auswahl von Vorgängen mag amüsieren, aber immerhin machen derartige Vorgänge mittlerweile etwa ein Prozent der Posteingänge aus (vergleiche auch das Diagramm im Tätigkeitsberichtsbeitrag unter 6.2.1 unten):

Unter anderem wendeten sich Personen an meine Behörde,

- um den Frauenarzt zu wechseln und mit der Ansprache „Meine Wahl ist dabei auf Sie gefallen.“,
- mit dem Hinweis, dass die eigene E-Mail-Adresse missbräuchlich verwendet worden sei und der Bitte, „die Bestellung zurückzunehmen“, man 17 Jahre alt sei und „solche Internetseiten sind erst ab 18 also mit sowas dürfte ich überhaupt noch nicht zu tun haben“,
- mit der Zusendung einer Ausweiskopie und der „meiner Mutti“ verbunden mit der Bitte um umgehenden Rückruf,
- mit einer Bewerbung aus Indien für eine Architekturstelle in englischer Sprache,
- mit einem Lastenheft für eine Ausschreibung zur Reinigung einer Lackieranlage eines Lkw- und Busbetriebs,
- mit der Bitte um Kontaktaufnahme, da man sein Bad umbauen und modernisieren lassen wolle,
- mit einer Zahlungsverweigerung,
- mit der Anfrage, dass die Tochter in diesem Jahr in die Schule und in den Hort gehe und man für mittags Essen bestellen wolle und der dringlichen Bitte „...Was soll ich tun? Bitte helfen Sie mir...“,
- mit der Information, dass „unser Geschäftsführer“ den Müll und den Zustand und die Verschmutzung des Parks mit Hundekot und frei herumlaufende Hunde moniere,
- mit der Anzeige eines in einem Straßenabschnitt „seit einiger Zeit“ abgestellten Volkswagens mit grüner Plakette, „...ohne Kfz Kennzeichen, allerdings mit fremdländisch beschrifteter Zigarettenschachtel im Fahrzeuginnenraum“,
- mit der Bestellung des Textes für eine Annonce für die verstorbene Mutter,
- mit der Anzeige der rechtswidrigen Ablagerung eines „alten Rollers“ mit Angabe des Kennzeichens und dem Fundort und der Bitte den Halter zur Rechenschaft zu ziehen und den Roller zu entsorgen.

6.2 Aufgabenbearbeitung im Berichtszeitraum und Statistik

6.2.1 Überblick und Arbeitsschwerpunkte

Im Berichtszeitraum stieg die Zahl der Postein- und -ausgänge signifikant an.

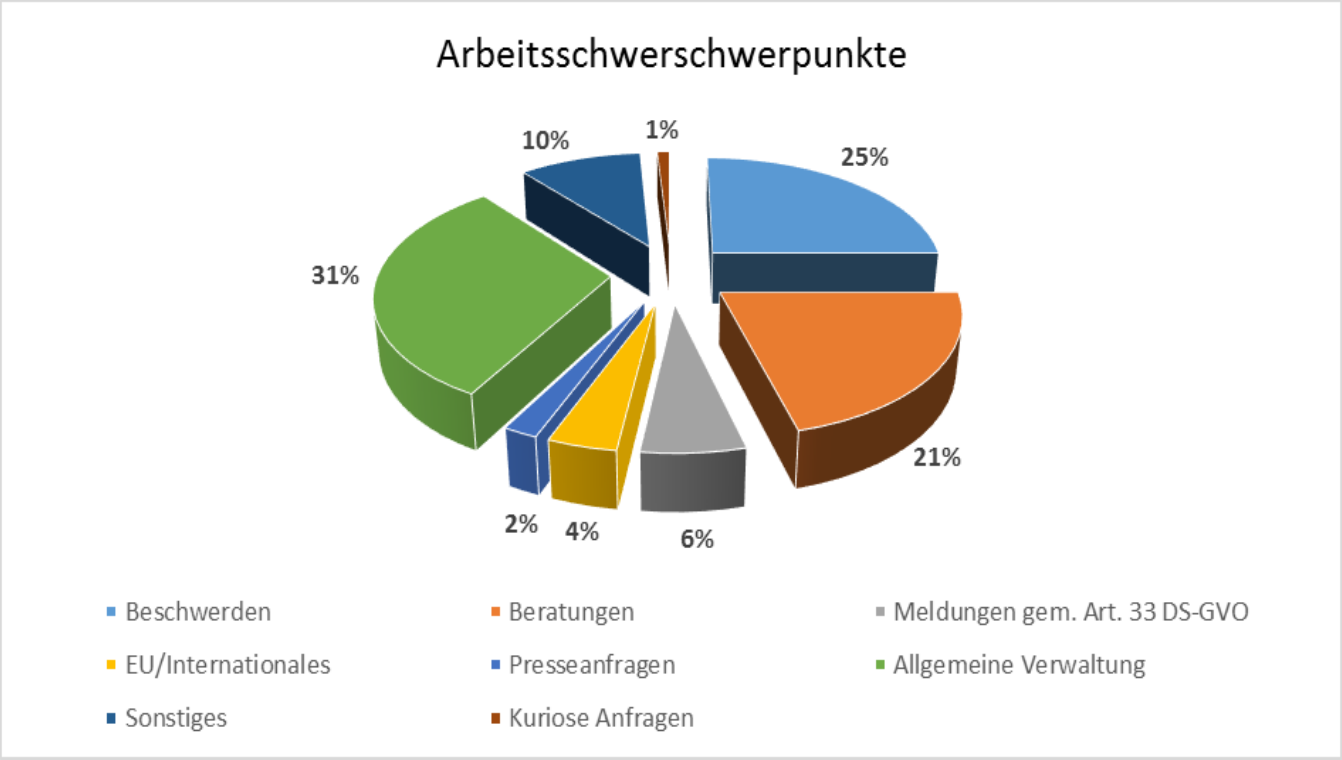
	25.05.2017 - 31.12.2017 (gesamt)	25.05.2018 - 31.12.2018 (gesamt)	Prozentualer Anstieg um (in Prozent)	um ein Vielfaches (Faktor)
Posteingänge	5423	8677	60	1,6
Postausgänge	2036	3247	59	1,6

Noch entscheidender als die Steigerung der Postein- und -ausgangszahlen war hingegen, dass ein nachhaltiger Anstieg von neu anzulegenden Vorgängen zu verzeichnen war:

Neu angelegte Vorgänge	1298	3558	174	2,7
davon Beschwerden	360	891	148	2,5
öB	*132*	*257*	*95*	*1,9*
nöB	*228*	*634*	*178*	*2,8*
davon Beratung	244	747	206	3,1
öB	*203*	*273*	*34*	*1,3*
nöB	*41*	*474*	*1056*	*12*
davon Meldungen gemäß Artikel 33 DSGVO	14	227	1521	16
öB	0	35	-	-
nöB	14	192	1271	14

Ein nicht unerheblicher Anteil an Bearbeitungsvorgängen betrifft die EU-Ebene, Korrespondenz mit anderen Datenschutzaufsichtsbehörden und die eigene Verwaltung, siehe Diagramm unten.

Aufgrund des Anstiegs der Bearbeitungszahlen und der vollständigen Personalauslastung konnten im Berichtszeitraum keine anlassfreien Aufsichtsmaßnahmen mehr ergriffen werden.



6.2.1.1 Umgang mit Petitionen, Hinweisen und Beratungsanfragen

Die Geschäftsstelle des Sächsischen Datenschutzbeauftragten versendet regelmäßig Eingangsmitteilungen an Petenten, Hinweisgeber und anfragende natürliche Personen und nicht-öffentliche Stellen. Die Mitteilung enthält lediglich eine Eingangsbestätigung und den Inhalt, dass der Vorgang dem zuständigen Referat zur Bearbeitung übergeben worden ist. Eine inhaltliche Prüfung oder eine Prüfung auf Vollständigkeit ist mit der Eingangsmitteilung damit noch nicht erfolgt. Aufgrund des hohen Geschäftsanfalls ist es möglich, dass erst nach einem gewissen Zeitablauf festgestellt wird, dass eingereichte Unterlagen unvollständig oder nicht verständlich sind.

Meine Dienststelle nimmt zwar auch anonyme Hinweise auf, aber soweit eine Antwort seitens der Petenten, Hinweisgeber und anfragenden Stellen erwartet wird, werden seitens meiner Behörde nicht nur eine E-Mail-Adresse, sondern auch vollständige Namens- und Anschriftenangaben benötigt, um auf dem herkömmlichen Briefpostweg antworten zu können. Soweit diese Informationen nicht vorliegen, werden diese regelmäßig seitens meiner Dienststelle unter erhöhtem Aufwand nachträglich abgefragt.

Zunehmend erhält meine Behörde auch Vorgänge zugesandt, die gar keine verständliche oder präzise Schilderung des Problems enthalten. Sollen die Bearbeitung verzögernde Rückfragen vermieden werden, sind die Bediensteten meiner Behörde darauf angewiesen, dass anfragende Personen und Stellen konkrete und allgemeinverständliche Sachverhaltsdarstellungen übermitteln. Bei vorgetragenen Streitgegenständen wird zudem regelmäßig auf bestimmte schriftliche und sonstige Korrespondenz Bezug genommen. Beschwerdeführer, Hinweisgeber und sonstige anfragende Personen oder Stellen

sollten daher belegende oder sich sonst auf den Vorgang beziehende Dokumente schon ihrem Vorgang beifügen, so dass diese nicht erst erfragt müssen.

Meine Behörde bietet ein Online-Formular für Petitionen an. Die Online-Funktionen bieten hierbei aus sicherheitstechnischen Gründen keine Möglichkeit, Anlagen und Belege hochzuladen bzw. an meine Dienststelle zu übersenden. Petenten sollten, soweit sie das Formular für die Online-Petition nutzen, daher für meine Behörde erforderliche Unterlagen nachträglich unter Nennung des mit der Eingangsbestätigung versendeten Geschäftszeichens unaufgefordert nachreichen. Dies erleichtert die Bearbeitung bei ohnehin hohem Geschäftsanfall.

Immer häufiger erhält meine Dienststelle per E-Mail Vorgänge betroffener Personen, die diese in Kopie auch meiner Behörde zuleiten. Nicht selten sind diese Vorgänge aufgrund fehlender Angaben und Bezüge durch meine Behörde nicht bearbeitbar bzw. sehen sich Bedienstete meiner Dienststelle wegen der Mitteilung als Kopie nicht aufgerufen, tätig zu werden. Betroffene Personen möchte ich daher bitten, die Möglichkeiten zu nutzen, soweit Anlass besteht, bei meiner Behörde eine verwertbare Sachverhaltsdarstellung einzureichen bzw. diese direkt an meine Dienststelle zu adressieren und nachrichtliche bzw. vorsorgliche Informationen, sofern nicht bereits ein datenschutzaufsichtlicher Vorgang eröffnet worden ist, zu unterlassen.

Soweit Beschwerdeführer selbst betroffene Personen sind, sollten sie dies ausdrücklich meiner Behörde gegenüber anzeigen. Bei Petitionen betroffener Personen kann es zudem seitens meiner Dienststelle notwendig werden, dass der Verantwortliche - die datenverarbeitende Stelle - zur Stellungnahme aufzufordern ist und es zur Klärung des Sachverhalts nicht zu vermeiden ist, dass die Identität des Betroffenen hierbei offenbart wird. Betroffene Personen bitte ich daher, bei Beschwerden mir gegenüber bereits im Voraus zu erklären, ob sie mit der Nennung ihrer Person einverstanden wären oder nicht.

Sobald ein Ergebnis der Prüfung feststeht, werden die Petenten gemäß Artikel 77 Absatz 2 DSGVO und anfragenden Stellen unaufgefordert unterrichtet. Die Vorschrift des Artikels 77 Absatz 2 DSGVO findet jedoch keine Anwendung bei Ordnungswidrigkeitenverfahren. In Ordnungswidrigkeitenverfahren unterliegt meine Dienststelle der Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates. Weder besteht die Möglichkeit einer förmlichen Rechtsbeschwerde, um eine Verfolgung zu erzwingen, noch ist eine Artikel 77 Datenschutz-Grundverordnung entsprechende Unterrichtung

des Anzeigeerstatters im Ordnungswidrigkeitenrecht vorgesehen, auch nicht, wenn der Anzeigeerstatter die betroffene Person ist.

Mit der Information über das Ergebnis der Prüfung der Beschwerde der Betroffenen Person – des Petenten – ist dieser gemäß Artikel 77 Absatz 2 Datenschutz-Grundverordnung auch über die Möglichkeit eines gerichtlichen Rechtsbehelfs gegen die Entscheidung meiner Behörde zu unterrichten. Daher ergeht seitens meiner Dienststelle regelmäßig der Hinweis, dass gegen die Entscheidung meiner Behörde Klage beim Verwaltungsgericht Dresden erhoben werden kann. Ein Fristhinweis erübrigt sich.

Hinweisgeber, auf deren Mitwirkung meine Behörde angewiesen ist, erhalten, sofern keine Nachfragen zur Bearbeitung erforderlich sind, von dem Fachreferat meiner Dienststelle lediglich eine abschließende Mitteilung, aber keine weiteren Angaben zum Prüfvorgang. Auch anonyme Zuschriften werden natürlich seitens meiner Behörde bearbeitet. Eine Antwort meiner Dienststelle unterbleibt dann jedoch selbstverständlich.

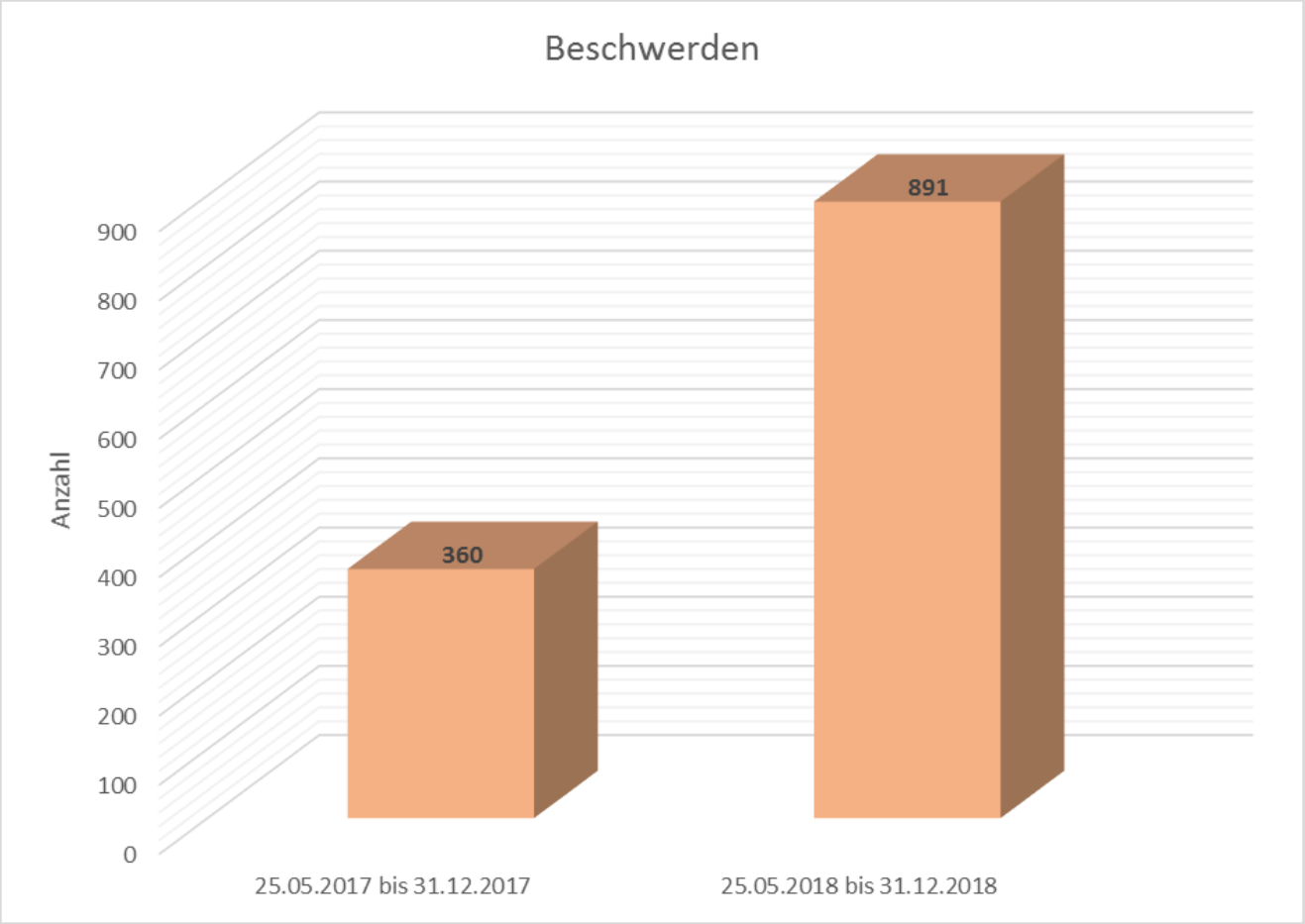
Aufgrund der mit der Datenschutz-Grundverordnung einhergehenden Fallmengen der Anfragen und Beschwerden ist es auch im letzten Abschnitt des Berichtszeitraums zum Teil zu erheblichen zeitlichen Verzögerungen bei der Bearbeitung gekommen, zumal Eingaben und Anfragen grundsätzlich in der Reihenfolge ihres Posteingangs abzuarbeiten gewesen sind. Hierfür bittet meine Dienststelle um Verständnis.

6.2.1.2 Umgang mit Eingaben zur Videoüberwachung öffentlich zugänglicher Bereiche

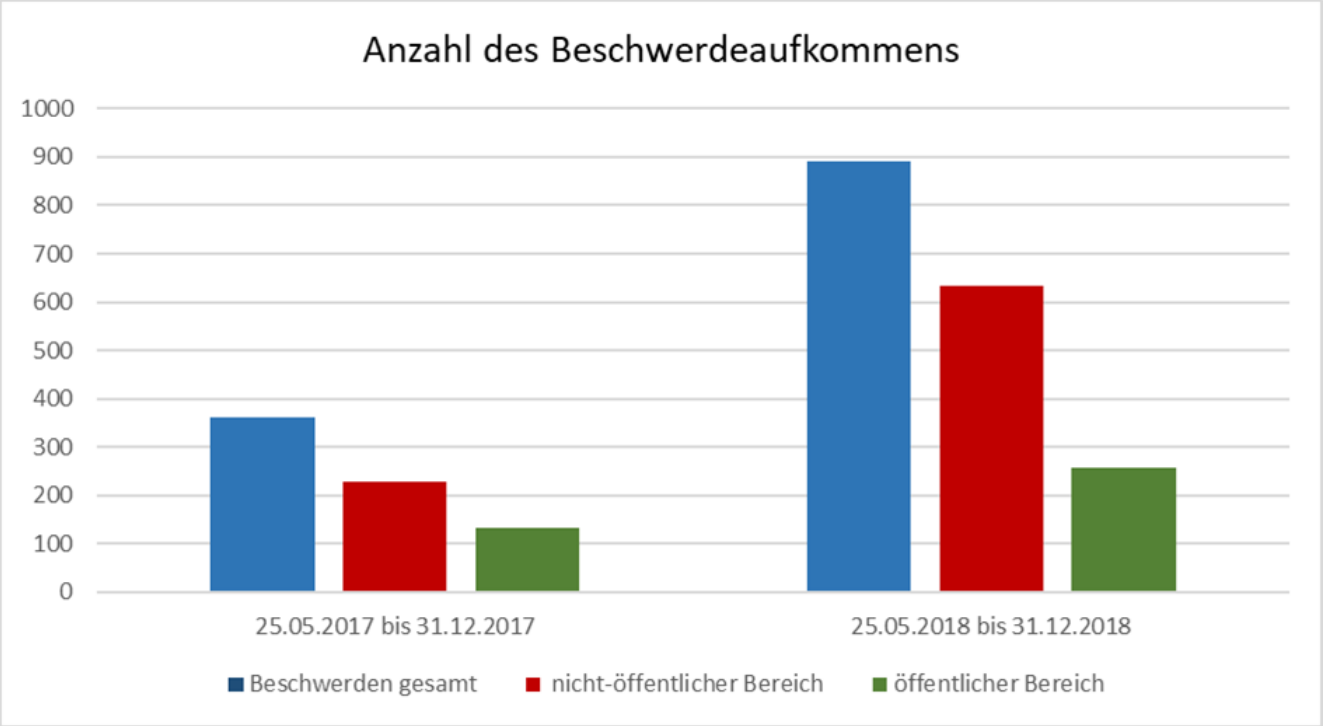
Eingaben zum Betrieb von Videoüberwachungskameras bildeten schon in der Vergangenheit – jedenfalls im nicht-öffentlichen Bereich (vgl. dazu auch meine Ausführungen unter Punkt 4 meines 9. TB im nicht-öffentlichen Bereich) – den unangefochtenen Schwerpunkt meiner anlassbezogenen Kontrolltätigkeit. Soweit es sich dabei um Außenkameras handelte, die auch oder ausschließlich in öffentlich zugängliche (Verkehrs-)Bereiche hinein filmten, war nicht immer klar, ob sich tatsächlich nur Betroffene an mich gewandt hatten oder ob es sich dabei nicht um bloße Hinweisgeber handelte, die es sich teilweise offensichtlich zum Sport gemacht hatten, durch die Straßen zu streifen und nach Videokameras Ausschau zu halten, um diese dann bei der Aufsichtsbehörde anzuzeigen. Naturgemäß fehlten dann zumeist erläuternde Informationen zum genauen Installationsort, Fotos der konkreten Umgebung und natürlich auch Angaben zum vermuteten Betreiber. Für mich war es dann regelmäßig mit großem Aufwand verbunden, die tatsächlichen Umstände der Videoüberwachung vor Ort zu bewerten und den jeweiligen Verantwortlichen zu ermitteln. Nicht selten stellte sich letztendlich heraus, dass die Kameras tatsächlich gar keine öffentlich zugänglichen Bereiche erfassten oder es sich lediglich um Kameraattrappen handelte.

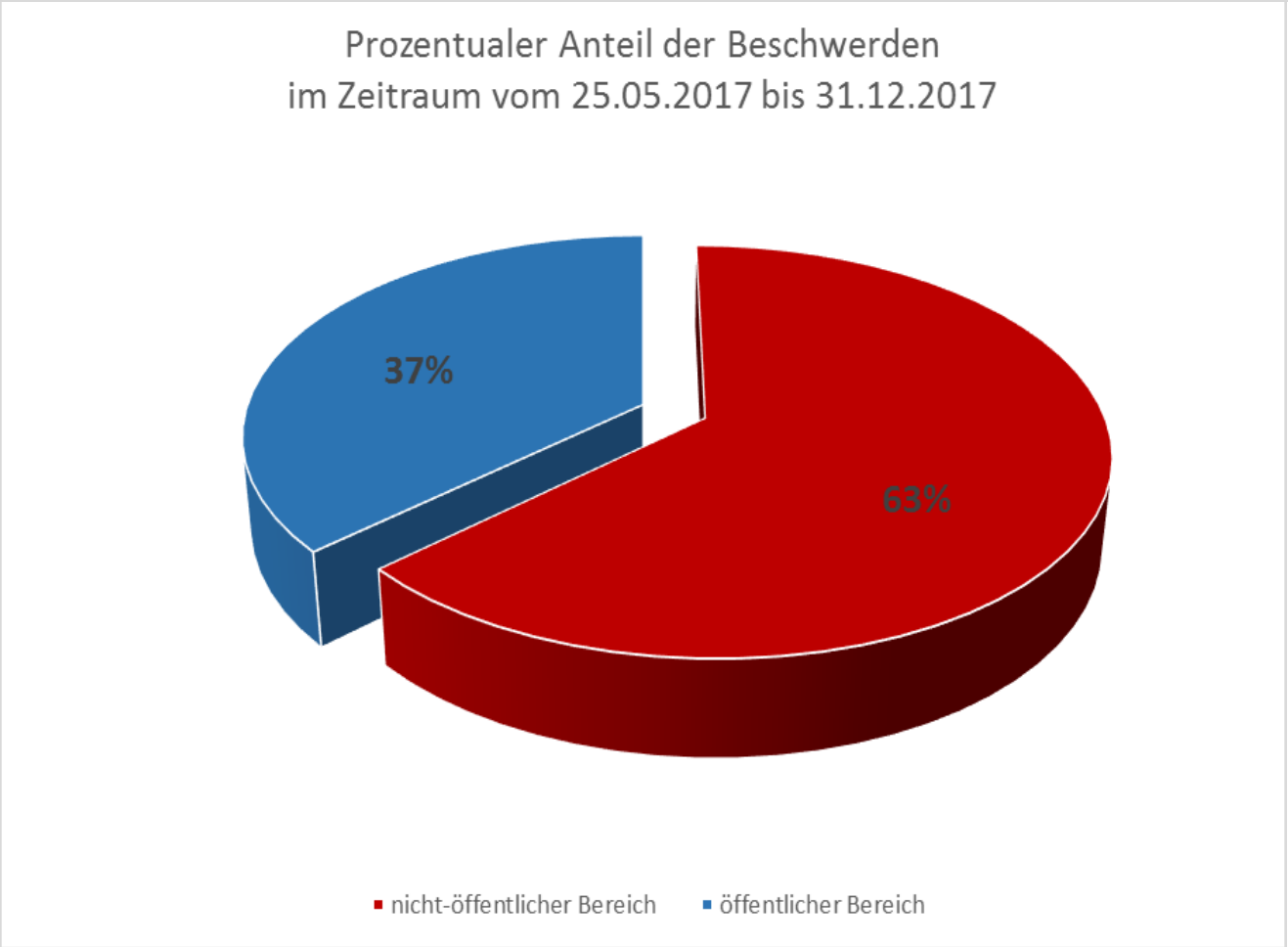
6.2.2 Petitionen, Beschwerden, Hinweise

Waren im Vorjahreszeitraum noch 361 Vorgänge angelegt worden, waren es im Berichtszeitraum bereits 891, vergleiche Beitrag 6.2.1 oben. Das nachstehende Diagramm stellt die Zunahme des Beschwerdeaufkommens im Berichtszeitraum im Vergleich zum Vorjahr dar:

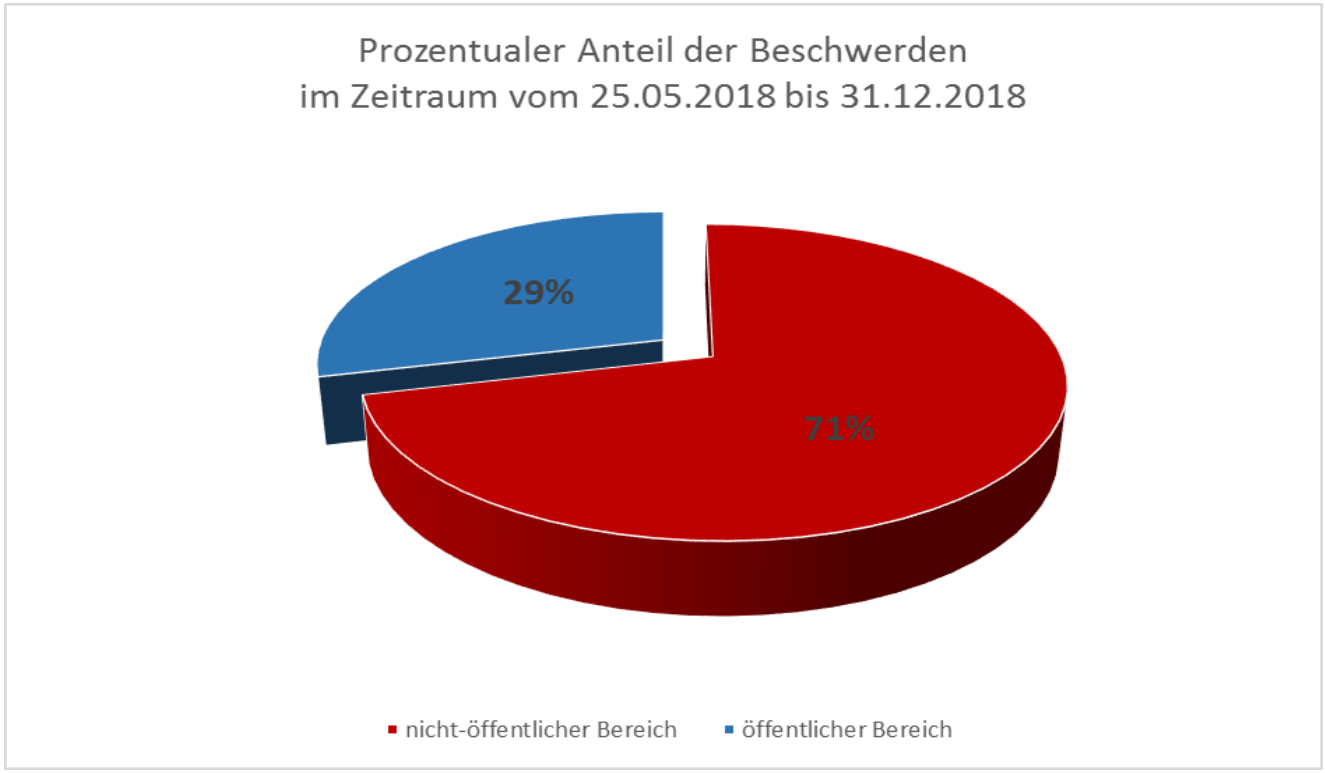


Aufgegliedert nach öffentlichem und nicht öffentlichem Bereich stellt sich der Anstieg im Diagramm folgendermaßen dar:



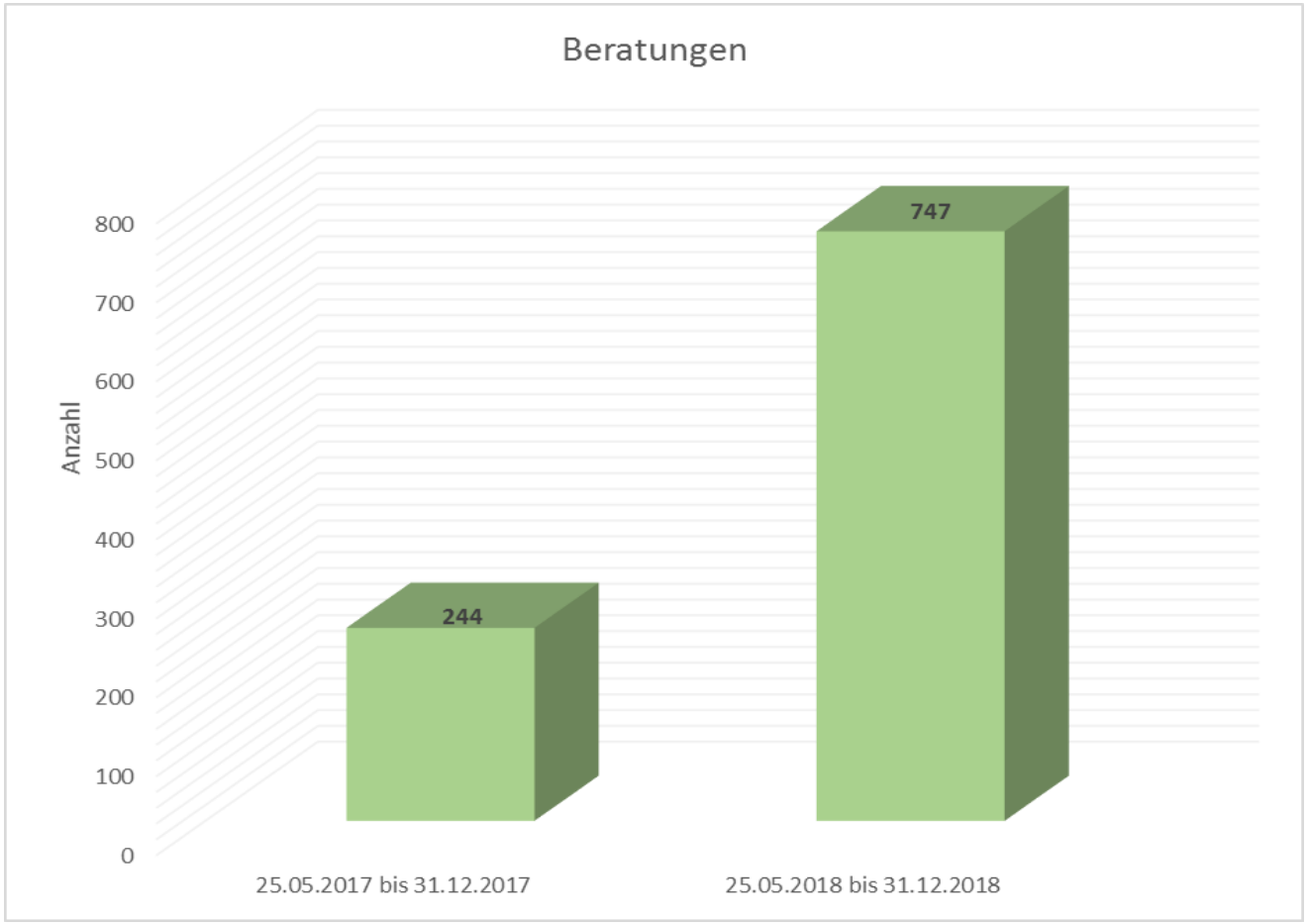


Betraf das Beschwerdeaufkommen vor Wirksamwerden der Datenschutz-Grundverordnung noch zu deutlich über einem Drittel den öffentlichen Bereich, vergleiche das Diagramm oben, nahm der Anteil der Beschwerden und Hinweise, die den nicht-öffentlichen Bereich betreffen, im Verhältnis weiter zu. Der den nicht-öffentlichen Bereich betreffende Anteil sank nachhaltig, siehe Diagramm unten.



