Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

TÄTIGKEITSBERICHT ZUM DATENSCHUTZ 2019

www.datenschutz.rlp.de

HERAUSGEBER
Der Landesbeauftragte
für den Datenschutz und die
Informationsfreiheit Rheinland-Pfalz
Hintere Bleiche 34 | 55116 Mainz
Postfach 30 40 | 55020 Mainz
Telefon +49 (0) 6131 208-2449
Telefax +49 (0) 6131 208-2497
poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

Oktober 2020

INHALT

VORWORT


Prof. Dr. Dieter Kugelmann

Das Jahr 2019 stand immer noch ganz im Zeichen der Neuerungen durch die Datenschutz-Grundverordnung. Diese Neuerungen sind zwar bereits seit dem 25. Mai 2018 wirksam geworden, ihre Verwirklichung und Konkretisierung hat aber bis in das Jahr 2019 hinein fortgewirkt. Dementsprechend war auch der 25. Mai 2019 ein magisches Datum für die Datenschutzbehörden, weil an mehreren Stellen nachgefragt wurde, wie denn nach einem Jahr die Datenschutz-Grundverordnung zu werten sei. Die Antwort fiel von Seiten der Datenschutzaufsichtsbehörden einhellig aus: Die Datenschutz-Grundverordnung ist ein Erfolg. Dieser Erfolg hat natürlich vielfältige Schattierungen und Wirkungen, aber dem Grunde nach hat der Datenschutz einen großen Fortschritt erzielt.

Dieser Fortschritt drückt sich zum einen materiell aus. Das konkretisierte sich in der erheblich angestiegenen Zahl von Beschwerden der Bürgerinnen und Bürger im Hinblick auf mögliche Verletzungen des Datenschutzes durch nicht-öffentliche oder öffentliche Stellen. Diese Beschwerden führten zu einem erwarteten Mehraufwand für die Datenschutzaufsichtsbehörden, der in diesem Umfang nicht vermutet worden ist. Es ist eine Vervier- bis Verfünffachung der Anzahl der Beschwerden eingetreten. Hinzu kam die Verzwölffachung der Meldungen von Datenpannen durch die Verantwortlichen. Die Verpflichtung, die Verletzungen von Datenschutzregeln unter bestimmten Voraussetzungen zu melden, wird ernstgenommen, da ein Verstoß gegen diese Verpflichtung mit Geldbuße belegt ist. Der Beratungsbedarf blieb hoch. Nach dem absoluten Höhepunkt in Sommer und Herbst des Jahres 2018 kamen nun die Folgefragen. In einer Vielzahl von Beratungen und Veranstaltungen hat der LfDI diesen Beratungsbegehren Rechnung getragen. Die Mitarbeiterinnen und Mitarbeiter haben schriftlich, telefonisch, aber auch im direkten Kontakt mit Verantwortlichen und Betroffenen spezifische und konkrete Informationen zu der Verwirklichung von Anforderungen der Datenschutz-Grundverordnung gegeben.

Die inhaltlichen Fortschritte des Datenschutzes führen zu erheblichen Folgerungen für die Behörde des LfDI. Der gewaltige Aufwand, den Beratungen, Informationen und Kontrollen verursachen, ist von der Verstärkung an Personal nicht in vollem Umfang abgefedert worden. Zwar hat

der Landtag des Landes Rheinland-Pfalz dem LfDI dankenswerter Weise weitere Stellen zur Verfügung gestellt, allerdings hat sich erwiesen, dass die gesteigerten Aufgaben doch nur mit zusätzlichen Kräften bewältigt werden konnten, die auf Zeit und vorübergehend Hilfe geleistet haben. Befristete Arbeitsverhältnisse können aber nur eine Interimslösung darstellen. Die Sicherung einer kontinuierlichen Arbeit setzt das beständige Vorhandensein entsprechender Ressourcen voraus.

Die vielfältigen Folgerungen der Datenschutz-Grundverordnung gingen einher mit vielfältigen Folgerungen aus neuen technischen Entwicklungen und gesellschaftlichen Rahmenbedingungen. Der LfDI hat im Bereich Schulen und Medienbildung, auf dem Gebiet des Gesundheitswesens oder im Zusammenhang der Kommunen umfangreiche gesetzliche und sonstige Rahmenbedingungen mitgeschärft. Die Kontakte zu den Akteuren blieben intensiv. Die auf Dauer gute Kooperation mit einer Vielzahl öffentlicher Stellen hat zu dem Erreichen der Ziele wesentlich beigetragen. Auch auf dem Gebiet der Privatwirtschaft wurden regelmäßige Veranstaltungen und Gespräche mit großen Unternehmen aus Rheinland-Pfalz durchgeführt. Die dauerhaften Kontakte haben den Bereich der privaten Unternehmen und insbesondere die betrieblichen Datenschutzbeauftragten als Ansprechpartner gestärkt. Nach wie vor ist ein wesentliches Merkmal der Tätigkeit des LfDI Rheinland-Pfalz, dass im Dialog mit den Verantwortlichen und Akteuren Verbesserungen herbeigeführt werden können, die insbesondere dann auch den Bürgerinnen und Bürgern zugutekommen. Die aufsichtsbehördlichen Maßnahmen und Kontrollen treten verstärkt hinzu. Die Datenschutz-Grundverordnung bietet dem LfDI nicht nur ein breites Instrumentarium an Maßnahmen, um Verstöße gegen den Datenschutz zu beheben und ggf. zu ahnden. Sie führt auch zu einem verstärkt behördlichen Auftreten des LfDI, da eingreifende Maßnahmen durch eine Verwaltung mit belastendem Charakter gegenüber den Bürgerinnen und Bürgern auch angegriffen werden können. Die Rechtschutzmöglichkeiten gegen Maßnahmen des LfDI wurden auch in Anspruch genommen. Dementsprechend war die Arbeit der Stelle Rechtsdurchsetzung in der Behörde des LfDI im Jahre 2019 eine der Tätigkeiten, die mit erheblich gesteigertem Aufwand und mit zunehmend erhöhter Intensität vorgenommen wurden. Eine Reihe von organisatorischen Maßnahmen hat dazu beigetragen, dass die Behörde des LfDI gut aufgestellt auf die Anforderungen reagieren konnte. Nichtsdestotrotz bleibt die Anpassung von Aufgabenverteilung und Organisation eine Daueraufgabe. Dazu konnten die Auswertungen, die

auf innerstaatlicher und europäischer Ebene vorgenommen wurden, einen Beitrag leisten.

Im Herbst des Jahres 2019 ließ sich der Schluss ziehen, dass ein erheblich verbessertes Niveau an Datenschutz in Rheinland-Pfalz und der Europäischen Union insgesamt erreicht wurde. Dies betrifft die sich auf hohem Niveau konsolidierende Anzahl der Beschwerden und Datenpannenmeldungen ebenso wie die Qualität des Datenschutzmanagements in Behörden oder Unternehmen. Dennoch bleibt noch viel zu tun. Der LfDI wird weiter seine Aufgabe wahrnehmen, das Datenschutzrecht durchzusetzen und damit die Grundrechte der Bürgerinnen und Bürger zu wahren.

Prof. Dr. Dieter Kugelmann

I.
GRUNDLINIEN DER ENTWICKLUNGEN DES DATENSCHUTZES IN DER BEHÖRDE

I. GRUNDLINIEN DER ENTWICKLUNGEN DES DATENSCHUTZES IN DER BEHÖRDE

1. ÖFFENTLICHKEITSARBEIT

Aufgrund der Notwendigkeit, nach Wirksamwerden der Datenschutz-Grundverordnung gekürte Datenschutzbeauftragte über die gesetzlichen Bestimmungen zu informieren, führt der LfDI regelmäßig in Kooperation mit den Unternehmen SCHOTT AG, Boehringer Ingelheim, Birkenstock bzw. BASF SE die Veranstaltungsreihe „X-Tage DSGVO – Beispiele aus der täglichen Praxis“ durch. Ziel der Veranstaltungsreihe ist der Austausch der Erfahrungen mit der Datenschutz-Grundverordnung zwischen Wirtschaft und Aufsichtsbehörde. Nach den Vorträgen dieser Kooperationspartner und des LfDI hat das aus Datenschutzbeauftragten bestehende Publikum Gelegenheit, datenschutzrechtliche Fragen zu stellen. So fand beispielsweise am 28. Oktober 2019 die Veranstaltung „DSGVO – neue Beispiele aus der Praxis“ in den Räumlichkeiten der BASF statt. Die Pressemitteilung finden Sie hier: **https://s.rlp.de/kooperationsveranstaltung-dsgvo**

Um das Thema „KI“ des DSK-Vorsitzjahres 2019 auch in den Veranstaltungen des LfDI hervorzuheben, führte dieser im Berichtsjahr die Kooperationsveranstaltung „Künstliche Intelligenz und die Folgen für Wirtschaft, Forschung, Arbeit und Gesellschaft“ am 17. September 2019 mit dem LfDI Baden-Württemberg durch. In das Podium waren Vertreterinnen der Enquête-Kommission „Künstliche Intelligenz - Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale“ des Deutschen Bundestages geladen, welche u.a. die Bedeutung der Ethik in der KI hervorhoben. Weitere Details zur Veranstaltung finden Sie hier: **https://s.rlp.de/veranstaltungki**

Um ein breiteres und zugleich junges Publikum für datenschutzrechtliche Aspekte zu begeistern und für einen bewussten Umgang mit Daten im Internet zu sensibilisieren, lud der LfDI 2019 ins Mainzer Kino „Ciné Mayence“ ein. Er zeigte beispielsweise am 16. September 2019 den Film „Hi, AI“, um den Zuschauerinnen und Zuschauern die Herausforderungen und Gefahren der Einführung von KI in die Gesellschaft zu vergegenwärtigen. Nach der Filmvorstellung stand der LfDI auch diesem Publikum zu Fragen hinsichtlich der rechtlichen und gesellschaftlichen Hintergründe zur Verfügung. Die Pressemitteilung, den Trailer sowie Informationen zur Vereinbarkeit von Datenschutz und KI finden Sie hier: **https://s.rlp.de/datenschutzgoeskino**

Darüber hinaus fand im Berichtsjahr die Veranstaltungsreihe „Mainzer Vorträge“ in Kooperation mit der Johannes Gutenberg-Universität Mainz statt, die regelmäßig Themen des IT-Recht und des Sicherheits- und Informationsrechts aufgreifen. In diesem Rahmen referierte beispielsweise Dr. Horst Heberlein, Referatsleiter bei der Europäischen Kommission, am 20. November 2019 zum Thema „Konkordanz der Grundrechte – multipler Grundrechtsschutz durch die Datenschutz-Grundverordnung“.

Informationen über die Veranstaltungen der Mainzer Vorträge zum Sicherheits- und Informationsrecht finden Sie unter **https://baecker.jura.uni-mainz.de/mzv-sr-infr/**. Dort besteht auch die Möglichkeit, sich für die Mailingliste der Mainzer Vorträge anzumelden.

Um die Presse- und die Öffentlichkeit über die interessantesten und skurrilsten Datenschutzfälle zu informieren, lädt der LfDI jährlich zum Pressegespräch „Best of Datenschutz“ ein. Dieses Gespräch fand am 27. August 2019 statt. Neben der Präsentation der interessantesten Datenschutzfälle, wie zum Beispiel unzulässige Kontaktierungen hübscher Damen im Rahmen eines Dienstverhältnisses, wurden ebenfalls Angaben zu Statistiken vor der Presse gemacht, z.B. über die Anzahl der eingereichten Beschwerden und Beratungsanfragen. Die Pressemitteilung sowie weitere Informationen finden Sie hier: **https://s.rlp.de/bestds2019**

Zudem werden jeden zweiten Monat im Jahr Leserinnen und Leser über die Neuigkeiten im Datenschutz und die Tätigkeiten durch den Newsletter des LfDI informiert. Der Newsletter wurde dementsprechend im Februar, April, Juni, August, Oktober und Dezember 2019 versandt. Das Archiv des Newsletter finden Sie unter **https://s.rlp.de/lfdinewsletter** und den die Anmeldung für den Newsletter des LfDI unter folgendem Link: **https://s.rlp.de/newsletteranmeldung**

2. INTERNATIONALER DATENTRANSFER

Im Bereich des internationalen Datentransfers war das Jahr 2019 geprägt von einigen bedeutenden rechtlichen und tatsächlichen Entwicklungen, die zahlreiche Nachfragen beim LfDI auslösten. Dazu gehören die lange Zeit unwägbaren Themen wie der Brexit und das Schrems II-Verfahren vor dem EuGH, welches in erster Linie die Rechtswirksamkeit der aktuellen EU-Standardvertragsklauseln in Frage stellt, also das vermutlich meist genutzte Transferinstrument des Kapitels V der DS-GVO, welches aber nebenbei auch über das Schicksal des EU-U.S. Privacy Shield entscheiden könnte. Zu den erfreulichen Nachrichten gehörten der Angemessenheitsbeschluss der EU-Kommission in Bezug auf Japan und die Veröffentlichung der Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679 vom 4.Juni 2019 des Europäischen Datenschutzausschusses, welche Rechtsklarheit in teilweise sehr kontrovers diskutierten Fragen schaffen. Die Optimierung des Genehmigungsverfahrens war Kern der Entwicklungen in Bezug auf verbindliche interne Datenschutzvorschriften, sog. Binding Corporate Rules.

Den Fragen zum Brexit ist der LfDI mit einem regelmäßig aktualisierten und umfassenden Online-Informationsangebot begegnet. Mit dem schließlich doch noch zustande gekommenen Abkommen über den Austritt des Vereinigten Königreichs, Großbritannien und Nordirland aus der Europäischen Union und der Europäischen Atomgemeinschaft vom 31. Januar 2020 (EU-Amtsblatt 2020/L 29/7) gibt es zumindest vorläufig Rechtsklarheit. Während eines Übergangszeitraums bis zum 31. Dezember 2020, der einmalig um ein oder zwei Jahre verlängert werden kann, gelten demnach die Datenschutz-Grundverordnung (mit Aus-

nahme ihres Kapitels VII), die JI-Richtlinie, die Datenschutz-Richtlinie für elektronische Kommunikation und alle sonstigen Bestimmungen des Unionsrechts über den Schutz personenbezogener Daten im Rahmen des Art. 71 des Abkommens weiter, zumindest solange und soweit die EU-Kommission keine entsprechenden Angemessenheitsbeschlüsse gemäß Art. 45 Abs. 3 DS-GVO bzw. Art. 36 Abs. 3 JI-Richtlinie erlassen hat (Art. 126, Art. 127, Art. 132 des Abkommens). Für weitere Informationen zu dem Abkommen und rund um den Brexit siehe: **https://s.rlp.de/brexit**

Seit dem 23. Januar 2019 gilt der von der EU-Kommission angenommene Angemessenheitsbeschluss in Bezug auf Japan, durch den personenbezogene Daten nun ungehindert zwischen den beiden Volkswirtschaften fließen können. Damit wurde der weltweit größte Raum für sicheren Datenverkehr geschaffen. Das im September 2018 eingeleitete Verfahren dauerte knapp eineinhalb Jahre. Weitere Informationen zu Angemessenheitsbeschlüssen der EU-Kommission: **https://s.rlp.de/angemessenheitsfeststellung**

Das EU-U.S. Privacy Shield hat auch der dritten jährlichen Überprüfung durch die EU-Kommission Stand gehalten. Wenn es auch vereinzelt Verbesserungen bei der Umsetzung gab, äußern sich die Aufsichtsbehörden weiterhin kritisch. Auf den Bestand des Privacy Shield könnte sich zudem die noch ausstehende Entscheidung des EuGH zur Rechtmäßigkeit der Standardvertragsklauseln (sog. Schrems II-Verfahren) auswirken. Der Generalanwalt des EuGH sprach sich zwar dafür aus, dies nicht in dem vorliegenden Verfahren zu entscheiden. Er nahm jedoch rechtlich Stellung und äußerte wegen der nach US-amerikanischem Recht zulässigen Aktivitäten der US-Sicherheitsbehörden fundierte Zweifel an der Wirksamkeit des Angemessenheitsbeschlusses zum Privacy Shield (Schlussantrag zu C-311/18 EuGH vom 19.12.2019, Rn. 161, Rn. 308). Es ist also möglicherweise nur eine Frage der Zeit, bis die Interessenvertreter ein entsprechendes gerichtliches Verfahren einleiten, welches ausdrücklich die Überprüfung der Rechtswirksamkeit des EU-U.S. Privacy Shield zum Gegenstand hat. Weitere Informationen zum Privacy Shield: **https://s.rlp.de/privacyshield**