6.2.3 Beratungen

Waren im Vergleichsvorjahreszeitraum noch 244 Beratungsanfragen eingegangen, erhielt meine Behörde im letzten Berichtszeitraum 747 Anfragen, vergleiche das Diagramm unten.



Der Anteil der Anfragen in Bezug auf den nicht-öffentlichen Bereich stieg exponentiell auf ein außergewöhnlich hohes Niveau an, vergleiche den Berichtsbeitrag unter 6.2.1 oben.

Anfragen, zum Beispiel von Rechtsanwaltskanzleien oder anderen rechtsberatenden Stellen, können seitens meiner Behörde, soweit nicht dargetan worden ist, dass diese für eine konkrete sächsische Stelle oder einen Beschwerdeführer in Sachsen tätig sind und der Anfrage keine anderweitige grundsätzliche Bedeutung zugemessen wird, aufgrund der hohen Fallmengenzahlen nicht mehr beantwortet werden.

Nicht selten sind auch bundesweite Anfragen an sämtliche Datenschutzaufsichtsbehörden zu verzeichnen gewesen. In vielen Fällen haben sich die Aufsichtsbehörden daher darauf geeinigt, dass bei bundesweiten Anfragen nur eine Beantwortung durch die für die anfragende Stelle zuständige Aufsichtsbehörde erfolgen soll. Regelmäßig wird die Beantwortung dabei nach dem Sitz der für die anfragende Stelle zuständigen Aufsichtsbehörde oder im Einzelfall der Vorsitzenden Aufsichtsbehörde eines für die Fachfrage zuständigen Arbeitskreises der Datenschutzkonferenz übertragen. Auch bei vermeintlichen Einzelanfragen, zum Beispiel eines Bundesverbandes, wird die für diese Stelle zuständige Aufsichtsbehörde regelmäßig über die eingegangene Anfrage in Kenntnis gesetzt.

6.2.4 Prüfungen - Rechtsetzung, Verwaltungsvorschriften (§ 20 SächsDSDG)

Im Zuge der Harmonisierung der sächsischen Rechtsvorschriften durch den Gesetzgeber und die Verwaltung mit der Datenschutz-Grundverordnung wurde meine Behörde bereits rechtzeitig vor dem letzten Berichtszeitraum auf Grundlage der Geschäftsordnung der Sächsischen Staatsregierung und in parlamentarischen Verfahren beteiligt, vergleiche auch den Berichtsbeitrag 1.1. Auf die Darstellung weiterer Vorgänge wird mangels einer Gewichtigkeit an dieser Stelle verzichtet.

6.2.4.1 Stellungnahmen zu Gesetzgebungsvorhaben im Polizei-, Justiz- und Verfassungsschutzbereich

Im Berichtszeitraum hat die Staatsregierung umfangreiche Gesetzgebungsaktivitäten zur Anpassung des sächsischen Rechts an die bis zum 6. Mai 2018 umzusetzende „Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI“ (im Folgenden: JI-RL) entfaltet. Sie hat diesen Anlass auch genutzt, um insbesondere im Polizeirecht Änderungen, da-

runter Befugniserweiterungen, vorzunehmen, die nicht durch die JI-RL bestimmt waren, sondern eigenen Erkenntnissen oder Bund-Länder-Abstimmungen entsprangen.

Ich habe zu diesen Gesetzentwürfen der Staatsregierung und später auch im parlamentarischen Verfahren, soweit dieses im Berichtszeitraum (1. April 2017 bis 31. Dezember 2018) bereits begonnen hatte, jeweils umfangreich schriftlich Stellung genommen und die Staatsregierung und den Sächsischen Landtag auch mündlich beraten. Damit habe ich von meiner im Berichtszeitraum noch nach § 30 Absatz 4 SächsDSG bestehenden Beratungsbefugnis (vgl. dazu hinsichtlich der zukünftigen Rechtslage auch Artikel 46 Absatz 1 Buchstabe c JI-RL) Gebrauch gemacht. Denn bei den Entwürfen von Rechtsvorschriften, die die „Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung“ regeln sollen, ergeben sich meine Beratungsbefugnisse nicht aus der DSGVO, sondern bis zum Inkrafttreten der Umsetzungsgesetze aus dem weiter geltenden Sächsischen Datenschutzgesetz.

Meine Stellungnahmen im vorparlamentarischen wie im parlamentarischen Raum waren erfreulicherweise in einigen Punkten erfolgreich. Einige meiner Anregungen wurden aufgegriffen und bereits in den Entwürfen umgesetzt. Für die damit zum Ausdruck gekommene Offenheit und Kooperationsbereitschaft danke ich der Staatsregierung und den Abgeordneten des Sächsischen Landtags, die meinen Argumenten offen gegenübergestanden haben.

Ich habe im Einzelnen zu den Gesetzentwürfen der Staatsregierung zur Neustrukturierung des Polizeirechts, zur Umsetzung der JI-Richtlinie 2016/680 im Justizbereich sowie zur Änderung des Sächsischen Verfassungsschutzgesetzes Stellung genommen. Soweit im Berichtszeitraum bereits Änderungsanträge der Fraktionen des Sächsischen Landtags zu den Gesetzentwürfen vorlagen, habe ich auch zu diesen Stellung genommen. Sämtliche diese im Berichtszeitraum noch nicht abgeschlossenen Gesetzgebungsvorhaben berührten in besonderer Weise die „Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Recht auf Schutz personenbezogener Daten“ (vgl. Artikel 1 Absatz 2 Buchstabe a JI-RL), also nach herkömmlichem deutschen Verständnis insbesondere deren Grundrechte auf informationelle Selbstbestimmung (Artikel 8 EGrCh, Artikel 16 AEUV, Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG, Artikel 33 SächsVerf) und auf Vertraulichkeit und Integrität informationstechnischer Systeme (Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG).

Im Einzelnen:

Mit dem schließlich am 18. September 2018 als Drucksache 6/14791 in den Sächsischen Landtag eingebrachten und im Berichtszeitraum noch im parlamentarischen Ver-

fahren befindlichen Entwurf eines aus 26 Artikeln bestehenden „Gesetzes zur Neustrukturierung des Polizeirechtes des Freistaates Sachsen“ soll im Wesentlichen das bisherige Polizeigesetz für den Freistaat Sachsen (SächsPolG) durch ein „Sächsisches Polizeivollzugsdienstgesetz“ und ein „Sächsisches Polizeibehördengesetz“ ersetzt werden. Darüber hinaus sollen auch andere, dem Polizeibereich zuzuordnende Gesetze wie etwa das Sächsische Wachpolizeigesetz, das Sächsische Versammlungsgesetz, das Sächsische Kontrollgesetz und nicht zuletzt das Sächsische Datenschutzgesetz geändert werden. Der Entwurf des neuen Polizeivollzugsdienstgesetzes (SächsPVDG-E) enthält dabei eine Vielzahl von datenschutzrechtlich relevanten Befugnissen wie z. B. zu stationären Kennzeichenerkennungssystemen, zu neuartigen Videografiesystemen an ausgewählten Standorten oder zur präventiven Telekommunikationsüberwachung.

Ich hatte zu dem entsprechenden Referentenentwurf der Staatsregierung bereits im Frühjahr 2018 Stellung genommen. Zunächst hatte ich grundsätzlich begrüßt, dass sich der Entwurf, was die Voraussetzungen für Eingriffsmaßnahmen im Vorfeld einer konkreten Gefahr angeht, eng an dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 zum Gesetz über das Bundeskriminalamt (BKAG) (Az. 1 BvR 966/09 und 1 BvR 1140/09) ausrichtet. Danach sind Eingriffsmaßnahmen, wenn als Anknüpfungspunkt für Prognosen über Gefährdungslagen nur das Verhalten einer Person herangezogen werden kann, nur zur Verhütung terroristischer Straftaten erlaubt. Maßnahmen zur Abwehr einer „drohenden Gefahr“ waren nach dem Entwurf erfreulicherweise nur in sehr beschränktem Umfang zulässig.

Bedenken hatte ich allerdings, soweit Eingriffsmaßnahmen von zum Teil erheblicher Intensität (Gewahrsam zur Durchsetzung einer Aufenthaltsanordnung; elektronische Aufenthaltsüberwachung; längerfristige Observation und verdeckter Einsatz technischer Mittel zu Bild- und Tonaufzeichnungen; Einsatz von V-Personen; Überwachung der Telekommunikation) zum Schutz von „Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist“, zulässig sein sollten. Ich habe meine starken Zweifel an der Bestimmtheit und Klarheit der Normen gegenüber dem SMI ausführlich begründet. Ich habe insb. darauf hingewiesen, dass ohne den Zusammenhang mit der Terrorismusbekämpfung, den die vom Bundesverfassungsgericht überprüften Vorschriften des BKAG a. F. aufwiesen, eine entscheidende Auslegungshilfe und Orientierung zur Bestimmung der zu schützenden Sachwerte fehlt. Ich habe deshalb das SMI gebeten, die Sachwerte, zu deren Schutz intensive und/oder heimliche Eingriffsmaßnahmen erlaubt werden sollen, unter Berücksichtigung meiner Überlegungen noch präziser zu bestimmen.

Im Übrigen habe ich eine klare Definition bestimmter Begriffe wie „Erforderlichkeit einer Eingriffsmaßnahme“ oder „Ordnungswidrigkeit von erheblicher Bedeutung“, eine

Reduzierung der Speicherdauer für (nichtrelevante) Videoaufzeichnungen von zwei auf einen Monat, ein Unterbleiben einer zweckändernden Weiterverwendung von Videodaten, die zur Verhütung von Straftaten bzw. zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit erhoben worden sind, für alle möglichen (einfachen) Ordnungswidrigkeiten, und vieles Weitere angemahnt. Unter diesem „Weiteren" möchte ich zwei Vorschriften besonders herausstellen: Mit § 59 SächsPVDG-E soll eine neuartige Eingriffsbefugnis geschaffen, nach der zur „Verhütung schwerer grenzüberschreitender Kriminalität" Bildaufzeichnungen des Verkehrs auf öffentlichen Straßen gefertigt und automatisiert mit anderen, bereits vorhandenen (Personen-)Daten, insbesondere biometrischen Daten und Kennzeichen genutzter Kraftfahrzeuge, abgeglichen werden dürfen. Diese Verknüpfung zweier polizeilicher Maßnahmen begegnet m. E. grundsätzlichen Bedenken, wobei diese nicht der bloßen Kombination zweier Maßnahmen entspringen. Auch bislang waren Polizeibeamte etwa befugt, an eine Identitätsfeststellung einen Datenabgleich anzuschließen, sofern die gesetzlichen Voraussetzungen vorlagen. Daneben gibt es auch im noch geltenden Polizeigesetz eine massenhafte Erfassung von Daten, die mit einem sofortigen Abgleich mit polizeilichen Datenbeständen verknüpft ist, namentlich die anlassbezogene (mobile) automatisierte Kennzeichenerkennung nach § 19a SächsPolG. Die Neuerung in § 59 SächsPVDG-E bestand in der Masse von biometrischen personenbezogenen Daten, die automatisiert verarbeitet werden. Die Automatisierung von Überwachungsmaßnahmen geht aber unweigerlich mit einer Ausweitung der Überwachung einher, der technische Fortschritt führt tendenziell zu einer immer weitergreifenden Erfassung personenbezogener Daten von immer mehr Betroffenen, die weder Störer noch Gefährder im polizeilichen Sinne sind. Die Überwachung nimmt auch in geografischer Hinsicht immer mehr Raum ein und rückt näher an den (unbescholtenen) Einzelnen heran. Dass diese Entwicklung nicht nur datenschutzrechtlich, sondern auch gesellschaftlich problematisch ist, liegt auf der Hand: Staatliche Überwachungsmaßnahmen verursachen Einschüchterungseffekte und haben einen negativen Einfluss auf die Bereitschaft zur Ausübung von Grundrechten. Eine weitere Neuerung fand sich in § 61 SächsPVDG-E, der die elektronische Aufenthaltsüberwachung erlauben soll. Ich habe starke Zweifel daran geäußert, ob die „elektronische Fußfessel" geeignet ist, Personen von der Begehung terroristischer Straftaten abzuhalten oder Verstöße gegen Kontaktverbote zu verhüten.

Zum Polizeibehördengesetz-Entwurf (PBG-E) hatte ich bereits im Frühjahr 2018 ebenfalls Stellung genommen. Ich hatte u. a. darauf hingewiesen, dass die vorgesehene Befugnis für Polizeibehörden, künftig öffentlich zugängliche Räume u. a. „bei Vorliegen einer abstrakten Gefahr" videoüberwachen zu dürfen, problematisch ist. Konkrete Maßnahmen wie die Videoüberwachung öffentlich zugänglicher Räume erfordern eine konkretisierte Gefahrenlage (signifikant erhöhte Kriminalitätsbelastung und durch Tatsachen begründete Erwartung von Straftaten). Das Kriterium der „abstrakten Gefahr" ist

im öffentlich zugänglichen Raum, wo überall und jederzeit „nach allgemeiner Lebenserfahrung oder den Erkenntnissen fachkundiger Stellen […] Sachlagen [möglich sind], durch die im Fall ihres Eintritts eine Gefahr für ein polizeiliches Schutzgut entsteht“ (so die auch für den SächsPBG-E maßgebliche Begriffsbestimmung in § 4 Nummer 3 Buchstabe f SächsPVDG-E), als Eingriffsschwelle schlicht ungeeignet.

Mit dem zum Ende des Berichtszeitraums noch nicht in den Sächsischen Landtag eingebrachten, zehn Artikel umfassenden (Referenten-) Entwurf eines Gesetzes „zur Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI für den Justiz- und Maßregelvollzug im Freistaat Sachsen“, dessen wesentlicher Bestandteil das „Gesetz zum Schutz personenbezogener Daten im Justizvollzug (Sächsisches Justizvollzugsdatenschutzgesetz – SächsJVollzDSG)“ ist, legte die Staatsregierung einen der Umsetzung der JI-RL für den Bereich des Justiz- und Maßregelvollzugs dienenden Gesetzentwurf vor. Im Justizvollzug ist der Datenschutz bislang in den einzelnen Justizvollzugsgesetzen, z. B. dem Sächsischen Untersuchungshaftvollzugsgesetz, speziell und im SächsDSG als Auffanggesetz allgemein geregelt. Aus systematischen Gründen sollen nunmehr die Datenschutzvorschriften aus den einzelnen Vollzugsgesetzen herausgelöst, gleichsam „vor die Klammer gezogen“ und in einem einzigen, im Justizvollzug anwendbaren Datenschutzgesetz zusammengefasst werden. Die darüber hinaus den Maßregelvollzug betreffenden Änderungen im Sächsischen Gesetz über die Hilfen und die Unterbringung bei psychischen Krankheiten (SächsPsychKG) verweisen größtenteils auf den Entwurf des SächsJVollzDSG.

Auch zu diesem Referentenentwurf der Staatsregierung hatte ich bereits frühzeitig Stellung genommen. Ich habe u. a. darauf hingewiesen, dass bestimmte beabsichtigte Verfahrenserleichterungen bei der Speicherung, Nutzung oder Übermittlung verbundener Daten m. E. zu Unrecht den Begriff der „berechtigten Interessen“ der Betroffenen und nicht deren Schutzwürdigkeit als Kriterium vorsehen. Denn „berechtigte Interessen" sind regelmäßig bei Personen oder Stellen zu berücksichtigen bzw. zu prüfen, die ihren Kenntnis- oder Wirkungskreis erweitern wollen und damit in Rechtskreise Dritter, betroffener Personen, eindringen. Datenschutzrechtlich problematisch an den beabsichtigten Verfahrenserleichterungen war darüber hinaus, dass das schutzwürdige Interesse der betroffenen Person hätte „offensichtlich“ überwiegen müssen. Ein einfaches Überwiegen schutzwürdiger Interessen einer betroffenen Person ist aber bereits ausreichend, um einen Grundrechtseingriff zu unterbinden.

Auch war die „allgemeine Generalklausel" für Übermittlungen für vollzugliche Zwecke m. E. deutlich zu weitgehend formuliert. Die Begründung der Vorschrift verschärfte deren Unbestimmtheit noch; ich habe deshalb angeregt, den Adressatenkreis auf öffentliche Stellen zu begrenzen und im Wortlaut klarzustellen, dass die Übermittlungsbefugnis gilt, soweit Vorschriften dieses Gesetzes nichts anderes bestimmen. Der Regelung wäre damit der Charakter einer „Grundbefugnis“ für Übermittlungen an öffentliche Stellen für vollzugliche Zwecke erhalten geblieben, zugleich aber würde deutlich erkennbar, dass u. U. besondere Voraussetzungen für Übermittlungen auch für vollzugliche Zwecke vorliegen müssen.

Ferner habe ich u. a. darum gebeten, die vorgesehene Vorschrift zur Überprüfung anstaltsfremder Personen (Besucher von Gefangenen, Personen, die in der Anstalt tätig werden, z. B. Handwerker), denen Zugang zur Anstalt gewährt werden soll, zu ändern. Ich habe angeregt, die bis dahin einwilligungslos zulässige Einholung von Auskünften bei Sicherheitsbehörden und Nachrichtendiensten künftig von der Zustimmung der betroffenen Person abhängig zu machen. Den betroffenen Personen würde damit die Möglichkeit eröffnet, selbst zu entscheiden, ob – um den Preis der Nichtgewährung des Zutritts – eine Anfrage der Anstalt bei Sicherheitsbehörden oder Nachrichtendiensten unterbleibt und damit auch eine Übermittlung von Daten an die Anstalt.

Im Hinblick auf die beabsichtigte, künftig als „normale“ besondere Sicherungsmaßnahme vorgesehene optisch-elektronische Überwachung von Hafträumen habe ich u. a. darauf hingewiesen, dass es bislang, aus guten Gründen, im Justizvollzug keine derartige Überwachung gab. Die hohe Eingriffsintensität in das Rechte der betroffenen Personen auf Privatheit und informationelle Selbstbestimmung ergibt sich m. E. aus der unausweichlichen Beobachtung (es gibt keine Rückzugsmöglichkeit in nicht überwachte Bereiche) und der Aufzeichnung der Überwachungsbilder. Damit ist nicht allein das Grundrecht auf informationelle Selbstbestimmung betroffen; auch der Schutzbereich des Artikel 1 Absatz 1 GG, die Unantastbarkeit der Würde der Gefangenen, ist tangiert. Ich habe mich deshalb dafür ausgesprochen, eine derart eingriffsintensive Maßnahme nur dann anzuwenden, wenn sie der Abwehr einer gegenwärtigen Gefahr für Leib oder Leben des Gefangenen dient. Darüber hinaus habe ich angeregt, eine Bestimmung aufzunehmen, wonach die optisch-elektronische Beobachtung unverzüglich zu beenden ist, sobald die Erforderlichkeit entfällt. Gesetzgeber und Verwaltung sind gehalten, Grundrechtseingriffe von höchster Intensität so kurz wie irgend möglich zu halten. Schließlich habe ich angeregt, den Personenkreis, der auf Aufzeichnungen aus Hafträumen zugreifen darf, eng zu begrenzen (etwa auf anordnungsbefugten Anstaltsleiter, auf Arzt und Psychologen).

Des Weiteren habe ich angeregt, Dolmetscher hinsichtlich der Offenbarung von Gesprächsinhalten, die sie übersetzt haben, den Berufsgeheimnisträgern in jedem Fall gleichzustellen, die Vorschrift über Auskunft und Akteneinsicht in Gesundheitsakten und Therapieakten klarer zu fassen und Ablichtungen aus Gesundheits- und Therapieakten unentgeltlich zu stellen. Besonders wichtig war mir des Weiteren, dass die m. E. zu langen Speicher- und Aufbewahrungsfristen des Gesetzentwurfs (vorgesehen waren in Dateisystemen hinsichtlich Gefangener und ihnen zuordenbarer Dritter fünf Jahre nach Entlassung oder Verlegung, hinsichtlich Dritter ohne Bezug zu Gefangenen drei Jahre nach Erhebung; für die Aufbewahrung von Akten mit in der Verarbeitung eingeschränkten Daten für Gefangenenpersonalakten, Gesundheitsakten und Therapieakten sowie für Gefangenenbücher eine Frist von 30 Jahren) – die im Vergleich zu aktuell geltenden Speicherfristen mehr als eine Verdoppelung bedeuten würden – reduziert werden. Denn nach Artikel 4 Absatz 1 Buchstabe e JI-RL haben die Mitgliedstaaten vorzusehen, dass personenbezogene Daten „nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht“. Dieser Grundsatz zur Dauer der Verarbeitung wird m. E. durch eine Speicherdauer von fünf Jahren ab Entlassung oder Verlegung verletzt.

Einen mir sehr frühzeitig vorgelegten Referentenentwurf zur Änderung des Sächsischen Verfassungsschutzgesetzes sowie des Gesetzes zur Ausführung des Artikel 10-Gesetzes im Freistaat Sachsen habe ich im Einzelnen geprüft und dazu Stellung genommen. Dabei habe ich generell kritisiert, dass m. E. eine Aufweichung des durch die verfassungsgerichtliche Rechtsprechung immer wieder betonten Gebots der (auch informationellen) Trennung von Polizei und Nachrichtendienst festzustellen ist. So habe ich die vorgesehene Verpflichtung zur Zusammenarbeit von Landesamt für Verfassungsschutz (LfV), Polizei und sonstigen Sicherheitsbehörden, die Anknüpfung an polizei- bzw. gefahrenabwehrrechtliche Tatbestände bei Eingriffsbefugnissen sowie Übermittlungsvorschriften sehr kritisch gewürdigt. Das Gleiche galt im Hinblick auf die Beobachtung „fortwirkender Strukturen und Tätigkeiten der Aufklärungs- und Abwehrdienste der ehemaligen Deutschen Demokratischen Republik“. Es erschien mir fraglich, ob 27 Jahre nach der Wiedervereinigung eine Beobachtung solcher Strukturen und Tätigkeiten notwendig ist. Ich kann mir nur schwer vorstellen, dass durch entsprechende Tätigkeiten nach wie vor eine Bedrohung der Verfassungsgüter des Artikel 73 Nummer 10 Buchstabe b und c GG besteht, die nicht auch im Rahmen der Beobachtung anderer Phänomenbereiche aufgeklärt werden könnte. Grundlegende Kritik habe ich auch an einer Entwurfsvorschrift über die zulässigen nachrichtendienstlichen Mittel üben müssen, gegen die ich starke Bedenken im Hinblick auf die vom Bundesverfassungsgericht aufgestellten Anforderungen an die Grundsätze der Normenbestimmtheit und Normenklarheit hatte. Danach muss der Betroffene anhand der gesetzlichen Regelung die Rechtslage so erkennen können, dass er sein Verhalten danach auszurichten vermag (siehe etwa BVerfG, Urt. v.

27.07.2005, Az. 1 BvR 668/04, BVerfGE 113, 348, 375 f.). Welche Arten von nachrichtendienstlichen Mitteln dem LfV zustehen und unter welchen Voraussetzungen diese eingesetzt werden dürfen, hätte sich nach dem Entwurf allerdings weitgehend der Kenntnis der Öffentlichkeit und der Betroffenen entzogen. Weitere Kritikpunkte betrafen die Entwurfsvorschriften zur Wohnraumüberwachung, zum Schutz von Berufsgeheimnissen, zur Verwendung von Daten aus der Wohnraumüberwachung, zur Unterrichtung der Parlamentarischen Kontrollkommission, zur Benachrichtigung des Betroffenen sowie zum Absehen von Benachrichtigung, zu den Speicherfristen für Daten über Erwachsene, zur Einschränkung der Verarbeitung statt einer an sich gebotenen Löschung, zur Einschränkung statt Löschung für Zwecke eines Untersuchungsausschusses, zum generellen Verzicht auf eine Begründung bei der Ablehnung der Auskunftserteilung, zu den Übermittlungsvorschriften und vieles mehr. Insofern wäre ich dem Entwurfsverfasser dankbar, wenn er meine Anmerkungen im weiteren Verfahren berücksichtigen und den Gesetzentwurf entsprechend anpassen würde.

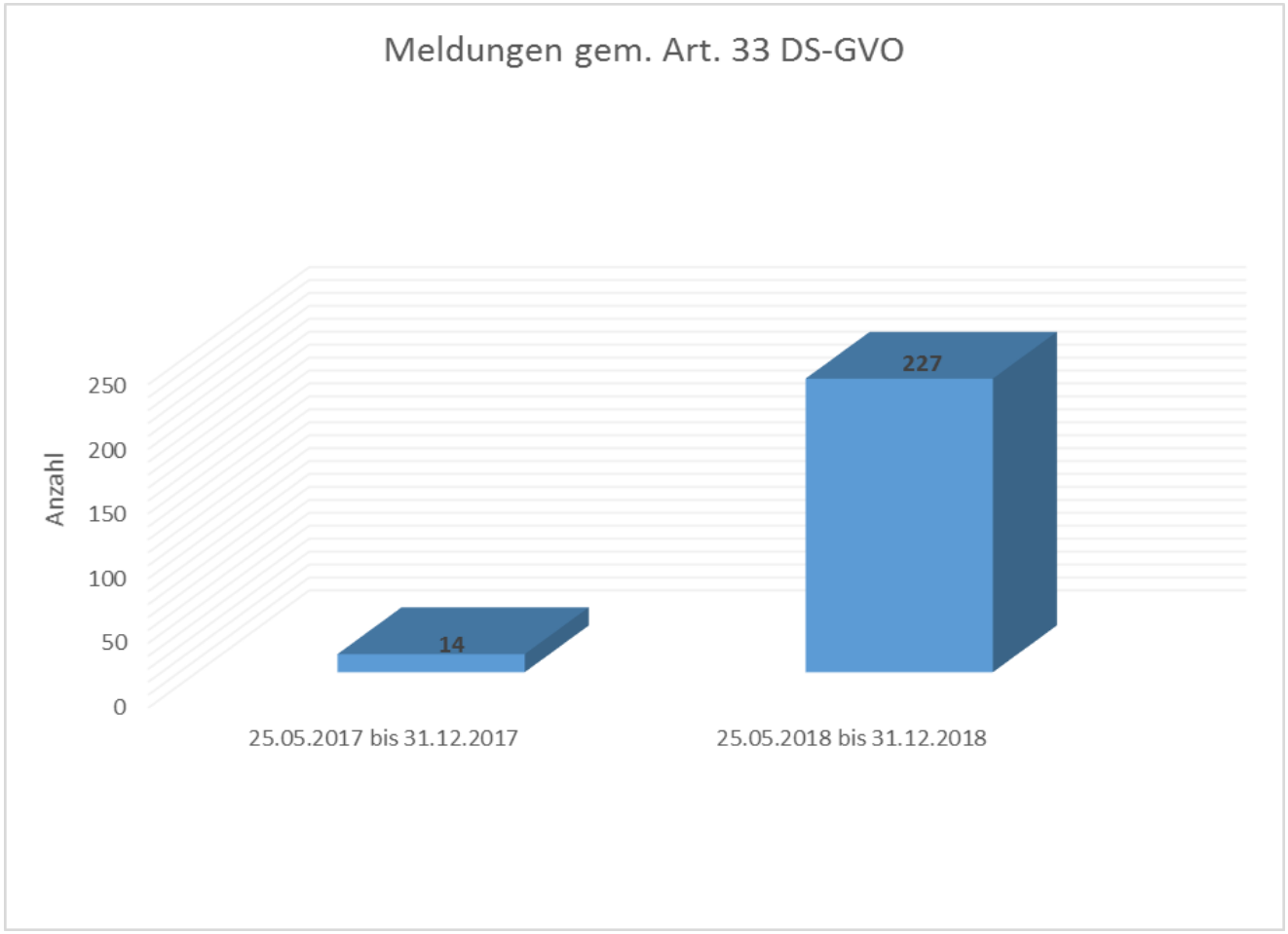
6.2.5 Register der benannten Datenschutzbeauftragten

Gemäß Artikel 37 Absatz 7 DSGVO teilen der Verantwortliche oder der Auftragsverarbeiter die Kontaktdaten des benannten Datenschutzbeauftragten der Aufsichtsbehörde mit. Zum Ende des Berichtszeitraums waren bei meiner Behörde ca. 9.000 entsprechende Meldungen eingegangen. Die überwiegende Anzahl der Mitteilungen zu den Datenschutzbeauftragten erfolgte zur Jahresmitte. Zwischenzeitlich gehen fortwährend monatlich etwa 200 neue Mitteilungen ein.

Auf der Internetpräsenz meiner Behörde sind ein Online-Formular und ein für den Druck vorgesehenes Mitteilungsformular eingestellt worden. Im Falle einer Mitteilung zu dem benannten Datenschutzbeauftragten wird zur besseren Verarbeitung der Informationen meinerseits vorzugsweise die Nutzung des Online-Formulars gebeten.

6.2.6 Verarbeitung der Meldungen von Datenschutzverletzungen gemäß Artikel 33 DSGVO

Im Berichtszeitraum waren 227 Meldungen in Bezug auf Datenschutzverletzungen gemäß Artikel 33 DSGVO eingegangen, vergleiche auch den Beitrag 6.2.1 - oben - und das untenstehende Diagramm.



Gegenüber den Mitteilungen von Datenschutzverletzungen nach Bundesdatenschutzgesetz a. F. generieren die zahlreichen unterschiedlichen Meldungen einen erheblichen Aufwand. Nachfragen und einzuleitende datenschutzaufsichtliche Verfahren werden z. T. erforderlich. Zur verbesserten Erfassung und Verarbeitung der Vorgänge bietet meine Dienststelle ein Online-Formular auf der eigenen Internetseite an, was von den meldenden Verantwortlichen zunehmend angenommen wird.

Zu den vielfältigen Inhalten der Meldungen vergleiche auch den entsprechenden Überblick gewährenden Berichtsbeitrag 4.6.1.

6.2.7 Konsultationen gemäß Artikel 36 DSGVO

Konsultationen meiner Dienststelle gemäß Artikel 36 DSGVO durch Verantwortliche wegen eines aufgrund einer Datenschutz-Folgenabschätzung festgestellten hohen Risikos erfolgten im Berichtszeitraum noch nicht. Die Öffnungsklausel, die eine Konsultation meiner Behörde gemäß Artikel 36 Absatz 5 DSGVO vorsieht, wurde noch nicht in Anspruch genommen.

In einem Vorgang, der die Videoüberwachung im Innenstadtbereich einer Großstadt betraf, wurden von den nach der Datenschutz-Grundverordnung Verantwortlichen die erstellten Datenschutz-Folgenabschätzungen angefordert. Aufgrund des räumlichen

Umfangs der Videoüberwachung und der potentiell hohen Anzahl betroffener Personen, ist meine Behörde in diesem Fall von einer "systematischen und umfangreichen" Datenverarbeitung gemäß Artikel 35 Absatz 3 Buchstabe c) DSGVO ausgegangen. Daneben sind die Auflösung und Sichtfelder der eingesetzten Kameratechnik, die vorgesehene Netzwerkverarbeitung und Zugriffsarchitektur und der wegen mehrerer Verantwortlicher breite Verwendungszweck der Videodatenverarbeitung maßgeblich gewesen, vergleiche auch die Berichtsbeiträge 4.7.1, 6.2.1, 8.1. Das aufsichtliche Verfahren war im Berichtszeitraum noch nicht abgeschlossen.

6.2.8 Prüfung von Verhaltensregeln und Zertifizierungen

Meine Behörde hatte im Berichtszeitraum keine entsprechenden Prüfungen von Verhaltensregeln und Zertifizierungen durchzuführen, vergleiche auch Artikel 40 bis 43 DSGVO.

Zu Zertifizierungen, vergleiche den einführenden Berichtsbeitrag unter 4.9.1 oben.

6.3 Datenschutzaufsichtliche Befugnisse, verwaltungsrechtliche Entscheidungen

6.3.1 Überblick zum Berichtszeitraum

Artikel 58 DSGVO stellt den Aufsichtsbehörden Befugnisse zur effektiven Durchsetzung der Vorschriften der Datenschutz-Grundverordnung zur Verfügung. Dem Vollzugsdefizit im Datenschutzrecht sollte seitens des Verordnungsgebers entgegengewirkt werden. Maßnahmen können gegenüber sämtlichen Verantwortlichen, die der Datenschutz-Grundverordnung und der Aufsicht meiner Behörde unterfallen, erlassen werden, auch öffentlichen Stellen. Neben den auch nach altem Recht im Wesentlichen schon vorhandenen Auskunfts- und Untersuchungsrechten, die mit den Untersuchungsbefugnissen gemäß Artikel 58 Absatz 1 DSGVO ebenso bestehen, verfüge ich nach der Verordnung auch über Abhilfebefugnisse, die die Durchsetzung datenschutzrechtlicher Entscheidungen ermöglichen. Die Auswahl der Befugnisse obliegt dem pflichtgemäßen Ermessen meiner Behörde. Förmliche Entscheidungen gemäß Artikel 58 waren bei Einzelvorgängen bereits im ersten Berichtszeitraum seit Wirksamwerden der Verordnung erlassen worden, allerdings nur in geringem Umfang, was in der Umstellung auf das neue Recht, den hohen zu bearbeitenden Fallmengen und der noch nicht erfolgten personellen Ausstattung und Umstrukturierungen begründet gewesen ist. So sprach meine Behörde unter anderem 4 Warnungen gemäß Artikel 48 Absatz 2 Buchstabe a), 3 Beschränkungen der Datenverarbeitung gemäß Absatz 2 Buchstabe f) und eine Aufforderung zur Einhaltung der Datenschutz-Grundverordnung gemäß Absatz 2 Buchstabe d) aus. Eine förmliche Verwarnung wurde bisher nicht erteilt, vergleiche Artikel 58 Absatz 2 Buchstabe b) DSGVO. Das Mittel der Anordnung zur Durchsetzung einer Entschei-

dung der Aufsichtsbehörde wird nicht in jedem Vorgang erforderlich sein. In dem nächsten Berichtszeitraum erwarte ich dennoch diesbezüglich einen signifikanten Anstieg, zumal etliche Verfahren, die nach der Datenschutz-Grundverordnung eingeleitet worden sind, noch nicht abgeschlossen werden konnten. Auch spezifische Entscheidungen im Rahmen der Befugnisse gemäß des Artikel 58 Absatz 3 DS GVO waren noch nicht ergangen, vergleiche auch den grundlegenden Beitrag 4.9.1 zu Zertifizierungen gemäß Artikel 42, 43 DSGVO.

6.3.2 Unterrichtung der verantwortlichen Stelle über das Ergebnis einer datenschutzaufsichtlichen Prüfung

Stellt meine Behörde in einem datenschutzaufsichtlichen Verfahren einen Datenschutzverstoß fest, wird der Verantwortliche in Kenntnis gesetzt und zur Abhilfe gebeten bzw. aufgefordert. Eine Unterrichtung soll in der Praxis meiner Dienststelle aber auch in den Fällen erfolgen, in denen kein Datenschutzverstoß festgestellt worden ist. Hierbei wird seitens meiner Behörde allerdings darauf zu achten sein, dass dem Verantwortlichen keine zusätzlichen bzw. neuen personenbezogene Information des Betroffenen, die dieser meiner Dienststelle mitgeteilt hat, übermittelt werden.

Eine Rechtsgrundlage für eine entsprechende Mitteilung des Prüfergebnisses an die verantwortliche Stelle erkenne ich gemäß Artikel 58 Absatz 3 Buchstabe b) DSGVO. Hiernach sind zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, selbstständig oder auf Anfrage datenschutzrechtliche Stellungnahmen an die Stellen, die es angeht, zu richten. Der auf eine Eingabe hin – ohne Feststellung eines Datenschutzverstoßes – geprüfte öffentliche oder nicht-öffentliche Verantwortliche ist eine Stelle im Sinne der vorgenannten Vorschrift. Die Mitteilung, dass die Überprüfung des in Rede stehenden Vorgangs keinen Verstoß ergeben hat, ist nach Überzeugung meiner Behörde eine „Stellungnahme“, mit der zu der streitigen personenbezogenen Datenverarbeitung (billigend) Stellung genommen wird. Zugleich erlangt der Verantwortliche dadurch Rechtssicherheit, Datenverarbeitungen weiterhin - ohne Datenschutzverstoß - durchführen zu können.

6.3.3 Überlassung von ungeschwärzten Personalausweisinformationen

Im zurückliegenden Berichtszeitraum erteilte ich einem Verantwortlichen aufgrund der Beschwerde einer betroffenen Person wegen der Aufforderung eine Kopie des Personalausweises ohne Schwärzungen zu übersenden, eine Warnung gemäß Artikel 58 Absatz 2 Buchstabe a) DSGVO. Dass Personalausweiskopien ohne Schwärzungen verlangt werden, ist ein im Geschäftsbetrieb meiner Behörde relativ häufig vorkommender Vorgang.

In dem Beispielsfall wurde durch eine betroffene Person gerügt, dass sie bei der Bewerbung um eine Mietwohnung von einer Mitarbeiterin ihrer Firma aufgefordert worden sei, eine ungeschwärzte Kopie ihres Personalausweises vorzulegen. Begründet worden sei die Anforderung mit „dies ist eine Vorgabe der Gesellschaft Schufa, dafür dass wir Schufa ziehen dürfen“. Nachdem die betroffene Person dies nach ihrer eigenen Darstellung abgelehnt hatte, sei ihr mitgeteilt worden, dass sie als Interessentin leider nicht mehr berücksichtigt werden könne.

Der Personalausweis kann nach § 20 Absatz 1 Personalausweisgesetz (PAuswG) als Identitätsnachweis verwendet werden. Der Ausweisinhaber darf nach § 20 Absatz 2 PAuswG eine Kopie seines Ausweises anfertigen. Die Ablichtung muss eindeutig und dauerhaft als Kopie erkennbar sein. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. Ausweisdaten, die nicht zur Identifizierung notwendig sind, können vom Ausweisinhaber auf der Kopie geschwärzt werden. Das Bundesministerium des Innern, für Bau und Heimat rät auf seiner Webseite (www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis), dass der Ausweisinhaber diese Ausweisdaten schwärzen soll: „Dies gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangsnummer sowie die Seriennummer, sofern nicht gesetzliche Regelungen diese Angaben erfordern.“

Vermieter bzw. Makler sind befugt, die Identität des Mietinteressenten, der für die zu vermietende Wohnung ausgewählt wurde, zu überprüfen. Dies kann z. B. im persönlichen Kundenkontakt durch Vorzeigen eines Personalausweises erfolgen. Angaben zur Identifikation sind Name, Vorname und Anschrift. Wird eine Kopie des Personalausweises gefordert bzw. von ihnen angefertigt, entscheidet der künftige Mieter, ob die Kopie ungeschwärzt bleibt, oder ob zur Identifikation nicht erforderliche Angaben geschwärzt werden. Bei einer Ausweiskopie werden eine Vielzahl von für die Identifizierung nicht erforderliche Daten verarbeitet. Die Verarbeitung dieser Daten der Ausweiskopie ist nicht erforderlich im Sinn von Artikel 6 Absatz 1 Buchstabe b) und Buchstabe f) DSGVO. Die Aufforderung an den potentiellen Mieter, eine Kopie des Personalausweises ohne Schwärzungen zu übergeben bzw. zu übersenden, ist deshalb datenschutzrechtlich unzulässig.

Vor diesem Hintergrund erging gemäß Artikel 58 Absatz 2 Buchstabe a) DSGVO die Warnung an den Verantwortlichen, dass er abzusehen habe von entsprechenden Aufforderungen bzw. Verfahrensweisen, Mietinteressenten, die für die zu vermietende Wohnung ausgewählt wurden, aufzufordern, eine Kopie des Personalausweises ohne Schwärzungen zu übergeben bzw. zu übersenden. Gleichzeitig erfolgte ein Hinweis auf ein mögliches Ordnungswidrigkeitenverfahren.

Der Grundsatz der Datenminimierung ist einzuhalten, Artikel 5 Absatz 1 Buchstabe c) DSGVO.

6.4 Geldbußen und Sanktionen, Strafanträge

6.4.1 Verfolgung Beschäftigter von Verantwortlichen und Auftragsverarbeitern bei Verstößen nach Artikel 83 Absatz 5 DSGVO nach Ordnungswidrigkeitenrecht

Ich ziehe in Bußgeldverfahren gegen Beschäftigte von Verantwortlichen und Auftragsverarbeitern auch Artikel 83 DSGVO heran. Das Verfahren richtet sich in diesen Fällen nach den Vorschriften des Ordnungswidrigkeitengesetzes (OWiG).

Zu verhängende Bußgelder richten sich nach Artikel 83 DSGVO grundsätzlich gegen Verantwortliche oder den Auftragsverarbeiter, nicht aber gegen Beschäftigte, die rechtswidrig (und vorsätzlich) anlässlich ihrer Tätigkeit und unter Nutzung der mit der Tätigkeit verbundenen Möglichkeiten Daten verarbeiten, außer – nach dem Wortlaut – im Falle des Absatz 5.

Im öffentlichen Bereich verweisen zudem bereichsspezifische Vorschriften, unter anderem die Bußgeldvorschrift des § 85 a SGB X über § 41 BDSG auf die Vorschriften der Artikel 83 Absatz 4 bis 6 DSGVO, für die die Vorschriften des OWiG dann sinngemäß gelten.

Meine Dienststelle vertritt zudem die Auffassung, dass rechtswidrig handelnde und Weisungen missachtende Beschäftigte im Falle der unbefugten Verarbeitung personenbezogener Daten im Einzelfall rechtlich selbst zu Verantwortlichen werden können.

§ 22 Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) findet hingegen grundsätzlich nur Anwendung auf ordnungswidrige Handlungen durch Mitarbeiter öffentlicher Stellen außerhalb des Anwendungsbereichs der Datenschutz-Grundverordnung, z. B. unstrukturierte Papiervorgänge und Stellen nach § 2 Absatz 4 SächsDSDG - vergleiche den Wortlaut der Vorschrift - sowie im Anwendungsbereich der Datenschutz-Grundverordnung, soweit die Verordnungsvorschriften des Artikel 83 nicht anwendbar sind.

6.4.2 Ordnungswidrigkeitenverfahren im nicht-öffentlichen Bereich

Die Befugnis der Datenschutzaufsichtsbehörden zur Verfolgung und Ahndung von Ordnungswidrigkeiten nach der Datenschutz-Grundverordnung ergibt sich aus Artikel 58 Absatz 2 Buchstabe i DSGVO. Danach obliegt es ihr, Geldbußen gemäß Artikel 83 DSGVO zu verhängen. Artikel 83 DSGVO legt einerseits in Absatz 2 die Bemessungskriterien für die Bußgeldhöhe fest, andererseits sind in den Absätzen 4 bis 6 auch die

konkreten Bußgeldtatbestände definiert. Im Gegensatz zur früheren Rechtslage gibt es jetzt nur noch sehr wenige Vorschriften ohne Bußgeldbewehrung; zudem sind die Sanktionen insgesamt – dies gilt auch für Nichtunternehmer – drastisch verschärft worden. Die Höchstwerte der möglichen Geldbußen liegen bei den Bußgeldtatbeständen des Absatzes 4 bei 10.000.000 € oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist; bei den Bußgeldbeständen der Absätze 5 und 6 sind sie hingegen sogar doppelt so hoch.

Neu ist insoweit auch die erweiterte Unternehmenshaftung für Mitarbeiterverschulden. Unternehmen haften jetzt im Rahmen des Artikels 83 DSGVO grundsätzlich für schuldhafte Datenschutzverstöße ihrer Beschäftigten. Dabei ist es weder erforderlich, dass für die Handlung ein gesetzlicher Vertreter oder eine Leitungsperson verantwortlich gemacht werden kann, noch muss die Geschäftsführung eines Unternehmens von dem konkreten Verstoß überhaupt Kenntnis haben oder zumindest eine Verletzung der Aufsichtspflicht vorliegen. So genannte Mitarbeiter-Exzesse, d. h. Handlungen von Beschäftigten, die bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden können, sind davon aber ausgenommen.

Zwei weitere in meiner Verfolgungs- und Ahndungszuständigkeit liegende Ordnungswidrigkeitentatbestände sind in § 43 Absatz 1 BDSG enthalten. Diese Tatbestände sehen Geldbußen für Verstöße gegen die speziellen Regelungen des § 30 BDSG – Verbraucherkredite – vor.

Im – vergleichsweise kurzen – Berichtszeitraum sind insgesamt 55 Bußgeldverfahren bei mir anhängig gewesen; 12 davon stammten noch aus der Zeit vor der Anwendbarkeit der DSGVO (vgl. dazu Pkt. 2.12 meines 9. TB im nicht-öffentlichen Bereich), bei den verbleibenden 43 Fällen handelt es sich ausschließlich um neue Anzeigen Dritter.

Rechnet man die neu eingegangenen Verfahren auf den bisher üblichen Zweijahreszeitraum hoch, kommt man auf 147 Verfahren, was den bislang höchsten Wert und gegenüber dem Berichtszeitraum meines 8. TB im nicht-öffentlichen Bereich eine Steigerung auf 144 % darstellt.

In vier Fällen hatte ich keine Zuständigkeit und habe die Verfahren daher an die zuständige Verfolgungsbehörde bzw. im Falle des Verdachts einer Straftat an die Staatsanwaltschaft abgegeben. Drei Verfahren habe ich eingestellt. Im Übrigen habe ich wegen meiner unverändert sehr angespannten Personalsituation im Berichtszeitraum noch keine weiteren Verfahren zum Abschluss bringen und somit auch keine Bußgelder nach der DSGVO verhängen können; mit 48 offenen Verfahren ist auch insoweit ein neuer

Höchstwert zu verzeichnen. Insbesondere im Ordnungswidrigkeitenbereich bin ich also mehr als dringend auf personelle Verstärkungen angewiesen.

6.4.3 Ordnungswidrigkeitenverfahren im öffentlichen Bereich

Vom 25. Mai 2018 bis zum 31. Dezember 2018 war ich im öffentlichen Bereich zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach

- *§ 38 Sächsisches Datenschutzgesetz (§ 38 Absatz 3 Satz 1 SächsDSG),*
- *Artikel 83 Datenschutz-Grundverordnung (Artikel 58 Absatz 2 Buchstabe i DSG-VO, § 14 Absatz 1 SächsDSDG),*
- *§ 22 Absatz 1 Sächsisches Datenschutzdurchführungsgesetz (§ 22 Absatz 3 SächsDSDG) und*
- *§ 111 Absatz 1 Nummer 1 des Vierten Buches Sozialgesetzbuch – Gemeinsame Vorschriften für die Sozialversicherung – (§ 15 Nummer 3 OWiZuVO i. V. m. § 111 Absatz 1 Nummer 1 SGB IV).*

Im Berichtszeitraum waren im öffentlichen Bereich insgesamt 52 Bußgeldverfahren anhängig. Davon wurden sieben mit einem Bußgeld abgeschlossen, wobei gegen einen Bußgeldbescheid Einspruch eingelegt worden ist. Weitere sieben Bußgeldverfahren habe ich eingestellt oder von der Verfolgung abgesehen. 38 Verfahren befanden sich zum Ende des Berichtszeitraumes noch in Bearbeitung.

Berichtszeitraum		**25.05.2018 – 31.12.2018**
anhängig gesamt		**52**
davon	Verfahren aus vorherigem Berichtszeitraum	40
	neu eingegangene Verfahren	12
abgeschlossen		**14**
davon	mit Bußgeld	7
	mit Verwarnungsgeld	0
	eingestellt/von Verfolgung abgesehen	7
noch in Bearbeitung		38
Summe rechtskräftige Bußgelder/ Verwarnungsgelder in €		**6.110**

Die Summe der rechtskräftigen Buß- und Verwarngelder, die dem allgemeinen Staatshaushalt zugutekommen, belief sich auf 6.110 Euro.

In 42 der 52 Verfahren (entspricht ca. 81 %) standen oder stehen Bedienstete der sächsischen Polizei in Verdacht, unbefugt personenbezogene Daten verarbeitet und/oder aus den polizeilichen Informationssystemen abgerufen zu haben. Dieser Umstand erklärt sich aus dem überdurchschnittlichen Anzeigeverhalten der Polizeidirektionen, die datenschutzrechtliches Fehlverhalten ihrer Bediensteten konsequent verfolgen. Er besagt nicht, dass andere Teile der Verwaltung weniger datenschutzrechtliche Ordnungswidrigkeiten begehen. Des Weiteren bestand gegen Bedienstete unterschiedlicher sächsischer Behörden der Verdacht, nicht offenkundige personenbezogene Daten unbefugt verarbeitet zu haben.

Auch an dieser Stelle sei – wie auch in meinen Ausführungen zum Berichtszeitraum 1. April 2017 bis zum Ablauf des 24. Mai 2018 – darauf hingewiesen, dass sich sowohl der personelle Engpass als auch der stetig steigende Bearbeitungsaufwand im Bereich der Ordnungswidrigkeiten negativ auf die Dauer der Verfahren auswirkt.

Bei den im Berichtszeitraum abgeschlossenen Verfahren handelt es sich ausschließlich um Vorgänge, die bereits vor der unmittelbaren Anwendbarkeit der Datenschutz-Grundverordnung am 25. Mai 2018 vorlagen bzw. um Verstöße von Polizeivollzugsbediensteten, für welche weiterhin das insoweit noch fortgeltende Sächsische Datenschutzgesetz anzuwenden war.

Bußgeldverfahren nach der DSGVO habe ich im Berichtszeitraum im öffentlichen Bereich noch nicht durchgeführt.

Drei Ordnungswidrigkeitenverfahren gegen sächsische Polizeibeamte aus dem vorherigen Berichtszeitraum, die nach eingelegtem Einspruch gegen den Bußgeldbescheid an das zuständige Amtsgericht abgegeben worden waren, wurden im Berichtzeitraum gerichtlich entschieden. In zwei Fällen sind den Betroffenen Geldbußen wegen ordnungswidrigen Handelns auferlegt worden, in einem Fall ist die Betroffene, nachdem sie erst im Rahmen der Hauptverhandlung dienstliche Gründe vorbrachte, freigesprochen worden, wobei sie ihre notwendigen Auslagen selbst zu tragen hatte.

Grundsätzlich muss bei den Ordnungswidrigkeiten im öffentlichen Bereich ab der Anwendbarkeit der DSGVO am 25. Mai 2018 unterschieden werden in:

1. Vorgänge, die ab dem 25. Mai 2018 nicht in den Anwendungsbereich der DSGVO fallen – Verstöße durch Bedienstete von Staatsanwaltschaften, Polizei- und Justizvollzugsdienst

Gemäß § 2 Absatz 1 SächsDSG gilt das Sächsische Datenschutzgesetz weiterhin für die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen des Freistaates Sachsen, Gemeinden und Landkreise sowie sonstige der Aufsicht des Freistaates Sachsen unterstehenden juristischen Personen des öffentlichen Rechts, soweit diese innerhalb des Anwendungsbereichs nach Artikel 2 Absatz 1 und 2 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates („JI-RL“, ABl. L 119 vom 4. Mai 2016, S. 89) tätig werden. Gemäß § 42 SächsDSG Satz 2 tritt § 2 Absatz 1 jedoch mit Ablauf des 30. Juni 2019 außer Kraft.

Für die am häufigsten im öffentlichen Bereich vorkommende Ordnungswidrigkeit – unbefugte Verarbeitung von personenbezogenen Daten bzw. unbefugter Abruf personenbezogener Daten aus den polizeilichen Informationssystemen durch Polizeivollzugsbedienstete – gilt demnach bis zum 30. Juni 2019 das Sächsische Datenschutzgesetz weiter.

2. Vorgänge, die ab 25. Mai 2018 in den Anwendungsbereich der DSGVO fallen – Verstöße nach Artikel 83 Absatz 4 bis 6 DSGVO

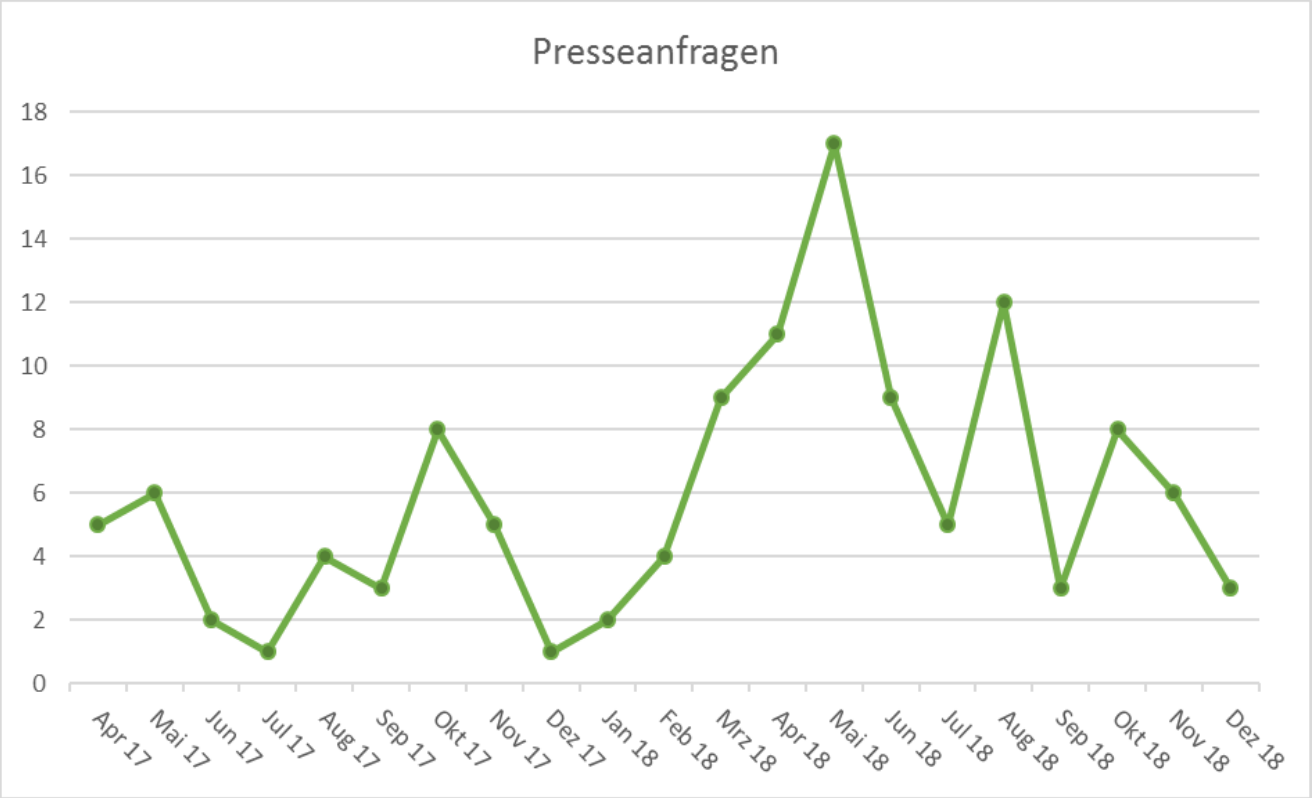
Für das Verfahren der Ahndung und Verfolgung von Verstößen nach Artikel 83 Absatz 4 bis 6 DSGVO gilt, auch im öffentlichen Bereich, nach § 41 BDSG (weiterhin) das Ordnungswidrigkeitengesetz (OWiG). Bei der Bearbeitung von Ordnungswidrigkeitenverfahren, bei denen der Tatzeitpunkt vor dem 25. Mai 2018 liegt, ist demnach § 4 Absatz 3 OWiG zu beachten, bei noch nicht beendeten Dauerverstößen § 4 Absatz 2 OWiG. § 4 Absatz 3 OWiG bestimmt für den Fall, dass das Gesetz, das bei Beendigung der Tat gilt, vor der Entscheidung der Verwaltungsbehörde geändert wird, das mildeste Gesetz anzuwenden ist. Somit muss ich in diesen Fällen entscheiden, ob die bisher geltenden nationalen Ordnungswidrigkeiten-Normen oder die DSGVO anzuwenden ist. In der Regel sind die bisher geltenden nationalen Ordnungswidrigkeiten-Normen das jeweils mildere Gesetz. Eine Einzelfallprüfung in jedem Vorgang bleibt jedoch unabdingbar.