In Bezug auf die EU-Standardvertragsklauseln spricht sich der Generalanwalt klar für ihre generelle Wirksamkeit aus. Sie könnten unabhängig vom Datenschutzniveau im jeweiligen Drittland für Datenübermittlungen dorthin verwendet werden. Dies hat viele Verantwortliche und Auftragsverarbeiter aufatmen lassen. Der Generalanwalt unterstreicht jedoch das Recht und die Verantwortung der Aufsichtsbehörden, im Einzelfall Maßnahmen zu ergreifen (Schlussantrag zu C-311/18 EuGH vom 19.12.2019, Rn. 158). Das heißt, die Aufsichtsbehörden sollen im Falle konkreter Datenschutzverstöße, also z.B. bei direkten Zugriffen von EU-Sicherheitsbehörden auf personenbezogene Daten beim Verantwortlichen oder Auftragsverarbeiter im Drittland, die Aussetzung von Datenübermittlungen an diesen beim Verantwortlichen oder Auftragsverarbeiter in der EU durchzusetzen. Das ist keine neue rechtliche Erkenntnis. Es setzt jedoch voraus, dass die Aufsichtsbehörden von dem konkreten Datenschutzverstoß Kenntnis erlangen. Dies dürfte nur einen geringen Anteil der tatsächlichen Fälle ausmachen. Dass ein tatsächlicher Schutz der Daten besteht, die in ein Drittland übermittelt werden, welches nationale Gesetze unterhält, die aus der Perspektive des EU-Rechts regelmäßige Datenschutzverstöße legitimieren, darf daher weiterhin in Frage gestellt werden. Das endgültige Urteil des EuGH im Schrems II-Verfahren wird mit Spannung erwartet. Der Schlussantrag des Generalanwalts und weitere Dokumente des EuGH zum Verfahren sind über einen

Link auf der folgenden Seite zu erreichen: **https://s.rlp.de/standardvertragsklauseln**

Etwas mehr Klarheit gibt es nun in Bezug auf die Anforderungen an Verhaltensregeln und Überwachungsstellen nach Art. 40, 41 DS-GVO. An der Entwicklung der Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679 vom 4. Juni 2019 des Europäischen Datenschutzausschusses wirkte der LfDI im Wege inhaltlicher Stellungnahmen mit. Eine der streitigsten Rechtsfragen sowohl auf deutscher als auch auf europäischer Ebene war, ob die Benennung einer Überwachungsstelle zwingend für die Genehmigungsfähigkeit von Verhaltensregeln ist. Dies wurde in den Leitlinien nun eindeutig bejaht (Rn. 27).

Noch keine Einigkeit herrscht über die Kriterien, die eine Überwachungsstelle erfüllen muss, damit sie von der zuständigen Aufsichtsbehörde für die Überwachungstätigkeit akkreditiert werden kann. Entsprechende Leitlinien entwickelt der Europäische Datenschutzausschuss derzeit in Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten. Die deutschen Aufsichtsbehörden brachten ihren Vorschlag für Akkreditierungskriterien ein, welchem eine monatelange Vorarbeit in einem eigens dafür gegründeten Arbeitskreis vorausging. In diesem wirkte der LfDI zu Beginn der Erarbeitung des Papiers aktiv mit, musste sich im weiteren Verlauf jedoch aus Kapazitätsknappheit weitgehend zurückziehen.

Nach wie vor attraktiv, zumindest für Konzerne und Unternehmensgruppen, ist die Schaffung geeigneter Garantien für Datenübermittlungen in Drittländer mithilfe von Binding Corporate Rules (BCR). Entsprechend ist der Beratungsbedarf bei den Verantwortlichen und Auftragsverarbeitern weiterhin hoch. Um die steigende Zahl der Anträge auf Genehmigung von BCR in einem angemessenen Zeitrahmen bewältigen zu können, gibt es in Deutschland und auch insgesamt in der EU nicht genügend Personal bei den Aufsichtsbehörden. Die Prüfung der Anträge ist sehr umfangreich und langwierig. Bei allen Genehmigungsverfahren sind grundsätzlich alle Aufsichtsbehörden zu beteiligen, mehrere Aufsichtsbehörden davon müssen sich vertieft mit den eingereichten Unterlagen auseinandersetzen. Kapazitäten für sog. Co-Prüfungen freizusetzen, war dem LfDI im Jahr 2019 nicht möglich. Die Optimierung des Genehmigungsverfahrens stand und steht regelmäßig auf der Agenda des zuständigen europäischen Arbeitskreises. Weitere Informationen zu Binding Corporate Rules: **https://s.rlp.de/bcr**

3. VORSITZ DES LFDI RHEINLAND-PFALZ IN DER DATENSCHUTZKONFERENZ

3.1 Leitthema „Künstliche Intelligenz“

Das Jahr seines Vorsitzes in der Datenschutzkonferenz (DSK) hat der LfDI unter das Leitthema „Künstliche Intelligenz“ gestellt. Daran anknüpfend hat er die Taskforce „Künstliche Intelligenz“ aus Mitarbeiterinnen und Mitarbeitern der deutschen Datenschutzbehörden geschaffen, die die „Hambacher Erklärung zur Künstlichen Intelligenz sowie die „Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen“ erarbeitet haben. Diese wurden schließlich auf der 97. DSK und 98. DSK verabschiedet. Die Papiere enthalten rechtliche Anforderungen für Systeme Künstlicher Intelligenz, die aus den Vorschriften der Datenschutz-Grundverordnung abgeleitet wurden.

Die Initiative zur „Künstlichen Intelligenz“ stieß auf ein reges Interesse in Presse- und Öffentlichkeit und wurde von der Privatwirtschaft wahrgenommen. Die Hambacher Erklärung ist abrufbar unter **https://s.rlp.de/hambacherer-klrung**

Die Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen sind abrufbar unter **https://s.rlp.de/kisysteme**

3.2 97. Konferenz in Hambach

Unter dem Vorsitz des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, Prof. Dr. Kugelmann, tagte die 97. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 3. und 4. April 2019 auf dem Hambacher Schloss. Der historische Ort des Kampfes um die Freiheit war gewählt worden, um den Willen der deutschen Datenschutzaufsichtsbehörden zu verdeutlichen, für einen effektiven Grundrechtsschutz einzutreten und ihren Beitrag zur Sicherung von Freiheit in der digitalen Welt zu leisten.

Landtagspräsident Hendrik Hering begrüßte die Teilnehmerinnen und Teilnehmer und stellte den Zusammenhang zwischen Demokratie und Datenschutz heraus. Er hob hervor:

„Die Parlamente und die Beauftragten für den Datenschutz sind Verbündete, wenn es darum geht, die Selbstbestimmung der Bürgerinnen und Bürger in einer demokratischen Gesellschaft zu schützen. Ein unabhängiger und professioneller Datenschutz ist unverzichtbar. Er ist unverzichtbar, um beides zu gewährleisten: Transparenz, wo sie möglich ist, und Privatheit und Vertraulichkeit, wo sie nötig sind.“

Einen Schwerpunkt der Konferenz bildete die Diskussion um die Künstliche Intelligenz (KI). Die deutschen Datenschutzaufsichtsbehörden haben die Hambacher Erklärung zur Künstlichen Intelligenz verabschiedet. Sie nennt beispielhaft den Einsatz von KI-Systemen in der Medizin, insbesondere in der Diagnose, in der Sprachassistenz und bei der Bewertung von Bewerbungsunterlagen in der Bewerberauswahl. Aus dem geltenden Datenschutzrecht werden sieben Anforderungen abgeleitet, die bereits heute eingehalten werden müssen. So muss der Einsatz von KI-Systemen nachvollziehbar und erklärbar sein, den Grundsatz der Datenminimierung enthalten, Diskriminierungen vermeiden und benötigt technische und organisatorische Standards. Die Datenschutzaufsichtsbehörden wollen die Entwicklung begleiten und fordern Wissenschaft, Politik und Anwender auf, die Entwicklung von KI im Sinne des Datenschutzes zu steuern. Im Kern geht es

darum, dass am Ende Menschen und nicht Maschinen über Menschen entscheiden.

Die DSK hat über die Konsequenzen eines ungeregelten Brexits beraten. Bereits am 8.3.2019 hat sie einen Beschluss gefasst, der auf die rechtlichen Pflichten der Verantwortlichen im Falle eines ungeregelten Austritts hinweist. Im Falle eines ungeregelten Austritts ist das Vereinigte Königreich als Drittland im Sinne der Datenschutz-Grundverordnung zu betrachten und dorthin führende Datentransfers sind dementsprechend gesondert abzusichern. In Ermangelung einer solchen Absicherung könnten Datenverarbeitungen ausgesetzt und Bußgelder verhängt werden.

Als Reaktion auf den Hackerangriff auf Politiker und Politikerinnen sowie Personen des öffentlichen Lebens im Januar 2019 haben die Datenschützer eine Orientierungshilfe „Anforderungen an Betreiber von Online-Diensten zur Zugangssicherung“ verabschiedet. Darin werden Online-Diensten Maßnahmen zur Zugangssicherung nach dem Stand der Technik empfohlen. Dies betreffen Vorgaben für Aufbau, Übertragung, Speicherung und Nutzung von Passwörtern sowie den Umgang mit Angriffen und fehlgeschlagenen Anmeldeversuchen.

Als Ergänzung zu der Positionsbestimmung der Datenschutzkonferenz vom 26.4.2018 bezüglich der Anwendbarkeit des Telemediengesetzes für nicht-öffentliche Stellen ab dem Wirksamwerden der Datenschutz-Grundverordnung wurde eine Orientierungshilfe beschlossen. Die Orientierungshilfe beschäftigt sich mit der Geltung des Telemediengesetztes im Rahmen der Wirksamkeit der Datenschutz-Grundverordnung und weist darauf hin, dass die Interessensabwägung im Rahmen des Art. 6 Abs. 1 lit. f der Datenschutz-Grundverordnung auf den konkreten Einzelfall bezogen werden sollte. Insbesondere konkretisiert sie anhand von Beispielen die Interessensabwägung beim Einsatz von Tracking-Tools.

Die Zahl der Analysen von Videoaufnahmen, bei der Gesichtsmerkmale erfasst und ausgewertet werden, um z.B. durch eine Analyse der Mimik Rückschlüsse auf die Gefühlslage eines Menschen (Emotional Decoding) zu erhalten oder um die Wirksamkeit von Werbung zu messen und genauer auf die gewünschten Zielgruppen zuzuschneiden, nimmt zu. Die Datenschutzkonferenz hat daher ein Positionspapier erstellt, in dem entsprechende Verfahren rechtlich bewertet und Empfehlungen zur Gestaltung abgeleitet werden.

Nach dem Urteil des EuGH zu Facebook-Fanpages hat sich die DSK in einem Beschluss zum (Weiter-)Betrieb von Facebook-Fanpages geäußert. In diesem wird verdeutlicht, dass Fanpage-Betreiber die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und in der Lage sein müssen, die Einhaltung der Grundsätze der Verarbeitung (Art. 5 Abs. 1 DSGVO) nachzuweisen. Die DSK unterstreicht die datenschutzrechtliche Verantwortlichkeit sowohl von Facebook wie der Fanpage-Betreiber und erwartet, dass sie ihrer Verantwortung entsprechend nachkommen.

Die Hambacher Erklärung finden Sie unter **https://s.rlp.de/hambachererklrung**

3.3 98. Konferenz in Trier

Auf ihrer überaus ertragreichen 98.Sitzung am 6. und 7. November 2019 in Trier hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (Datenschutzkonferenz) eine Reihe von Entschließungen und Beschlüssen gefasst.

Die Bandbreite der Themen reichte dabei von der Kritik an einer massenhaften automati-

sierten Erfassung von Kfz-Kennzeichen bis zu Empfehlungen für den datenschutzgerechten Einsatz von Künstlicher Intelligenz , für die in Konkretisierung der „Hambacher Erklärung“ vom April 2019 ein Positionspapier verabschiedet wurde.

Einen weiteren Schwerpunkt bildete der Gesundheitsbereich. Angesichts der fortschreitenden Digitalisierung des Gesundheitswesens fordert die Datenschutzkonferenz mit Blick auf die damit verbundenen Risiken sicherzustellen, dass, unabhängig von der Größe medizinischer Einrichtungen, Patientendaten nach dem Stand der Technik geschützt werden. Auch Gesundheitswebseiten und –Apps müssen die Erwartungen ihrer Nutzerinnen und Nutzer an Vertraulichkeit gewährleisten und bei der Weitergabe personenbezogener Daten bestimmte Anforderungen einhalten. Für den Einsatz von Messenger-Diensten im Krankenhausbereich wurden in einem „Whitepaper“ technische Anforderungen zusammengestellt, die als Grundlage weiterer Diskussionen dienen sollen. Veröffentlicht wurde weiterhin die Version 2.0 des Standard-Datenschutzmodells.

Hinsichtlich der mit Sprachassistenzsystemen und Panoramadiensten verbundenen Datenschutzfragen sowie den Anforderungen an die Sicherstellung einer angemessenen Digitalen Souveränität hat die Konferenz Prüfungsaufträge an die entsprechenden Arbeitskreise erteilt.

Für eine verbesserte Abstimmung und Zusammenarbeit mit den Europäischen Aufsichtsbehörden hat die Konferenz verschiedene Verfahrensregelungen beschlossen.

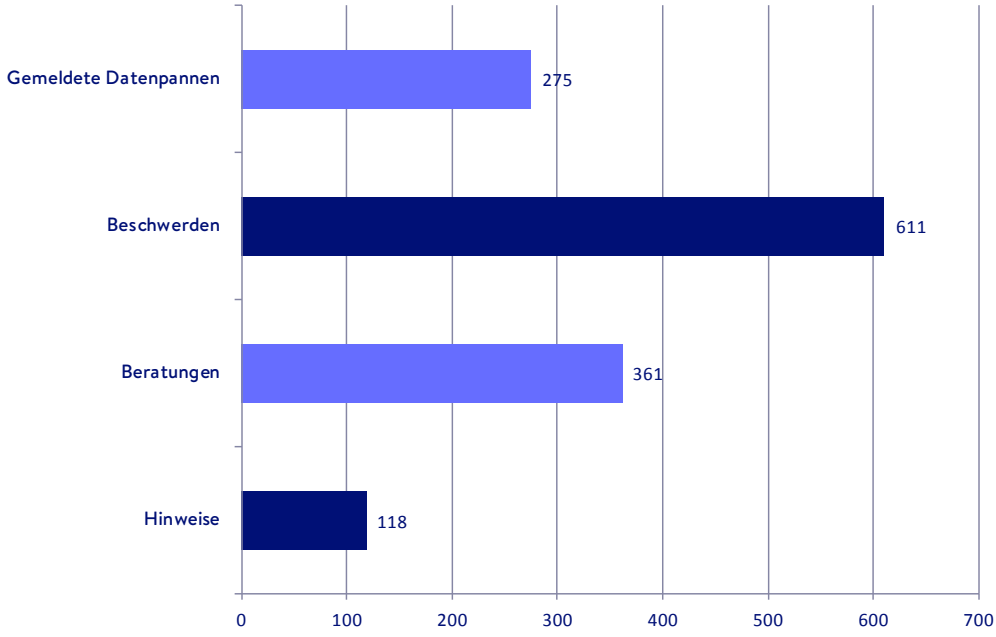
Darüber hinaus hat die Konferenz einen Erfahrungsbericht über die Anwendung der Datenschutz-Grundverordnung beschlossen, der einen Beitrag zur Erstellung eines Berichts auf europäischer Ebene leisten soll.