Der Bundesgesetzgeber hat im Rahmen der durch die DSGVO veranlassten Gesetzesänderungen auch den alten Bußgeldparagraphen im SGB X (§ 85 SGB X a. F.) geändert; die an die Stelle getretene Vorschrift (§ 85a SGB X – Bußgeldvorschriften) bestimmt für Sozialdaten die entsprechende Geltung von § 41 BDSG. Wie oben bereits erwähnt, gilt gemäß § 41 BDSG für Verstöße nach Artikel 83 Absatz 4 bis 6 DSGVO und das Verfahren wegen solcher das Ordnungswidrigkeitengesetz (OWiG). Verstöße von Mitarbeitern von sächsischen Sozialbehörden werde ich daher nunmehr gemäß § 85a SGB X und § 41 BDSG nach Artikel 83 Absatz 5 DSGVO verfolgen.

6.5 Öffentlichkeitsarbeit, Internetauftritt und Presse

Mit dem Wirksamwerden der Datenschutz-Grundverordnung waren die bisher bestehenden Inhalte auf der Internetpräsenz des Sächsischen Datenschutzbeauftragten auf ihren Fortbestand hin zu überprüfen. In einem ersten Schritt wurden zunächst alte und der Rechtslage nicht mehr entsprechende Webseiten-Inhalte entfernt. Die zahlreichen und umfassenden Hilfen, die mit der Beteiligung meiner Dienststelle seitens der Datenschutzkonferenz erarbeitet und herausgegeben wurden, finden sich dann auch im Wesentlichen auf der Internetseite meiner Behörde unter https://www.saechsdsb.de. Ein Beschwerdeformular und Vorlagen zur Mitteilung oder Meldung von Datenschutzverstößen gemäß Artikel 33 DSGVO sowie des benannten Datenschutzbeauftragten sind ebenfalls auf der Seite abrufbar. Zusätzlich sind auch Informationen zur Richtlinie (EU) 2016/680, die für die Polizei, Strafverfolgung und -vollstreckung und Bußgeldverfahren anwendbar ist, vorhanden.

Einen Überblick über die Entwicklung der eingegangenen Presseanfragen, die aufgrund des medialen Interesses im letzten Jahr stark angestiegen waren, bietet die nachstehende Darstellung:



Nicht wenige Anfragen und Beschwerden gingen bei meiner Dienststelle wegen einer sogenannten, scheinbar mit Sitz im Land Brandenburg gelegenen sogenannten "Datenschutzauskunft-Zentrale" ein. Selbst Behörden, aber auch Freiberufler und Gewerbetreibende erhielten Fax-Nachrichten der benannten Stelle, die den Anschein erwecken, es handele sich um eine behördliche Aufforderung. In dieser wurden sie veranlasst, ein Formular auszufüllen und zu unterschreiben, unter der Vorgabe, hiermit den Vorschriften der Datenschutz-Grundverordnung nachzukommen. Hierbei handelte sich jedoch um ein teures und kostenpflichtiges Abonnement. Datenschutzaufsichtlich konnte ich nicht handeln, sah mich aber gehalten, gemäß Artikel 58 Absatz 3 Buchstabe b) DSGVO mit einer Pressemitteilung die Öffentlichkeit zu informieren.

6.6 Vortrags- und Schulungstätigkeit

Meine Dienststelle hat im zurückliegenden Berichtszeitraum aufgrund des Inkrafttretens der Datenschutz-Grundverordnung eine sehr hohe Anzahl von Anfragen zu Schulungen und Vorträgen zu verzeichnen gehabt. Die Nachfragen, insbesondere von Behörden, Berufsverbänden und sonstigen berufsständischen Vereinigungen und auch Vereinen bestehen unverändert fort. Leider ist meine Behörde aufgrund der personellen Situation, durchzuführenden internen Umstrukturierungen und wegen des immensen Geschäftsanfalls nicht in der Lage gewesen, dem geltend gemachten Informationsbedarf und Interesse in jedem Fall gerecht zu werden. Sehr viele Anfragen waren daher abschlägig zu beantworten. Hierfür bitte ich um Verständnis. Eine gleichmäßige und flächendeckende Schulung der Verwaltung, Wirtschaft und benannten Datenschutzbeauftragten ist seitens meiner Behörde nicht zu leisten. Eine gezielte strukturierte Weiterbildung über

Schlüsselbereiche und Multiplikatoren der Verwaltung und Wirtschaft bleiben zunächst ein mittelfristiges Ziel.

Gleichwohl wurden zahlreiche Schulungen zum Thema Datenschutz und Informationssicherheit unter Beachtung der neuen Rechtslage durchgeführt. Im behördlichen Bereich wurde zu Änderungen im Bereich des Sozialgesetzbuches aufgrund der Datenschutz-Grundverordnung referiert, bei kommunalen Stellen im gesamten Freistaat Sachsen, bei der Statistik- und Archivverwaltung, beim Fortbildungszentrum des Freistaates Sachsen in Meißen, bei sonstigen kommunalen Fortbildungseinrichtungen, beim Sächsischen Landkreistag und auch bei Schulungen der Rechtsreferendare wurden über Rechtsentwicklungen und Änderungen im Zuge der Einführung der Datenschutz-Grundverordnung durch Bedienstete und meine Behörde informiert.

7 Zusammenarbeit der Datenschutzaufsichtsbehörden, Datenschutzkonferenz

7.1 Zusammenarbeit, Amtshilfe und gemeinsame Maßnahmen der Aufsichtsbehörden

Mehr als ein halbes Jahr ist seit dem ersten Tag der unmittelbaren Anwendbarkeit der Europäischen Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 mittlerweile vergangen. Nicht nur Verantwortliche und Auftragsverarbeiter wie Unternehmen oder Vereine haben mit der DSGVO Neuland betreten, auch für mich haben sich erhebliche Veränderungen ergeben.

Eine wichtige Neuerung der DSGVO ist die Art und Weise, wie die Aufsichtsbehörden der Mitgliedstaaten der Europäischen Union zusammenarbeiten, um eine einheitliche Anwendung der DSGVO und einen einheitlichen Schutz von betroffenen Personen bei der Verarbeitung ihrer Daten in der gesamten EU zu gewährleisten.

7.1.1 „One-Stop-Shop“

Neu ist der in Artikel 56 DSGVO zu findende Ansatz des „One-Stop-Shops“. Damit wird das Prinzip bezeichnet, dass dem jeweiligen Verantwortlichen oder Auftragsverarbeiter bei grenzüberschreitenden Sachverhalten lediglich eine einzige, die sog. federführende, Aufsichtsbehörde als Ansprechpartner zur Verfügung steht.

Bislang war die wechselnde Zuständigkeit von unterschiedlichen Aufsichtsbehörden in der Praxis ein erhebliches Problem. So konnte es passieren, dass ein Unternehmen der Aufsicht mehrerer Aufsichtsbehörden in unterschiedlichen Mitgliedsstaaten unterlag. Auch der Betroffene einer Datenschutzverletzung wiederum musste sich an die Aufsichtsbehörde des anderen Mitgliedsstaates wenden, in der der Verantwortliche seinen Sitz hatte. Diese Problematik gehört nunmehr der Vergangenheit an.

Die Vorteile des Prinzips liegen auf der Hand: Der Aufwand soll sowohl für die Behörden als auch für die Unternehmen reduziert werden, da jede Fragestellung nur einmal geklärt wird. Zudem soll dadurch ausgeschlossen werden, dass verschiedene Datenschutzbehörden, trotz eigentlich einheitlicher gesetzlicher Grundlage, unterschiedliche Auffassungen vertreten. Erste Erfahrungen sind vielversprechend.

7.1.2 Grenzüberschreitende Verarbeitung

Die Anwendung des Artikels 56 Absatz 1 DSGVO setzt das Vorliegen einer „grenzüberschreitenden Datenverarbeitung“ gemäß Artikel 4 Nummer 23 DSGVO voraus. Eine solche ist bei der Verarbeitung im Rahmen der Tätigkeit von Niederlassungen eines

Verantwortlichen oder Auftragsverarbeiters in mehr als einem Mitgliedstaat gegeben. Von einer grenzüberschreitenden Verarbeitung ist jedoch auch in den Fällen auszugehen, in denen die Tätigkeit eines Verantwortlichen oder Auftragsverarbeiters in einem Mitgliedsstaat erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann. Insbesondere im Zeitalter von Internetdienstleistungen und international tätiger Konzerne ist grenzüberschreitende Datenverarbeitung in zahlreichen Fällen gegeben.

Erfolgt die Datenverarbeitung des Verantwortlichen jedoch nur in einem Mitgliedstaat, verfügt der Verantwortliche auch über keine Niederlassung in einem anderen Mitgliedsstaat und sind auch keine erheblichen Auswirkungen auf betroffene Personen in mehr als einem Mitgliedsstaat anzunehmen, dann ist von einem ausschließlich lokalen Fall auszugehen. Auf diesen findet das „One-Stop-Shop“-Verfahren keine Anwendung.

Diese Abgrenzung bereitet den Aufsichtsbehörden in der EU nach meiner Einschätzung jedoch derzeit noch Schwierigkeiten.

Betrifft die Datenverarbeitung nämlich ausschließlich eine bestimmte Niederlassung und ist keine erhebliche Auswirkung auf betroffene Personen in anderen Mitgliedsstaaten gegeben, verbleibt es bei der Zuständigkeit der örtlich zuständigen Datenschutzbehörde, auch wenn der Verantwortliche weitere Niederlassungen in anderen Mitgliedsstaaten hat.

Darüber hinaus hat sich das Verfahren für von einer Datenschutzverletzung betroffene Personen vereinfacht. Musste man sich vor Geltung der DSGVO an die Aufsichtsbehörde des Mitgliedstaats wenden, in dem das Unternehmen seinen Hauptsitz oder seine Niederlassung hat, etwa wenn man eine Datenschutzverletzung in einem sozialen Netzwerk vermutete, so kann man sich seit der Geltung der DSGVO ungeachtet des Sitzes des Unternehmens an die Behörde seines Aufenthaltsortes wenden.

7.1.3 Federführende Aufsichtsbehörde

Bei Anwendung des Artikel 56 Absatz 1 DSGVO bedarf es zudem der Feststellung der federführenden Aufsichtsbehörde anhand der (Haupt-)Niederlassung gemäß Artikel 4 Nummer 16 DSGVO.

Im „Normalfall“ ist die Hauptverwaltung des betreffenden Unternehmens in der EU die Hauptniederlassung. Notwendig in diesem Zusammenhang ist jedoch die Prüfung, ob die Entscheidungen über Zwecke und Mittel einer Verarbeitung ggf. in einer anderen Niederlassung getroffen werden. Hierbei wird die konkrete Verarbeitungstätigkeit in den Blick genommen. Es sind Konstellationen denkbar, in denen für eine bestimmte Verarbeitung die Hauptverwaltung als Hauptniederlassung gilt, für eine andere jedoch

eine andere Niederlassung. Für unterschiedliche grenzüberschreitende Verarbeitungen im selben Unternehmen können damit unterschiedliche Aufsichtsbehörden federführend sein.

7.1.4 Betroffene Aufsichtsbehörde

Neben der federführenden Aufsichtsbehörde gibt es noch die „andere betroffene Aufsichtsbehörde“. Darunter versteht man die Aufsichtsbehörden der Mitgliedstaaten, in denen sich weitere Niederlassungen des Unternehmens befinden, sowie solche, in denen Personen leben, auf die die Verarbeitung erhebliche Auswirkungen hat oder haben kann.

Ich bin beispielsweise „betroffene Aufsichtsbehörde“, wenn ein Verantwortlicher im Freistaat Sachsen über eine Niederlassung verfügt oder die Verarbeitung personenbezogener Daten erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Freistaat Sachsen hat. Betroffene Aufsichtsbehörde bin ich auch, wenn eine betroffene Person bei mir die entsprechende Beschwerde eingereicht hat.

Ob ich eine „betroffene Aufsichtsbehörde“ bin, muss ich immer dann prüfen, wenn die Aufsichtsbehörde eines Mitgliedstaats einen Fall grenzüberschreitender Verarbeitung in dem dafür vorgesehenen Informationssystem „IMI“ (siehe dazu unten) bekannt gibt. Bis Dezember 2018 betraf dies ca. 245 Fälle. Ist das Ergebnis der Prüfung, dass ich betroffen bin, muss dies entsprechend erklärt werden.

Die federführende Aufsichtsbehörde bindet bei ihrer Entscheidungsfindung alle betroffenen Aufsichtsbehörden ein.

7.1.5 Kooperations- und Kohärenzverfahren

An das Verfahren der Bestimmung einer federführenden und von betroffenen Aufsichtsbehörden schließt sich das Kooperationsverfahren nach Artikel 60 DSGVO an, um in grenzüberschreitenden Fällen Konsens zwischen der federführenden und den betroffenen Aufsichtsbehörden bezüglich einer geplanten Entscheidung zu erzielen.

Die federführende Aufsichtsbehörde übermittelt die verfügbaren Informationen und einen Beschlussentwurf an die betroffenen Aufsichtsbehörden. Diese können Einspruch gegen den Entscheidungsvorschlag einlegen.

Ergibt der Abstimmungsprozess ein einhelliges Ergebnis, ergeht der entsprechende Beschluss gegenüber der Hauptniederlassung des Verantwortlichen oder des Auftragsverarbeiters.

Wird im beschriebenen Kooperationsverfahren hingegen kein Konsens erzielt, ist das sogenannte Kohärenzverfahren nach Artikel 63, 65 DSGVO durchzuführen.

Dies wird eingeleitet, wenn eine betroffene Aufsichtsbehörde Einspruch gegen den Beschlussentwurf einlegt und die federführende Aufsichtsbehörde sich diesem nicht anschließt.

Im Kohärenzverfahren hat der Europäische Datenschutzausschuss (EDSA) die Befugnis, zur Lösung des Konflikts verbindliche Beschlüsse zu treffen. Im EDSA wird Deutschland durch einen gewählten Gemeinsamen Vertreter oder dessen Stellvertreter vertreten, der an einen von Bund und Ländern erarbeiteten gemeinsamen Standpunkt gebunden ist.

7.1.6 Binnenmarktinformationssystem (Internal Market Information System, IMI)

Um die genannten Verfahren EU-weit in der Praxis zu koordinieren, wird das sog. Binnenmarktinformationssystem (Internal Market Information System, IMI) genutzt. Das IMI ist ein IT-gestütztes Netzwerk zum Informationsaustausch zwischen öffentlichen Stellen im Binnenmarkt. Es ist von der Europäischen Kommission zusammen mit den Mitgliedsstaaten der EU entwickelt worden, um die Verwaltungszusammenarbeit über Grenzen hinweg zu vereinfachen und zu beschleunigen. Seit dem vergangenen Jahr wird das IMI auch genutzt, um die Datenschutzaufsichtsverfahren zu koordinieren.

Mir obliegt es, wie oben dargestellt, in jedem einzelnen eingestellten Fall zu prüfen, ob ich entweder als federführende Aufsichtsbehörde handeln muss, weil beispielsweise das Unternehmen, bei dem eine mutmaßliche Datenschutzverletzung zu prüfen ist, seinen Hauptsitz im Freistaat Sachsen hat, oder ob ich betroffene Aufsichtsbehörde bin, weil der Verantwortliche eine Niederlassung im Freistaats Sachsen hat oder die Verarbeitung erhebliche Auswirkung auf betroffene Personen in Sachsen hat oder haben kann.

Die Prüfungsschritte innerhalb der von der DSGVO vorgesehenen Verfahren hinsichtlich einer möglichen Betroffenheit stellen mich vor nicht unerhebliche zeitliche und organisatorische Herausforderungen.

7.1.7 Fazit

Das mit der DSGVO eingeführte „One-Stop-Shop“-Prinzip stellt einen wichtigen Schritt zur einheitlichen Rechtsanwendung in der EU dar. Insbesondere international tätigen Unternehmen kann dies neben der Verringerung des Verwaltungsaufwands die dringend benötigte Rechtssicherheit geben. Aber auch für von Datenschutzverletzungen betroffene Personen ergeben sich Vereinfachungen.

Bis zum Ende des Jahres wurden jedoch trotz der relativ kurzen Reaktions- und Stellungnahmefristen im Kooperations- sowie im Kohärenzverfahren nur sehr wenige der o.g. 245 Fälle grenzüberschreitender Verfahren zum Abschluss geführt, so dass eine Bewertung dieser neuen Instrumente verfrüht wäre.

Anfängliche Unsicherheiten bezüglich einer grenzüberschreitenden Verarbeitung werden langsam abgelegt, doch der Lernprozess ist derzeit weder auf der Seite der Verantwortlichen noch auf der Seite der Datenschutzaufsichtsbehörden abgeschlossen.

7.2 Materialien der Datenschutzkonferenz

7.2.1 Internetpräsenz der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)

Im Jahre 2018 wurde seitens der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine offizielle Internetseite eingerichtet (https://www.datenschutzkonferenz-online.de).

Auf der Seite werden neben weiteren Informationen Kurzpapiere, Entschließungen, Beschlüsse, Orientierungshilfen, Anwendungshinweise, Protokolle der DSK, Pressemitteilungen, Beschlüsse des Arbeitskreises Wirtschaft (Düsseldorfer Kreis), Dokumente des Europäischen Datenschutzausschusses (EDSA) und genehmigte Verhaltensregeln bereitgestellt.

In den nachstehenden Beitragstexten finden Sie Entschließungen, Beschlüsse und Orientierungshilfen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) des Berichtszeitraums aufgeführt. Auf verfügbare Kurzpapiere und Anwendungshinweise wird angesichts der Verfügbarkeit auf der benannten Internetseite und wegen möglicher Fortschreibungen und Ergänzungen lediglich verwiesen.

7.2.2 Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11.06.2018: 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 DSGVO 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 DSGVO 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 DSGVO. Auf die hohen Anforderungen an die Freiwilligkeit nach Art. 7 Abs. 4 DSGVO 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 Absatz 1 S. 1 lit. b DSGVO 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 DSGVO 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.

7.2.3 Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. Juni 2018 in Düsseldorf: 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 (DSGVO) 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 DSGVO 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 DSGVO erfüllt.

- Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage-Betreibern ist in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtung der DSGVO 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.

7.2.4 Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 5. September 2018 in Düsseldorf: 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 nichtöffentliche 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.

7.2.5 Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 5. September 2018 in Düsseldorf: 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.

7.2.6 Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 5. September 2018 in Düsseldorf: 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.

7.2.7 Geschäftsordnung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder mit Beschluss vom 5. September 2018

Mit Beschluss vom 5.9.2018 hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) eine Geschäftsordnung verabschiedet, in der Zusammensetzung, Zweck, Aufgaben der Konferenz und deren Arbeitsweise festgelegt wurden. Die Geschäftsordnung umfasst auch die Einrichtung und Arbeit von (Fach-) Arbeitskreisen und die Mitwirkung der deutschen Aufsichtsbehörden in Gremien der Europäischen Union. Die Geschäftsordnung ist auf der Internetpräsenz der DSK unter der Rubrik Beschlüsse abrufbar (https://www.datenschutzkonferenz-online.de/beschluesse-dsk.html).

7.2.8 Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 7. November 2018 in Münster: 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 Verhal-

ten 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!

7.2.9 Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DSGVO)

Stand: November 2018

Inhalt

1. Datenschutz-Grundverordnung (DSGVO) und Direktwerbung

1.1 Begriff der Werbung im Sinne der DSGVO

Werbung bzw. Direktwerbung im Sinne der DSGVO ist zum einen die von Unternehmen, Selbständigen, Verbänden und Vereinen usw. durchgeführte Wirtschaftswerbung zum Aufbau und zur Förderung eines Geschäftsbetriebs. „Werbung“ wird hierzu in Art. 2 lit. a der EU-Richtlinie 2006/114/EG über irreführende und vergleichende Werbung vom 12. Dezember 2006 definiert als „jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen, einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen, zu fördern“.

Diese weitgreifende Betrachtungsweise von Werbung legen auch die Gerichte in ihren Entscheidungen zu Grunde und sehen z. B. damit auch Zufriedenheitsnachfragen bei Kunden nach einem Geschäftsabschluss, Geburtstags- und Weihnachtsmailings usw. als Werbung an.

Zum anderen ist Werbung bzw. Direktwerbung im Sinne der DSGVO aber auch die Kontaktaufnahme durch Parteien, Verbände und Vereine oder karitative und soziale Organisationen mit betroffenen Personen, um ihre Ziele bekannt zu machen oder zu fördern (siehe zur Werbung von politischen Parteien z. B. BVerfG-Beschluss vom 01.08.2002, 2 BvR 2135/01).

1.2 Keine Detailregelungen dazu in der DSGVO

Mit der DSGVO sind alle detaillierten Regelungen des bisherigen Bundesdatenschutzgesetzes (BDSG) zur Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung weggefallen (siehe bisher insbesondere § 28 Abs. 3 und 4 sowie § 29 BDSG-alt).

Grundlage für die Beurteilung der Zulässigkeit einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung ist in der DSGVO, abgesehen von einer Einwilligung der betroffenen Person, eine Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO. Danach muss die Verarbeitung zur Wahrung der berechtigten Interessen des

Verantwortlichen erforderlich sein, sofern nicht die Interessen der betroffenen Person überwiegen. Anhaltspunkte für die zu treffende Abwägungsentscheidung enthält Erwägungsgrund (ErwGr.) 47 DSGVO, der u. a. ausführt: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden."

1.3 Interessenabwägung

Die DSGVO verlangt eine Abwägung im konkreten Einzelfall sowohl im Hinblick auf die Interessen der Verantwortlichen bzw. Dritten als auch der betroffenen Person. Ein bloßes Abstellen auf abstrakte oder auf vergleichbare Fälle ohne Betrachtung des Einzelfalls genügt den Anforderungen der DSGVO nicht.

Insoweit ergibt sich für die Interessenabwägung u. a. aus ErwGr. 47, dass die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen sind. Damit ist auch auf die subjektiven Erwartungen der betroffenen Person im Einzelfall abzustellen.

Neben diesen ist aber auch zu fragen, was objektiv vernünftigerweise erwartet werden kann und darf. Entscheidend ist daher auch, ob die Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung in bestimmten Bereichen der Sozialsphäre typischerweise akzeptiert oder abgelehnt wird.

Die Erwartungen der betroffenen Person werden bei Maßnahmen zur Direktwerbung auch durch die Informationen nach Art. 13 und 14 DSGVO zu den Zwecken der Datenverarbeitung bestimmt. Informiert der Verantwortliche transparent und umfassend über eine vorgesehene Verarbeitung von Daten für Zwecke der Direktwerbung, geht die Erwartung der betroffenen Personen in aller Regel auch dahin, dass ihre Kundendaten entsprechend genutzt werden. Allerdings kann durch Transparenz der gesetzliche Abwägungstatbestand nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO nicht beliebig erweitert werden, da die Erwartungen an dem objektiven Maßstab der Vernunft gemessen werden müssen.

Die Datenverarbeitung muss ferner insgesamt im Hinblick auf die berechtigten Interessen erforderlich sein.

Zudem sind bei der Interessenabwägung die ohnehin geltenden allgemeinen Grundsätze aus Art. 5 Abs. 1 DSGVO zu berücksichtigen, also insbesondere:

- faire Verfahrensweise,
- dem Verarbeitungszweck angemessen,
- in einer für die betroffene Person nachvollziehbaren Weise (insbesondere Nennung der Quelle der Daten, wenn Fremddaten verarbeitet werden)

1.3.1 Praxisfälle Interessenabwägung

Vorbehaltlich der konkreten Abwägung im Einzelfall und den ergänzenden Ausführungen zu Punkt 1.4 und 1.5. können folgende Grobkategorien für die Abwägung in der Praxis relevant werden:

Schutzwürdige Interessen dürften in der Regel nicht überwiegen, wenn im Nachgang zu einer Bestellung allen Kunden (ohne Selektion) postalisch ein Werbekatalog oder ein Werbeschreiben zum Kauf weiterer Produkte des Verantwortlichen zugesendet wird.

Sofern es anhand eines Selektionskriteriums zu einer Einteilung in Werbegruppen kommt und sich kein zusätzlicher Erkenntnisgewinn aus der Selektion ergibt, wird die Interessenabwägung in der Regel ebenfalls zugunsten des Verantwortlichen ausfallen.

Eingriffsintensivere Maßnahmen wie automatisierte Selektionsverfahren zur Erstellung detaillierter Profile, Verhaltensprognosen bzw. Analysen, die zu zusätzlichen Erkenntnissen führen, sprechen hingegen dafür, dass ein Interesse der betroffenen Person am Ausschluss der Datenverarbeitung überwiegt. In diesen Fällen handelt es sich um Profiling, das nicht mehr auf Art. 6 Abs. 1 lit. f) DSGVO gestützt werden kann und damit die Einholung einer Einwilligung vor der Datenverarbeitung erforderlich macht. Das Widerspruchsrecht des Art. 21 DSGVO reicht dann nicht aus.

Auch die Erstellung eines Profils unter Verwendung externer Datenquellen (z. B. Informationen aus sozialen Netzwerken) für Zwecke der Direktwerbung (Werbescores) wird in der Regel zu einem Überwiegen der schutzwürdigen Interessen der betroffenen Person führen.

Hinsichtlich der Übermittlung von Daten für Werbezwecke an Dritte sowie der Nutzung von Fremdadressen ist zu prüfen, ob dem Interesse der betroffenen Person ein höherer Stellenwert einzuräumen ist als dem Interesse des Verantwortlichen an der Übermittlung sowie des Dritten zur Nutzung von Fremdadressen zur Werbung. Insoweit erläutert ErwGr 47, dass die Erwartungshaltung des Betroffenen auch davon bestimmt wird, ob

eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn diese Kunde des Verantwortlichen ist. Die Vorgaben des Art. 6 Abs. 4 DSGVO sind ggf. zu beachten (Punkt 1.5.).

1.4 Spezifische Regelungen für verschiedene Kontaktwege

Zu den konkreten Formen der Direktwerbung, also dem Kontaktweg zu den betroffenen Personen (Ansprache per Telefonanruf, E-Mail, Fax etc.), regelt das Wettbewerbsrecht, § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG), in welchen Fällen von einer unzumutbaren Belästigung der Beworbenen auszugehen und eine Werbung dieser Art unzulässig ist.

Weil Art. 6 Abs. 1 Satz 1 lit. f DSGVO eine Verarbeitung personenbezogener Daten nur für zulässig erklärt, soweit die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, sind auch bei der datenschutzrechtlichen Beurteilung einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung die Wertungen in den Schutzvorschriften des UWG für die jeweilige Werbeform mit zu berücksichtigen. Wenn für den werbenden Verantwortlichen ein bestimmter Kontaktweg zu einer betroffenen Person danach nicht erlaubt ist, kann die Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO auch nicht zugunsten der Zulässigkeit einer Verarbeitung dieser Kontaktdaten für Zwecke der Direktwerbung ausfallen.

1.4.1 Nutzen der E-Mail-Adressen von Bestandskunden

E-Mail-Adressen, die unmittelbar von den betroffenen Personen im Rahmen einer Geschäftsbeziehung (Bestandskunden) erhoben wurden, können grundsätzlich für E-Mail-Werbung genutzt werden, wenn dieser Zweck der E-Mail-Werbung entsprechend Art. 13 Abs. 1 lit c DSGVO den betroffenen Personen bei der Datenerhebung transparent dargelegt worden ist. Überwiegende schutzwürdige Interessen der betroffenen Person nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO sind insbesondere dann nicht gegeben, wenn die in § 7 Abs. 3 UWG enthaltenen Vorgaben für elektronische Werbung eingehalten werden.

1.4.2 Nutzen von Telefonnummern

Für Anrufe bei Verbrauchern zu Zwecken der Direktwerbung sieht das UWG (§ 7 Abs. 2 Nr. 2) keine Ausnahme vom Einwilligungserfordernis vor, so dass ein solches Nutzen von Telefonnummern ohne vorherige Einwilligung wegen der besonderen Auswirkungen dieser Werbeform (stärkere Belästigung/Störung) datenschutzrechtlich an den überwiegenden schutzwürdigen Interessen der betroffenen Personen gemäß Art. 6 Abs. 1 Satz 1 lit. f DSGVO scheitert.

Bei Werbung mit einem Telefonanruf gegenüber einem sonstigen Marktteilnehmer (B2B) kommt es für die Zulässigkeit gemäß § 7 Abs. 2 Nr. 2 UWG darauf an, dass von dessen zumindest mutmaßlicher Einwilligung ausgegangen werden kann. Im B2B-Bereich stehen deshalb bei einem Nutzen von Telefonnummern für Werbeanrufe datenschutzrechtlich nicht von vorne herein überwiegende schutzwürdige Interessen der telefonisch anzusprechenden Gewerbetreibenden nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO entgegen.

Siehe zum Verbot der Telefonwerbung gegenüber Gewerbetreibenden dazu ergänzend auch BGH, Urteil vom 16. November 2006, Az. I ZR 191/03, und BGH, Urteil vom 20. September 2007, Az. I ZR 88/05.

1.5. Zweckänderung

Sofern personenbezogene Daten für Werbezwecke verwendet werden sollen, die ursprünglich nicht (auch) zu Zwecken der Werbung erhoben worden sind, sind die Regelungen des Art. 6 Abs. 4 DSGVO (Zweckänderung) zu beachten. Eine Zweckänderung kann auch bei Fällen der Übermittlung an Dritte für Werbezwecke und bei der Nutzung von Fremdadressen für Werbung einschlägig sein, wenn sich die Datenverarbeitung nicht im Rahmen des Erhebungszweckes bewegt.

Um herauszufinden, ob der Werbezweck mit der ursprünglichen Zweckbestimmung vereinbar ist, müssen Verantwortliche eine sog. Kompatibilitätsprüfung durchführen.

2. Informationspflichten

2.1 Unterrichtung bei der Datenerhebung

Werden personenbezogene Daten unmittelbar bei der betroffenen Person erhoben, z. B. für Kauf- und Dienstleistungsverträge, Prospektanforderungen oder Gewinnspiele, ist diese umfassend nach Art. 13 Abs. 1 und 2 DSGVO u. a. über die Zwecke der Verarbeitung der Daten zu unterrichten. Eine schon geplante oder in Betracht kommende Verarbeitung oder Nutzung der Daten für Zwecke der Direktwerbung ist daher der betroffenen Person von Anfang an transparent darzulegen.

Bei einer nachträglichen Änderung der Verarbeitung auch für Zwecke der Direktwerbung schreibt Art. 13 Abs. 3 DSGVO eine vorherige Information vor. Diese Information ist mit einem Hinweis auf das Werbewiderspruchsrecht zu versehen.

Grundsätzlich ist vom Verantwortlichen zum Zeitpunkt der Datenerhebung über alle Themen nach Art. 13 Abs. 1 und 2 DSGVO zu informieren. Allerdings besteht schon rein praktisch nicht immer die Möglichkeit, der betroffenen Person alle Informationen

aus Art. 13 Abs. 1 und 2 DSGVO sofort vollständig geben zu können, z. B. bei Bestell-Postkarten als Zeitschriften-Beilage, bei Bestellungen am Telefon oder bei Kaufverträgen an Automaten. Die Aufsichtsbehörden unterstützen daher den Vorschlag der Artikel 29-Gruppe (WP 260, S. 17) für ein zweistufiges Informationsmodell.

Aus den Informationspflichten nach Art. 13 Abs. 1 und 2 DSGVO ergeben sich in der Regel folgende grundsätzliche Mindestanforderungen (entscheidend ist aber stets der Informationsbedarf im Einzelfall), die regelmäßig auf einer ersten Stufe umgesetzt werden müssen:

- Identität des für die Verarbeitung Verantwortlichen (Name einschließlich Kontaktdaten)
- Kontaktdaten des betrieblichen Datenschutzbeauftragten (soweit benannt)
- Verarbeitungszwecke und Rechtsgrundlage in Schlagworten
- Angabe des berechtigten Interesses, soweit die Verarbeitung darauf beruht
- Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- Übermittlung in Drittstaaten
- Widerspruchsrecht nach Art. 21 DSGVO
- Hinweis auf Zugang zu den weiteren Pflichtinformationen gem. Art. 13 Abs. 1 und 2 DSGVO (wie Auskunftsrecht, Beschwerderecht), z. B. auch mittels QR-Code oder Internet-Link

2.2 Zeitpunkt der Information nach Art. 14 DSGVO

Sollen personenbezogene Daten der betroffenen Person für Zwecke der Direktwerbung verarbeitet werden, die nicht von dieser Person selbst erhoben wurden, sind die Informationspflichten nach Art. 14 Abs. 1 und 2 DSGVO zu beachten.

Eine unverzügliche oder separate Information fordert das Gesetz zwar nicht. Die Information muss jedoch innerhalb einer angemessenen Frist, jedenfalls zum Zeitpunkt der Aussendung einer Werbung, spätestens aber innerhalb eines Monats nach einer Verarbeitung erfolgen. Erfolgt die Information in Verbindung mit der ersten Werbezusendung, sind beide Bestandteile (Information und Werbetext) klar voneinander zu trennen und die Information (einschließlich Hinweis auf das Werbewiderspruchsrecht) entsprechend deutlich herauszustellen.

2.3 Information des Bestandes („Altfälle“)

Art. 13 und 14 DSGVO stellen für die Informationspflichten vom Wortlaut her gesehen zunächst auf Datenerhebungen nach Wirksamwerden der DSGVO ab („Werden personenbezogene Daten … erhoben…“).

Die Art.-29-Gruppe geht jedoch im Hinblick auf ErwGr. 171 Satz 2 („Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden.“) und der Grundsätze aus Art. 5 Abs. 1 lit. a DSGVO zur Transparenz bei der Erarbeitung des WP 260 davon aus, dass bei den künftigen Kontakten mit den betroffenen Personen die neuen Informationspflichten in angemessener Weise umzusetzen bzw. nachzureichen sind (siehe dazu unter Nr. 2.1, Mindestinformationen, Verweis, wo alle Informationen unschwer zu erlangen sind).

3. Einwilligung in die Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung

3.1 Gestaltung der Einwilligung

Die Einwilligung ist als eine Rechtmäßigkeitsvoraussetzung für die Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 Satz 1 lit. a DSGVO nur wirksam, wenn sie freiwillig und – bezogen auf einen bestimmten Fall – informiert abgegeben wird. Informiert setzt voraus, dass auch die Art der beabsichtigten Werbung (Brief, E-Mail/SMS, Telefon, Fax), die Produkte oder Dienstleistungen, für die geworben werden soll, und die werbenden Unternehmen genannt werden, um den Transparenzanforderungen von Art. 12 Abs. 1 und Art 13 Abs. 1 lit. c DSGVO sowie der bisher insoweit ergangenen Rechtsprechung zu genügen (siehe z. B. BGH-Urteil vom 14.03.2017, Az. VI ZR 721/15).

Erforderlich ist nach Art. 4 Nr. 11 und Art. 7 Abs. 2 DSGVO eine unmissverständlich abgegebene Willensbekundung in Form einer Erklärung in einer klaren und einfachen Sprache oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person ihr Einverständnis zur Verarbeitung der sie betreffenden Daten erteilt.

Die Schriftform für datenschutzrechtliche Einwilligungen sieht die DSGVO nicht als Regelfall vor.

Verantwortliche haben allerdings gemäß Art. 5 Abs. 2 DSGVO die Einhaltung der Rechtmäßigkeitsvoraussetzungen der Datenverarbeitung und gemäß Art. 7 Abs. 1 DSGVO auch speziell das Vorliegen einer Einwilligung nachzuweisen. Um dieser Verpflichtung nachkommen zu können, ist den Verantwortlichen anzuraten, sich regelmä-

ßig um eine Einwilligung in Schriftform mit handschriftlicher Unterschrift oder mindestens in Textform (z. B. E-Mail) zu bemühen.

Für Einwilligungen ist regelmäßig ein gesonderter Text oder Textabschnitt ohne anderen Inhalt zu verwenden. Soll sie zusammen mit anderen Erklärungen (insbesondere vertraglichen Erklärungen) schriftlich oder in einem elektronischen Format erteilt werden, so ist die datenschutzrechtliche Einwilligungserklärung gemäß Art. 7 Abs. 2 Satz 1 DSGVO in einer von anderen Sachverhalten klar unterscheidbaren Weise darzustellen.

3.2 Einwilligung mit Übergabe von Visitenkarten

Visitenkarten, die von den betroffenen Personen auf Messen oder sonstigen Veranstaltungen ausdrücklich zur Informationszusendung oder weiteren geschäftlichen Kontaktaufnahme hinterlassen werden, können grundsätzlich eine wirksame Einwilligung im Sinne von Art. 4 Nr. 11 DSGVO darstellen, wenn infolge weiterer Umstände für den Verantwortlichen eine Nachweisbarkeit der Einwilligung gegeben ist.

3.3 Double-Opt-In-Verfahren für elektronische Einwilligungen

Für das elektronische Erklären einer Einwilligung ist - zur Verifizierung der Willenserklärung der betroffenen Person - das Double-Opt-In-Verfahren geboten (je nach konkreter Art des Kontaktes: E-Mail oder SMS), wobei die Nachweis-Anforderungen des Art. 5 Abs. 2 DSGVO und des BGH (Urteil vom 10. Februar 2011, I ZR 164/09) bei der Protokollierung zu berücksichtigen sind. Das bloße Abspeichern der IP-Adressen von Anschlussinhabern und die Behauptung, dass von diesen eine Einwilligung vorliege, genügen dem BGH nicht. Der Nachweis der Einwilligung erfordert mehr, z. B. die Protokollierung des gesamten Opt-In-Verfahrens und des Inhalts der Einwilligung.

Ein solcher Nachweis reicht jedoch nicht im Fall der vorgesehenen Nutzung von über Website-Eintragungen erlangten Telefonnummern für Werbeanrufe aus. Mit der Übersendung einer Bestätigungs-E-Mail kann nämlich der Nachweis der Identität zwischen dem die Einwilligung mittels E-Mail Erklärenden und dem Anschlussinhaber der Telefonnummer nicht geführt werden. Eine schriftliche Einwilligung in die Nutzung einer E-Mail-Adresse und/oder einer Telefonnummer zu Werbezwecken ist regelmäßig die beste Möglichkeit für eine spätere Belegbarkeit einer Einwilligung.

3.4 „Koppelungsverbot“, Art. 7 Abs. 4 DSGVO

Das bisher schon bestehende Koppelungsverbot für Werbung findet sich auch in der DSGVO wieder, ist aber nicht mehr davon abhängig, ob ein anderer Zugang zu gleichwertigen vertraglichen Leistungen möglich ist. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, ist dem Umstand in größtmöglichem Umfang Rechnung zu tra-

gen, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrages nicht erforderlich ist (Art. 7 Abs. 4 DSGVO).

3.5 „Verfall" der Einwilligung, Verwirkung

Die Zivilgerichte sehen bei erteilten Einwilligungen zur werblichen Kontaktaufnahme teilweise keine unbegrenzte Gültigkeit. So hat das LG München I mit Urteil vom 8. April 2010, Az. 17 HK O 138/10, entschieden, dass eine vor 17 Monaten erteilte und bisher nicht genutzte Einwilligung zur E-Mail-Werbung „ihre Aktualität verliert" und deshalb insoweit keine rechtliche Grundlage mehr ist.

3.6 Ohne Einwilligung keine werbliche Nutzung besonderer Datenkategorien

Art. 9 DSGVO enthält keine Erlaubnisnorm für die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke der Werbung. Dies ist nur bei Vorliegen einer ausdrücklichen Einwilligung der betroffenen Person zulässig. Von Relevanz ist dies z. B. für Unternehmen und Berufe des Gesundheitswesens (Apotheken, Sanitätshäuser, Optiker, Orthopäden usw.).

4. Spezielle Sachverhalte bei der Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung

4.1 Veröffentlichung von Kontaktdaten in Rufnummernverzeichnissen

Telekommunikationsdienste-Anbieter müssen für die Zulässigkeit der Veröffentlichung von Telefonnummern und weiteren Kontaktdaten von Anschlussinhabern berücksichtigen, was die betroffene Person bei Vertragsabschluss oder später beantragt (keinerlei Veröffentlichung, Veröffentlichung nur in gedruckten oder auch in elektronischen Verzeichnissen). Andere Verzeichnisanbieter müssen dies bei der Interessenabwägung von nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO zu beurteilenden Sachverhalten beachten.

Eine darüber hinaus gehende Verarbeitung solcher Kontaktdaten in Rufnummernverzeichnissen wäre unzulässig.

4.2 Datenerhebung anlässlich von Preisausschreiben, Katalog-/Prospektanforderungen

Eine Verarbeitung von Postadressdaten für Zwecke der eigenen Direktwerbung aus der Durchführung von Preisausschreiben und Gewinnspielen sowie aufgrund von Katalog-

und Prospektanforderungen ist nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO zulässig, wenn über die werbliche Datenverarbeitung informiert wurde; eine Einwilligung der betroffenen Personen ist bei solchen Sachverhalten dann nicht erforderlich. Die Anforderungen aus Nr. 2.1 sind zu beachten.

4.3 Keine Verwendung der Daten aus dem Impressum

Nicht zulässig ist hingegen das Auslesen der Daten aus einem Online-Impressum zum Zweck der werblichen Nutzung. Zwar sind diese Daten allgemein zugänglich, sie werden jedoch nicht freiwillig, sondern aufgrund der gesetzlichen Verpflichtung zur Anbieterkennzeichnung gem. § 5 TMG bzw. § 55 Abs. 2 RStV veröffentlicht. Mangels Freiwilligkeit der Veröffentlichung führt die Interessenabwägung gem. Art. 6 Abs. 1 lit. f DSGVO regelmäßig dazu, dass die werbliche Nutzung so erhobener Daten unzulässig ist. Zur Vermeidung einer werblichen Ansprache mit diesen Daten kann ein Anbieter einer Internetseite vorsorglich einen Werbewiderspruch in sein Impressum aufnehmen.

4.4 Nennung des für die Verarbeitung der Daten Verantwortlichen sowie der Quelle von personenbezogenen Daten bei Fremdadressenbewerbung

Unter der Voraussetzung der Zulässigkeit der Datenübermittlung an Dritte (Punkt 1.3. bzw. Punkt 1.5) müssen der für die personenbezogenen Daten Verantwortliche, das werbende Unternehmen und die Quelle der Daten aus einer Werbung eindeutig hervorgehen und klar ersichtlich sein. Ein Verantwortlicher ist als konkrete juristische Person bzw. Firma mit ladungsfähiger Anschrift einschließlich E-Mail-Adresse zu nennen. Kurzbezeichnungen (wie XY-Group) oder Postfachanschriften genügen den Transparenzanforderungen von Art. 12 Abs. 1 Satz 1, Art. 13 Abs. 1 lit. a und Art. 14 Abs. 1 lit a DSGVO nicht.

4.5 Vertragliche Informationen, die gleichzeitig auch werbliche Informationen enthalten („Beipack-Werbung“)

Wenn Vertragspartnern vertragliche Informationen und damit verbunden auch eigene oder fremde werbliche Informationen per Brief zugesandt werden, ist dies in den Grenzen von Art. 6 Abs. 1 Satz 1 lit. f DSGVO möglich, solange von der betroffenen Person kein Werbewiderspruch nach Art. 21 Abs. 2 DSGVO vorliegt.

Bei E-Mail-Werbung sind die Wertungen von § 7 Abs. 3 UWG zu beachten, wonach für Fremdwerbung keine Erleichterungen gelten.

4.6 Direktwerbung anhand von Dritten erlangten Postadressdaten („Freundschaftswerbung“)

Einer Praxis, weitere Postadressdaten bei Kunden- und Interessentenbesuchen durch Befragen Dritter zu erheben und für Zwecke der Direktwerbung zu verarbeiten, stehen regelmäßig die Grundsätze einer fairen und transparenten Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 lit. a und Art. 12 Abs. 1 DSGVO entgegen.

4.7 Empfehlungswerbung

Der BGH sieht in einem Urteil vom 12. September 2013, I ZR 208/12 unverlangt versandte Empfehlungs-E-Mails als unzulässige Werbe-E-Mails an (ein Unternehmen hatte auf seiner Website die Möglichkeit für Nutzer eingerichtet, die E-Mail-Adresse eines Freundes anzugeben, um diesem dann unverlangt eine sog. Empfehlungs-E-Mail schicken zu können). Es komme für die Einordnung als Werbung nicht darauf an, dass das Versenden der Empfehlungs-E-Mails eines Unternehmens letztlich auf dem Willen eines Dritten beruhe.

Der BGH hat mit Urteil vom 14. Januar 2016, Az. I ZR 65/14, die Versendung von durch Facebook generierten E-Mails im Zusammenhang mit der Anmeldeprozedur „Freunde finden“ als unzumutbar belästigende und damit unerlaubte Werbung eingestuft, weil diese E-Mails ohne vorherige ausdrückliche Einwilligung des Adressaten versandt werden.

Damit wird von den Gerichten klargestellt, dass über solche Konstrukte der Empfehlungswerbung das geltende Einwilligungserfordernis in E-Mail-Werbung nach § 7 Abs. 2 Nr. 3 UWG außerhalb von Bestandskundenverhältnissen im Sinne des § 7 Abs. 3 UWG nicht umgangen werden kann.

4.8 Mögliche Nutzungsdauer von Kontaktdaten der betroffenen Person für Zwecke der Direktwerbung

Nicht eindeutig zu beantworten ist die Frage, wie lange Kontaktdaten nach dem letzten aktiven Geschäfts- oder Direktwerbekontakt zu einer betroffenen Person für die werblichen Zwecke der Reaktivierung, Rückgewinnung etc. noch genutzt werden dürfen, bzw. ab wann nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO überwiegende schutzwürdige Interessen der betroffenen Person einer länger währenden werblichen Nutzung entgegenstehen.

Eine konkrete Frist hat der Gesetzgeber nicht vorgesehen.

Entscheidend ist, ob aufgrund der Art der Geschäftsbeziehung noch eine Erforderlichkeit zur weiteren Nutzung der Daten für Zwecke der Direktwerbung von dem Verant-

wortlichen nachvollziehbar dargelegt werden kann. Wenn nach der Rechtsprechung eine vor 17 Monaten erteilte und bisher nicht genutzte Einwilligung zur E-Mail-Werbung „ihre Aktualität verliert“ und deshalb insoweit keine rechtliche Grundlage mehr ist (siehe hierzu unter 3.5), kann dieser zeitliche Maßstab auch bei der Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO zu den vernünftigen Erwartungen der betroffenen Person eine Orientierung bieten, wenn nach einer langen „Werbepause“ die Kontaktdaten der Person plötzlich wieder für eine Werbezusendung verarbeitet werden. Auch dürfen keine überwiegenden schutzwürdigen Interessen der betroffenen Personen einer werblichen Nutzung entgegenstehen. So kann z. B. die Konditionenabfrage bei einem Bestattungsunternehmen keine längerfristige Datennutzung für werbliche Zwecke rechtfertigen.

5. Hinweise zu Art. 21 Abs. 2 bis 4 DSGVO

5.1 Werbewiderspruch und Wunsch nach Datenlöschung

Für die Umsetzung der Betroffenenrechte ist im Zweifelsfall von der betroffenen Person klarzustellen bzw. bei ihr zu klären, was sie mit ihrer Willenserklärung bewirken möchte. Möchte sie vorrangig von einer werblichen Ansprache durch das Unternehmen verschont bleiben, ist dafür die Aufnahme ihrer Kontaktdaten in eine Werbesperrdatei bei diesem Unternehmen das richtige Mittel zur Berücksichtigung ihres Willens. Bei der Nutzung von Fremddaten kann dann durch Abgleich mit der Werbesperrdatei sichergestellt werden, dass die Kontaktdaten dieser betroffenen Person nicht verwendet werden.

Solche Werbesperrdateien sind damit aufgrund von Art. 21 Abs. 3, Art. 17 Abs. 3 lit. b und Art. 6 Abs. 1 Satz 1 lit. f DSGVO zur Berücksichtigung der Werbewidersprüche von betroffenen Personen zulässig (zur notwendigen Sicherstellung der Beachtung des geltend gemachten Rechtsanspruchs).

Die betroffenen Personen müssen im Zusammenhang mit der Unterrichtung (Art. 12 Abs. 3 DSGVO) über die Beachtung ihres Werbewiderspruchs auch über den Sinn und Zweck der Aufnahme ihrer Daten in eine Sperrdatei unterrichtet werden.

Wünscht eine betroffene Person ausdrücklich und allein eine Löschung aller Daten, sollte sie darauf hingewiesen werden, dass sie bei einem künftigen - rechtlich zulässigen - Einsatz von Fremddaten eventuell wieder Werbung erhalten kann.

Der Werbewiderspruch einer betroffenen Person kann sich, je nach ihrer Willenserklärung, datenschutzrechtlich gegen den Dateneigner und/oder den Werbenden als Verantwortliche nach Art. 4 Nr. 7 DSGVO richten. Beide müssen ggfls. diesen Werbewiderspruch künftig berücksichtigen (durch Aufnahme in eine Werbesperrdatei). Im Hinblick auf Art. 12 Abs. 2 Satz 1 DSGVO haben die Verantwortlichen für die effektive Durch-

setzung des Widerspruchsrechts der betroffenen Person zusammenzuwirken (z. B. Weiterleitung des Widerspruchs).

Ergänzend kann ein Hinweis für die betroffene Person auf die sog. Robinsonlisten der Werbewirtschaft hilfreich sein, siehe z. B. unter www.ichhabediewahl.de oder www.robinsonliste.de.

5.2 Unterrichtung über das Werbewiderspruchsrecht

Art. 21 Abs. 4 DSGVO verlangt, dass die betroffene Person in verständlicher und von anderen Informationen getrennter Form auf ihr Widerspruchsrecht gegen eine Verarbeitung ihrer personenbezogenen Daten für Zwecke der Direktwerbung einschließlich einem eventuellen damit in Verbindung stehenden Profiling hingewiesen werden muss. Aus Gründen der Nachweisbarkeit empfiehlt es sich, den Hinweis auf das Widerspruchsrecht bei jeder Werbesendung anzubringen.

Es ist nur dann von einer wirksamen Information im Sinne des Gesetzes auszugehen, wenn eine betroffene Person beim üblichen Umgang mit der Werbung oder mit Vertragsinformationen von dem Hinweis auf das Widerspruchsrecht Kenntnis erlangt. Das "Verstecken" der Information in langen AGB oder in umfangreichen Werbematerialien stellt keinen Hinweis im Sinne von Art. 21 Abs. 4 DSGVO dar.

Im Sinne des Art. 12 Abs. 2 Satz 1 DSGVO ist für die Einlegung des Werbewiderspruchs auch eine elektronische Kommunikationsmöglichkeit anzubieten.

5.3 Umsetzungsfrist des Werbewiderspruchs nach Art. 21 Abs. 3 DSGVO

Die Umsetzung des Widerspruchs gegen die künftige Verarbeitung der Kontaktdaten einer betroffenen Person für Zwecke der Direktwerbung einschließlich einem eventuell damit in Verbindung stehenden Profiling muss in dem betreffenden Unternehmen unverzüglich erfolgen.

Wenn konkrete Werbeaktionen angelaufen sind und sich die Kontaktdaten der betroffenen Person schon in der technischen Verarbeitung befinden, kann es im Einzelfall für das Unternehmen unzumutbar sein, einen zwischenzeitlich eingegangenen Werbewiderspruch noch mit erheblichem Aufwand umzusetzen, z. B. einen bestimmten bereits adressierten Brief aus einer großen Menge heraus zu sortieren.

Auch hier ist betroffenen Personen überwiegend nicht bewusst, dass bereits "angelaufene" Werbeaktionen regelmäßig nicht mehr ohne weiteres gestoppt werden können.

Zur Vermeidung von unnötigen Beschwerden sollten die Werbetreibenden die betroffenen Personen in einem individuellen Antwortschreiben erstens auf die Beachtung des Werbewiderspruchs und zweitens über die Tatsache, dass sie über einen möglichst genau zu benennenden kurzen Zeitraum noch Werbung erhalten können, unterrichten.

7.2.10 Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz

Die Orientierungshilfe zeigt den datenschutzrechtlichen Rahmen und Regelungsmöglichkeiten zu Whistleblowing-Hotlines auf. Sie soll es den Arbeitgebern und den Interessenvertretungen der Beschäftigten erleichtern, im Unternehmen klare Regelungen zum Umgang mit Whistleblowing-Hotlines zu erreichen.

Stand: 14. November 2018

Inhaltsverzeichnis

A Einführung

Firmeninterne Whistleblowing-Hotlines sind Angebote von Unternehmen an ihre Beschäftigten, ein nicht regelkonformes Verhalten anderer Beschäftigter dem Unternehmen zu melden. Mit der Meldung von Verstößen gegen Verhaltenspflichten geht die Verarbeitung von personenbezogenen Daten einher. Für jegliche automatisierte und nichtautomatisierte Verarbeitung von Beschäftigtendaten sind die Datenschutz-Grundverordnung (DSGVO)[14] und § 26 Bundesdatenschutzgesetz (BDSG)[15] in Verbindung mit Art. 88 DSGVO anzuwenden. Betroffene Personengruppen sind vor allem die Hinweisgeberinnen und Hinweisgeber sowie die beschuldigten Personen.

Die Aufsichtsbehörden beschränken sich auf die Beurteilung der datenschutzrechtlichen Zulässigkeit der personenbezogenen Datenverarbeitung bei Meldeverfahren unter Einsatz von firmeninternen Whistleblowing-Hotlines nach den Vorschriften der DSGVO. Die Übermittlung von personenbezogenen Daten in Drittstaaten – beispielsweise aufgrund des US-amerikanischen Sarbanes-Oxley Act (SOX) – ist nicht Gegenstand der datenschutzrechtlichen Beurteilung der vorliegenden Orientierungshilfe.

Die Orientierungshilfe richtet sich in erster Linie an die Wirtschaft.

B Verstöße

Interne Verfahren zur Meldung von Missständen werden in der Regel aus dem Bedürfnis eingerichtet, zuverlässige Grundsätze der Unternehmensführung in den täglichen Betrieb der Unternehmen einzuführen. Verfahren zur Meldung von Missständen sind als zusätzlicher Mechanismus für die Beschäftigten gedacht, um Missstände intern über einen bestimmten Kanal zu melden. Sie ergänzen die regulären Informations- und Meldekanäle der Einrichtung, wie beispielsweise Arbeitnehmervertretungen, Linienmanagement, Qualitätskontrollpersonal oder interne Auditoren, die eigens dafür eingestellt sind, solche Missstände zu melden. Die Meldung von Missständen ist als Ergänzung zum internen Management zu sehen und nicht als Ersatz dafür. Bei der Einführung von unternehmensinternen Verhaltensregeln sind arbeitsrechtliche Erfordernisse zu berücksichtigen und Mitbestimmungsrechte des Betriebsrats zu wahren.

Verstöße, die über ein internes Verfahren als Missstand gemeldet werden, können sein:

1. Verhaltensweisen, die einen sich gegen das Unternehmensinteresse richtenden Straftatbestand erfüllen (insbesondere Betrug und Fehlverhalten in Bezug auf die Rechnungslegung sowie interne Rechnungslegungskontrol-

[14] Amtsblatt der Europäischen Union vom 04.05.2016 – L 119/1 -
[15] Bundesgesetzblatt I vom 05.07.2017, S. 2097 ff.

len, Wirtschaftsprüfungsdelikte, Korruption, Banken- und Finanzkriminalität, verbotene Insidergeschäfte),

2. Verhaltensweisen, die gegen Menschenrechte (beispielsweise Ausnutzung günstiger Produktionsbedingungen im Ausland durch in Kauf genommene Kinderarbeit), Umweltschutzbelange oder gegen Vorschriften nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) verstoßen,
3. Verhaltensweisen, die unternehmensinterne Ethikregeln beeinträchtigen (beispielsweise Wal-Mart-Fall).[16]

C Datenströme beim Whistleblowing

Bei der Meldung von Verstößen gegen Verhaltensregeln werden personenbezogene Daten verarbeitet. Die Datenerhebung umfasst Angaben über die beschuldigte Person, die (angeblichen) Verhaltensverstöße sowie die entsprechenden Sachverhalte. Sofern ein Meldeverfahren regelt, dass Hinweise anonym erfolgen können, werden, falls Hinweisgeberinnen und Hinweisgeber sich nicht selbst anders äußern, keine personenbezogenen Daten über sie erhoben. Andernfalls kommen personenbezogene Angaben wie Name der meldenden Person, ihre Position im Unternehmen und gegebenenfalls auch die Umstände ihrer Beobachtung in Betracht. Je nach Ausgestaltung des Meldeverfahrens besteht die Möglichkeit der weiteren internen Verarbeitung durch die dafür vorgesehene Abteilung (beispielsweise Revision, Compliance). Bei verbundenen Unternehmen ist eine Übermittlung der personenbezogenen Daten an die Konzernmutter oder andere zum Konzern gehörende Unternehmen denkbar.

D Datenschutzrechtliche Zulässigkeit (Rechtsgrundlagen)

Die Verarbeitung personenbezogenen Daten ist nur rechtmäßig, wenn die DSGVO, eine spezifischere Rechtsvorschrift oder eine Kollektivvereinbarung nach Art. 88 DSGVO dies erlaubt oder die betroffene Person eingewilligt hat (Art. 6 Abs. 1 lit a DSGVO).

D 1 Vertragsverhältnis gemäß Art. 6 Abs. 1 lit. b DSGVO

Art. 6 Abs. 1 lit. b DSGVO ist nicht anzuwenden, weil das Beschäftigungsverhältnis bei der von der Unternehmensleitung veranlassten oder ihr zuzurechnenden Datenerhebung nicht unmittelbar betroffen ist. Beurteilungsgrundlage sind vielmehr Art. 6 Abs. 1 lit. c und lit. f DSGVO.

[16] vgl. Mitbestimmung des Betriebsrates: Beschluss des LAG Düsseldorf vom 14.11.2005 – 10 TaBV 46/05 –

D 2 Rechtliche Verpflichtung gemäß Art. 6 Abs. 1 lit. c DSGVO

Eine rechtliche Verpflichtung zur Einrichtung einer firmeninternen Whistleblowing-Hotline ergibt sich für den Bankensektor aus § 25a Abs. 1 Satz 6 Nr. 3 Gesetz über das Kreditwesen (KWG). Auch im Zusammenhang mit der Korruptionsbekämpfung bestehen rechtliche Verpflichtungen zur Einrichtung von verstärkten Kontrollmechanismen. Klarstellend wird darauf hingewiesen, dass hierbei nur rechtliche Verpflichtungen aus dem Unionsrecht oder dem Recht eines Mitgliedsstaates in Betracht kommen.

D 3 Abwägung nach Art. 6 Abs. 1 lit. f DSGVO

D 3.1 Erforderlichkeit zur Wahrung der berechtigten Interessen des Unternehmens

Die Einrichtung von Verfahren zur Meldung von Missständen kann zur Verwirklichung des berechtigten Interesses für erforderlich gehalten werden. Solche Interessen haben die für die Verarbeitung Verantwortlichen sowie Dritte, denen die Daten übermittelt werden. Das Ziel der Gewährleistung der finanziellen Sicherheit auf den internationalen Finanzmärkten und insbesondere die Verhütung von Betrug und Fehlverhalten in Bezug auf die Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung sowie die Bekämpfung von Korruption, Banken- und Finanzkriminalität oder Insider-Geschäften kann ein berechtigtes Interesse des Arbeitgebers darstellen, das die Verarbeitung personenbezogener Daten mittels Verfahren zur Meldung von Missständen in diesen Bereichen rechtfertigt. Eine Datenverarbeitung zur Wahrung dieses Interesses wäre jedoch nur zulässig, sofern die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen.

D 3.2 Interessen, Grundrechte und Grundfreiheiten der betroffenen Person

Bei einem Verfahren zur Meldung von Missständen besteht die Gefahr der Viktimisierung (eine Person „zum Opfer machen“) und Stigmatisierung (Zuschreibung von Merkmalen und Eigenschaften, die diskreditierbar sind) der belasteten Person. Eine Prüfung schutzwürdiger Interessen dieser Person wird bei konkreten, auf relevante Verfehlungen hinweisenden Verdachtsmomenten besonders sorgfältig vorzunehmen sein.