Im Zusammenhang mit der automatisierten Übertragung sogenannter Telemetriedaten bei Windows Betriebssystem- und Anwendungslösungen hat die Konferenz im Nachgang auf hochrangiger Ebene Gespräche mit Vertretern von Microsoft geführt. Ziel ist es dabei, den Personenbezug von Nutzungsdaten zu vermindern bzw. deren Übertragung in die Entscheidung der Nutzerinnen und Nutzer zu stellen. In diesem Zusammenhang hat die Datenschutzkonferenz ein Prüfschema für das Betriebssystem Windows 10 veröffentlicht, das Verantwortlichen die Möglichkeit gibt, die datenschutzrelevanten Fragen im Zusammenhang mit dem Einsatz der Software, der Übertragung von Telemetriedaten sowie der Update-Konfiguration zu bewerten. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Prof. Dr. Dieter Kugelmann, zog folgendes Fazit des diesjährigen rheinland-pfälzischen Vorsitzes in der Datenschutzkonferenz: „Die umfangreichen Tagesordnungen der 98. Datenschutzkonferenz sowie der vorhergehenden zeigen einmal mehr, dass die fortschreitende Digitalisierung Datenschutzfragen in nahezu allen Lebensbereichen aufwirft. Die Datenschutzbeauftragten stehen dabei vor der Herausforderung, relevante Entwicklungen frühzeitig zu erkennen und den Datenschutz so einzubringen, dass Risiken begegnet wird und Chancen nicht vergeben werden. Ich freue mich daher, dass es im Jahr des rheinland-pfälzischen Vorsitzes der Konferenz gelungen ist, für das Zukunftsthema „Künstliche Intelligenz“ entsprechende Empfehlungen zu erarbeiten.“

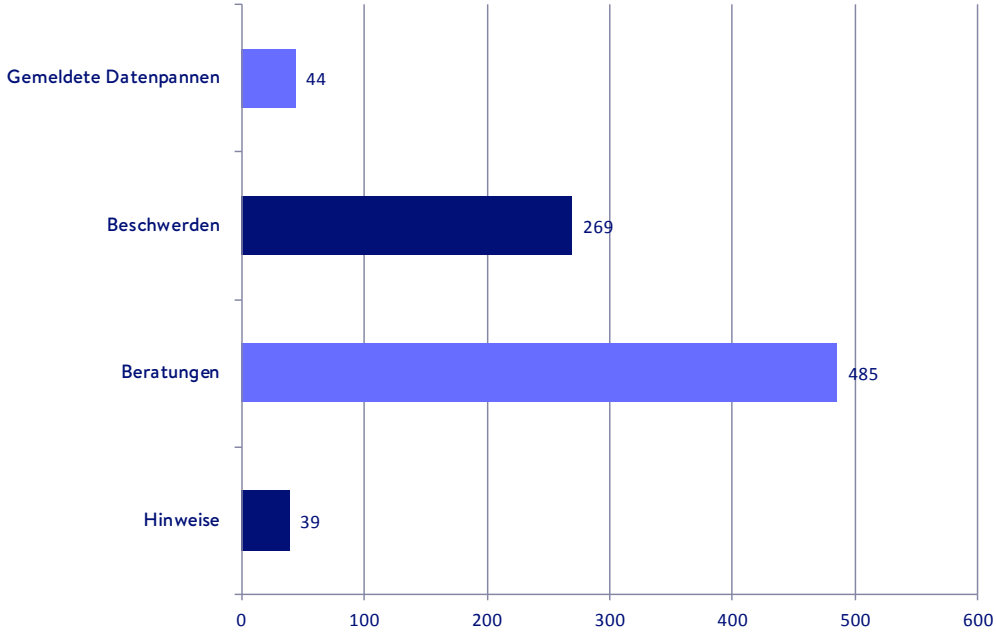
Die Entschließungen der Datenschutzkonferenz finden Sie unter **https://s.rlp.de/DSKEntschliessungen**

II.
ZAHLEN UND FAKTEN

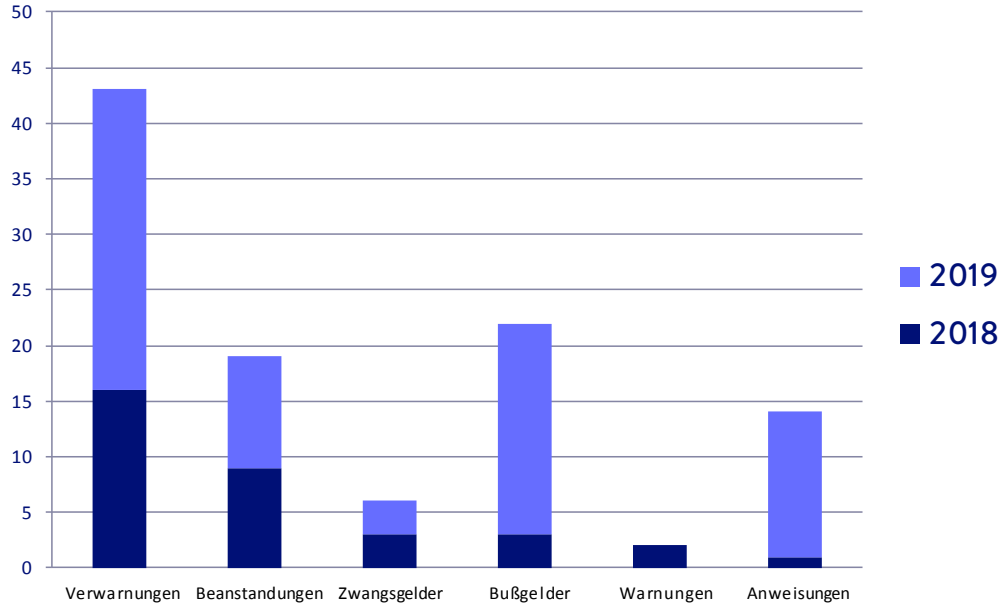
1. Geschäftsstatistik 2019: Privater Bereich



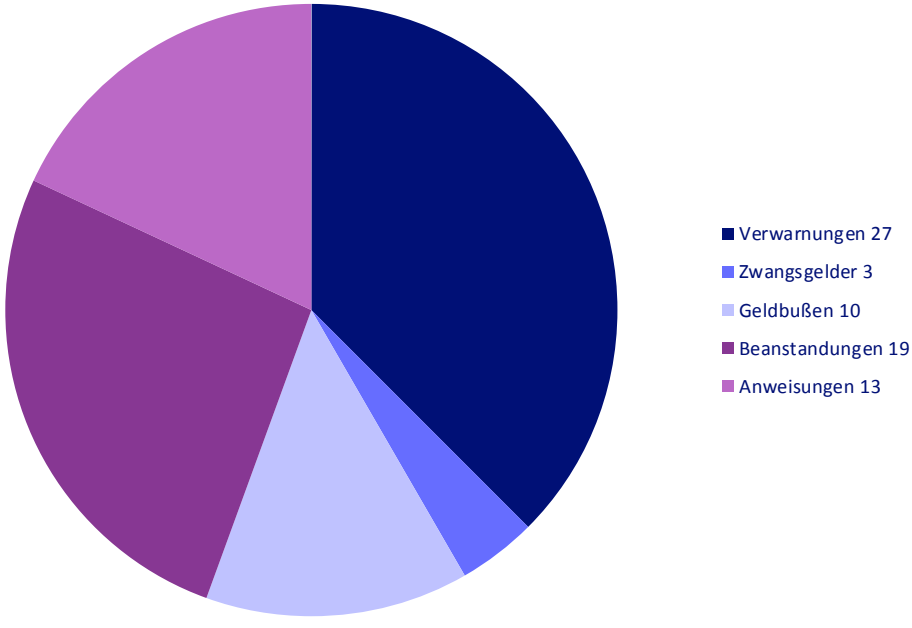
2. Geschäftsstatistik 2019: Öffentlicher Bereich



3. Ausgeübte Befugnisse 2018 und 2019



4. Ausgeübte Befugnisse 2019



III.
SACHGEBIETE

III. SACHGEBIETE

1. EUROPÄISCHE ZUSAMMENARBEIT

1.1 Zusammenarbeit mit anderen Aufsichtsbehörden auf nationaler und europäischer Ebene

Der LfDI hat im Berichtsjahr 2019 weiterhin an dem Ziel, ein möglichst weitgehend harmonisiertes Datenschutzrecht in der EU zu erhalten, mitgewirkt – insbesondere durch die Zusammenarbeit mit den anderen Datenschutzaufsichtsbehörden auf nationaler und auch auf europäischer Ebene. Beispielsweise wurden Hospitationen in den Schwesterbehörden in Irland, Österreich, Estland und Lettland durchgeführt, wo sich Mitarbeiter des LfDI Einblicke in die Organisation der Behörden verschafften und über das jeweilige nationale Datenschutzanpassungsgesetz informiert wurden. Der LfDI selbst führte eine Hospitation in der polnischen Datenschutzaufsichtsbehörde durch.

Die multilaterale – und nun auch vermehrt – die bilaterale Kommunikation mit den europäischen Datenschutzaufsichtsbehörden wurde verstärkt über die Web-Plattform „IMI“ (Internal Market Information System – zu deutsch „Binnenmarkt-Informationssystem) durchgeführt. Diese Kommunikation übernahm federführend die im Jahr 2018 geschaffene „IMI-Stelle“, die sich um die Prüfung von grenzüberschreitenden Bezügen datenschutzrechtlicher Sachverhalte und die darauffolgende Kommunikation mit den anderen Aufsichtsbehörden und den Beschwerdeführern kümmert.

Die Zusammenarbeit zwischen den Aufsichtsbehörden in der EU in grenzüberschreitenden Verfahren hat sich seit 2018 stark weiterentwickelt. Einige Rechtsfragen aus dem Bereich der Kohärenzmechanismen wurden bereits geklärt, andere werden weiter diskutiert. Innerhalb Deutschlands besteht in den wesentlichen Fragen des Kohärenzverfahrens und der Anwendung von IMI Einigkeit. Diese wird hauptsächlich über den Arbeitskreis Grundsatz sowie den Arbeitskreis Organisation und Struktur hergestellt. Auch im Verhältnis zu anderen EU-Aufsichtsbehörden wird die Zusammenarbeit als konstruktiv wahrgenommen. Allerdings bestehen auf dieser Ebene mehr Rechtsfragen, auf die noch nicht in allen Fällen eindeutige Antworten gefunden wurden. Eine große Rolle bei der Vereinheitlichung der Vorgehensweisen spielt das EDSA-Sekretariat. Während im Jahr 2018 noch die Bestimmung der federführenden Aufsichtsbehörde nach Art. 56 DS-GVO eine wesentliche Rolle spielte, traten von diesen grenzüberschreitenden Verfahren im Jahr 2019 bereits einige in die Entscheidungsphase im Rahmen des Verfahrens nach Art. 60 DS-GVO ein. Erfahrungen mit Entscheidungsvorschlägen der federführenden Aufsichtsbehörden und Einsprüchen oder Zustimmungen der weiteren betroffenen Aufsichtsbehörden konnten gesammelt werden. Insgesamt liefen diese Verfahrensschritte in den Augen des LfDI konstruktiv und effektiv.

1.2 Ländervertretung IT Users Subgroup des Europäischen Datenschutzausschusses

Die Vertretung der Länder in der Datenschutzexpertengruppe „IT Users Subgroup“ des Europäischen Datenschutzausschusses (EDSA) wurde vom LfDI fortgeführt. Dort wurden Änderungen im Kommunikationssystem IMI mit den europäischen Schwesterbehörden sowie dem EDSA-Sekretariat diskutiert und mit dem

Ziel der effizienten Zusammenarbeit umgesetzt. Beschlossen und für die europäischen Datenschutzbehörden eingeführt wurden 2019 auch ein Videokonferenztool sowie ein Wissenschaftsmanagementsystem, in dem alle Leitlinien, Tagesordnungen und Protokolle der Sitzungen der Expertengruppen sowie der Plenarsitzungen für den internen Gebrauch aufgeführt sind.Über die in der IT User Subgroup besprochenen Änderungen informierte der LfDI die anderen deutschen Datenschutzbehörden auf Arbeitskreissitzungen sowie den deutschen Ländervertreter der Plenarsitzung.

Zudem hat sich der LfDI auch in die Bearbeitung anderer interner oder öffentlicher Leitlinien des EDSA eingebracht und die Entwicklungen in den verschiedenen Expertengruppen und dem Plenum beobachtet und an regelmäßigen Umfragen zu Statistik und Arbeitserfahrungen (beispielsweise mit IMI) teilgenommen.

2. SICHERHEIT

2.1 Tag des Datenschutzes bei der Polizei Rheinland-Pfalz

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz unterstützte auch in diesem Jahr die Hochschule der Polizei am Flugplatz Hahn bei der Durchführung des „Tag des Datenschutzes“. Eingeleitet wurden die Hochschultage jeweils mit einem Einführungsvortrag durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz. Zwei Einstellungsjahrgängen mit insgesamt ca. 500 jungen Polizeibediensteten wurden im Rahmen von Workshops u. a. durch Referenten der Behörde datenschutzrechtliche Themen näher gebracht, die sowohl dienstlichen wie auch privaten Bezug hatten.

Der Landesbeauftragte sieht in der Möglichkeit der Unterstützung des Hochschultages die Chance, einen großen Kreis von Personen, die während ihrer beruflichen Tätigkeit eine Vielzahl von sensiblen personenbezogenen Daten rechtskonform verarbeiten müssen, frühzeitig für die Themen des Datenschutzes zu sensibilisieren. Beiderseits ist die Fortführung der Zusammenarbeit in dieser Form auch in den nächsten Jahren gewünscht.

2.2 Beschwerdeaufkommen bei der Zentralen Bußgeldstelle des Polizeipräsidiums Rheinpfalz

Der LfDI beschäftigte sich mit einer Vielzahl von Anfragen und Beschwerden, die im Wesentlichen die Ermittlungsarbeit der Zentralen Bußgeldstelle (ZBS) in Speyer betrafen. Die

ZBS ist dem Polizeipräsidium Rheinpfalz in Ludwigshafen angegliedert. Die Beschwerden richteten sich z. B. gegen Lichtbildabgleiche und damit verbundene Anfragen bei den Meldebehörden oder gegen Abfragen in den Informationssystemen zur Ermittlung von Mitbewohnern, die als Fahrzeugführer in Frage kommen. Mehrfach wurden auch Sachverhalte mitgeteilt, die durch eine fehlerhafte Bearbeitung bei der Identifizierung des Fahrzeugführers zur Verarbeitung von personenbezogenen Daten geführt haben, obwohl sich die Personen lediglich als Beifahrer im Fahrzeug befanden. Meine Behörde hat diese Fälle beanstandet und um Prüfung gebeten, ob diese Fehlerquelle durch technisch-organisatorische Maßnahmen eingedämmt werden kann.

Die Ermittlungsarbeit der ZBS war auch Anlass für einen informativen Meinungsaustausch in der zweiten Jahreshälfte unter Beteiligung des Polizeipräsidenten, des Leiters der ZBS, Vertretern des Innenministeriums und Vertretern meiner Behörde.

Unter Berücksichtigung der zu bearbeitenden Datenmenge im Rahmen von Verwarnungs- und Bußgeldverfahren im Straßen- und Güterverkehr ist die Anzahl der datenschutzrechtlichen Verstöße als gering zu betrachten. Trotzdem ist das Beschwerdeaufkommen für den LfDI nicht unerheblich.

2.3 Prüfung der Rechtsextremismusdatei (RED)

Der LfDI hatte bereits im Oktober 2018 eine Prüfung der RED beim LKA Rheinland-Pfalz vorgenommen (siehe TB 2018, Pkt. 2.5) und diese im Jahr 2019 bei den Polizeipräsidien fortgeführt.

Im Ergebnis werden die Zugriffe auf die Datenbank RED grundsätzlich ordnungsgemäß protokolliert. Es haben sich jedoch unterschiedliche Verfahrensweisen in der Dokumentation der Voraussetzungen zur Einstellung in die RED ergeben, die aus datenschutzrechtlicher Sicht vereinheitlicht werden sollten. Weiterhin ergaben sich Differenzen im Abgleich der vom LKA mitgeteilten Anzahl der Löschungen von Personen in der RED mit den Protokollierungsausdrucken des Bundekriminalamtes. Zur Verifizierung der Ursache befindet sich das LKA derzeit noch im Austausch mit dem BKA. Insgesamt wird der Mehrwert der RED von den Fachkommissariaten als gering bewertet, da alle Datenbestände, die in der RED abgebildet sind bundes- und landesweit zur Verfügung stehen und über diese Systeme abgerufen werden können.

2.4 Erste Evaluation der Online-Wache – Speicherung von IP-Adressen

Seit 06.12.2018 befindet sich die Online-Wache der Polizei Rheinland-Pfalz in Betrieb (siehe TB 2018, Pkt. 2.6). Der LfDI hatte mit Blick auf die vom Landesbetrieb Daten und Information(LDI) als Dienstleister dargestellte veränderte Lage bei gegen IT-Strukturen gerichteten Angriffen keine Bedenken gegen die vollständige Speicherung der Zugriffe einschließlich der IP-Adresse für die Zwecke der IT-Sicherheit. Problematisch erschien diese Speicherungsfrist hingegen für die Nutzung zu anderen Zwecken, insbesondere in Verbindung mit einer allgemeinen Zugriffsmöglichkeit über den Button „IP-Adresse offenlegen“, da die IP-Adresse aufgrund der Manipulations- und Verschleierungsmöglichkeiten kein verlässliches Instrument zur Identifizierung der Nutzer darstellt. Dies gilt nicht zuletzt mit Blick auf etwaige nachfolgende eingriffsintensive polizeiliche Maßnahmen.

Insoweit wurde der Vorschlag, die direkte Offenlegung der IP-Adresse im Rahmen der Ge-

staltung der Zugriffsrechte nur im sogenannten „Back-Office"-Bereich (z.B. Lagedauerdienst) zur Verfügung zu stellen und nicht bei der jeweiligen polizeilichen Sachbearbeitung, begrüßt.

Im Evaluationsergebnis zeigte sich, dass die Möglichkeit der Ermittlung der IP-Adresse im Backoffice im Auswertzeitraum 06.12.2018 – 31.05.2019 zur Ermittlung von insgesamt 22 IP-Adressen geführt hat. Setzt man die erforderlichen IP-Adressen-Ermittlungen ins Verhältnis zur Gesamtzahl der Vorgänge, so ergibt sich ein Anteil von 0,30%. Beispielhaft wurden die IP-Adressen im Rahmen anonymer / pseudonymer Anzeigen, des Verdachts einer falschen Personalienangabe oder des Verdachts des Vortäuschens einer Straftat ermittelt.

2.5 Änderung des Polizei- und Ordnungsbehördengesetzes Rheinland-Pfalz

Im Jahr 2019 hat der LfDI zum Entwurf eines Landesgesetzes zur Änderung des Polizei- und Ordnungsbehördengesetzes (POG-E) sowie beamtenrechtlicher Vorschriften im Rahmen der im Rahmen des Beteiligungs- und Anhörungsverfahrens gem. §§ 27, 28 der Gemeinsamen Geschäftsordnung (GGO) Stellung genommen.

Diese betrafen insbesondere die Verarbeitung besonderer Kategorien personenbezogener Daten, die Gewährleistung von Betroffenenrechten und die Ausgestaltungen der Verarbeitungsgrundlagen, insbesondere der Speicherungs- und Übermittlungsgrundlagen sowie die Anforderungen an die Protokollierungen von Verarbeitungen und Kennzeichnung von Daten.

Der Gesetzentwurf zur Änderung des Polizei- und Ordnungsbehördengesetzes sowie beamten-rechtlicher Vorschriften setzt die Vorgaben der Richtlinie (EU) 2016/680 auf fachspezifischer Ebene um und dient – wie bereits das Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes vom 30. Juni 2017 (GVBl. S. 123) – der Umsetzung der Vorgaben des Urteils des Bundesverfassungsgerichts (BVerfG) zum Bundeskriminalamtgesetz (BKAG) vom 20. April 2016 (BVerfGE 141, 220).

Das Gesetzgebungsverfahren wurde überwiegend dazu genutzt, das neue europäische Rechtsregime systematisch und normenklar auch im Sicherheitsrecht umzusetzen. Auch die Umsetzung der Vorgaben des Urteils des Bundesverfassungsgerichts (BVerfG) zum Bundeskriminalamtgesetz (BKAG) vom 20. April 2016 (BVerfGE 141, 220) ist grundsätzlich gelungen. Es werden damit Mechanismen eingeführt und ausgebaut, die das Datenschutzniveau der polizeilichen Datenverarbeitung in Rheinland-Pfalz stärken werden. Insbesondere die Betroffenenrechte wurden – auch aufgrund der Anforderungen der Richtlinie (EU) 2016/680 – gestärkt.

Trotzdem bestand Verbesserungsbedarf dahingehend, die Transparenz und Legitimität der polizeilichen Datenverarbeitung unter Wahrung der europarechtlichen und verfassungsrechtlichen Vorgaben zu steigern. Dies betraf insbesondere die neu geschaffenen Rechtsgrundlagen zur Zuverlässigkeitsüberprüfung. Auch hinsichtlich der umfassenden Protokollierung, technisch-organisatorischen Maßnahmen, Kennzeichnung und der Ermöglichung eines ausreichenden individuellen und aufsichtlichen Rechtsschutzes bestand weiterer Überarbeitungsbedarf des Gesetzentwurfes, um die Position der betroffenen Personen und der Datenschutzaufsicht angemessen und in Einklang mit den rechtlichen Vorgaben zu stärken. Dazu leistete der LfDI mit zahlreichen Verbesserungsanregungen und Regelungsvorschlägen

im Rahmen seiner Stellungnahme konstruktive Unterstützung. Das Gesetzgebungsverfahren 2020 wird zeigen, inwiefern diese Vorschläge auf fruchtbaren Boden stießen.

3. JUSTIZ

3.1 Auskunftsanspruch nach Art. 15 DS-GVO

Mehrfach beschäftigte sich der LfDI im Rahmen von Beschwerden auch wieder mit dem Auskunftsanspruch nach Art. 15 DS-GVO gegenüber Rechtsanwälten. Diese berufen sich zumeist auf ihr Berufsgeheimnis, was bei Auskunftsersuchen Dritter interessengerecht sein mag. Gegenüber den eigenen Mandanten erscheint die Auskunftsverweigerung mit Berufung auf das Berufsgeheimnis indes befremdlich, weshalb der LfDI hier stets im Einzelfall prüft.

3.2 Unabhängigkeit der Justiz

Eine wegen nicht erteilter Auskunft erhobene Beschwerde gegen ein rheinland-pfälzisches Gericht veranlasste den LfDI zur erneuten Befassung mit der Reichweite seiner Aufsichtsbefugnis gegenüber der Justiz. Der vollen Kontrolle durch die Datenschutzaufsicht unterliegen die Gerichte im Rahmen ihrer Verwaltungstätigkeit. Dazu gehören Abrechnungsvorgänge und Personalverwaltung oder die Gewährung von Akteneinsicht nach Abschluss eines Verfahrens. Indes kann der LfDI keine Datenverarbeitungsvorgänge der Gerichte im Rahmen ihrer justiziellen Tätigkeit kontrollieren, Art. 55 Abs. 3 DS-GVO und § 41 Abs. 2 LDSG. Denn eine unparteiliche und sachliche Rechtsprechung muss frei von behördlicher Kontrolle sein.

Die eindeutige Zuordnung einer Datenverarbeitung zur justiziellen Tätigkeit ist aber häufig schwierig und einzelfallabhängig. Ent-

sprechende Prüfungen sind deshalb regelmäßiger Bestandteil der Arbeit des LfDI. Justizielle Tätigkeit meint alle Datenverarbeitungsvorgänge die unmittelbar mit der Rechtsfindung und Rechtsprechung zusammenhängen, wie das Verlesen von Gutachten oder die Befragung von Personen über ihre Vermögensverhältnisse während einer Verhandlung. Die Freistellung von der Datenschutzaufsicht erstreckt sich somit auf sämtliche Tätigkeiten, die mit der gerichtlichen Entscheidungsfindung in Zusammenhang stehen.

Im o.g. Fall verweigerte das Gericht zunächst die Auskunft mit der Begründung, dass dem Beschwerdeführer ein prozessuales Akteneinsichtsrecht zustehe, welches den datenschutzrechtlichen Anspruch verdränge. Der Anspruch auf Auskunft gemäß Art. 15 DS-GVO hat aber eine grundsätzlich andere Zielrichtung als das Recht auf Akteneinsicht in einem laufenden Verfahren, welches dem Ersuchenden in der Regel wesentlich mehr Informationen zuteil werden lässt. Gerade wenn es um personenbezogene Daten von Kläger oder Beklagten außerhalb eines konkreten Verfahrens geht, muss der Auskunftsanspruch umfassend erfüllt werden. Im vorliegenden Fall hatte der Beschwerdeführer allgemein Auskunft über seine beim Sozialgericht Mainz gespeicherten personenbezogenen Daten verlangt und nicht etwa über Inhalte aus einem laufenden Verfahren. Es ging also nicht um Daten, die im Rahmen justizieller Tätigkeit gemäß Art. 55 Abs. 3 DS-GVO, sondern im Rahmen der allgemeinen Verwaltungstätigkeit der Gerichte verarbeitet wurden. Nach eingehender Prüfung und Befassung verschiedener Stellen bat der LfDI, erneut die Auskunft zu erteilen, dem das Gericht schließlich nachkam.

3.3 Vollstreckung

Auch die Datenverarbeitung im Rahmen der Vollstreckung ist immer wieder Gegenstand von Beschwerden beim LfDI.

Ein Amtsgericht übersandte den in einem Zwangsvollstreckungsverfahren erlassenen Zuschlagsbeschluss. In diesem Fall hielt der LfDI eine Verwarnung für erforderlich.

Anders als die Richterschaft unterstehen Gerichtsvollzieherinnen der vollen datenschutzrechtlichen Kontrolle durch den LfDI. Bei seinem Arbeitstreffen mit dem Justizministerium tauschte sich daher der LfDI auch mit dem Referat für Gerichtsvollzieherrecht aus und beschloss hier noch enger zusammen zu arbeiten. Konkreter Anlass war eine längst überfällige Löschung von Schuldnerdaten auf dem Laptop eines Gerichtsvollziehers. Der Gerichtsvollzieher verweigerte zunächst die Löschung mit Verweis darauf, dass es zu umständlich sei, für jeden Schuldner einzeln zu prüfen, wann dessen Daten zu löschen seien. Nachdem der LfDI bei verschiedenen Stellen Informationen über die verwendete Software eingeholt und gemeinsam mit dem Justizministerium erneut zur Löschung aufgefordert hatte, beendete der Gerichtsvollzieher schließlich die rechtswidrige Speicherung.

3.4 Überwachung der Kommunikation von Gefangenen

Die Überwachung des Schriftverkehrs und der Telekommunikation Gefangener ist regelmäßig Beschwerdegegenstand beim LfDI. Thema war unter anderem ein Einwilligungsformular, welches eine JVA unter den Gefangenen zirkuliert hatte. Mit der Unterschrift erklärte der Gefangene, freiwillig darin einzuwilligen, dass nicht nur seine eigenen personenbezogenen Daten,

sondern auch Namen und Beziehung zu seinen Gesprächspartnern an den Betreiber der Telefon- und Fernsehanlage übermittelt würden. Im Falle eines Widerrufs würden die Daten des Kontos beim Betreiber gelöscht.

Jedoch war gar keine Einwilligung seitens der Gefangenen erforderlich. Das Formular war somit missverständlich. Denn die Erfassung der Daten Dritter im Rahmen der Telefonüberwachung ist gemäß § 8 Landesjustizvollzugsdatenschutzgesetz rechtmäßig. Danach können Daten über Personen, die nicht Gefangene sind, ohne deren Kenntnis bei Gefangenen oder sonstigen Dritten erhoben werden, soweit dies für die Erfüllung der Aufgaben des Vollzugs unerlässlich ist und schutzwürdige Interessen der Betroffenen hierdurch nicht beeinträchtigt werden. Die JVA erklärte nachvollziehbar, dass es für die Erreichung der Vollzugsziele, die Strafgefangenen zu befähigen, künftig ein Leben ohne Straftaten zu führen und die Allgemeinheit vor weiteren Straftaten zu schützen, unerlässlich sei, auch die sozialen Beziehungen der Gefangenen zu Dritten zu kennen. So könne man den „sozialen Empfangsraum der Gefangenen“ erfassen und diese gezielter für die Zeit nach der Haft vorzubereiten. Das Interesse der Betroffenen, also der Personen, die mit Ihnen in Kontakt stehen, musste hier hinter diesen Vollzugszielen zurücktreten. Dies erklärte der LfDI auch gegenüber den Beschwerdeführern.

Die JVA hat angekündigt, das insoweit missverständliche Formular für die Benutzung der Anlage entsprechend zu ändern, um weiteren Beschwerden vorzubeugen.

3.5 Entwurf für ein neues Landesjustizvollzugsdatenschutzgesetz

Rheinland-Pfalz hat bereits seit geraumer Zeit ein Landesjustizvollzugsdatenschutzgesetz. Dieses Landesjustizvollzugsdatenschutzgesetz bedurfte allerdings im Zuge der Umsetzung der Richtlinie für Polizei und Justiz der Änderung.

Angelehnt an einen Musterentwurf der Justizvollzugsdatenschutzreferenten der Länder aus dem Jahr 2018 hat das Ministerium für Justiz im August 2018 einen Referentenentwurf vorgelegt, der die Richtlinie für Polizei und Justiz im Justizvollzugsbereich umsetzen soll.

Zu diesem Entwurf hat der LfDI bereits eine Stellungnahme abgegeben.

3.6 Pressearbeit der Justiz

Der LfDI erhielt einen Hinweis, wonach auf der Webseite einer Staatsanwaltschaft sich Pressemitteilungen zu Verfahren veröffentlicht waren, die bis ins Jahr 2007 zurück reichten und teilweise recht genaue Rückschlüsse auf die betroffenen Personen zuließen. So enthielt eine Meldung den Name und Sitz des Unternehmens zweier Angeklagter sowie die Angabe gegen einen „früheren leitenden Mitarbeiter einer Firma der xx-Unternehmensgruppe in yy (Ort)“.

Als Teil der öffentlichen Gewalt ist die Staatsanwaltschaft verpflichtet, Presse und Öffentlichkeit über die Erfüllung ihrer Aufgaben zu informieren und darf in diesem Zusammenhang auch personenbezogene Daten verarbeiten. Nach den Vorgaben der Pressegesetze der Länder und der Richtlinien für Straf- und Bußgeldverfahren (RiStBV) ist dabei im Einzelfall prüfen, ob das Interesse der Öffentlichkeit an einer vollständigen Berichterstattung gegenüber den Persönlichkeitsrechten des Beschuldigten oder anderer Beteiligter, insbesondere auch des Verletzten, überwiegt.

Nach Auffassung des LfDI erfordert das Informationsinteresse der Öffentlichkeit jedoch nicht, die im Ermittlungsverfahren betroffenen Personen so genau zu beschreiben. Auch sollte bei einem Verfahren, das nahezu 12 Jahre zurückliegt, das Recht auf Löschung nach Art. 17 DS-GVO geprüft werden. Nachdem der LfDI der Staatsanwaltschaft diese Rechtsauffassung mitgeteilt hatte, überarbeitete diese ihre Webseite. Nunmehr werden nur noch Mitteilungen zu Verfahren veröffentlicht, die weniger als 5 Jahre zurückliegen.

Die justizielle Medienarbeit im Strafverfahren war auch Thema einer Veranstaltung des Arbeitskreises Strafprozessrecht und Polizeirecht (ASP) am 6. Mai in der Akademie der Wissenschaften, Mainz. Der ASP, an dem auch der LfDI beteiligt ist, stellte einen Gesetzentwurf vor, der verbindliche Regelungen zu der bislang lediglich in den RiStBV erwähnten Materie treffen soll. Im Anschluss nahm der LfDI an der Podiumsdiskussion „Erteilung von Auskünften durch Justizbehörden an Medien – Ein Minenfeld zwischen Pressefreiheit, Persönlichkeitsrecht und Unschuldsvermutung“ teil. Die Diskussion zeigte die Schwierigkeit, zwischen den sich gegenüberstehenden, gewichtigen Grundrechtspositionen einen schonenden Ausgleich zu finden.

3.7 Sonstiges

Unter dem Motto „Datenschutz im Schiedsamt“ fand am im März 2019 in Grünstadt erstmals eine Fortbildung des LfDI für Schiedspersonen in Rheinland-Pfalz statt. Diese Schnittstelle zwischen Ehrenamt und Justiz ist in der Diskussion zu den datenschutzrechtlichen Neuerungen bislang kaum beleuchtet worden. Deshalb hatte die Bezirksvereinigung Mainz / Bad Kreuznach / Frankenthal des Bunds Deutscher Schiedsmänner und Schiedsfrauen e. V. eine Referentin des LfDI zu ihrer Mitgliederversammlung eingeladen, um sich weiterzubilden. In einem Vortrag bekamen die Schiedsfrauen und -männer einen Überblick über die wichtigsten datenschutzrechtlichen Anforderungen und Neuerungen seit Wirksamwerden der DS-GVO. Anschließend gab es Gelegenheit zu Fragen. Thema war unter anderem die Vereinbarkeit der Vorgaben aus der Schiedsamtsordnung zur Protokollierung und die gleichzeitige Beachtung von Löschfristen. Wegen der verantwortungsvollen Aufgabe, die die ehrenamtlich tätigen Schiedspersonen mit außergerichtlichen Schlichtungsversuchen erfüllen, begrüßt der LfDI die Bereitschaft zur Weiterbildung und freut sich auf ähnliche Kooperationen in der Zukunft.