Die Verarbeitung von personenbezogenen Daten, die mit der Aufdeckung von Verstößen der in den Abschnitten B 1 und B 2 beschriebenen Kategorien (sogenannte „harte Faktoren“) in Zusammenhang stehen, kann als zulässig angesehen werden. In der Regel wird die Interessenabwägung zugunsten des berechtigten Interesses des Unternehmens ausfallen, da die Meldung solcher Verstöße rechtliche Konsequenzen durch beispiels-

weise Strafverfolgung, Schadensersatzforderungen und Imageschaden vermeiden hilft, wenn das Verfahren im Übrigen datenschutzgerecht ausgestaltet ist (Kapitel E).

Bei Verhaltensweisen entsprechend der Kategorie B 3 (sogenannte „weiche Faktoren“) ist die Zulässigkeit ebenso nur im Einzelfall zu beurteilen. Hierbei ist zu berücksichtigen, dass bestimmte Verhaltensweisen von vornherein nicht in eine Beurteilung oder Interessenabwägung einbezogen werden dürfen.[17]

Grundsätzlich ist bei Fallgruppe B 3 anzunehmen, dass die schutzwürdigen Interessen der Betroffenen überwiegen. Dabei sind auch arbeitsrechtliche Grundsätze zu beachten. Für die „weichen Faktoren“ der internen Verhaltensregeln (beispielsweise „Freundlichkeit bei der Kundenbetreuung“) fehlt es zumeist schon an einer klar umrissenen Definition, um einen Verstoß einwandfrei identifizieren zu können. Außerdem ist ein Zusammenhang zwischen dem Verstoß und einem erheblichen Schaden für das Unternehmen (vergleichbar der in den Abschnitten B 1 und B 2 beschriebenen Kategorien) nicht erkennbar, so dass schon Zweifel an einem berechtigten Interesse des Verantwortlichen bestehen. Daher dürfte in diesen Fällen im Grundsatz davon auszugehen sein, dass überwiegende Interessen der betroffenen Person bestehen und eine Verarbeitung personenbezogener Daten insoweit unzulässig ist.

D 4 Spezifischere Vorschriften gemäß Art. 88 DSGVO

Eine spezifischere Vorschrift im Sinne des Art. 88 DSGVO ist § 26 Abs. 1 Satz 2 BDSG. Danach dürfen zur Aufdeckung von Straftaten personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Des Weiteren muss der Verantwortliche geeignete Maßnahmen treffen, um sicherzustellen, dass insbesondere die in Art. 5 DSGVO dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden (§ 26 Abs. 5 BDSG). Die Vorschrift des § 26 Abs. 1 Satz 2 BDSG ist jedoch nur anwendbar, wenn es sich um die Aufdeckung von Straftaten im Beschäftigungskontext handelt (Verhaltensweisen nach Abschnitt B 1).

---

[17] s. LAG Düsseldorf, Beschluss vom 14.11.2005, NZA 2006,63. Nach Ansicht des Gerichts ist der Regelungskomplex „Private Beziehungen/ Liebesbeziehungen“ wegen Verstoßes gegen Art. 1 und 2 GG grundgesetzwidrig und damit unwirksam.

Nach § 26 Abs. 4 Satz. 1 BDSG können Kollektivvereinbarungen, das heißt Tarifverträge und Betriebsvereinbarungen, Grundlage für die Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis sein. Bei der Abfassung einer solchen Vereinbarung sind die Vorgaben der DSGVO zu beachten. So muss eine Betriebsvereinbarung, die Verhaltensregeln beinhaltet, gemäß Art. 5 Abs. 1 lit. b DSGVO die Datenerhebung und -weiterverarbeitung eindeutig regeln. Die bloße Beschreibung einer Aufgabe oder eines Zwecks reicht nicht aus, auch wenn zu deren Erledigung personenbezogene Beschäftigtendaten verarbeitet werden müssen.

Zusätzlich muss eine Betriebsvereinbarung angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder eine Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachung am Arbeitsplatz umfassen. (§ 26 Abs. 4 Satz 2 BDSG in Verbindung mit Art. 88 Abs. 2 DSGVO).

D 5 Einwilligung der betroffenen Person gemäß Art. 6 Abs. 1 lit. a DSGVO

Die Wirksamkeit einer Einwilligung im Rahmen eines solchen Verfahrens muss insbesondere an die Kriterien der Freiwilligkeit und Information über die Datenverarbeitung anknüpfen. § 26 Abs. 2 Satz 1 BDSG gibt vor, dass für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt wird, zu berücksichtigen sind.

Die besondere Bedeutung der Freiwilligkeit der Einwilligung wird schon allgemein in Art. 7 Abs. 4 DSGVO ausdrücklich betont. Anforderungen an eine wirksame Einwilligung finden sich in Art. 7 DSGVO sowie Erwägungsgrund (EG) 32, 42 und 43. Insbesondere ist die Einwilligung nur dann freiwillig, wenn die betroffene Person eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.

Gleichwohl kann die Verarbeitung personenbezogener Daten für firmeninterne Warnsysteme aufgrund der Rechtsvorschriften des Art. 6 Abs. 1 lit. f DSGVO und des § 26 Abs. 1 Satz 2 BDSG grundsätzlich nicht auf die Einwilligung gestützt werden, sondern nur auf diese Vorschriften. Einzige Ausnahme ist die Einwilligung einer Hinweisgeberin oder eines Hinweisgebers, soweit die betroffene Person ihre Identität gewollt oder bewusst dem Arbeitgeber oder der externen Stelle preisgegeben möchte (siehe Abschnitt E 3).

E Datenschutzgerechte Gestaltung eines Meldeverfahrens mittels Hotline

E 1 Grundsätze

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben und dürfen nicht in einer damit nicht zu vereinbarenden Weise weiterverarbeitet werden (Art. 5 Abs. 1 lit. b DSGVO). Darüber hinaus müssen die verarbeiteten Daten den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erforderlich sein und sich auf das notwendige Maß beschränken. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – beispielsweise Pseudonymisierung – die dafür ausgelegt sind, die Datenschutzgrundsätze – etwa Datenminimierung – wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Personen zu schützen (Art. 25 Abs. 1 DSGVO).

Der Verantwortliche muss Maßnahmen treffen, die sicherstellen, dass nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden. Informationen an die betroffene Person zu dem mit einer Whistleblowing-Hotline verfolgten Zweck müssen in klarer, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt werden. Missverständnisse, jede auch nur geringfügige oder lediglich vermutete Unregelmäßigkeit sei zu melden, sollten vermieden werden. Klar sein muss, dass kein Interesse an unkonkretisierten Beschuldigungen besteht.

E 2 Betroffener Personenkreis

Nach dem Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO hat der Verantwortliche zu prüfen, inwieweit der für eine Meldung in Betracht kommende Personenkreis bei einer Whistleblowing-Hotline möglichst eingegrenzt und konkret bestimmt werden kann. Das Unternehmen, das ein Verfahren zur Meldung von Missständen einführt, sollte ebenfalls sorgfältig prüfen, ob es angebracht wäre, die Zahl der Personen zu begrenzen, die über das Verfahren gemeldet werden können, insbesondere in Anbetracht der Schwere der gemeldeten mutmaßlichen Verstöße. Entscheidend kommt es dabei jedoch auf die Umstände im Einzelfall an.

E 3 Anonymer oder personenbezogener Hinweis

Anonymität begünstigt gegenüber der namentlichen Nennung von ‚Ross und Reiter' eher Missbrauch und Denunziantentum. Einer durch anonymen Hinweis gemeldeten Person bleibt keine Möglichkeit, sich gegen eine etwaige Verleumdung in einem rechtsstaatlichen Verfahren zur Wehr zu setzen. Ein von vornherein auf die Erhebung personenbezogener Daten über Whistleblower abstellendes Verfahren hat jedoch den Nachteil, dass auch bei gewünschten Hinweisen ein Abschreckungseffekt besteht. Hinweisgeberinnen und Hinweisgeber müssen nämlich damit rechnen, ihren Arbeitsplatz zu verlieren, wenn sie unter Offenbarung ihrer Identität Missstände in ihrem Unternehmen aufdecken. Nach § 626 Abs. 1 Bürgerliches Gesetzbuch (BGB) ist die fristlose Kündigung eines Arbeitsvertrags erlaubt, wenn dem Kündigenden (hier: Arbeitgeber) die Fortsetzung des Dienstverhältnisses aus einem „wichtigen Grund" nicht zugemutet werden kann.

Der Europäische Gerichtshof für Menschenrechte (EGMR) stellte 2011 fest, dass der Staat der Pflicht unterliege, die Wahrnehmbarkeit der Meinungsfreiheit auch im privaten Verhältnis von Arbeitgeber und Arbeitnehmer zu schützen. Der gutgläubig agierende Arbeitnehmer habe prinzipiell das Recht, strafbare Handlungen auch seines Arbeitgebers zur Anzeige zu bringen. Jede Person, die Informationen preisgibt, müsse nach den Umständen des Einzelfalls prüfen, ob die Informationen zutreffend und verlässlich sind. Von dem gutgläubigen Erstatter einer Strafanzeige könne aber vernünftigerweise nicht erwartet werden, vorherzusehen, ob die strafrechtlichen Ermittlungen auch zu einer Anklage führen werden.[18]

Die Informationsfreiheitsbeauftragten in Deutschland verlangen, dass Whistleblowern die vertrauliche Behandlung des Hinweises zugesagt werden muss, ebenso einen gesetzlich geregelten effektiven Schutz von Whistleblowern, die über Rechtsverstöße im öffentlichen und nicht öffentlichen Bereich berichten.[19] Der Europarat hat in seiner Empfehlung zum Whistleblowerschutz am 30.04.2014 ihre Mitgliedstaaten aufgefordert, einen gesetzlichen Rahmen zu schaffen, der Menschen schützt, die auf Verletzungen und Gefährdungen des Öffentliches Interesses im Zusammenhang mit ihrer Arbeit hinweisen.[20]

Gleichwohl gibt es derzeit in Deutschland keinen gesetzlich geregelten oder wirksamen Whistleblowerschutz, ausgenommen § 25a Abs. 1 Satz 6 Nr. 3 KWG.

---

18 EGMR Nr. 28274/08 (5. Kammer) – Urteil vom 21.07.2011

19 Entschließungen der 18. und 27. Konferenz der Informationsfreiheitsbeauftragten vom 24.06.2009 und 28.11.2013

20 https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c5ea5

Zudem gibt es keine gesicherten Erkenntnisse, ob und in welchem Umfang Hinweise auf Missstände in einem Unternehmen unbegründet waren. Nach den Erfahrungen der Datenschutz-Aufsichtsbehörden haben sich - auch anonyme - Hinweise über Datenschutzverstöße regelmäßig nicht als unbegründet erwiesen.

In Abwägung der genannten Interessen ist das folgende Vorgehen zu empfehlen:

Verfahren zur Meldung von Missständen stellen sicher, dass Hinweise regelmäßig anonym erfolgen. Für die Verarbeitung von Angaben zur Identität der Hinweisgeberin oder des Hinweisgebers gibt es keine Rechtsgrundlage (Kap. D 5 letzter Absatz). Soweit eine Person eine Meldung mit Hilfe eines solchen Verfahrens unter bewusster oder gewollter Darlegung ihrer Identität machen möchte, sollte sie bei der ersten Kontaktaufnahme mit dem System vorher darauf hingewiesen werden, dass ihre Identität während aller internen oder außergerichtlichen Schritte des Verfahrens vertraulich behandelt wird, allerdings auch, dass die beschuldigte Person über die Identität der Hinweisgeberin oder des Hinweisgebers grundsätzlich spätestens einen Monat nach der Meldung informiert werden muss (Art. 14 Abs. 3 lit. a DSGVO, näher hierzu unter 4.1).

Wenn die Hinweisgeberin oder der Hinweisgeber trotz dieser Hinweise ihre Identität bewusst und gewollt preisgeben möchte und die Angaben verarbeitet werden sollen, kommt eine Einwilligung dieser Person in Frage. Daher ist die betroffene Person vor der Einwilligung über ihr Recht nach Art. 7 Abs. 2 DSGVO in Kenntnis zu setzen, dass sie die Einwilligung widerrufen kann, dies jedoch nur bis zu einem Monat nach erfolgter Meldung wirksam möglich ist. Die Einwilligung der betroffenen Person in die Preisgabe ihrer Identität ist nach Art. 7 Abs. 1 DSGVO vom Arbeitgeber oder der externen Stelle nachzuweisen. Gleichwohl ist der Arbeitgeber oder die externe Stelle trotz dieser Einwilligung verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, die diese auch nur vorübergehende Vertraulichkeit der Identität der betroffenen Person gewährleisten (siehe Nr. 4 und 5).

E 4 Unterrichtungs- und Auskunftspflichten

Der Verantwortliche muss, wenn personenbezogene Daten bei betroffenen Personen erhoben werden, diese nach Art. 13 DSGVO insbesondere über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unterrichten. Dies gilt nicht, wenn und soweit die betroffene Person bereits über die Informationen verfügt (Art. 13 Abs. 4 DSGVO). Sofern Betriebsvereinbarungen über das Meldeverfahren mit Regelungen zur personenbezogenen Datenverarbeitung abgeschlossen wurden, hat sie das Unternehmen so auszulegen, dass sämtliche Beschäftigten, auch die neu eingestell-

ten, in der Lage sind, sich ohne besondere Umstände mit dem Inhalt vertraut zu machen (§ 77 Abs. 2 Betriebsverfassungsgesetz - BetrVG).[21]

E 4.1Information der beschuldigten Person

Werden personenbezogene Daten für die Meldung von Missständen ohne Kenntnis der betroffenen Person erhoben, ist diese nach Art. 14 DSGVO insbesondere von der Speicherung, der Art der Daten, der Zweckbestimmung Verarbeitung und der Identität des Verantwortlichen und gegebenenfalls der Hinweisgeberin oder des Hinweisgebers zu informieren.

Wenn das Risiko erheblich wäre, dass eine solche Unterrichtung die Fähigkeit des Unternehmens zur wirksamen Untersuchung des Vorwurfs oder zur Sammlung der erforderlichen Beweise gefährden würde, kann die zu erfolgende Information der beschuldigten Person so lange aufgeschoben werden, wie diese Gefahr besteht. Grundlage hierfür ist Art. 14 Abs. 5 lit. b DSGVO, wonach die Information nicht erteilt werden muss, wenn die Verwirklichung der Ziele der Verarbeitung zumindest ernsthaft beeinträchtigt würde. Andernfalls müsste die Information nach spätestens einem Monat gegeben werden (Art. 14 Abs. 3 lit. a DSGVO). Eine dauerhafte Geheimhaltung dürfte angesichts einer möglichen Beeinträchtigung der Persönlichkeitsrechte der beschuldigten Person und seiner Verteidigungsrechte ausgeschlossen sein. Als Maßnahme zum Schutz der berechtigten Interessen der beschuldigten Person nach Art. 14 Abs. 5 lit. b DSGVO muss die Information daher dann nachgeholt werden, sobald der Grund für den Aufschub entfallen ist.

Eine Pflicht zur Benachrichtigung besteht auch nicht, wenn personenbezogene Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen. (Art. 14 Abs. 5 lit. d DSGVO). Das Gleiche gilt, wenn diese Pflicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten zum Zweck des Schutzes der betroffenen Person oder Rechte und Freiheiten anderer Personen beschränkt wird (Art. 23 Abs. 1 lit. i DSGVO). Eine derartige Regelung enthält das BDSG jedoch nicht. Die Vorschrift des § 29 Abs.1 Satz 1 Bundesdatenschutzgesetz (BDSG) schränkt die Informationspflichten des Arbeitgebers oder einer externen Stelle hinsichtlich der Identität der Hinweisgeberin oder des Hinweisgebers wirksam ein. Danach besteht eine Pflicht zur Information nicht, soweit durch ihre Erfüllung Informationen offenbart würden, die wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen.

[21] Fitting, Anm. 25 zu § 77 BetrVG

E 4.2 Auskunft

Nach Art. 15 DSGVO hat die betroffene Person, sowohl die Hinweisgeberin oder der Hinweisgeber als auch die beschuldigte Person, Anspruch auf Auskunft der zu ihrer Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen. Der Auskunftsanspruch der beschuldigten Person kollidiert hinsichtlich der Identität der meldenden Person grundsätzlich mit einer für das Meldeverfahren vorgesehenen anonymen Meldung (siehe dazu Abschnitt E 3). Allerdings besteht keine Auskunftsverpflichtung, wenn diese durch Rechtsvorschriften der Union oder der Mitgliedstaaten zur Verhütung oder Aufdeckung von Straftaten oder zum Zweck des Schutzes der betroffenen Person oder Rechte und Freiheiten anderer Personen beschränkt wird (Art. 23 Abs. 1 lit. d und lit. i DSGVO). Diese Beschränkung regelt § 29 Abs.1 Satz 2 BDSG, wonach das Recht auf Auskunft nicht besteht, soweit durch die Auskunft Informationen offenbart würden, die wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen.

E 5 Weitergabe an Dritte

Grundsätzlich ist eine Weitergabe personenbezogener Daten der beschuldigten Person an Dritte nicht zulässig. Akteneinsichtsrechte in einem etwaigen Strafverfahren bleiben unberührt. Personenbezogene Daten der beschuldigten Person können nach Art. 6 Abs. 1 lit. f DSGVO in Verbindung mit § 24 Abs. 1 Nr. 1, letzte Alternative BDSG zur Verfolgung von Straftaten übermittelt werden.

E 6 Berichtigung, Sperrung und Löschung

Nach Art. 5 Abs. 1 lit. d DSGVO müssen personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke der Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Art. 18 DSGVO gibt der betroffenen Person unter bestimmten Voraussetzungen zudem das Recht, die Einschränkung der Verarbeitung zu verlangen. Grundsätzlich sollten Daten innerhalb von zwei Monaten nach Abschluss der Untersuchung gelöscht werden. Eine darüber hinausgehende Speicherung ist nur für die Dauer der Klärung erforderlicher weiterer rechtlicher Schritte wie Disziplinarverfahren oder Einleitung von Strafverfahren zulässig. Personenbezogene Daten im Zusammenhang mit Meldungen, die von der Organisationseinheit, die für die Bearbeitung der Meldung zuständig ist, als grundlos erachtet werden, sollten unverzüglich gelöscht werden.

E 7 Widerspruch

Die betroffene Person hat nach Art. 21 Abs. 1 DSGVO das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 lit. e oder f DSGVO erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffen Person überwiegen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

E 8 Beteiligung der Datenschutzbeauftragten

Bei Whistleblowing-Systemen handelt es sich um Verfahren, bei denen nach Art. 38 Abs. 1 DSGVO die Datenschutzbeauftragten ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden sind.

E 9 Datenschutz-Folgenabschätzung

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch (Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1 DSGVO). Ein Verfahren zur Meldung von Missständen unterliegt wegen des besonders hohen Risikos für die Rechte und Freiheiten natürlicher Personen einer Datenschutz-Folgenabschätzung.

E 10 Beauftragung externer Stellen

Wenn Unternehmen externe Dienstleister mit einem Teil der Verwaltung des Systems zur Meldung von Missständen beauftragen, behalten sie dennoch die Verantwortung für die daraus hervorgehenden Verarbeitungen, soweit diese als Auftragsverarbeiter im Sinne des Art. 28 Abs. 1 DSGVO tätig werden. Der Auftragsverarbeiter muss dabei im Auftrag des Verantwortlichen hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Der hierfür abzuschließende Vertrag sieht gemäß Art. 28 Abs. 3 Satz 2 lit. a DSGVO unter anderem vor, dass der Auftragsverarbeiter die

personenbezogenen Daten nur auf dokumentierte Weise des Verantwortlichen verarbeitet - auch in Bezug auf die Datenübermittlung an ein Drittland.

Andernfalls liegt bei der Beauftragung externer Stellen im Rahmen einer Funktionsübertragung eine Übermittlung vor, deren Zulässigkeit nach Art. 6 Abs. 1 lit. f DSGVO zu beurteilen ist. Je nach Ausgestaltung des Meldeverfahrens ist zwischen dem berechtigten Interesse der verantwortlichen Stelle und den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Personen abzuwägen. Die Zulässigkeit der Übermittlung an externe Stellen ist ebenfalls Gegenstand der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO.

Nach Art. 35 Abs. 1 DSGVO entscheidet der für Datenverarbeitung Verantwortliche über die Durchführung einer Datenschutz-Folgenabschätzung. Wenn eine externe Stelle damit beauftragt werden soll, kann davon ausgegangen werden, dass dies angesichts ihrer Komplexität (beispielsweise Erfordernisse nach Art. 35 Abs. 7 DSGVO) nur im Rahmen einer Funktionsübertragung möglich ist.

Die Beauftragung einer externen Stelle außerhalb der Unternehmensorganisation (Konzernverbund) kann sich bei Beachtung der datenschutzrechtlichen Vorschriften im Übrigen als vorteilhaft erweisen, weil möglicherweise eine gewisse, das Missbrauchsrisiko verringernde Hemmschwelle entsteht.

E 11 Technische und organisatorische Maßnahmen

Um die Vorgaben des Art. 32 DSGVO zu erfüllen, sind geeignete technische und organisatorische Maßnahmen zu treffen. Dies gilt insbesondere wegen der zugesicherten Vertraulichkeit und für die Löschungsverpflichtung. Bei interner Datenverarbeitung ist zu empfehlen, dass die Whistleblowing-Hotline nicht innerhalb der Personalverwaltung organisiert und betrieben wird. Um zu gewährleisten, dass Unbefugte Datenverarbeitungssysteme nicht nutzen können, bieten sich neben einem Berechtigungskonzept und einer Passwortrichtlinie auch Verschlüsselungsverfahren im Hinblick auf die Sensibilität der Daten an.[22] Zu den Maßnahmen gehören auch Protokollierung von Dateneingaben und Löschroutinen.

F Ergebnis

Das Meldeverfahren mittels firmeninterner Whistleblowing-Hotlines lässt sich unter besonderer Berücksichtigung des von dem Unternehmen verfolgten Zwecks und der Einrichtungsmodalitäten datenschutzgerecht gestalten und betreiben. Für Unternehmen, die solche Warnsysteme beabsichtigen einzurichten, empfiehlt sich eine rechtzeitige

[22] BSI-IT-Grundschutzhandbuch

Abstimmung mit allen zu Beteiligenden (beispielsweise Innenrevision, Beauftragte der Geschäftsleitung, Datenschutzbeauftragte, Betriebsvertretung). Zur Klärung von Zweifelsfragen stehen auch die Datenschutzbehörden zur Verfügung.

7.2.11 Kurzpapiere der DSK - Darstellung mit Verweis

Zu drängenden und häufigen Rechtsfragen im Zusammenhang mit der Einführung der Datenschutz-Grundverordnung hat sich die Datenschutzkonferenz darauf geeinigt, zur rechtlichen Orientierung Kurzpapiere herauszugeben.

Die Kurzpapiere, die sowohl auf der Seite der Datenschutzkonferenz als auch auf der Internetseite meiner Dienststelle (https://www.saechsdsb.de/hinweise) zum Abruf bereitstehen, werden hier nachstehend in einem Überblick aufgeführt:

- Kurzpapier Nr. 1: Verzeichnis von Verarbeitungstätigkeiten - Art. 30 DSGVO
  [referenziert auf Art. 30 DSGVO]

- Kurzpapier Nr. 2: Aufsichtsbefugnisse/Sanktionen
  [referenziert auf Art. 58, 83 DSGVO]

- Kurzpapier Nr. 3: Verarbeitung personenbezogener Daten für Werbung
  [referenziert auf Art. 6 Abs. 1 Buchst. f), Art. 7, 13, 14, 21 Abs. 2 und Abs. 3 DSGVO]

- Kurzpapier Nr. 4: Datenübermittlung in Drittländer
  [referenziert auf Art. 45, 46, 49 DSGVO]

- Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DSGVO
  [referenziert auf Art. 35, 36 DSGVO]

- Kurzpapier Nr. 6: Auskunftsrecht der betroffenen Person, Art. 15 DSGVO
  [referenziert auf Art. 12, 15 DSGVO]

- Kurzpapier Nr. 7: Marktortprinzip: Regelungen für außereuropäische Unternehmen
  [referenziert auf Art. 3 Abs. 2 DSGVO]

- Kurzpapier Nr. 8: Maßnahmenplan „DSGVO“ für Unternehmen
  [Empfehlungen wegen des Wirksamwerdens der DSGVO]

- Kurzpapier Nr. 9: Zertifizierung nach Art. 42 DSGVO
  [referenziert auf Art. 42 DSGVO]

- Kurzpapier Nr. 10: Informationspflichten bei Dritt- und Direkterhebung
  [referenziert auf Art. 13, 14 DSGVO]

- Kurzpapier Nr. 11: Recht auf Löschung/„Recht auf Vergessenwerden“
  [referenziert auf Art. 17, 21, 23 DSGVO, § 35 BDSG]

- Kurzpapier Nr. 12: Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern
  [referenziert auf Art. 37, 38, 39 DSGVO]

- Kurzpapier Nr. 13: Auftragsverarbeitung, Art. 28 DSGVO
  [referenziert auf Art. 4 Nr. 7, Art. 28, 29 DSGVO]

- Kurzpapier Nr. 14: Beschäftigtendatenschutz
  [referenziert auf Art. 7, 9, 88 DSGVO, § 26 BDSG]

- Kurzpapier Nr. 15: Videoüberwachung nach der Datenschutz-Grundverordnung
  [referenziert auf Art. 6, 7, 12 ff. DSGVO]

- Kurzpapier Nr. 16: Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO
  [referenziert auf Art. 6, 26, 28 DSGVO]

- Kurzpapier Nr. 17: Besondere Kategorien personenbezogener Daten
  [referenziert auf Art. 4 Nr. 13, Nr. 14, Nr. 15, Art. 6, 9 DSGVO, § § 22, 27 und 28 BDSG]

- Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen
  [referenziert auf Art. 5, 6, 12 ff., 24, 25, 32 bis 36 DSGVO]

- Kurzpapier Nr. 19: Unterrichtung und Verpflichtung auf Beachtung der datenschutzrechtlichen Anforderungen nach der DSGVO
  [referenziert auf Art. 5, 24, 28, 29, 32 DSGVO]

- Kurzpapier Nr. 20: Einwilligungen nach der DSGVO
  [referenziert auf Art. 4 Nr. 11, Art. 6 Abs. 1 Buchst. f), 7, 8, 9 Abs. 1 Buchst. a), Art. 13 DSGVO, § 26 Abs. 2 Satz 3 BDSG]

7.2.12 Anwendungshinweise der DSK - Darstellung mit Verweis

Die seitens der Datenschutzkonferenz herausgegebenen Anwendungshinweise enthalten unter anderem eine Liste von Verarbeitungsvorgängen nach Artikel 35 Absatz 4 DSGVO für den nicht-öffentlichen Bereich in englischer Sprachfassung (vergleiche auch den

Beitrag 4.7.1), die aktuelle Version des Standard-Datenschutzmodells (vergleiche den Beitrag 4.1.1) sowie Muster und Hinweise zum Verzeichnis der Verarbeitungstätigkeiten gemäß Artikel 30 Absatz 1, Absatz 2 DSGVO, vergleiche den Auftritt unter https://www.datenschutzkonferenz-online.de.

7.3 Entscheidungen und Materialien des Europäischen Datenschutzausschusses

7.3.1 Tätigkeit des Europäischen Datenschutzausschusses

Der Europäische Datenschutzausschuss (EDSA) bildet rechtlich eine unabhängige Einrichtung auf Ebene der EU, die aus Vertretern der nationalen Datenschutzaufsichtsbehörden und dem Europäischen Datenschutzbeauftragten zusammengesetzt ist. Der Sitz ist in Brüssel, Belgien.

Der Europäische Datenschutzausschuss hat die Aufgabe, eine verbindliche und einheitliche Spruchpraxis der Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten sicherzustellen. Hierzu veranlasst der Europäische Datenschutzausschuss allgemeine Anleitungen, unter anderem Leitlinien und Empfehlungen, um Transparenz in der Rechtsanwendung und Rechtssicherheit herzustellen. Darüber hinaus hat der Ausschuss eine Beratungsfunktion gegenüber der Europäischen Kommission.

Der europäische Datenschutzausschuss gibt auch einen Jahresbericht heraus. Auf der Internetseite sind darüber hinaus Stellungnahmen und verbindliche Beschlüsse sowie ein Register über die Entscheidung der Aufsichtsbehörden und Gerichte zu den in Kohärenzverfahrens behandelten Fragen vorgesehen. Auch auf der Internetseite der Datenschutzkonferenz finden sich für die Rechtspraxis wichtigen Dokumente des Europäischen Datenschutzausschusses, vergleiche den Beitrag 7.2.1 oben. Aktuell zu nennen und von erhöhter Relevanz sind unter anderem die Leitlinien zu Verhaltensregeln und den Überwachungsstellen gemäß Art. 40, 41 DSGVO sowie die Leitlinien zu AkkreditierungAkt von Zertifizierungsstellen gemäß Art. 43 der Datenschutz-Grundverordnung. Der Europäische Datenschutzausschuss gibt auch Leitlinien und Empfehlungen in Bezug auf die Datenschutzrichtlinie im Bereich von Justiz und Inneres heraus. Die Internetseite ist über https://edpb.europa.eu/edpb_de in deutscher Sprache abrufbar.

8 Richtlinienbereich – Richtlinie (EU) 2016/680 – und sonstige Bereiche

8.1 Polizeiliche Videoüberwachung in der Innenstadt von Chemnitz

Seit Anfang 2018 war die Videoüberwachung von Teilen der Chemnitzer Innenstadt durch die Stadt Chemnitz, die Messegesellschaft der Stadt, die Chemnitzer Verkehrsbetriebe (CVAG) und nicht zuletzt durch die Polizeidirektion Chemnitz auch öffentlichkeitswirksam angekündigt worden. Ich habe die beteiligten kommunalen Stellen als auch die Polizeidirektion Chemnitz von Anfang an datenschutzrechtlich beraten. Was die Polizeidirektion angeht, habe ich auf Folgendes aufmerksam gemacht:

Die Polizeidirektion ist eine der vier Projektverantwortlichen für die Videoüberwachung in der Chemnitzer Innenstadt.