3.8 Datenpannen

Die häufigste Meldung von Verletzungen nach Art. 33 DS-GVO bzw. § 54 LDSG im Justizbereich betraf den Versand von Dokumenten durch Rechtsanwälte und Notare an unberechtigte Empfänger, etwa durch falsche Eingabe einer E-Mail-Adresse. Die E-Mails wurden in der Regel unverschlüsselt versandt, so dass teilweise sensible Informationen an die falsche Adresse gerieten. Verantwortliche sind nach Art. 24 Abs. 1 und Art. 32 DS-GVO verpflichtet, geeignete technische und organisatorische Maßnahmen für eine verordnungskonforme Verarbeitung zu treffen. Die Verschlüsselung ist in Art. 32 Abs. 1 lit a DS-GVO auch exemplarisch genannt und nach Auffassung des LfDI für vertrauliche E-Mail-Kommunikation geeignet und effektiv. Betrifft die Kommunikation besondere Kategorien personenbezogener Daten nach Art. 9 DS-GVO (wie etwa die ethnische Herkunft, politische Überzeugungen oder Gesundheit) ist die unverschlüsselte Kommunikation besonders kritisch. Sie ist dann allenfalls nach ausdrücklicher vorheriger Einwilligung

und Information der betroffenen Personen über die damit verbundenen Risiken möglich. Aber auch bei anderen vertraulichen Daten, wie etwa Finanzdaten oder Eigentumsverhältnisse, sollte die Verschlüsselung der Regelfall sein. Deshalb mahnte der LfDI auch gegenüber Rechtsanwälten und Notaren immer wieder die Verschlüsselung an.

4. VIDEOÜBERWACHUNG

Hinsichtlich der gesellschaftlichen Relevanz des Themas Videoüberwachung unterscheidet sich das Jahr 2019 nur geringfügig vom Vorjahr. Opto-elektronische Geräte sind weit verbreitet und leistungsfähige Aufnahmegeräte sind bereits zu niedrigen Preisen verfügbar. Das Bewusstsein über die mit dem Einsatz verbundenen rechtlichen Probleme ist oftmals sehr gering ausgeprägt. Dies gilt nicht selten auch für Gewerbebetriebe, die betriebliche Datenschutzbeauftragte bestellt haben.

In der Aufsichtspraxis spiegelt sich die gesellschaftliche Debatte zur Videoüberwachung wieder. Die Eingriffstiefe einer Videoüberwachung wird hier ebenfalls sehr unterschiedlich beurteilt. Videoüberwachung wird von manchen Menschen als schwerwiegende Beeinträchtigung empfunden – andere erachten sie als unerheblich. Die Rechtsprechung ist hier jedoch eindeutig und fordert ein hohes Schutzniveau für die betroffenen Personen. Selbst Kameraattrappen können durch die bloße Möglichkeit einer Videoüberwachung zu einer Verhaltensänderung der betroffenen Personen führen und damit ihre Rechte beeinträchtigen.

In diesem spannungsgeladenen gesellschaftlichen Konfliktfeld kommt den Transparenz- und Informationspflichten der Verantwortlichen eine besonders große Bedeutung zu. Die Pflichtinformationen über eine Videoüberwachung sind mehr als eine bürokratische Pflichtübung. Sie sind eine proaktive Kommunikation gegenüber den betroffenen Personen. Diese kann zahlreiche Konflikte beheben, bevor eine Beschwerde bei der Aufsichtsbehörde eingereicht wird. Eine ordnungsgemäße Hinweisbeschilderung kann Bedenken bezüglich der Rechtmäßigkeit der Videoüberwachung aus-

räumen und Verständnis für die Gründe der Überwachung wecken.

Bezüglich der betroffenen Personen wird nicht selten zu früh der Kontakt mit der Aufsichtsbehörde gesucht. Dies bindet erhebliche Ressourcen. Nicht bei jeder als problematisch empfundenen Videoüberwachungskamera ist die Einleitung eines Verwaltungsverfahrens zweckmäßig. Die Datenschutz-Grundverordnung stattet betroffene Personen mit einem umfangreichen Katalog an Rechten aus (vgl. https://s.rlp.de/IhreRechte /). In vielen Fällen ist es zumutbar und sachgerecht, sich zuerst an den Verantwortlichen zur Klärung der Angelegenheit zu wenden. Das Recht betroffener Personen, sich vertraulich und gegebenenfalls auch anonym an die Aufsichtsbehörde zu wenden, wird davon selbstverständlich nicht eingeschränkt. Es sind jedoch zahlreiche Fälle zu verzeichnen, in denen eine vorherige Kontaktaufnahme mit dem Verantwortlichen zumutbar und zweckmäßig gewesen wäre. Die dadurch gebundenen Ressourcen fehlen für die Bearbeitung gravierenderer Fälle.

Der LfDI ist vor diesem Hintergrund dazu übergegangen, bei Bagatellfällen, zu denen zahlreiche Nachbarschaftsstreitigkeiten gezählt werden können, eine stärkere Mitwirkung der Beschwerdeführer im Verwaltungsverfahren einzufordern. Auf Grundlage von § 26 Abs. 2 VwVfG wird nun, unter Berücksichtigung der Umstände des jeweiligen Einzelfalls, die Substantiierung des Sachvortrages durch Beibringen geeigneter Bildaufnahmen und die Geltendmachung geeigneter Betroffenenrechte verlangt. Dies erlaubt eine bessere Konzentration auf schwerwiegendere Fälle, in denen den Parteien nicht, wie in Nachbarschaftsstreitigkeiten, zivilgerichtlicher Rechtsschutz möglich und zumutbar ist.

Es verbleiben indes zahlreiche Fälle, in denen der Sachverhalt allein durch die Mitwirkung der Parteien nicht hinreichend aufgeklärt werden kann. In diesen Fällen wurde 2019 erstmals systematisch auf Amtshilfe (gem. § 16 Abs. 4 LDSG) durch kommunale Ordnungsämter zurückgegriffen. Ohne die präzise und bereitwillige Mithilfe der kommunalen Ordnungsämter und der kommunalen Vollzugsdienste hätten viele Verfahren deutlich mehr Zeit beansprucht.

Die auf diesem Wege freigesetzten Ressourcen konnten verwendet werden, um die Präsenz des Landesdatenschutzbeauftragten vor Ort zu erhöhen. Bei zahlreichen Verantwortlichen wurden anlasslose Ortsbegehungen durchgeführt, um die aufsichtsbehördliche Kontrolldichte auch außerhalb konkreter anlassbezogener Beschwerden und Eingaben zu erhöhen.

Ein weiterer Schwerpunkt lag in der Einleitung und Durchsetzung von Bußgeldverfahren. Hier standen Fälle mit betroffenen Personen im Straßenverkehr, namentlich Dashcams, und Fälle in Gaststätten- und Industriebetrieben im Mittelpunkt. Die gegen Privatpersonen, etwa wegen Dashcams, verhängten Geldbußen lagen überwiegend im dreistelligen Euro-Bereich. Die gegen Gewerbebetriebe verhängten Bußgelder lagen im fünfstelligen Bereich.

Im öffentlichen Bereich ist das Beratungsaufkommen nach wie vor hoch. Nicht selten wurde verkannt, dass eine Videoüberwachung kein vernachlässigbarer, sondern ein erheblicher Eingriff in die Grundrechte der Bürgerinnen und Bürger ist. Auch wird die Einrichtung einer Videoüberwachung häufig vorschnell als einzige Lösung bestehender Probleme angesehen. Alternative mildere Mittel werden zu selten geprüft. Vor diesem Hintergrund ist es besonders erfreulich, dass im öffentlichen Bereich wegen Videoüberwachung lediglich eine Warnung als Maßnahme gem. Art. 58 Abs. 2 DS-GVO ausgesprochen werden musste. Vielmehr konnten möglicherweise rechtswidrige Maßnahmen ganz überwiegend im Vorfeld verhindert werden.

5. WIRTSCHAFT

5.1 Informationspflichten durch Inkassounternehmen

Im Jahr 2019 hat sich aufgrund zahlreicher Eingaben im Inkassobereich gezeigt, dass einige dieser Unternehmen ihren Informationspflichten nur unzureichend nachkommen.

Wenn Inkassounternehmen beim Forderungseinzug eingeschaltet werden, werden hierbei auch personenbezogene Daten übermittelt, die für den Forderungseinzug benötigt werden. Dies ist grundsätzlich datenschutzrechtlich zulässig (vgl. 27. Tätigkeitsbericht., Ziffer 5.3) Allerdings müssen dann aber die Inkassounternehmen die betroffenen Personen im oben dargestellten Sinne zu dem Zeitpunkt informieren, zu dem sie das erste Mal den (vermeintlichen) Schuldner in der Regel mit einer Zahlungsaufforderung anschreiben. Denn die Informationspflichten bestehen gem. Art. 14 DS-GVO auch dann, wenn die Daten nicht bei der betroffenen Person selbst, sondern bei Dritten erhoben werden.

Dabei ist über ihre Identität, die Art der der verarbeiteten Daten, Zweck und Rechtsgrundlage, Speicherdauer, Betroffenenrechte und insbesondere über die Quelle der Daten zu informieren.

Der Verantwortliche muss in einer angemessenen Frist informieren. Die Datenschutz-Grundverordnung hält einen Monat für angemessen. Sollten die Daten bereits früher verwendet werden, ist schon zu diesem Zeitpunkt zu informieren

Nur unter bestimmten Voraussetzungen darf diese Information unterbleiben, z.B. wenn die betroffene Person bereits darüber verfügt oder die personenbezogenen Daten vertraulich zu behandeln sind.

5.2 Kreditinstitute und Kundeneinwilligungen

Kreditinstitute verarbeiten in der Regel umfangreich Daten ihrer Kundeninnen und Kunden. Grundlage hierfür ist ein Vertrag, der z.B. die Abwicklung des Giroverkehrs, die Unterhaltung eines Wertpapierdepots oder die Verwaltung sonstiger Spareinlagen zum Inhalt haben kann. Für Datenverarbeitungen, die zur Erfüllung des entsprechenden Vertrages erforderlich sind, bedarf es dann keiner gesonderten Einwilligung der Bankkunden.

Sollen darüber hinaus weitere Daten zu anderen Zwecken verarbeitet werden, ist hierfür eine Einwilligung einzuholen. Typische Fälle sind die Weitergabe von Daten an sog. Verbundpartner der Kreditinstitute wie z.B. Versicherungen. Darüber hinaus sind Kreditinstitute sehr daran interessiert, die Daten aus dem Giroverkehr ihrer Kunden auszuwerten, um diese Analyseergebnisse für zielgerichtete Werbung zu nutzen. Hierzu bedarf es immer einer separaten Einwilligung. Denn Die Auswertung von Kontodaten dient nicht mehr der Abwicklung des Giroverkehrs und damit nicht mehr dem Vertragszweck und kann damit nicht auf Art. 6 Abs. 1 lit. b DS-GVO gestützt werden. Die Auswertung der Girokontodaten kann zwar als erforderlich zur Wahrung berechtigter Interessen des Kreditinstituts angesehen werden. Jedoch überwiegt das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung (Art. 6 Abs. 1 lit. f DS-GVO). Es werden bei der Abwicklung des Giroverkehrs sehr sensitive Daten verarbeitet. Damit liegen den Kreditinstituten nicht nur eine Menge Daten vor, sondern auch sehr aussagekräftige Informationen, da Vorgänge des täg-

lichen Lebens über das Girokonto abgewickelt werden. Aus der Gesamtheit der Daten kann sehr schnell ein Persönlichkeitsprofil des Kunden erstellt werden. Da die Teilnahme am Wirtschaftsleben heute fast vollständig über Girokonten läuft, erlangt das Kreditinstitut Kenntnis von Daten mit hoher Persönlichkeitsrelevanz. Gerade in der Zusammenführung auf dem Girokonto und der möglichen Auswertung lassen sich umfangreiche Schlüsse auf das Privatleben der Bankkunden ziehen.

Diese Rechtslage galt bereits vor Wirksamwerden der Datenschutz-Grundverordnung und gilt auch nun. Leider sind dem LfDI einige Fälle bekannt geworden, in denen bei Bankkunden in Rheinland-Pfalz offensichtlich der Eindruck entsteht, dass sie wegen der Datenschutz-Grundverordnung in die Analyse ihrer Girokontendaten einwilligen müssten, da ansonsten auch die Girogeschäfte nicht mehr abgewickelt werden könnten. Der LfDI weist ausdrücklich darauf hin, dass das Girogeschäft unabhängig vom Erteilen weiterer Einwilligungen allein auf Grundlage des mit der Bank abgeschlossenen Vertrages abgewickelt wird. Eine Kopplung an weitere Einwilligungen ist nicht zulässig.

5.3 Auskunftsrecht nach Art. 15 DS-GVO

Auch im Jahr 2019 erreichten den LfDI wieder zahlreiche Beschwerden wegen nicht oder nicht vollständig gemäß Art. 15 DS-GVO erteilter Auskünfte. Grund dafür waren häufig unterschiedliche Auffassungen zum Umfang des Auskunftsrechts und Unsicherheiten darüber, welche Daten als personenbezogen anzusehen sind. Zum Teil fehlte das Bewusstsein, dass Art. 15 DS-GVO auch zu einer sog. Negativ-Auskunft verpflichtet, wonach der Verantwortliche der anfragenden Person auch dann innerhalb der Monatsfrist des Art. 12 Abs. 3 DS-GVO antworten muss, wenn er keine Daten über diese gespeichert hat oder sonst verarbeitet. In diesem Fall ist genau dies mitzuteilen.

Zu Datenschutzverstößen im Rahmen des Auskunftsrechts kam es teilweise auch dann, wenn der Verantwortliche zwar grundsätzlich gewillt war, die gewünschte Auskunft zu erteilen, aber bei der Identifikation der anfragenden Person über das Ziel hinausschoss. Um nicht der falschen Person die Auskunft über die verarbeiteten personenbezogenen Daten zu erteilen, ist es richtig und wichtig, dass sich der Verantwortliche hinsichtlich der Identität der anfragenden Person sicher ist. Dazu ist es legitim, zum Abgleich Daten bei der anfragenden Person zu erfragen. Diese Datenerhebung muss sich jedoch im Rahmen der Erforderlichkeit bewegen, sich also gemäß Art. 5 Abs. 1 lit. c DS-GVO „auf das für die Zwecke der Verarbeitung notwendige Maß beschränken“. Das Anfordern von Ausweiskopien überschreitet diesen Grundsatz bei Weitem und stellt darüber hinaus ein hohes Risiko für die betroffene Person dar (z.B. Identitätsdiebstahl), wenn die Kopie missbräuchlich verwendet wird oder Dritten bei der Übermittlung oder aufgrund einer Datenpanne zugänglich wird. Zulässig ist z.B. neben dem Namen oder einer E-Mail-Adresse der Person noch ein weiteres Datum abzufragen. Bei einer besonders großen Kundenkartei oder in dem Fall, dass die anfragende Person viele Namensvettern hat, ist ggf. die Erhebung weiterer Daten erforderlich und deshalb datenschutzrechtlich zulässig.

Mit der Geltendmachung des Auskunftsrechts verbinden die Anfragenden häufig ein Löschbegehren. Es ist selbstredend, dass das Löschbegehren erst dann umgesetzt werden darf, wenn die Auskunft vollständig erteilt wurde. Hierbei empfiehlt sich eine Wartefrist. D.h. der Verantwortliche sollte den Anfragenden mit der Erteilung der Auskunft nach Art. 15 DS-GVO darüber informieren,

dass seine löschfähigen Daten nach einer vom Verantwortlichen bestimmten angemessenen Wartefrist gelöscht werden, sofern sich der Anfragende innerhalb dieser Frist nicht bei ihm meldet. Nach Ablauf der Frist ist dem Anfragenden die Löschung der Daten zu bestätigen und anschließend die Löschung vorzunehmen.