Seit Anfang Oktober 2018 werden in der Chemnitzer Innenstadt bestimmte stark frequentierte Bereiche des öffentlichen Straßenraums (z. B. der Bereich der Zentralhaltestelle und des Stadthallenparks) kameraüberwacht. Die Aufnahmen werden für 10 Tage auf einem Server der CVAG gespeichert. Die Polizei schätzt die überwachten Bereiche als Kriminalitätsschwerpunkte i. S. v. § 19 Absatz 1 Nummer 2 SächsPolG ein, für die eine Videoüberwachung gemäß § 37 Absatz 2 SächsPolG grundsätzlich zulässig ist. Ferner kommt § 37 Absatz 1 SächsPolG als Rechtsgrundlage für die Videoüberwachung in Betracht. Voraussetzung dafür ist, dass Tatsachen die Annahme rechtfertigen, dass Straftaten aus Ansammlungen heraus begangen werden. Die Polizei will die Kameras zur „Live-Bild-Betrachtung“ nutzen, wenn sie Anlass, z. B. einen konkreten Hinweis, hat, dass sich dort eine Gefahrensituation anbahnt. Zum anderen will sie im Rahmen der Strafverfolgung auf die Aufzeichnungen zugreifen, Rechtsgrundlagen hierfür sind die §§ 163, 94, 98, 100h Absatz 1 Nummer 1 StPO. Anlass der Aufschaltung auf das Kamerasystem durch die Polizei ist somit jeweils eine konkrete Meldung oder Anzeige, eine dauerhafte Überwachung der Echtzeitdaten oder der Aufzeichnungen findet nicht statt.

Das Verfahren dient damit zum einen dem Zweck, als präventiv-polizeiliche Maßnahme Straftaten im überwachten Bereich zu verhindern, die Interventionszeiten bei Gefahren für die öffentliche Sicherheit und Ordnung zu verkürzen und Straftäter zu identifizieren. Darüber hinaus sollen auch Gefahren für die öffentliche Sicherheit abgewehrt und Störungen der öffentlichen Sicherheit unterbunden bzw. beseitigt werden, die auch der Straftatenverhütung unterfallen (z. B. Suche nach vermissten Personen oder Gefahrerforschung bei herrenlosen Gegenständen).

Eine Inbetriebnahme zur „Live-Bild-Betrachtung“ findet derzeit (Januar 2019) nicht statt, da die hierfür erforderlichen Unterlagen (Errichtungsanordnung, Dienstanweisung, Datenschutzfolgenabschätzung) noch nicht in vom SMI genehmigter Form vorliegen. Da die PD Chemnitz mich bereits in der Planungsphase des Projekts einbezogen hat, werde ich auch hierbei meine Beratung anbieten.

Ich werde den Vorgang im Auge behalten.

8.2 Sechs Jahre Löschmoratorium

Im 18. Tätigkeitsbericht berichtete ich über Probleme, die die sächsische Polizei mit einer möglichst grundrechtsschonenden Umsetzung des sog. Löschmoratoriums zu Daten mit Bezug zum Rechtsextremismus hatte (18. TB, Beitrag 5.9.4). Das weitere Fortbestehen des Löschmoratoriums gibt Anlass, den Blick noch einmal auf den tatsächlichen und rechtlichen Hintergrund der über sechs Jahre andauernden Aussetzung gesetzlicher Löschungsvorschriften durch eine Entscheidung der Exekutive zu richten.

Nachdem Ende 2011 der sog. Nationalsozialistische Untergrund (NSU) aufgedeckt worden war und im März 2012 der Sächsische Landtag die Einsetzung eines Untersuchungsausschusses zur Rolle der sächsischen Behörden bei der Suche nach den Ende der 1990er Jahre untergetauchten Mitgliedern des NSU beschlossen hatte, verfügten das Sächsische Staatsministerium des Innern und das Sächsische Staatsministerium der Justiz im Sommer 2012, dass Daten und Unterlagen der sächsischen Polizei, des Landesamtes für Verfassungsschutz sowie der sächsischen Staatsanwaltschaften, die Bezüge zu rechtsextremistischen Straftaten und Bestrebungen aufwiesen, auch dann nicht zu löschen bzw. zu vernichten seien, wenn kein Zusammenhang mit Aktivitäten des NSU erkennbar sei und die gesetzlichen Speicher- und Aufbewahrungsfristen abgelaufen seien. Damit sollte sichergestellt werden, dass Akten, deren Relevanz für die Untersuchung sich möglicherweise erst später zeigt, auch nach Ablauf der gesetzlichen Aufbewahrungsfristen dem Untersuchungsausschuss noch zur Verfügung gestellt werden könnten.

Als sich 2014 gegen Ende der 5. Legislaturperiode abzeichnete, dass ein Untersuchungsausschuss auch im noch zu wählenden 6. Sächsischen Landtag eingesetzt würde, um die parlamentarische Untersuchung fortzuführen, wurden die Löschmoratorien verlängert. Meine mit zunehmendem Zeitablauf immer stärker werdenden Bedenken gegen diese behördlichen Entscheidungen, gesetzliche Löschfristen zu ignorieren, habe ich den beteiligten Staatsministerien ebenso dargelegt wie dem erwartungsgemäß eingesetzten 1. Untersuchungsausschuss des 6. Sächsischen Landtags.

Datenschutzrechtlich problematisch ist der Umstand, dass die Löschmoratorien in das Grundrecht der betroffenen Personen auf informationelle Selbstbestimmung eingreifen,

ohne dass hierfür eine gesetzliche Grundlage besteht. Die Pflicht zur Löschung personenbezogener Daten in behördlichen Dateien und zur Vernichtung personenbezogener Unterlagen nach bestimmten Fristen im Sächsischen Polizeigesetz, in der Strafprozessordnung und im Sächsischen Verfassungsschutzgesetz ist die einfachgesetzliche Umsetzung des Grundrechts auf informationelle Selbstbestimmung. Wird durch ein Moratorium die Erfüllung dieser Pflicht ausgesetzt, greift dies unmittelbar in das Grundrecht der Betroffenen ein. Für die Aufgabenerfüllung der betroffenen Behörden sind die Daten und Unterlagen nicht mehr erforderlich; sie werden nur noch aufgrund der Moratorien gespeichert und aufbewahrt. Dabei sind – längerfristige – Löschmoratorien für eine gesetzes- und verfassungskonforme Unterstützung des Untersuchungsausschusses durch die Behörden gar nicht notwendig. Die Pflicht sächsischer Behörden zur unmittelbaren Vorlage von Akten und zur Erteilung von Auskünften an einen Untersuchungsausschuss des Sächsischen Landtags ergibt sich direkt aus § 14 UAusschG. Der Einsetzungsbeschluss und die konkreten Beweisbeschlüsse des Untersuchungsausschusses bestimmen den Umfang der Akten, die dem Untersuchungsausschuss vorzulegen sind. Akten mit Bezug zu den Untersuchungsaufträgen waren nach den weit gefassten und weit auszulegenden Beweisbeschlüssen dem 3. Untersuchungsausschuss des 5. Sächsischen Landtags sowie dem 1. Untersuchungsausschuss des 6. Sächsischen Landtags vorzulegen, später aufgefundene Akten waren umgehend nachzureichen. Diesen Pflichten korrespondierten und korrespondieren selbstverständlich entsprechende Löschungs- und Vernichtungsverbote hinsichtlich vorzulegender Unterlagen bei den vorlagepflichtigen Stellen. Insoweit gehen § 14 UAusschG und die gesetzlich vorgesehene Nutzung der Unterlagen durch den Untersuchungsausschuss den gesetzlichen Löschungs- und Vernichtungspflichten der Behörden vor. Die Löschmoratorien betrafen und betreffen aber einen sehr breiten, den Untersuchungsbereich der Ausschüsse weit überschreitenden Datenkreis und erfassen Daten und Unterlagen, die von den vorlagepflichtigen Behörden gerade als nicht relevant für den jeweiligen Untersuchungsausschuss eingestuft wurden (andernfalls hätten sie ja vorgelegt werden müssen). Diese Unterlagen werden also mangels Relevanz nicht dem Untersuchungsausschuss vorgelegt und verbleiben bei den Behörden, werden dort aber gleichwohl nicht gelöscht bzw. vernichtet, obwohl die gesetzlichen Speicherfristen zum Teil schon seit Jahren abgelaufen sind.

Um die aus diesem rechtstaatlich zweifelhaften Vorgehen resultierenden Grundrechtsbeeinträchtigungen für einzelne Betroffene abzuschwächen, legten die zuständigen Staatsministerien Verfahren fest, nach denen die betreffenden – löschungsreifen – Datensätze aus den täglich genutzten Dateien bzw. Datenbanken ausgesondert, aber eine Vernichtung der Papierakten verhindert und die Auffindung letzterer ermöglicht werden sollte, wenn sich doch noch einmal Bedarf ergeben würde. Eine solche Verfahrensweise hielt ich – unter Zurückstellung meiner ganz grundsätzlichen Bedenken gegen ein über Jahre währendes Aussetzen von gesetzlich vorgesehenen Löschungen – für datenschutz-

rechtlich gerade noch akzeptabel, weil damit ein schneller, müheloser Zugriff auf die Daten nur noch einem sehr kleinen Kreis von Personen möglich gewesen wäre.

Während für das Landesamt für Verfassungsschutz und die sächsischen Staatsanwaltschaften eine Umsetzung unproblematisch erfolgte, traten bei der sächsischen Polizei die im 18. TB beschriebenen Schwierigkeiten auf. Eine technische Verknüpfung von Löschungen in der Datei PASS (Polizeiliches Auskunftssystem Sachsen) mit dem Befehl zum Vernichten der Papierakten in den betreffenden Dienststellen ließ Polizei und Staatsministerium des Innern befürchten, dass Akten entgegen dem Löschmoratorium vernichtet würden. In der Folge wurde die Umsetzung des Verfahrens gestoppt, gesetzlich eigentlich zu löschende, aber dem Löschmoratorium unterfallende Datensätze blieben im PASS gespeichert – und über Jahre für sämtliche Nutzer des PASS (im Prinzip also für sämtliche Polizeivollzugsbeamte des Freistaates) sichtbar. Ihre Kennzeichnung als „gesperrte“ Daten änderte an ihrer Sichtbarkeit nichts.

Im Berichtszeitraum habe ich gegenüber dem Staatsministerium des Innern und dem Landeskriminalamt wiederholt darauf gedrängt, dem datenschutzrechtlich inakzeptablen Zustand abzuhelfen und endlich ein Verfahren zu finden, das den Ankündigungen von 2015 auch bei der Polizei entspricht. Im Dezember 2018 informierte mich das SMI darüber, dass ein Weg gefunden worden sei, löschungsreife und vom Moratorium erfasste Daten in der Datei PASS wieder den an gesetzlichen Fristen ausgerichteten Löschroutinen zu unterziehen. Kopierte und gesicherte Daten sowie die dazugehörigen Papierakten würden künftig nur einem eng begrenzten Personenkreis zugänglich sein (Mitarbeiter, die mit der Bearbeitung von Beweisbeschlüssen des Untersuchungsausschusses betraut sind sowie Mitarbeiter der Datenstationen, die mit der Datenpflege beauftragt sind). Der operativen Auswertung durch Abfragen oder Recherchen im PASS seien diese Daten dann entzogen.

Auch wenn damit nun bei allen von den Löschungsmoratorien betroffenen Behörden des Freistaates die mit der Aufschiebung der Löschung verbundenen Grundrechtsverletzungen in ihrer Intensität beschränkt werden, muss ich erneut darauf hinweisen, dass behördlich bestimmte Aussetzungen der Erfüllung grundrechtssichernder und gesetzlich vorgeschriebener Maßnahmen rechtstaatlich nur in besonderen Ausnahmefällen und kurzfristig akzeptabel sein können; das gilt auch, wenn parlamentarische Untersuchungen im Raum stehen. Das Grundrecht auf informationelle Selbstbestimmung ist ein Recht von Verfassungsrang, es steht weder den Verantwortlichen nicht zu, es zu ignorieren.

8.3 Auskunftsersuchen der Polizei an Unternehmen in Ermittlungsverfahren

Gelegentlich erreichen mich Anfragen von Unternehmen, die sich im Rahmen von Auskunftsverlangen von Polizei oder Staatsanwaltschaft in Ermittlungsverfahren mit der Forderung konfrontiert sehen, Kundendaten offenzulegen. Unsicherheit besteht dabei hinsichtlich des Verhältnisses etwaiger rechtlicher Pflichten, solchen Forderungen nachzukommen, einerseits und datenschutzrechtlicher Verpflichtungen gegenüber den Kunden andererseits.

Welche Angaben die nach der Strafprozessordnung ermittelnde Polizei für die Erforschung von Sachverhalten für erforderlich hält und wen sie dazu befragt, entscheidet sie bzw. die das Ermittlungsverfahren leitende Staatsanwaltschaft. Die Strafverfolgungsbehörden sind für die Rechtmäßigkeit ihrer Ermittlungen verantwortlich. Ihre Ermittlungsbefugnisse sind im Rahmen der Strafprozessordnung breit gefächert. Nach §§ 161, 163 StPO sind Polizei bzw. Staatsanwaltschaft berechtigt, Ermittlungen zur Erforschung von Straftaten vorzunehmen und dabei auch Auskünfte auch von Unternehmen über deren Kunden bzw. Geschäftspartner zu verlangen.

Eine gesetzliche Pflicht, auf Ladung vor der Polizei zu erscheinen und auszusagen (es sei denn, es bestehen Zeugnis- oder Auskunftsverweigerungsrechte), besteht seit August 2017 nach § 163 Absatz 3 Satz 1 StPO, „wenn der Ladung ein Auftrag der Staatsanwaltschaft zugrunde liegt“. Zuvor galt eine solche Pflicht nur gegenüber den Staatsanwaltschaften (§ 161a StPO) und Gerichten. Sobald eine Aussagepflicht besteht, ist für Abwägungen auf Seiten des Zeugen (Unternehmen bzw. Unternehmensmitarbeiter) hinsichtlich „Ob“ und Umfang der Offenlegung von Daten zu Kunden oder Geschäftspartnern kein Raum, weil dann die gesetzliche Verpflichtung besteht, die geforderten Angaben zu machen. In das Recht auf informationelle Selbstbestimmung betroffener Personen wird durch die gesetzlichen Vorschriften zur Erforschung von Straftaten eingegriffen. Ein bedeutender Ausnahmefall besteht, wenn – wiederum strafprozessual vorgesehene – Zeugnisverweigerungsrechte von Berufsgeheimnisträgern wie Ärzten oder Verteidigern gegeben sind, §§ 53, 53a StPO. Dagegen können sich beispielsweise Banken, Vermieter, Verkehrsunternehmen und deren Mitarbeiter nicht auf diese Zeugnisverweigerungsrechte berufen.

Im Regelungssystem der DSGVO sind die Fälle der Offenlegung von Kundendaten gegenüber Strafverfolgungsbehörden zur Erfüllung strafprozessualer Aussagepflichten als Fall rechtmäßiger Verarbeitung nach Artikel 6 Absatz 1 Buchstabe c DSGVO anzusehen.

Besteht keine Aussagepflicht gemäß gesetzlicher Vorschriften der Strafprozessordnung – und mithin keine rechtliche Verpflichtung des Verantwortlichen (Unternehmens) im Sinne von Artikel 6 Absatz 1 Buchstabe c DSGVO, – richtet sich die Zulässigkeit der Übermittlung von Daten von Kunden oder Geschäftspartnern an Strafverfolgungsbehörden nach § 24 Absatz 1 Nummer 1 BDSG n. F. Dies betrifft z. B. die Fälle, in denen (noch) keine Ladung vorliegt oder das Unternehmen Daten initiativ übermitteln möchte (etwa zur Anzeige von Straftaten). Während oben beschriebene, strafprozessuale Aussagepflichten die Belange der betroffenen Personen (Kunden, Geschäftspartner) nicht berücksichtigen, hat das verantwortliche Unternehmen bei Übermittlungen auf Grundlage von § 24 Absatz 1 Nummer 1 BDSG n. F. die Interessen der Betroffenen am Ausschluss der Verarbeitung (Übermittlung) zu beachten; es hat also eine Abwägung zwischen dem Zweck der Verfolgung von Straftaten und den Interessen der Betroffenen am Unterbleiben der Offenlegung sie betreffender Angaben gegenüber Strafverfolgungsbehörden vorzunehmen. Abwägungsaspekte können dabei die Schwere der Tat bzw. des Tatverdachts und der Charakter der Angaben, die gemacht werden sollen, sein.

Vor diesem Hintergrund und angesichts des Umstands, dass Art und Form polizeilicher Anfragen in Ermittlungsverfahren (mit)bestimmen, ob angefragte Unternehmen zur Offenlegung personenbezogener Daten verpflichtet oder (nur) berechtigt sind, halte ich es für wichtig, dass Ermittlungsbehörden ihre Anfragen klar formulieren und deren Rechtsgrundlagen benennen. Es lässt sich gerade mit dem in den Berichtszeitraum fallenden Beginn der unmittelbaren Anwendung der DSGVO leicht vorstellen – und die mich erreichenden Anfragen bestätigen das –, dass Unternehmen in einen gewissen Konflikt geraten, wenn sie polizeilich aufgefordert werden, Daten von Vertragspartnern offenzulegen. Präzise formulierte Anfragen und die Bereitschaft der Ermittler, auf Nachfragen erläuternde Hinweise zu geben, dürften eventuelle Rechtsunsicherheiten bei angefragten Unternehmen beseitigen und zugleich die Arbeit der Ermittlungsbehörden beschleunigen. Bei Anfragen der Polizei sollten deshalb stets das Aktenzeichen des Vorgangs und, wie erwähnt, die Rechtsgrundlage der Anfrage bezeichnet werden. Andererseits ist die Polizei nicht verpflichtet, (potentiellen) Zeugen ihre Erkenntnisse gänzlich offenzulegen, um ihre Fragen aus Sicht des Zeugen plausibel zu machen.

9 Rechtsprechung zum Datenschutz

9.1 Betreiber einer Facebook-Fanpage sind Verantwortliche - EuGH, Urteil vom 5. Juni 2018, C-210/16

Im letzten Berichtszeitraum entschied der Europäische Gerichtshof (EuGH), dass nicht nur das Unternehmen Facebook, sondern auch die Nutzer und Betreiber von Fanpages datenschutzrechtlich Verantwortliche sind. Der Gerichtshof urteilte, dass der Betreiber einer Fanpage zusammen mit Facebook als „gemeinsam Verantwortlicher“ gilt.

Die Entscheidung erregte medial Aufsehen. Zwar wurde die Entscheidung noch auf Grundlage der Richtlinie (EU) 95/46/EG entschieden, die nach Wirksamwerden der Datenschutz-Grundverordnung außer Kraft getreten ist, doch haben die aufgestellten Grundsätze zur datenschutzrechtlichen Verantwortung auch für Entscheidungen des Gerichts nach neuer Rechtslage Indizwirkung. So bezog sich das Gericht unter anderem darauf, dass der Fanpagebetreiber über die Zwecke und Mittel der Datenverarbeitung mitentscheide, vergleiche Rdnr. 39 der Entscheidung. Von grundsätzlicher Bedeutung dürfte hierbei auch die Einschätzung des Gerichts sein, dass ein Betreiber einer Internetpräsenz. Der auf einer Plattform eines Social Media-Unternehmens nicht aufgrund der Nutzung einer fremden Infrastruktur von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreit bzw. exkulpiert sein soll.

Ich habe in der Vergangenheit immer wieder vor der Nutzung von interaktiven und mit auf Fremdseiten führenden Elementen versehenen Fanpages gewarnt. Neben den häufig nicht ausreichenden Angaben zur Erfüllung der Informationspflichten seitens der Fanpagebetreiber wären durch die Verantwortlichen offene Fragen in Bezug auf Artikel 26 DSGVO zu klären. Auch der Umstand, dass gemeinsam Verantwortliche letztendlich gesamtschuldnerisch haften, sollte in Anbetracht der fortwährenden Datenschutzskandale im Zusammenhang mit Social Media-Plattformen zu denken geben. Insbesondere erwarte ich, dass Verantwortliche des öffentlichen Bereichs ihrer Vorbildfunktion Rechnung tragen.

9.2 Videoüberwachung, Beschäftigtendatenschutz - BAG, 23.08.2018 - 2 AZR 133/18

Im letzten Berichtszeitraum entschied das Bundesarbeitsgericht über einen Streitfall, der eine Auswertung von einem halben Jahr alten Bilddaten einer ansonsten rechtmäßigen und offenen Videoüberwachung, die vor Straftaten von Arbeitnehmern schützen sollte, zum Gegenstand hatte. Die arbeitgeberseitige Auswertung des Videomaterials, die zur Entlassung einer Arbeitnehmerin in einem Tabakwarenladen führte, die Einnahmen nicht in die Registrierkasse eingeordnet hatte, wurde seitens des Bundesarbeitsgerichts

für zulässig angesehen. In den Vorinstanzen hatten das Arbeitsgericht und das Landesarbeitsgericht Hamm noch die Kündigung der Arbeitnehmerin wegen einer nicht mehr vertretbaren Beweisverwertbarkeit aufgrund der langen Speicherdauer der Bilddaten aufgehoben.

Die Entscheidung bezog sich noch auf gesetzliche Rechtsgrundlagen alter Fassung, § 6b Absatz 1 Nummer 3 BDSG a. F. und auf die beschäftigtendatenschutzrechtliche Vorschrift des § 32 Absatz 1 Satz 1 BDSG a. F. Nach dem Urteil wird die Datenerhebung im Hinblick auf die unerlaubten Handlungen der Beschäftigten sowohl nach § 6b Absatz 1 Nummer 3 und daneben gemäß § 32 Absatz 1 Satz 1 als Erlaubnisvorschriften als zulässig erkannt. Ein Verwertungsverbot aufgrund langer Speicherdauer verneinte das Bundesarbeitsgericht in Anbetracht einer geringen Schutzwürdigkeit eines rechtmäßig gefilmten Vorsatztäters und noch nicht verwirkter Kündigungsrechte sowie möglicher Schadensersatzansprüche, die eine Erforderlichkeit einer fortwährenden Speicherung der streitigen Bildaufnahmen erforderlich mache, vergleiche Rdnr. 28, 30, 31 der Entscheidung. Seitens meiner Dienststelle als überraschend und als kritikwürdig wurde die Einschätzung des Gerichts gewertet, dass seitens des Arbeitgebers keine Pflicht bestanden habe, das gesamte Bildmaterial zeitnah zu sichten, vergleiche Rdnr. 27, 33. Eine „etwaige“ Pflicht, Bildmaterial zeitnah zu sichten, diene allein dazu, nicht zweckrelevante Sequenzen zu identifizieren und zu löschen. Eine Missachtung einer Löschpflicht ließe den Bedarf der Verarbeitung zweckrelevanter Passagen nicht entfallen, Rdnr. 27 unter Verweis auf parlamentarische Unterlagen zu § 6b BDSG a. F. Einem rechtsstaatswidrigen planmäßigen Unterlaufen der Löschpflicht, so das Bundesarbeitsgericht, habe zudem entgegenstanden, dass die Betroffene etwaige Löschansprüche habe selbst geltend machen und sie gegebenenfalls gerichtlich habe durchsetzen können, Rdnr. 35. Miterfasste personenbezogene Daten Dritter – unter anderem Kunden – hätten die fortwährende Speicherung unter der Voraussetzung nicht bestehender Missbrauchsgefahr der Aufzeichnungen zu dulden, Rdnr. 32.

Die Entscheidung ist bei nicht wenigen unabhängigen Datenschutzbehörden auf Widerspruch gestoßen. Auch meine Behörde verlangt trotz nicht bestehender konkreter Fristen eine adäquate und kurze Speicherdauer. In ähnlich gelagerten Fällen wird regelmäßig eine wenige Tage dauernde Speicherdauer als ausreichend angesehen. Die Speicherdauer von Videodaten kann nach Überzeugung meiner Dienststelle auch nicht in Abhängigkeit von parallel bestehenden andauernden Ansprüchen und Rechten entgegen bestehenden Grundsätzen für die Verarbeitung personenbezogener Daten ausgedehnt werden, ohne dass dies im Einzelfall erforderlich wäre, Artikel 5 Absatz 1 Buchstabe c DSGVO. Die Entscheidung des Bundesarbeitsgerichts ist in Bezug auf den Streitfall bisher solitär. Meine Behörde betont, dass sie dem Urteil, abgesehen von der Tatsache, dass es sich um eine Einzelfallentscheidung handelt und sich künftig die Zulässigkeit

der Verarbeitung an der Datenschutz-Grundverordnung zu bemessen hat, keine Rechtfertigung für Verantwortliche zuerkennt, längere Speicherfristen zu begründen. Meine Dienststelle wird ihre datenschutzrechtliche Spruchpraxis in gleichgelagerten Fällen, was die Dauer der Verarbeitung der personenbezogenen Daten anbelangt, fortsetzen und gegebenenfalls mit Anordnungen durchsetzen. Meine Behörde ist nicht an gerichtliche Entscheidungen mit datenschutzrechtlichem Bezug, in denen sie nicht selbst Partei gewesen ist, gebunden.

9.3 Wettbewerbsrechtliche Abmahnung wegen Verstoßes gegen die DSGVO - LG Bochum, Urteil vom 07.08.18, I-12 O 85/18 und LG Würzburg, Beschluss vom 13.09.2018, O 1741/18

In Bezug auf die Entscheidungen des Landgerichts Bochum und des Landgerichts Würzburg wird auf den Tätigkeitsberichtsbeitrag unter 3.1.2 verwiesen.

9.4 Verhältnis der Datenschutz-Grundverordnung zum Kunsturhebergesetz - LG Frankfurt a. M., Urteil vom 13.09.2018 – 2/3 O 283/18

In einer Entscheidung zur Veröffentlichung von Videos auf Facebook setzte sich das Landgericht Frankfurt mit dem anzuwendenden Rechtsrahmen auseinander, ohne sich allerdings zur Frage der Fortgeltung des Kunsturhebergesetzes zu positionieren.

In der Sache ging es um eine betroffene Person, die bei einem Friseur eine Haarverlängerung hatte anfertigen lassen. Während der Prozedur oder in der Folge wurde sie fotografiert und videografiert. Der Friseur veröffentlichte Fotos und ein Video auf dem die betroffene Kundin zu erkennen war. Im Nachgang forderte die betroffene Person die Entfernung des Fotos und des Films von der Fanpage. Das Video blieb aber weiter über das Internet zugänglich. Im einstweiligen Rechtsschutzverfahren forderte die betroffene Person die Beendigung der Verbreitung des Videos.

Bei seiner Entscheidung prüfte das Landgericht Artikel 6 Absatz 1 Buchstabe a) und Artikel 6 Absatz 1 Buchstabe f DSGVO), aber auch mögliche Ausnahmen von der Einwilligungspflicht gemäß § 23 Kunsturhebergesetz (KunstUrhG) und es führte aus, dass es die Grundsätze der §§ 22, 23 KunstUrhG und die dazu ergangene Rechtsprechung als Gesichtspunkte im Rahmen von Artikel 6 Absatz 1 Buchstabe f) DSGVO einbezogen habe, vgl. Rdnr. 24, 25, 32, 37. Die Glaubhaftmachung einer behaupteten Einwilligung wurde hingegen seitens des Gerichts verneint, Rdnr. 33 ff. Im Hinblick auf die Interessenabwägung urteilte das Gericht, dass eine Verarbeitung zum Zweck der Direktwerbung grundsätzlich als berechtigtes Interesse anerkannt werden könne, es aber bei der

Verbreitung der personenbezogenen Bildaufnahmen an der Erforderlichkeit mangele, Rdnr. 39 f. Zudem entspreche es nicht den vernünftigen Erwartungen eines Kunden in einem Friseursalon, dass Videoaufnahmen von Kunden angefertigt und verbreitet würden, Rdnr. 41 der Entscheidung.

Vergleiche auch die Tätigkeitsberichtsbeiträge 2.2.7, 2.3.2, 2.3.3 zur Verbreitung von Bilddaten.

9.5 Weite Auslegung des zu berücksichtigenden berechtigten Interesses nach der DSGVO und gemäß § 242 BGB, Weitergabe von Kundendaten, Daten mit Drittbezug - OLG München 24.10.2018, 3 U 1551/17

In einem erfolgreichen Berufungsverfahren einer Streitigkeit eines Vertragshändlers mit einem Hersteller vor dem Oberlandesgericht München beantragte der zunächst unterlegene und widerklagende Beklagte und Vertragshändler Auskunft, an welche Abnehmer in einem bestimmten Zeitraum und bestimmten Regionen jeweils Güter verkauft worden und welcher Kaufpreis jeweils vereinbart wurde, da er sich im Unklaren über einen ihm zustehenden Gegenanspruch befand. Zu prüfen war damit gerichtlich auch der Schutz der Wirtschaftsdaten betroffener Kunden.

Das Gericht führte in Rn. 32 der Entscheidung aus, dass, soweit die Auffassung vertreten werde, der Auskunftserteilung stünden Bestimmungen der Datenschutz-Grundverordnung entgegen, auf Artikel 6 Absatz 1 Satz 1 Buchstabe f) DSGVO zu verweisen sei. Bei der erforderlichen Abwägung seien auch die Erwägungsgründe, dass die vernünftigen Erwartungen der betroffenen Personen, die auf der Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen, Erwägungsgrund 47 Satz 1 Halbsatz 2. Satz 2 des Erwägungsgrundes führe hierbei als Beispiel an, dass der Betroffene ein Kunde des Verantwortlichen sei oder in seinen Diensten stehe. Auslegungsmethodisch sei vor dem Hintergrund von Artikel 6 Absatz 1 Satz 1 Buchstabe f) DSGVO ein Ausgleich zwischen den Interessen des Betroffenen und des Verantwortlichen zu schaffen. Dabei seien nicht nur rechtliche Interessen von Bedeutung, sondern auch wirtschaftliche oder ideelle Interessen des Verarbeiters zu berücksichtigen. Soweit die von dem Verantwortlichen begehrten Informationen dem Beklagten zur Ermittlung eines Schadensersatzanspruchs aus der Verletzung eines Vertragshändlervertrages dienten und gemäß § 242 BGB eine Erteilung einer solchen Information vorzunehmen sei, könne der Gesichtspunkt des Schutzes der wirtschaftlichen Daten der jeweiligen Kunden nicht höher anzusetzen sein.