Weiterführende Informationen zum Recht auf Auskunft und zu weiteren Informationspflichten sind unter dem folgenden Link abrufbar: https://s.rlp.de/auskunftsrecht

6. LEBEN DIGITAL

6.1 Selbstauskünfte von Mietinteressenten – Was der neue Vermieter fragen darf

Der LfDI wird immer häufiger mit Fragen und Beschwerden von Wohnungssuchenden konfrontiert, die sich durch zukünftige Vermieter in ihrem Recht auf Schutz personenbezogenen Daten verletzt sehen. Da die Suche nach einer neuen Wohnung vielerorts schwierig ist, sind Suchende oft bereit, für eine neue Wohnung viel von sich preiszugeben. Dies nutzen Vermieter, Makler und Hausverwalter in manchen Fällen aus und fragen weit über das zulässige und für den Abschluss eines Mietvertrages erforderliche Maß.

Die DSK hat dieses in ganz Deutschland bestehende Problem zum Anlass genommen, eine Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressen“ zu veröffentlichen. In dieser wird nicht nur dargelegt, welche personenbezogenen Daten nach der DS-GVO erhoben werden dürfen, sondern auch, auf welcher Rechtsgrundlage dies geschehen darf, um den Vermietern eine Hilfestellung beim Erfüllen ihrer Informationspflichten nach Art. 13 DS-GVO zu geben.

In der Praxis zeigt sich jedoch, dass den Informationspflichten oft nur teilweise nachgekommen wird, die Informationen fehlerhaft, unvollständig oder schlichtweg für den Interessenten nicht verfügbar sind.

Häufig werden allein für den Besichtigungstermin vom Interessenten schon weitreichende Informationen abgefragt. Zulässig ist in diesem Stadium nach Art. 6 Abs. 1 lit. f) DS-GVO jedoch lediglich die Frage nach den Kontakt-

daten. Erklärt der Mietinteressent, eine konkrete Wohnung anmieten zu wollen, entsteht ein vorvertragliches Schuldverhältnis zu dem künftigen Vermieter, so dass dann Art. 6 Abs. 1 lit. b) DSGVO maßgebend ist. Stehen Vermietern für die Datenerhebung eine gesetzliche Grundlage nach Art. 6 Abs. 1 lit. b) oder lit. f) DSGVO zur Verfügung, so ist ein Rückgriff auf das Konstrukt der Einwilligung unzulässig, denn für die Mietinteressen würde der Eindruck entstehen, dass die Offenbarung und weitere Verarbeitung der Informationen ihrem Wahlrecht unterläge. Erst wenn sich auch der Vermieter für den Mietinteressenten als Mieter entschieden hat, dürfen Fragen zum vorhergehenden Mietverhältnis, zu den Einkommensverhältnis oder die Vorlage von Bonitätsauskünften verlangt werden.

Mietinteressenten sind zwar gut beraten, unzulässige Fragen nicht zu beantworten, jedoch verlieren sie so in vielen Fällen die Chance, als Mieter ausgewählt zu werden. Ihnen bleibt in solchen Fällen nur, die Fragen zu beantworten und nach Abschluss eines Mietvertrages die Löschung der zu Unrecht erhobenen Daten zu verlangen. Für die Beurteilung, welche Fragen der Vermieter stellen darf, ist bei Fragen, die nicht zwingend für die Vertragsabwicklung erforderlich sind, nach Art. 6 Abs. 1 lit. f) DS-GVO entscheidend, inwieweit die begehrten Angaben mit dem Mietverhältnis in einem objektiven Zusammenhang stehen und ob schutzwürdige Interessen der Mietinteressen am Ausschluss der Datenerhebung bestehen. Der LfDI unterstützt die betroffenen Personen nicht nur bei der Durchsetzung ihres Löschungsbegehrens gegenüber dem Vermieter, sondern kann auch die unzulässige Datenerhebung durch Vermieter mit Verwarnungen und Bußgeldern ahnden.

6.2 Unerwünschte Werbezusendungen

Die Zahl der Beschwerden über unerwünschte Werbezusendungen per Post oder E-Mail nimmt auch weiterhin zu. Dies liegt zum einen an der hohen Zahl an täglich versandter Werbung aber auch an der mittlerweile eingetretenen Sensibilisierung der Empfänger von unerlaubterer Werbung, die die Verarbeitung ihrer Daten nachvollziehen und unterbinden wollen.

Viele Beschwerdeführer wenden sich daher richtigerweise im ersten Schritt an den Verantwortlichen, der ihnen die Werbung zugesendet hat und verlangen Auskunft über die zu ihrer Person gespeicherten Daten sowie deren Herkunft. In manchen Fällen gestaltet sich bereits die Ermittlung des Verantwortlichen schwierig, weil für die betroffenen Personen nur schwer zu ermitteln ist, wer genau die Werbung versandt hat. Dies liegt daran, dass in diesen Fällen die Verantwortlichen ihren Informationspflichten nach Art. 13 DS-GVO zum Teil gar nicht oder nur unzureichend nachkommen.

Viele Verantwortliche reagieren auf das Auskunftsverlangen nicht oder erst verspätet, sodass sich die betroffenen Personen beim LfDI beschweren. Zumeist erteilen die Verantwortlichen den betroffenen Personen nach einem ersten Informationsersuchen die verlangte Auskunft. In einigen Fällen ist die Auskunft dann jedoch fehlerhaft oder die Daten wurden gelöscht, bevor dem Auskunftsverlangen nachgekommen wurde.

Verantwortliche mit Sitz in Rheinland-Pfalz, die sich aber zur Versendung der Werbung eines Adresshändlers mit Sitz im Ausland - zum Teil im außereuropäischen Raum - bedienen, werden vom LfDI als gemeinsame Verantwortliche für die Datenverarbeitung zu Werbezwecken betrachtet. Die betroffenen Personen haben somit grundsätzlich gegenüber den Verant-

wortlichen in Rheinland-Pfalz einen Anspruch auf Auskunft.

Ein weiterer Beschwerdekomplex betrifft die fehlende Bestätigung der Löschung durch den Verantwortlichen. Die betroffene Person verlangt die Löschung, jedoch antwortet der Verantwortliche darauf nicht. Nach Art. 12 Abs. 3 DS-GVO muss der Verantwortliche der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 DS-GVO ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung stellen. Das bedeutet, dass der Verantwortliche auch über die Löschung innerhalb eines Monats nach Eingang des Antrags auf Löschung die betroffene Person unterrichten muss. Löscht der Verantwortliche die Daten nicht, muss er dies der betroffenen Person innerhalb eines Monats mitteilen sowie begründen und sie über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen, informieren (Art. 12 Abs. 4 DS-GVO). Jedoch hat sich in manchen Fällen gezeigt, dass trotz bestätigter Löschung die Daten zum Teil noch vorhanden sind und die betroffenen Personen dennoch weitere Werbezusendungen erhalten.

Der LfDI hat im Jahr 2019 nicht nur in vielen Fällen Verwarnungen gegenüber Verantwortlichen aufgrund fehlerhafter Auskunft und Löschung ausgesprochen, sondern musste auch in einigen Fällen die Erteilung von Auskünften und Löschungen von Daten anordnen.

7. BESCHÄFTIGTENDATEN-SCHUTZ

7.1 Die Amtsträgertheorie und ihre Grenzen

Häufig wird im Rahmen von Beschwerden vorgetragen, dass Arbeitgeber oder Dienstherren Kontaktdaten der Beschäftigten auf der unternehmens- oder behördeneigenen Website veröffentlichen.

Zunächst ist festzuhalten, dass auch nach Inkrafttreten der DS-GVO die sog. Amtsträgertheorie anwendbar bleibt, wonach es einem Arbeitgeber oder Dienstherrn gestattet ist, im Rahmen seines Organisationsermessen darüber zu entscheiden, wie er sein Unternehmen oder seine Behörde nach außen darstellen möchte. In diesem Zusammenhang steht es ihm grundsätzlich auch frei, die Namen und die dienstlichen Erreichbarkeiten seiner Beschäftigten zu veröffentlichen.

Die Veröffentlichung ist aber auf die dienstlichen Erreichbarkeiten, also die dienstlichen Telefonnummern und E-Mail-Adressen zu beschränken. Weitergehende Daten, wie beispielsweise Fotografien der Beschäftigten, dürfen nur auf Grundlage einer Einwilligung der Beschäftigten veröffentlicht werden. Außerdem ist es ausreichend, lediglich die Daten derjenigen Beschäftigten zu veröffentlichen, deren Tätigkeit typischerweise einen Kunden- oder Bürgerkontakt mit sich bringt. Nicht darunter fallen beispielsweise Personen, die im Archiv, der Registratur, dem Botendienst oder in der internen Buchhaltung beschäftigt sind. Im Übrigen entbindet die Anwendung der Amtsträgertheorie den Arbeitgeber oder Dienstherren nicht von seiner Fürsorgepflicht. So kann es in besonderen Fällen angezeigt sein, auf

die Veröffentlichung von Beschäftigtendaten gänzlich zu verzichten (z.B. bei Stalkingopfern).

In diesem Zusammenhang hat der LfDI eine Beanstandung gegenüber einer Ortsgemeinde ausgesprochen, welche die private Mobilnummer eines Gemeindemitarbeiters auf ihrer Internetseite veröffentlicht und auch nach mehrmaliger Aufforderung des Beschäftigten nicht entfernt hatte. Dabei konnte die Ortgemeinde nicht nachweisen, dass die von ihr behauptete mündliche Einwilligung des Gemeindemitarbeiters tatsächlich vorlag.

7.2 Kennzeichnung von Justizvollzugsbeamten

Im Bereich des Justizvollzugs im Land Rheinland-Pfalz besteht eine Vorgabe des Justizministeriums dahingehend, dass die Strafvollzugsbediensteten an ihrer Dienstkleidung ein Namensschild anzubringen haben, auf welchem auch ein Bild der oder des jeweiligen Bediensteten zu sehen ist.

Gegen diesen Umstand hatte sich ein Justizvollzugsbeamter gewandt. So komme es häufiger vor, dass Bedienstete und deren Familien von Gefangenen bedroht würden. Anhand der Namen der Bediensteten sei es über Profilsuchen im Internet schnell möglich, beispielsweise über Social-Media-Plattformen oder Anfragen bei Meldebehörden Erkenntnisse über die Bediensteten selbst oder auch deren Familien zu erlangen.

Im vorliegenden Fall ließ sich das Erfordernis eines Namensschildes auf § 2 S. 2, 3 Abs. 1 Landesjustizvollzugsgesetz bzw. § 2 Landessicherungsverwahrungsvollzugsgesetz stützen, wonach die Sicherstellung des Verbleibs der Gefangenen in den Einrichtungen gesetzliche Aufgabe des Justizvollzugsbeamten ist. Das Tragen von Namensschildern mit Fotografien durch Justizvollzugsbedienstete innerhalb der Einrichtung ist zur Erfüllung dieser Aufgabe erforderlich. So ist beispielsweise denkbar, dass sich Gefangene Zugang zu Dienstkleidung verschaffen und versuchen können, als Justizvollzugsbedienstete gekleidet die Anstalt zu verlassen. Durch einen Abgleich des Namens und der Fotografie auf dem Namensschild mit der tatsächlichen Trägerin oder dem Träger können diese versuchten Täuschungen aufgedeckt und ein Entweichen von Gefangenen aus dem Justizvollzug verhindert werden.

Die Verwendung einer Dienstnummer oder einer pseudonymen Kennzeichnung ist für diese Zwecke nicht geeignet, da der Dienstherr der Erfüllung seiner gesetzlich zugewiesenen Aufgabe, nämlich die Gewährleistung der öffentlichen Sicherheit und Ordnung, nur noch mit einem unverhältnismäßigen Aufwand Rechnung tragen könnte. Die Identifizierung eines als Justizvollzugsbediensteter getarnten Gefangenen würde erheblich erschwert. Insbesondere in größeren Einrichtungen kann nicht sichergestellt werden, dass sich die Bediensteten untereinander persönlich kennen und so einen Täuschungsversuch unmittelbar aufdecken könnten. Die Vorgabe des Justizministeriums war somit nicht zu beanstanden. Um den Persönlichkeitsrechten der Beschäftigten Rechnung zu tragen, wurde vom Justizministerium die Eintragung von melderechtlichen Auskunftssperren unterstützt.

7.3 Übermittlung von Gehaltsabrechnungen im Rahmen von Förderprojekten

In der Vergangenheit wurde vermehrt die Frage an den LfDI herangetragen, ob im Rahmen der Bereitstellung von Fördermitteln durch Ministerien die die Bewilligung vornehmende nachgeordnete Behörde die Vorlage von Ge-

haltsnachweisen des aus den Fördermitteln finanzierten Personals verlangen darf.

Gemäß § 23 der Landeshaushaltsordnung (LHO) dürfen Ausgaben und Verpflichtungsermächtigungen für Leistungen an Stellen außerhalb der Landesverwaltung zur Erfüllung bestimmter Zwecke (Zuwendungen) veranschlagt werden, wenn das Land an der Erfüllung durch solche Stellen ein erhebliches Interesse hat, das ohne die Zuwendungen nicht im notwendigen Umfang befriedigt werden kann. In diesem Zusammenhang normiert § 44 Abs. 1 LHO, dass zu bestimmen ist, wie die zweckentsprechende Verwendung der Zuwendungen nachzuweisen ist.

Hierzu wurden Regelungen in der Anlage der Verwaltungsvorschrift zum Vollzug der Landeshaushaltsordnung (VV-LHO) getroffen. Gemäß Ziffer 1.3 der allgemeinen Nebenbestimmungen für Zuwendungen zur Projektförderung (ANBest-P), die zum Bestandteil der Bewilligungsbescheide zumachen sind, ist anlässlich der Prüfung des Antrags auf Förderung unter anderem zu prüfen, ob der Zuwendungsempfänger seine Beschäftigten finanziell nicht besser stellt als vergleichbare Landesbedienstete. Höhere Vergütungen als nach dem TV-L bzw. dem TVöD sowie sonstige über- und außertarifliche Leistungen dürfen nicht gewährt werden.

Um die Einhaltung dieser Nebenbestimmungen prüfen zu können, ist regelmäßig die Vorlage eines Gehaltsnachweises erforderlich, aus dem neben der Entgeltgruppe und der Entgeltstufe alle weiteren Bestandteile der Vergütung (wie z.B. Jahressonderzahlungen, Leistungsprämien, Bonuszahlungen, vermögenswirksame Leistungen etc.) hervorgehen, um diese für die Vergleichsberechnung zur Prüfung des Besserstellungsverbotes aus Ziffer 1.3 ANBest-P heranzuziehen.

Um eine Vergleichsberechnung zur Prüfung des Besserstellungsverbotes aus Ziffer 1.3 AN-Best-P durchführen zu können, sind in Zusammenhang mit Personalkosten u. a. die Eingruppierung (Entgeltgruppe und Entgeltstufe) der eingesetzten Personen sowie der entsprechende Arbeitsanteil, zu dem diese im Projekt tätig sind, anzugeben. Die Personalkosten selbst umfassen den Bruttoarbeitslohn zuzüglich der Arbeitgeberanteile zur Sozialversicherung. Darüber hinausgehende Angaben in den Gehaltsnachweisen (z. B. Familienstand und Konfession) können hingegen unkenntlich gemacht werden.

Die Vorlage einer anonymisierten Gehaltsabrechnung ist allerdings nicht ausreichend, da ansonsten nicht sichergestellt werden kann, dass nur diejenigen Mitarbeiterinnen und Mitarbeiter aus den Zuwendungen bezahlt werden, welche in dem mit den Zuwendungen finanzierten Projekt tätig sind.

7.4 Verarbeitung biometrischer Daten im Beschäftigtenverhältnis

Im Zusammenhang mit der Verarbeitung von Beschäftigtendaten am Arbeitsplatz wurde die Frage an den LfDI herangetragen, ob Beschäftigte es dulden müssen, dass der Arbeitgeber den Zugang zum dienstlichen Rechner durch biometrische Daten, in diesem Fall einen Fingerabdruck der oder des jeweiligen Beschäftigten, absichert.

Bei biometrischen Daten handelt es sich um besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DS-GVO. Die Verarbeitung solcher Daten in einem Beschäftigungsverhältnis ist gemäß § 26 Abs. 3 BDSG nur zulässig, wenn dies zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Si-

cherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Bei dieser Norm handelt es sich um eine abschließende Regelung, sodass für darüber hinausgehende Verarbeitungsszenarien in einem Beschäftigungsverhältnis nur Raum bleibt, wenn diese explizit gestattet werden. Dies ist beispielsweise mit der Regelung von § 22 Abs. 1 Nr. 1 lit. b BDSG der Fall, welcher die Verarbeitung besonderer Kategorien personenbezogener Daten zur Beurteilung der Arbeitsfähigkeit von Beschäftigten erlaubt.

Die in den entsprechenden spezialgesetzlichen Erlaubnistatbeständen in den Blick genommenen Kategorien besonderer personenbezogener Daten dürften derweil in erster Linie Gesundheitsdaten sein. Die Verarbeitung biometrischer Daten im Beschäftigungsverhältnis dürfte nur in den allerwenigsten Fällen angezeigt sein. Denkbar wäre dies beispielsweise bei Personen, die in sicherheitssensiblen Bereichen, wie z. B. klassifizierten Forschungsprojekten oder militärischen Einrichtungen, beschäftigt sind. Hier könnte ein Interesse daran bestehen, den Zugang zu Bereichen oder Informationen durch einen zusätzlichen Faktor, wie eben ein biometrisches Merkmal, abzusichern. Bei einer gewöhnlichen Tätigkeit besteht dieses Bedürfnis hingegen nicht, weshalb die Zulässigkeit einer derartigen Verarbeitung biometrischer Daten nicht gegeben ist.

Auch Arbeitsgerichte haben sich in jüngster Zeit zu diesem Thema geäußert und dabei die Position des LfDI bestätigt. So hat das Arbeitsgericht Berlin in seinem Urteil vom 16.10.2019 (Az. 29 Ca 5451/19) entschieden, dass eine Zeiterfassung per Fingerabdruck nicht ohne Einwilligung der Beschäftigten erfolgen darf.

7.5 Zulässigkeit anlassloser Mitarbeiterscreenings

Aufgrund der EU-Antiterror-Verordnungen und den darin enthaltenen Bereitstellungsverboten sehen sich viele Unternehmen dazu gezwungen, anlasslose Anti-Terror-Mitarbeiterscreenings durchzuführen und ihre Beschäftigten turnusmäßig mit den Namenslisten der entsprechenden Verordnungen abzugleichen. Einerseits geschieht dies aus Angst vor Sanktionen nach dem Außenwirtschaftsgesetz (AWG), andererseits um den Status eines „zugelassenen Wirtschaftsbeteiligten“ zu erhalten bzw. aufrecht zu erhalten.

Mit der Zulässigkeit dieser Vorgehensweise hat sich der LfDI anlässlich einer Anfrage der Industrie- und Handelskammer auseinandergesetzt.

Zunächst ist anzumerken, dass die Anti-Terror-Verordnungen selbst keine Regelungen bezüglich der Verarbeitung von personenbezogenen Daten im Rahmen von Mitarbeiterscreenings enthalten. Sie ordnen lediglich an, dass den in einschlägigen Listen genannten natürlichen und juristischen Personen sowie Organisationen keine wirtschaftlichen Ressourcen bereitgestellt und ihnen gegenüber keine Leistungen erbracht werden dürfen. Dies schließt auch die Auszahlung von Lohn, Gehalt oder anderen vermögenswirksamen Leistungen ein (Bereitstellungsverbot).

Die einschlägige Rechtsgrundlage für anlasslose Anti-Terror-Mitarbeiterscreenings ist § 26 Abs. 1 S. 1 Bundesdatenschutzgesetz (BDSG). Dieser normiert, dass personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses unter anderem dann verarbeitet werden dürfen, wenn dies für die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung erforder-

lich ist. Zu diesen Zwecken gehören auch regelmäßige Entgeltzahlungen an Beschäftigte.

Anlasslose Listenabgleiche aufgrund dieser Rechtsgrundlage sind jedoch nur dann zulässig, wenn sie auch im Rahmen dieses Zweckes erforderlich sind. Eine Erforderlichkeit ist immer dann gegeben, wenn die personenbezogenen Daten für die Aufgabenerfüllung des Verantwortlichen unabdingbar sind. Dies ist wiederum der Fall, wenn die Aufgabe ohne die Kenntnis der Information nicht, nicht rechtzeitig, nur mit unverhältnismäßigem Aufwand oder nur mit sonstigen unverhältnismäßigen Nachteilen erfüllt werden kann.

Einen solchen unverhältnismäßigen Nachteil für den Fall, dass ein Listenabgleich nicht erfolgt, stellen die in den Straf- und Bußgeldvorschriften des AWG in Aussicht gestellten Sanktionen bei Zuwiderhandlung dar. Die Höhe dieser Sanktionen hängt davon ab, ob von einer vorsätzlichen oder fahrlässigen Verwirklichung eines entsprechenden Bußgeldtatbestandes ausgegangen wird.

Vorsatz setzt voraus, dass der Arbeitgeber Kenntnis davon hat, dass einer seiner Mitarbeiter auf einschlägigen Listen geführt wird. Für die Beurteilung des Merkmals der Fahrlässigkeit ist auf die Kenntnis des Arbeitgebers bezüglich der Möglichkeit des Eintritts der Tatbestandsverwirklichung abzustellen. Es ist zu fragen, in welchem Maße der Arbeitgeber auf die anlasslosen Anti-Terror-Mitarbeiterscreenings angewiesen ist, um die Möglichkeit der Tatbestandsverwirklichung überhaupt zu erkennen. Dieses dürfte in kleinen und mittelgroßen Betrieben, in welchem der Geschäftsführer oder sonstige vertretungsberechtigte Organe dazu in der Lage sind, das Verhalten ihrer Mitarbeiter zu beobachten und daraus Schlüsse auf eine mögliche Zugehörigkeit zu terroristischen Netzwerken zu schließen, eher gering sein.

In Großkonzernen hingegen, die von einer diffizilen und schwer überblickbaren Unternehmensstruktur geprägt sind, dürften regelmäßige Screenings die einzige Möglichkeit für die im Sinne des AWG Verantwortlichen sein, den Vorwurf der fahrlässigen Begehungsweise entfallen zu lassen, da ihnen aufgrund der Tatsache, dass sie unmöglich jeden einzelnen Mitarbeiter persönlich kennen können, keine anderen Anhaltspunkte zur Verfügung stehen, um die möglicherweise bestehende Zugehörigkeit zu terroristischen Netzwerken beurteilen zu können.

Die Erforderlichkeit der Verarbeitung von Beschäftigtendaten in Form eines Listenabgleichs kann also nicht für alle Unternehmen einheitlich beantwortet werden, sondern hängt maßgeblich von der Unternehmensstruktur ab.

Ähnlich verhält es sich auch mit dem Abgleich der Anti-Terror-Listen zur Erlangung oder Aufrechterhaltung des Status eines „zugelassenen Wirtschaftsbeteiligten“ (Authorised Economic Operator – AEO) im Sinne des Unionszollkodex (UZK) und der Erteilung eines AEO-Zertifikates.

Wie die Nachweisführung zu erfolgen hat, ist in den verschiedenen europäischen Rechtsakten nicht geregelt. Jedoch verlangt die Bundeszollverwaltung zwingend einen regelmäßigen Abgleich des in sicherheitsrelevanten Bereichen eingesetzten Personals gegen die Anti-Terror-Listen. Auch hier geschieht der Listenabgleich zu Zwecken des Beschäftigungsverhältnisses, da es sich um Unternehmen handelt, die für den Bereich des grenzüberschreitenden Warenverkehrs bestimmte Erleichterungen bei der Abwicklung ihrer Tätigkeit, wie sie mit den AEO-Zertifikaten verbunden sind, in Anspruch nehmen wollen und die Erteilung dieser Zertifikate von Sicherheitsvorkehrungen in Form einer Überprüfung das Personals abhängig gemacht wird.

Die Erforderlichkeit des Listenabgleichs kann bejaht werden, weil bei stark vom internationalen Handel abhängigen Verantwortlichen der Verzicht auf eine AEO-Zertifizierung zu erheblichen Nachteilen im Wettbewerb führen kann, die im Einzelfall existenzgefährdende Ausmaße annehmen können. Ohne Zertifizierung ist die Zollabwicklung mit einem deutlich höheren Aufwand verbunden, sodass Unternehmen mit hohem Zollumschlag ohne Zertifizierung kaum am Markt bestehen können.

Unter Zurückstellung von Bedenken ob des rasterfahndungsartigen Charakters der Anti-Terror-Mitarbeiterscreenings kann dieses auch im zweiten Fall auf § 26 Abs. 1 S. 1 BDSG gestützt werden, obgleich es wünschenswert wäre, dass der Gesetzgeber eine diesbezügliche explizite Regelung schafft.

Da es sich bei den in Rede stehenden Listenabgleichen um Eingriffe hoher Intensität handelt, ist der Grundsatz der Verhältnismäßigkeit dadurch erhöht Rechnung zu tragen, dass Screening-Maßnahmen auf das absolut erforderliche Minimum beschränkt werden. Dies kann durch die Wahl eines angemessenen großen Intervalls bewerkstelligt werden. Auch hier sind wieder die unternehmensspezifischen Besonderheiten zu beachten. Sofern im Einzelfall kein konkreter Anlass besteht, ist ein jährlicher anlassloser Abgleich nicht zu beanstanden. In sicherheitsrelevanten Bereichen, beispielsweise der Rüstungs- oder Atomindustrie, sowie bei erhöhter Risikolage kann allerdings eine engmaschigere Prüffrequenz angezeigt sein.

Ein Abgleich aller der in der Terrorliste enthaltenen Daten mit den im Unternehmen vorliegenden Beschäftigtendaten ist aber nicht angezeigt. Abgeglichen werden sollten ausschließlich diejenigen Daten, die zur eindeutigen Identifizierung eines Beschäftigten unbedingt notwendig sind. Dies sind in aller Regel der Vor- und der Nachname. Lediglich im Falle eines konkreten Verdachts oder bei Zweifeln an der Identität einer Person, beispielsweise bei übersetzungsbedingten abweichenden Namensschreibweisen, kann ein Abgleich weiterer Identifikationsmerkmale angezeigt sein.

Aufgrund der erhöhten Eingriffsintensität und um dem Grundsatz der Datenminimierung Rechnung zu tragen, ist es sinnvoll, die Listenabgleiche unternehmensintern vorzunehmen, damit ein weiterer Übermittlungsvorgang an einen das Screening durchführenden Dienstleister vermieden wird. Wird ein solcher eingeschaltet, handelt es sich um eine Auftragsverarbeitung, welche sich an den in der DS-GVO niedergelegten Anforderungen messen lassen muss.

7.6 Zustellung von Entgeltabrechnungen

Im Rahmen einer Beschwerde musste der LfDI sich mit den datenschutzrechtlichen Anforderungen an die Zustellung von Entgeltabrechnungen auseinandersetzen.

Der Beschwerdeführer war bei einer Ortsgemeinde beschäftigt und hatte seine Dienstherrin aufgrund einer längeren Erkrankung darum gebeten, seine Entgeltabrechnungen bis auf Weiteres übersandt zu bekommen. Statt dem Beschwerdeführer die Entgeltabrechnung auf postalischem Wege zur Verfügung zu stellen, bediente sich die Dienstherrin des Kindergartenrucksacks des Sohnes des Beschwerdeführers, welcher die Kindertagestätte der Ortsgemeinde besuchte, als Übermittlungsmedium. Dort fand die Lebensgefährtin des Beschwerdeführers die Entgeltabrechnung abends vor.

Diese Art der Übermittlung entsprach nicht den technisch-organisatorischen Anforderungen nach Art. 32 DS-GVO. Der Arbeitgeber bzw. Dienstherr ist nach § 108 Abs. 1 Gewer-

beordnung und der Entgeltbescheinigungsverordnung verpflichtet, dem Arbeitnehmer eine Entgeltbescheinigung in Textform zur Verfügung zu stellen. Diese muss dergestalt auf den Weg zu dem oder der Beschäftigten gebracht werden, dass sie in dessen oder deren Machtbereich gelangt und der oder die Beschäftigte sodann unter gewöhnlichen Umständen von der Abrechnung Kenntnis nehmen kann.

Die Art und Weise, wie dieser Verpflichtung entsprochen wird, ist ein zum Rechtskreis des Arbeitgebers/Dienstherrn zugehöriges Geschäft. Dementsprechend muss der Arbeitgeber/Dienstherr bei der Wahl des Übertragungsweges auch die erforderlichen technisch-organisatorischen Datenschutzmaßnahmen treffen, um die Gefahr einer Fehlleitung, eines Verlustes oder einer Kenntnisnahme durch Unbefugte weitestgehend auszuschließen. Dem wurde mit der durch die Ortsgemeinde gewählten Form der Übergabe nicht entsprochen.

7.7 Das Recht auf Erhalt einer Kopie im Arbeitsverhältnis

Seit Wirksamwerden der DS-GVO mehren sich Beschwerden zu Auskunftsansprüchen gegenüber dem ehemaligen Arbeitgeber. Hinsichtlich des letzten Punktes ist auffällig, dass die gefassten Auskunftsansprüche der DS-GVO, insb. das „Recht auf Erhalt einer Kopie“ nach Art. 15 Abs. 3 DS-GVO nicht selten instrumentalisiert werden, um einem ehemaligen Arbeitgeber möglichst viele Unannehmlichkeiten zu bereiten. Die Annahme, es bei einem Datenschutzverstoß des Arbeitgebers selbst in der Hand zu haben, ob ein Bußgeldverfahren eingeleitet wird, nutzen einige Beschwerdeführer, um ihre Verhandlungsposition in Bezug auf die Höhe der Abfindung verbessern zu wollen.

Auf der Basis der DS-GVO sind zwei gerichtliche Entscheidungen erwähnenswert, die sich mit dem Thema bereits befasst haben:

Zum einen das LAG Baden-Württemberg (20.12.2018, AZ: 17 Sa 11/18), das eine weite Auslegung des Rechts auf Erhalt einer Kopie vorgenommen hat und andererseits die Entscheidung des LG Köln (18.3.2019, AZ: 26 O 25/18), welches eine einschränkende Auslegung präferiert („dient nicht der vereinfachten Buchführung des Betroffenen“).

Bislang vertritt der LfDI dabei folgende Position, wobei künftige Anpassungen aufgrund neuerer höchstrichterlicher Rechtsprechung sowie der Abstimmung mit anderen Datenschutzaufsichtsbehörden nicht ausgeschlossen sind:

Sofern spezialgesetzliche Regelungen, wie dies im Bereich des Beschäftigtendatenschutz in Bezug auf die Personalakte der Fall ist, das Recht auf Akteneinsichtnahme regeln, handelt es sich hierbei um das am weitestgehend Recht (s. hierzu die grundlegenden Äußerungen von Dr. Globig in: Festschrift für Prof. Dr. Walter Rudolf zum 70. Geburtstag, „Völkerrecht und Deutsches Recht“, 2001, S. 452; Zitat: „Aus dem oben Dargelegten über die maßgeblichen Aspekte des Sinnes und Zwecks des Auskunftsanspruchs gegenüber dem Betroffenen folgt, dass die Gewährung von Akteneinsicht grundsätzlich deshalb die optimale Grundrechtsverwirklichung zur Folge hat, weil damit dem Betroffenen am umfassendsten, authentischsten und deutlichsten offenbart wird, welche Erkenntnisse die speichernde Stelle über ihn besitzt“).

Die DS-GVO hat hieran nichts geändert: Im Rahmen einer Akteneinsichtnahme kann der (ehemalige) Beschäftigte auch Kopien verlangen. Der Arbeitgeber hat dem nachzukommen, sofern dies nicht mit einem unverhältnismäßigen Aufwand (z.B. aufgrund des Umfangs der

Personalakte) verbunden ist. Der Arbeitgeber ist aber nicht verpflichtet, sämtliche personenbezogene Daten des Beschäftigten (z.B. aus vorangegangenem E-Mail-Verkehr oder aus sonstigen Sachakten) bei der Geltendmachung des Rechts auf Erhalt einer Kopie zusammenzutragen.

7.8 Bußgelder gegen öffentlich Bedienstete

Auch musste sich der LfDI vermehrt mit Fällen auseinandersetzen, in denen Polizeibeamte zu privaten Zwecken Personenabfragen in polizeilichen Informationssystemen vorgenommen hatten. Zwar sind Bußgelder gegenüber öffentlichen Stellen nach wie vor nicht möglich. Eine neue Regelung im Landesdatenschutzgesetz (§ 24 LDSG) eröffnet jedoch diese Möglichkeit gegenüber einem Beschäftigten im Falle eines sog. Exzesses. Dies ist insbesondere bei ausschließlich privat motivierten Datenabfragen und –nutzungen der Fall. Sofern dem LfDI solche Fälle bekannt wurden, wurden Bußgeldverfahren gegen die Beamten eingeleitet.