Eine Offenbarung und Weitergabe der Kundendaten hatte damit nach dem Oberlandesgericht zu erfolgen.

9.6 Auslegung von Artikel 15 Absatz 3 Satz 1 Datenschutz-Grundverordnung, Recht auf Kopie – LAG Baden-Württemberg, Urteil vom 20.12.2018 – 17 Sa 11/18

Für große Aufmerksamkeit sorgte das Urteil des Landesarbeitsgerichts in der Berufung zu einem Kündigungsstreitverfahren, da sich erstmals ein Obergericht mit der Auslegung des Artikels 15 Absatz 1 Satz 1 Datenschutz-Grundverordnung auseinandersetzte.

Der Arbeitnehmer und Kläger verlangte von der Arbeitgeberin Auskunft über bei dieser gespeicherten und nicht in der Personalakte enthaltenen personenbezogenen „Leistungs- und Verhaltensdaten“ und eine Kopie dieser Daten. Gestützt wurde der Anspruch hierbei auf Artikel 15 Absatz 1 und Absatz 3 Datenschutz-Grundverordnung. Das Gericht gab den konkreten Anträgen auf Auskunft, Kopie und Einsichtnahme statt. Im Tenor der Entscheidung unter III heißt es zusammengefasst, dass dem Arbeitnehmer Auskunft über die von der Arbeitgeberin verarbeiteten und nicht in der Personalakte des Arbeitnehmers gespeicherten personenbezogenen Leistungs- und Verhaltensdaten des Klägers zu erteilen sei und dies im Hinblick auf die Zwecke der Datenverarbeitung, die Empfänger, gegenüber denen die Arbeitgeberin die personenbezogenen Daten des Arbeitnehmers offengelegt habe, die Speicherdauer, die Herkunft der personenbezogenen Daten des Arbeitnehmers sowie dem Arbeitnehmer eine Kopie seiner personenbezogenen Leistungs- und Verhaltensdaten, die Gegenstand der von der Arbeitgeberin vorgenommenen Verarbeitung seien, zur Verfügung zu stellen seien.

In seiner Entscheidung legt das Landesarbeitsgericht das in Artikel 15 Absatz 3 Satz 1 Datenschutz-Grundverordnung enthaltene Recht auf Kopie weit aus, vergleiche Rn. 196 ff. der Entscheidung. Hervorgehoben wird unter anderem, dass Artikel 15 Absatz 3 Satz 1 auch auf Arbeitsverhältnisse Anwendung finde, Rn. 196 und 198. Der Anspruch sei im Streitfall auch nicht durch berechtigte Interessen Dritter eingeschränkt, Rn. 204 ff. Schützenswerte Interessen Dritter seien von der Arbeitgeberin nicht vorgetragen worden bzw. es sei nur pauschal auf ein Schutzbedürfnis von Hinweisgebern verwiesen worden, Rn. 208 f.

In der Fachliteratur werden zur Auslegung von Artikel 15 Absatz 3 Satz 1 Datenschutz-Grundverordnung unterschiedliche Meinungen vertreten. Eine herrschende Meinung hat sich noch nicht herausgebildet. Ob die insoweit weite Auslegung des Rechts auf Kopie nach Artikel 15 Absatz 3 Satz 1 Datenschutz-Grundverordnung Bestand haben wird, wird sich erweisen. Die im Dezember 2018 ergangene Entscheidung des Landesarbeitsgerichts Baden-Württemberg ist noch nicht rechtskräftig. Aufgrund der grundsätzlichen

Bedeutung der Frage hatte das Landesarbeitsgericht die Revision zum Bundesarbeitsgericht zugelassen.

Zur Auslegung von Artikel 15 Absatz 3 Satz 1 Datenschutz-Grundverordnung verfolgen die unabhängigen Datenschutzbehörden des Bundes und der Länder noch keine einheitliche Meinung. Auf die Rechtsfrage werde ich daher in meinem nächsten Tätigkeitsbericht zurückkommen.

9.7 Verwaltungsgerichtliche Entscheidungen in Verfahren unter Beteiligung des Sächsischen Datenschutzbeauftragten

Im letzten Berichtszeitraum war meine Behörde an nicht wenigen Verwaltungsgerichtsverfahren beteiligt. Überwiegend handelte es sich um Verstöße wegen rechtswidrig betriebener Videoüberwachungsanlagen. Betroffene Dienstleister und Unternehmer suchten mit Anfechtungsklagen wegen erfolgter Kosten- bzw. Heranziehungsbescheide meiner Behörde Rechtsschutz. Zu betrachtende Erlaubnisnormen waren u. a. das Bundesdatenschutzgesetz und das Sächsische Datenschutzgesetz in seiner alten Fassung.

Nachstehende Fallbeispiele gewähren einen Einblick in die Verfahren vor dem zuständigen Verwaltungsgericht Dresden.

a. Anfechtungsklage wegen Kostenbescheids, Einstellung nach Klagerücknahme in Hauptverhandlung

Kontrollgegenstand war eine im Bereich der Theke eines Coffeeshops betriebene Videokamera. Der Betrieb dieser u. a. den kompletten Mitarbeiterbereich hinter der Theke erfassenden Kamera war datenschutzrechtlich unzulässig. Auf eine wirksame Einwilligung der Mitarbeiter konnte die Videoüberwachung mangels Freiwilligkeit nicht gestützt werden. Auch die Voraussetzungen des § 32 BDSG a. F. lagen nicht vor; es handelte sich um eine verdachtsunabhängige und dauerhafte Videoüberwachung des gesamten Arbeitsbereiches der Mitarbeiter an der Theke.

Der Kontrollvorgang wurde mit der Feststellung der Rechtswidrigkeit der Videoüberwachung und einer darauf basierenden Kostenfestsetzung abgeschlossen. Seine dagegen gerichtete Klage nahm der Inhaber in der Hauptverhandlung mangels Aussicht auf Erfolg wieder zurück.

b. Anfechtungsklage wegen Kostenbescheids, Klageabweisung

Ein Logopäde hatte im Eingangsbereich des mit einer sozialen Beratungsstelle gemeinsam genutzten Gebäudes eine Videokamera installiert. Eine weitere Kamera hatte er in seinem eigenen Flur im allein genutzten Obergeschoss betrieben. Dies wurde der Auf-

sichtsbehörde durch den Träger der sozialen Beratungsstelle mitgeteilt. Meine Behörde hatte den Sachverhalt geprüft, beide Kameras als rechtswidrig bewertet und den Logopäden infolge dieses Datenschutzverstoßes mit entsprechenden Kosten belegt. Die dagegen gerichtete Klage wies das Verwaltungsgericht ab.

Bei der vom Kläger durchgeführten Videobeobachtung des Eingangs- und Flurbereichs der Praxis handelte es sich nach Einschätzung des Gerichts um die Beobachtung eines öffentlich zugänglichen Raums mit optisch-elektronischen Einrichtungen. Der Anwendungsbereich des § 6b Absatz 1 BDSG a. F. war damit nach Auffassung des Verwaltungsgerichts eröffnet. Zu der Praxis habe jedermann Zutritt gehabt und habe eintreten und sich im Eingangsbereich im Erdgeschoss und dem Praxisbereich im Obergeschoss aufhalten können. Unbeachtlich seien auch die Eigentumsverhältnisse an dem Gebäude. Öffentlich zugänglich könnten auch Räume im Privatbesitz sein.

Die durch den Praxisbetreiber erfolgte Videoüberwachung war nach dem Gericht hinsichtlich beider Videokameras nicht mit der Regelung des § 6b Absatz 1 BDSG a. F. vereinbar.

Die im Praxisbereich im Gebäudestockwerg angebrachte Videokamera war nach gerichtlicher Einschätzung weder in präventiver noch in repressiver Hinsicht zur Wahrnehmung des Hausrechts im Hinblick auf die vom Kläger behaupteten Störungen im Erdgeschoss des Gebäudes geeignet, da mit ihr allein das Geschehen im Flurbereich der Praxis beobachtet werden konnte. Zudem hätte es mildere Mittel der Beobachtung gegeben, die das allgemeine Persönlichkeitsrecht der Betroffenen weniger beeinträchtigt hätten. Dem Praxisbetreiber sei es zuzumuten gewesen, den Zutritt zu seinen Praxisräumen manuell bzw. durch Personal zu kontrollieren.

Darüber hinaus sei die Beobachtung der beiden Überwachungsbereiche mit einer Videoanlage auch nicht umfassend und ununterbrochen gewesen, da die hiermit betrauten Praxisbeschäftigten gleichzeitig durch Verwaltungstätigkeit im Empfangsbereich und Behandlung von Patienten gebunden und in der Regel nur nebenbei die Videomonitoranlage beaufsichtigen könnten. Damit sei die Videoüberwachung für eine zweckentsprechende wirksame Kontrolle des Eingangs- und Praxisbereichs nicht geeignet gewesen.

Das Gericht äußerte sich darüber hinaus auch im Hinblick auf die betroffenen Personen. Überwiegende schutzwürdige Interessen der betroffenen Praxisbesucher stünden dem Einsatz der Videoüberwachung entgegen. Diese greife mit dem erzeugten Überwachungsdruck erheblich in das grundgesetzlich geschützte allgemeine Persönlichkeitsrecht ein. Der Eingriff, der nicht von jedermann gleichermaßen empfunden werde, sei als erheblich anzusehen, da für die Betroffenen nur erkennbar sei, dass sie einer Kame-

rabeobachtung ausgesetzt seien, aber nicht ob und von wem sie beobachtet würden. Die Betroffenen müssten demzufolge ständig damit rechnen, beobachtet zu werden, während es zur freien Entfaltung der Persönlichkeit gehöre, Gewissheit zu haben, wann und von wem man beobachtet werde. Damit unterscheide sich die Intensität der Videobeobachtung von der einer Beobachtung durch eine anwesende und sichtbare Aufsichtsperson. Demgegenüber, so das Gericht abwägend, komme den vom Praxisbetreiber mit der Videobeobachtung verfolgten Interessen geringeres Gewicht zu. Die vom Betreiber der Praxis behauptete Gefahrenlage sei auch nicht wesentlich anders als bei anderen Arztpraxen, die ihre Besucher aber keiner Videoüberwachung unterzögen, ohne dass Sicherheitsdefizite bekannt seien. Letztendlich gebe es auch sonstige zumutbare Maßnahmen, um Gefahren zu begegnen und dass Straftaten begangen würden und Unglücksfälle eintreten könnten, sei Ausdruck des allgemeinen Lebensrisikos, das es allein nicht rechtfertige, Videoüberwachung zum Einsatz zu bringen.

Aufgrund des festgestellten Verstoßes gegen § 6b Absatz 1 BDSG a. F. erkannte das Gericht die Kostenerhebung meiner Behörde gemäß § 40 Absatz 1 und 2 SächsDSG a. F. in Verbindung mit Ziffer 1a der Kostenanlage in vollständiger Höhe als rechtmäßig. Dabei war für das Gericht auch nicht im Sinne einer Kostenminderung entscheidend, dass meine Behörde aufgrund eines Hinweises eines Dritten tätig geworden war und dass die Videokameras bereits nachträglich entfernt worden waren, da allein objektive Anhaltspunkte für ein Tätigwerden und der zuvor bestandene Anlass einer stattfindenden Videoüberwachungsmaßnahme für die Kostenerhebung zum Zeitpunkt der getroffenen Maßnahme meiner Behörde entscheidend gewesen sei.

c. Anfechtungsklage wegen Heranziehungsbescheids, Anhörung, formloses Auskunftsersuchen, Klageabweisung

In dem Verfahren einer datenschutzrechtlichen Beschwerde eines Mitglieds einer Wohnungseigentümergemeinschaft gegen einen Immobilienmakler hatte das Verwaltungsgericht zunächst darüber zu entscheiden, ob ein formloses Auskunftsersuchen der Aufsichtsbehörde einerseits wie auch ein formelles, zugleich als Anhörung nach § 28 VwVfG formuliertes Auskunftsersuchen (Ankündigung eines Heranziehungsbescheides für den Fall der Auskunftsverweigerung) einen Verwaltungsakt darstellen. Dies hatte das Verwaltungsgericht verneint und die Klage insoweit wegen Unzulässigkeit abgewiesen.

Das Gericht führte aus, dass Verwaltungsakt nach § 35 Satz 1 VwVfG jede Verfügung, Entscheidung oder andere hoheitliche Maßnahme sei, die eine Behörde zur Regelung eines Einzelfalls auf dem Gebiet des öffentlichen Rechts treffe und die auf unmittelbare Rechtswirkung nach außen gerichtet ist. Ob die Aufforderung zur Auskunftserteilung als tatsächliches Verwaltungshandeln anzusehen sei oder bereits Verwaltungsaktcharak-

ter aufweise, hänge vom objektiven Erklärungswert des Verwaltungshandelns ab, d.h., wie der Adressat unter Bezug auf Form, Abfassung, Begründung und Beifügung einer Rechtsbehelfsbelehrung und weiterer Umstände nach Treu und Glauben bei Auslegung analog §§ 157, 133 Bürgerliches Gesetzbuch (BGB) die Erklärung oder das Verhalten der Behörde habe verstehen müssen. Für einen Verwaltungsakt, so das Gericht, spreche, dass die entsprechenden Schreiben mit einem dem Hinweis auf die gesetzliche Verpflichtung der Klägerin zur Erteilung der Auskunft nach § 38 BDSG, einer Fristsetzung und dem Hinweis auf eine mögliche Geldbuße im Falle der Verweigerung der Auskunft versehen gewesen seien. Damit stelle sich die Erklärung äußerlich als eine verpflichtende Regelung dar. Allerdings seien diese Schreiben im Unterschied zu der späteren Erklärung nicht mit „Bescheid“ überschrieben gewesen, hätten keine Rechtsbehelfsbelehrung, keine Kostenentscheidung und keine Zwangsgeldandrohung beinhaltetet und es sei überdies im zweiten Schreiben eben der Erlass eines förmlichen Bescheids für den Fall der Nichterteilung der Auskünfte ausdrücklich angekündigt worden (Anhörung nach § 28 VwVfG). Die Maklerfirma habe die zuerst erfolgten Schreiben somit als „unförmliche Auskunftsverlangen“ verstehen müssen, die im Falle der Nichterteilung der Auskünfte einen Bescheid zur Folge hätten. Insoweit konnte die Klage daher nicht erfolgreich sein.

Meine Dienststelle schreibt regelmäßig datenverarbeitende Stellen - Verantwortliche – mittels derartiger unförmlicher Auskunftsverlangen an.

Darüber hinaus hatte sich der Makler aber auch gerichtlich gegen den Heranziehungsbescheid meiner Behörde gewandt. Als Besonderheit ist dazu zu vermerken, dass er dabei nach Klagerhebung von seinem Auskunftsverweigerungsrecht Gebrauch gemacht hatte. Diese Klage war zwar zulässig, jedoch aus Sicht des Gerichts unbegründet. Das Gericht befand, dass soweit sich der Makler gegen den Heranziehungsbescheid wende, die Anfechtungsklage als statthafte Klageart zulässig sei. Auch sei, so das Gericht, trotz des zwischenzeitlich geltend gemachten Auskunftsverweigerungsrechts keine Erledigung eingetreten, da die Verfügung als Grundlage für die Erhebung von Verwaltungskosten weiterhin Rechtswirkung entfalte.

Unter Bezugnahme auf den Inhalt des Heranziehungsbescheids und die ergangene Auskunftsverpflichtung sei diese hinreichend bestimmt im Sinne des § 37 Absatz 1 VwVfG i.V.m. § 1 SächsVwVfZG gewesen, so dass der Adressat bereits aus dem Wortlaut der Verfügung habe hinreichend genau erkennen können, welche Auskünfte von ihm verlangt werden. Auch seien die verlangten Auskünfte, die der Wahrnehmung der Kontrollbefugnis aus § 38 Absatz 1 BDSG a. F. gedient hätten, hierzu geeignet, erforderlich und verhältnismäßig im engeren Sinne gewesen. Der Makler sei nicht unangemessen in seinen geschäftlichen Interessen verletzt worden.

Das Gericht schloss seine Überlegungen dahingehend ab, dass die geforderten Auskünfte zur Erfüllung der Datenschutzaufsicht auch geeignet und erforderlich gewesen seien. So habe der Makler auf die in die zunächst mit formlosem Schreiben erbetenen Auskünfte nicht im erfragten Umfange Antwort erteilt und mit einem weiteren Schreiben sei zur Beantwortung der Auskünfte eine weitere Frist von einem Monat unter Ankündigung des Erlasses eines Heranziehungsbescheides gewährt worden. Hierauf habe der Makler nicht reagiert. Ein milderes Mittel zur Erfüllung der Aufgabe nach § 38 Absatz1 BDSG a. F. habe meiner Behörde nicht zur Verfügung gestanden.

Abkürzungsverzeichnis

Vorschriften

Nachstehend werden Gesetze und andere Vorschriften nach der alphabetischen Reihenfolge der *amtlichen, in Ausnahmefällen auch nichtamtlichen Abkürzung, ersatzweise der amtlichen Kurzbezeichnung* aufgeführt.

AO	Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), zuletzt geändert durch Artikel 6 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745)
ASiG	Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit vom 12. Dezember 1973 (BGBl. I S. 1885), zuletzt geändert durch Artikel 3 Absatz 5 des Gesetzes vom 20. April 2013 (BGBl. I S. 868)
BDSG	in Teil 1 des Tätigkeitsberichts: Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I Satz 66), zuletzt geändert durch Artikel 10 Absatz 2 des Gesetzes vom 31. Oktober 2017 (BGBl. I Satz 3618)
	in Teil 2 des Tätigkeitsberichts: Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 7 des Gesetzes vom 30. Juni 2017 (BGBl. I S. 2097)
BeamtStG	Beamtenstatusgesetz vom 17. Juni 2008 (BGBl. I S. 1010), zuletzt geändert durch Artikel 2 des Gesetzes vom 8. Juni 2017 (BGBl. I S. 1570)
BewachV	Bewachungsverordnung in der Fassung der Bekanntmachung vom 10. Juli 2003 (BGBl. I S. 1378), zuletzt geändert durch Artikel 1 der Verordnung vom 1. Dezember 2016 (BGBl. I S. 2692)
BGB	Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Artikel 1 des Gesetzes vom 20. Juli 2017 (BGBl. I S. 2787)

BKAG	Bundeskriminalamtgesetz vom 7. Juli 1997 (BGBl. I S. 1650), zuletzt geändert durch Artikel 2 des Gesetzes vom 1. Juni 2017 (BGBl. I S. 1354)
BMG	Bundesmeldegesetz vom 3. Mai 2013 (BGBl. I S. 1084), geändert durch Artikel 11 Absatz 4 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745)
BtMG	Betäubungsmittelgesetz in der Fassung der Bekanntmachung vom 1. März 1994 (BGBl. I S. 358), zuletzt geändert durch Artikel 1 der Verordnung vom 16. Juni 2017 (BGBl. I S. 1670)
BZRG	Bundeszentralregistergesetz in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 BGBl. I S. 195), zuletzt geändert durch Artikel 1 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2732)
GewO	Gewerbeordnung in der Fassung der Bekanntmachung vom 22. Februar 1999 (BGBl. I S. 202), zuletzt geändert durch Artikel 1 des Gesetzes vom 20. Juli 2017 (BGBl. I S. 2789)
GG	Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 1 des Gesetzes vom 13. Juli 2017 (BGBl. I S. 2347)
GO	Geschäftsordnung des Sächsischen Landtags 6. Wahlperiode vom 12. November 2014 (SächsABl. S. 1497)
HGB	Handelsgesetzbuch in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 3 des Gesetzes vom 10. Juli 2018 (BGBl. I S. 1108) geändert worden ist
KKG	Gesetz zur Kooperation und Information im Kinderschutz vom 22. Dezember 2011 (BGBl. I S. 2975), zuletzt geändert durch Artikel 20 Absatz 1 des Gesetzes vom 23. Dezember 2016 (BGBl. I S. 3234)
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 3 § 31 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266)

NachwG	Nachweisgesetz vom 20. Juli 1995 (BGBl. I S. 946), zuletzt geändert durch Artikel 3a des Gesetzes vom 11. August 2014 (BGBl. I S. 1348)
OWiG	Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), zuletzt geändert durch Artikel 5 des Gesetzes vom 27. August 2017 (BGBl. I S. 3297)
PaßG	Paßgesetz vom 19. April 1986 (BGBl. I S. 537), zuletzt geändert durch Artikel 2 des Gesetzes vom 7. Juli 2017 (BGBl. I S. 2310)
PAuswG	Personalausweisgesetz vom 18. Juni 2009 (BGBl. I S. 1346), zuletzt geändert durch Artikel 4 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745)
Richtlinie (EU) 2016/680 auch: JI-RL	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates
SächsAGBMG	Sächsisches Gesetz zur Ausführung des Bundesmeldegesetzes vom 9. Juli 2014 (SächsGVBl. S. 76), zuletzt geändert durch Artikel 2 des Gesetzes vom 26. Oktober 2016 (SächsGVBl. S. 504)
SächsArchivBenVO	Sächsische Archivbenutzungsverordnung vom 24. Februar 2003 (SächsGVBl. S. 79)
SächsDSDG	Sächsisches Datenschutzdurchführungsgesetz vom 26. April 2018 (SächsGVBl. S. 198, 199)
SächsDSG	Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz) vom 25. August 2003 (SächsGVBl. S. 330), zuletzt geändert durch Artikel 17 des Gesetzes vom 29. April 2015 (SächsGVBl. S. 349)
SächsEGovG	Gesetz zur Förderung der elektronischen Verwaltung im Freistaat Sachsen (Sächsisches E-Government-Gesetz) vom 9. Juli 2014 (SächsGVBl. S. 398), geändert durch die Verordnung vom 4. April 2015 (SächsGVBl. S. 374)
SächsGemO	Sächsische Gemeindeordnung in der Fassung der Bekanntmachung vom 3. März 2014 (SächsGVBl. S. 146), zuletzt geändert durch Artikel 2 des Gesetzes vom 13. Dezember 2016 (SächsGVBl. S. 652)

SächsJG	Sächsisches Justizgesetz vom 24. November 2000 (SächsGVBl. S. 482; 2001 S. 704), zuletzt geändert durch Artikel 7 des Gesetzes vom 15. Dezember 2016 (SächsGVBl. S. 630)
SächsJStVollzG	Sächsisches Jugendstrafvollzugsgesetz vom 12. Dezember 2007 (SächsGVBl. S. 558), zuletzt geändert durch Artikel 2 des Gesetzes vom 16. Mai 2013 (SächsGVBl. S. 250)
SächsKAG	Sächsisches Kommunalabgabengesetz in der Fassung der Bekanntmachung vom 26. August 2004 (SächsGVBl. S. 418; 2005 S. 306), zuletzt geändert durch Artikel 1 des Gesetzes vom 26. Oktober 2016 (SächsGVBl. S. 504)
SächsPolG	Polizeigesetz des Freistaates Sachsen in der Fassung der Bekanntmachung vom 13. August 1999 (SächsGVBl. S. 466), zuletzt geändert durch Artikel 1 des Gesetzes vom 17. Dezember 2013 (SächsGVBl. S. 890)
SächsPresseG	Sächsisches Gesetz über die Presse vom 3. April 1992 (SächsGVBl. S. 125), zuletzt geändert durch Artikel 2 des Gesetzes vom 17. Dezember 2013 (SächsGVBl. S. 896)
SächsSchulG	Sächsisches Schulgesetz in der Fassung der Bekanntmachung vom 16. Juli 2004 (SächsGVBl. S. 298), zuletzt geändert durch Artikel 1 des Gesetzes vom 26. April 2017 (SächsGVBl. S. 242)
SächsStVollzG	Sächsisches Strafvollzugsgesetz vom 16. Mai 2013 (SächsGVBl. S. 250)
SächsSWG	Sächsisches Sicherheitswachtgesetz vom 12. Dezember 1997 (SächsGVBl. S. 647), zuletzt geändert durch Artikel 9 des Gesetzes vom 18. Dezember 2013 (SächsGVBl. S. 970)
SächsUHaftVollzG	Sächsisches Untersuchungshaftvollzugsgesetz vom 14. Dezember 2010 (SächsGVBl. S. 414), geändert durch Artikel 3 des Gesetzes vom 16. Mai 2013 (SächsGVBl. S. 250)
SächsVerf	Verfassung des Freistaates Sachsen vom 27. Mai 1992 (SächsGVBl. S. 243), zuletzt geändert durch Gesetz vom 11. Juli 2013 (SächsGVBl. S. 502)
SächsVSG	Gesetz über den Verfassungsschutz im Freistaat Sachsen (Sächsisches Verfassungsschutzgesetz) vom 16. Oktober 1992 (SächsGVBl. S. 459), zuletzt geändert durch Artikel 3 des Gesetzes vom 17. Dezember 2013 (SächsGVBl. S. 890)

SäHO	Sächsische Haushaltsordnung in der Fassung der Bekanntmachung vom 10. April 2001 (SächsGVBl. S. 153), zuletzt geändert durch Artikel 1 des Gesetzes vom 14. Dezember 2018 (SächsGVBl. S. 782)
SchfHwG	Schornsteinfeger-Handwerksgesetz vom 26. November 2008 (BGBl. I S. 2242), zuletzt geändert durch Artikel 1 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2495)
SGB I	Erstes Buch Sozialgesetzbuch – Allgemeiner Teil – (Artikel I des Gesetzes vom 11. Dezember 1975, BGBl. I S. 3015), zuletzt geändert durch Artikel 5 des Gesetzes vom 14. August 2017 (BGBl. I S. 3214)
SGB V	Fünftes Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), zuletzt geändert durch Artikel 4 des Gesetzes vom 14. August 2017 (BGBl. I S. 3214)
SGB VIII	Achtes Buch Sozialgesetzbuch – Kinder und Jugendhilfe – in der Fassung der Bekanntmachung vom 11. September 2012 (BGBl. I S. 2022), zuletzt geändert durch Artikel 3 des Gesetzes vom 20. Juli 2017 (BGBl. I S. 2780)
SGB X	Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), zuletzt geändert durch Artikel 2 Absatz 6 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2739)
SGB XI	Elftes Buch Sozialgesetzbuch – Soziale Pflegeversicherung – (Artikel 1 des Gesetzes vom 26. Mai 1994, BGBl. I S. 1014, 1015), geändert durch Artikel 9 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2757)
SGB XII	Zwölftes Buch Sozialgesetzbuch – Sozialhilfe – (Artikel 1 des Gesetzes vom 27. Dezember 2003, BGBl. I S. 3022, 3023), zuletzt geändert durch Artikel 2 des Gesetzes vom 17. August 2017 (BGBl. I S. 3214)
StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 1 des Gesetzes vom 17. August 2017 (BGBl. I S. 3202)
StPO	Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Artikel 1 des Gesetzes vom 27. August 2017 (BGBl. I S. 3295)

StVG	Straßenverkehrsgesetz in der Fassung der Bekanntmachung vom 5. März 2003 (BGBl. I S. 310, 919), zuletzt geändert durch Artikel 6 des Gesetzes vom 17. August 2017 (BGBl. I S. 3202)
TMG	Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Artikel 2 des Gesetzes vom 1. September 2016 (BGBl. I S. 3352)
ÜSchuldStatG	Gesetz über die Statistik der Überschuldung privater Personen (Überschuldungsstatistikgesetz) vom 22. Dezember 2011 (BGBl. I S. 3083)
UWG	Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bekanntmachung vom 3. März 2010 (BGBl. I S. 254), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Februar 2016 (BGBl. I S. 235)
Verordnung (EU) 2016/679 auch: DSGVO	Datenschutz-Grundverordnung – Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG
VwVfG	Verwaltungsverfahrensgesetz in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), zuletzt geändert durch Artikel 11 Absatz 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2752)
ZPO	Zivilprozessordnung in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), zuletzt geändert durch Artikel 2 des Gesetzes vom 12. Juli 2018 (BGBl. I S. 1151)

Sonstiges

a. F.	alte Fassung
AG	Arbeitsgruppe
ASD	Allgemeiner Sozialer Dienst
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof

BKA	Bundeskriminalamt
BR-Drs.	Bundesrats-Drucksache
BSG	Bundessozialgericht
BSGE	Bundessozialgerichtsentscheidung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
BVerwGE	Bundesverwaltungsgerichtsentscheidung
d. h.	das heißt
DSK	Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder – Datenschutzkonferenz
etc.	et cetera
EU	Europäische Union
ggf.	gegebenenfalls
i. V. m.	in Verbindung mit
IVO	Integriertes Vorgangsbearbeitungssystem für die Landespolizei
JVA	Justizvollzugsanstalt
KSV	Kommunaler Sozialverband Sachsen
LfV	Landesamt für Verfassungsschutz des Freistaates Sachsen
LG	Landgericht
LKA	Landeskriminalamt Sachsen
LT-Drs.	Landtags-Drucksache
n. F.	neue Fassung

m. w. N.	mit weiteren Nachweisen
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
SächsABl.	Sächsisches Amtsblatt
SächsGVBl.	Sächsisches Gesetz- und Verordnungsblatt
SächsVerfGH	Sächsischer Verfassungsgerichtshof
SID	Staatsbetrieb Sächsische Informatik Dienste
SMF	Sächsisches Staatsministerium der Finanzen
SMI	Sächsisches Staatsministerium des Innern
SMJus	Sächsisches Staatsministerium der Justiz
SMK	Sächsisches Staatsministerium für Kultus
SMS	Sächsisches Staatsministerium für Soziales
SMUL	Sächsisches Staatsministerium für Umwelt und Landwirtschaft
SMWA	Sächsisches Staatsministerium für Wirtschaft, Arbeit und Verkehr
SMWK	Sächsisches Staatsministerium für Wissenschaft und Kunst
StA	Staatsanwaltschaft
SVN	Sächsisches Verwaltungsnetz
u. a.	unter anderem
VwV	Verwaltungsvorschrift
z. B.	zum Beispiel

Verweise im Text auf Ausführungen in früheren Tätigkeitsberichten des Sächsischen Datenschutzbeauftragten sind durch Angabe der Nummer des jeweiligen Tätigkeitsberichtes sowie der jeweiligen Abschnitt-Nummer – getrennt durch einen Schrägstrich – gekennzeichnet (z. B. 4/5.1.2.6).

Stichwortverzeichnis