8. MEDIEN

8.1 Veröffentlichung von Bildern

Weiterhin wenden sich regelmäßig Beschwerdeführer dagegen, dass andere Personen Bilder oder Videos von ihnen auf Webseiten oder in sozialen Netzwerken veröffentlichen. Veröffentlichungen erfolgen z.B. durch Vereine, Arbeitgeber, Kommunen oder Privatpersonen. Der LfDI prüft bei derartigen Beschwerden, ob eine Rechtsgrundlage für die Veröffentlichung der personenbezogenen Daten vorliegt. Liegt eine solche nicht vor, wirkt er auf die Löschung der Veröffentlichungen hin.

Die Veröffentlichung von Bildnissen lässt sich in aller Regel auf eine Einwilligungserklärung der Betroffenen stützen.. Diese hat nach Art. 6 Abs. 1 lit. a, Art. 7 DS-GVO informiert, freiwillig und ausdrücklich zu erfolgen. Als Rechtsgrundlage für die Veröffentlichung von Personenfotografien durch privatrechtliche Verantwortliche kann in bestimmten Konstellationen aber auch die Verarbeitung aufgrund berechtigter Interessen des Verantwortlichen gemäß Art. 6 Abs. 1 lit. f DS-GVO in Betracht kommen. Im Rahmen der Interessenabwägung nach dieser Norm können die Fallgruppen des § 23 Kunsturhebergesetz als Leitlinien herangezogen werden.

In beiden Fällen - sowohl bei der Verarbeitung aufgrund einer Einwilligung als auch bei der Verarbeitung aufgrund berechtigter Interessen - können die betroffenen Personen auch im Nachhinein die Löschung der Fotografien verlangen. Während eine Einwilligung mit Wirkung für die Zukunft zurückgenommen werden kann, besteht für die Verarbeitung nach Art. 6 Abs. 1 lit. f DS-GVO ein Widerspruchsrecht.

Um für betroffene Personen und Verantwortliche mehr Sicherheit bei der Veröffentlichung von Fotos und Videos zu schaffen, hat der LfDI im Jahr 2019 einen umfangreichen Katalog mit Fragen und Antworten zu dem Thema Recht am eigenen Bild auf seinem Internetangebot veröffentlicht: **https://s.rlp.de/raeb**

8.2 Datenschutzkonformität von Webseiten

Die Überprüfung von Webseiten auf einen datenschutzkonformen Betrieb hat den LfDI weiterhin besonders stark beschäftigt.

Den LfDI erreichten weiterhin zahlreiche Hinweise zu Webseiten, die nicht den Anforderungen der DS-GVO entsprachen. Diesen Hinweisen ging der LfDI 2019 verstärkt nach. Regelmäßig ergab die Überprüfung der Webseiten, dass Datenschutzerklärungen nicht den Anforderungen der DS-GVO entsprachen und Tracking-Mechanismen eingesetzt wurden, die zumindest in der betriebenen Form nicht zulässig waren. Häufig reagierten die Webseitenbetreiber schon auf ein Informationsersuchen des LfDI mit der Überarbeitung ihrer Datenschutzerklärung.

Aufwändiger ist die Rechtsdurchsetzung im Bereich Tracking. Webseitenbetreiber, Werbepartner und Datenunternehmen setzen verschiedenste Mittel und Techniken ein, um das Nutzungsverhalten im Internet zu erfassen und auszuwerten. Mit Geltungsbeginn der DS-GVO gewann die Frage der datenschutzrechtlichen Zulässigkeit von Webtracking neue Aktualität.

8.3 Tracking auf Webseiten: Was ist nach der DS-GVO erlaubt, was nicht?

Viele Verantwortliche vertraten zu Beginn der Geltung der DS-GVO den Standpunkt, das Tracking der Webseitennutzer, z.B. durch Cookies oder Analyse-Diensten wie Google Analytics, sei gemäß Art. 6 Abs. 1 lit. f DS-GVO als Verarbeitung für berechtigte Interessen zulässig. Die Verantwortlichen gingen teilweise von einer Fortführung der bisherigen Erlaubnis zur Profilbildung aus § 15 Abs. 3 TMG aus. Diese Rechtsauffassung ist auch als „opt-out-Lösung“ bekannt, weil davon ausgegangen wird, dass die personenbezogenen Daten der Webseitennutzer ohne deren Erlaubnis verarbeitet werden dürfen, sofern nicht die Nutzer der Verarbeitung aktiv widersprechen. Allerdings erlaubte auch § 15 Abs. 3 TMG schon nicht die Übermittlung der Nutzungsprofile an andere Verantwortliche.

Die DSK hat sich bereits am 26.4.2018, also etwa einen Monat vor Geltungsbeginn der DS-GVO, mit einer Positionsbestimmung zur Rechtslage geäußert. Die DSK stellte darin zunächst fest, dass die datenschutzrechtlichen Bestimmungen des Telemediengesetzes durch die Erlaubnistatbestände der DS-GVO verdrängt werden und nicht mehr anwendbar sind. Bis zur Verabschiedung und Geltung der angekündigten ePrivacy-Verordnung ist die Verarbeitung von Nutzungsdaten der Webseitenbesucher daher ausschließlich an den Rechtsgrundlagen in Art. 6 Abs. 1 DS-GVO zu messen.

Die DSK hat sich in der Positionsbestimmung außerdem dahingehend geäußert, dass die Interessenabwägung im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO in der Regel zuungunsten der Verantwortlichen ausschlägt, wenn das Verhalten von Personen im Internet nachvollziehbar gemacht wird und Nutzerprofile angelegt werden. Dies bedeutet, dass in vielen Fällen die Verarbeitung gerade nicht aufgrund berechtig-

ter Interessen durchgeführt werden kann, sondern einer ausdrücklichen Einwilligung der betroffenen Personen bedarf. Die Verarbeitung darf also nur dann stattfinden, wenn die Nutzer eingewilligt haben („opt-in-Lösung"). Die Positionsbestimmung der DSK wurde am 29.3.2019 durch eine ausführliche Orientierungshilfe für Telemedienanbieter konkretisiert und ausdifferenziert.

Aufgrund dieser abgestimmten Position der DSK begann der LfDI im Jahr 2019 mit der Verfolgung von Verstößen gegen die Vorgaben der DS-GVO beim Einsatz von Tracking auf Webseiten. In vielen Verfahren zeigten sich die Verantwortlichen bereits nach dem Informationsersuchen einsichtig und passten den Betrieb ihrer Internetseiten den Anforderungen der DS-GVO beim Tracking an. In zwei Fällen musste der LfDI im Jahr 2019 jedoch Anordnungen gegen Webseitenbetreiber erlassen. In diesen Anordnungen verlangte der LfDI, dass die Betreiber, die Übermittlung von Nutzungsdaten an andere Verantwortliche nur aufgrund von Einwilligungen der Webseitennutzer vornehmen. Beide Betreiber gingen gegen die Anordnungen gerichtlich vor. Ein Betreiber hat im Klageverfahren seinen Webseitenbetrieb umgestellt und die Klage daher für erledigt erklärt. Das zweite Verfahren wird im Jahr 2020 gerichtlich entschieden werden.

Die große Zahl an Beschwerden über den Einsatz des Tracking-Werkzeuges Google Analytics haben die Datenschutzaufsichtsbehörden in Deutschland zum Anlass genommen eine gemeinsam Pressemitteilung zu diesem Thema zu veröffentlichen. In dieser stellt der LfDI nochmals klar, dass Analyse-Tools, die Daten über das Nutzungsverhalten an Dritte weitergeben, nur mit Einwilligung genutzt werden dürfen, wenn diese Dritten die Daten auch zu eigenen Zwecken verwenden.

Mittlerweile hat sich gezeigt, dass zahlreiche Webseitenbetreiber die von der DSK vertretene Position zum Tracking zur Kenntnis genommen haben und den Betrieb ihrer Webseiten umstellen. Gerade bei Internetseiten von großen Unternehmen in Rheinland-Pfalz konnte der LfDI zwischenzeitlich Anpassungen feststellen.

Der datenschutzkonforme Betrieb von Webseiten liegt in der Verantwortung der Betreiber. Eine Einzelfallberatung durch den LfDI ist nicht leistbar. Allerdings enthält das Webangebot des LfDI die wichtigsten Informationen und Arbeitsmaterialien zu diesem Themenbereich.

Allgemeine Hinweise und Arbeitshilfen zu diesem Themenbereich finden sich im Webangebot des LfDI: **https://s.rlp.de/hilfestellungdse https://s.rlp.de/googleanalytics**

8.4 Facebook-Fanpages und gemeinsame Verantwortung

Am 5.6.2018 entschied der EuGH (Az: C-210/16), dass Facebook-Fanpage-Betreiber und Facebook „gemeinsame Verantwortliche" für die Datenverarbeitung durch Facebook beim Betrieb von Fanpages sind. Die DSK hat bereits am 5.9.2018 einen Beschluss zu diesem Thema gefasst und darin festgestellt, dass daraus eigene Pflichten für die Fanpage-Betreiber entstehen. Diese können die Verantwortung für die Verarbeitung der Nutzungsdaten der Besucher ihrer Fanpages nicht einseitig an Facebook abgeben, sondern sind für die Einhaltung der Regelungen der DS-GVO mitverantwortlich. Daher müssen sie gegenüber Facebook darauf hinwirken, dass die Voraussetzungen für einen datenschutzkonformen Betrieb der Fanpages geschaffen werden.

Hierzu ist es einerseits erforderlich, die Verarbeitung der Nutzungsdaten auf eine geeignete Rechtsgrundlage zu stützen: Zumindest für

nicht bei Facebook angemeldete Besucher der Fanpage wird hierzu eine Einwilligung erforderlich sein. Einen technischen Mechanismus zur Erteilung von Einwilligungen bietet Facebook aber bisher nicht. Anderseits ist gemäß Art. 26 DS-GVO eine Vereinbarung zwischen Facebook und den Fanpage-Betreibern erforderlich, die insbesondere klarstellt, wie zwischen diesen Parteien die Erfüllung der Pflichten aus der DS-GVO erfolgt. Facebook hat hierauf reagiert, indem die sogenannte „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen" veröffentlicht wurde. Obwohl Facebook hiermit einen Vorschlag veröffentlicht und auch bereits aktualisiert hat, entspricht dieser bisher nicht den Anforderungen an eine Vereinbarung nach Art. 26 DS-GVO. Ein datenschutzkonformer Betrieb von Facebook-Fanpages ist daher nach derzeitigem Stand nicht möglich.

Mit Urteil vom 11. September 2019 stellte das Bundesverwaltungsgericht ergänzend klar, dass die Datenschutzaufsichtsbehörden gegen die Betreiber von Facebook-Fanpages selbst vorgehen können, wenn bei dem Betrieb von Facebook-Fanpages Datenschutzverstöße begangen werden. Eine Datenschutzaufsichtsbehörde muss nicht stattdessen gegen Facebook vorgehen, weil dies wegen der fehlenden Kooperationsbereitschaft von Facebook mit erheblichen tatsächlichen und rechtlichen Unsicherheiten verbunden wäre. Das Gericht entschied weiter, dass es verhältnismäßig sei, die Außerbetriebnahme der Fanpage anzuordnen, wenn die von Facebook zur Verfügung gestellte digitale Infrastruktur schwerwiegende datenschutzrechtliche Mängel aufweise.

Die Thematik betrifft neben den privatrechtlichen Fanpage-Betreibern auch öffentliche Stellen in Rheinland-Pfalz (Siehe bereits 25. Tätigkeitsbericht, S. 38 f.). Für diese hat der LfDI schon im Jahr 2016 einen Handlungsrahmen zur Nutzung sozialer Medien veröffentlicht. Nach der nunmehr endgültigen gerichtlichen Klärung wird der Handlungsrahmen nunmehr entsprechend aktualisiert. Die Veröffentlichung ist für das erste Quartal 2020 vorgesehen.

8.5 Zuständigkeit für E-Mail-Anbieter in Rheinland-Pfalz

Mit Urteil vom 13.6.2019 hat der Europäische Gerichtshof entschieden, dass der Webmail-Dienst Gmail kein Telekommunikationsdienst im Sinne der der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und dienste ist.

Bis zu diesem Zeitpunkt wurde die datenschutzrechtliche Aufsicht über E-Mail-Dienste gemäß § 115 Abs. 4 des Telekommunikationsgesetzes, das die o.g. Richtlinie umsetzt, durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) ausgeübt. Die Aufsicht über privatwirtschaftliche Unternehmen in Rheinland-Pfalz, die keine Telekommunikationsdienste erbringen, wird vom LfDI ausgeübt. Da davon auszugehen ist, dass die Feststellungen zu Gmail auch für andere Webmail-Dienste gelten, übernahm der LfDI in Abstimmung mit dem BfDI vorläufig die Aufsicht über die E-Mail-Anbieter mit Hauptsitz in Rheinland-Pfalz, da diese nicht mehr unter § 115 Abs. 4 TKG fallen. Hierzu zählen insbesondere die beiden zum Unternehmen IONOS (1&1) gehörenden Dienste GMX und Web.de. Schon zuvor übte der LfDI die Aufsicht über das Geschäft von IONOS aus, soweit dies nicht E-Mail, Telefondienste oder den Internetanschluss betraf. Festnetztelefonie, Mobilfunk und Internetanschlüsse bleiben weiterhin in der Zuständigkeit des BfDI. Die Übernahme der Aufsicht über die E-Mail-Dienste führte zu einem deutlichen Mehraufkommen von Beschwerden im Medienbereich beim LfDI. Nicht erfolgte Löschungen von Nutzerkonten durch den E-Mail-Anbieter sind hier der häufigste Beschwerdegrund.

8.6 Unerwünschte Werbezusendungen

Die Zahl der Beschwerden über unerwünschte Werbezusendungen per Post oder E-Mail nimmt auch weiterhin zu. Dies liegt zum einen an der hohen Zahl an täglich versandter Werbung aber auch an der mittlerweile eingetretenen Sensibilisierung der Empfänger von unerlaubterer Werbung, die die Verarbeitung ihrer Daten nachvollziehen und unterbinden wollen.

Viele Beschwerdeführer wenden sich daher richtigerweise im ersten Schritt an den Verantwortlichen, der ihnen die Werbung zugesendet hat und verlangen Auskunft über die zu ihrer Person gespeicherten Daten sowie deren Herkunft. In manchen Fällen gestaltet sich bereits die Ermittlung des Verantwortlichen schwierig, weil für die betroffenen Personen nur schwer zu ermitteln ist, wer genau die Werbung versandt hat. Dies liegt daran, dass in diesen Fällen die Verantwortlichen ihren Informationspflichten nach Art. 13 DS-GVO zum Teil gar nicht oder nur unzureichend nachkommen.

Viele Verantwortliche reagieren auf das Auskunftsverlangen nicht oder erst verspätet, sodass sich die betroffenen Personen beim LfDI beschweren. Zumeist erteilen die Verantwortlichen den betroffenen Personen nach einem ersten Informationsersuchen die verlangte Auskunft. In einigen Fällen ist die Auskunft dann jedoch fehlerhaft oder die Daten wurden gelöscht, bevor dem Auskunftsverlangen nachgekommen wurde.

Verantwortliche mit Sitz in Rheinland-Pfalz, die sich aber zur Versendung der Werbung eines Adresshändlers mit Sitz im Ausland - zum Teil im außereuropäischen Raum - bedienen, werden vom LfDI als gemeinsame Verantwortliche für die Datenverarbeitung zu Werbezwecken betrachtet. Die betroffenen Personen haben somit grundsätzlich gegenüber den Verantwortlichen in Rheinland-Pfalz einen Anspruch auf Auskunft.

Ein weiterer Beschwerdekomplex betrifft die fehlende Bestätigung der Löschung durch den Verantwortlichen. Die betroffene Person verlangt die Löschung, jedoch antwortet der Verantwortliche darauf nicht. Nach Art. 12 Abs. 3 DS-GVO muss der Verantwortliche der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 DS-GVO ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung stellen. Das bedeutet, dass der Verantwortliche auch über die Löschung innerhalb eines Monats nach Eingang des Antrags auf Löschung die betroffene Person unterrichten muss. Löscht der Verantwortliche die Daten nicht, muss er dies der betroffenen Person innerhalb eines Monats mitteilen sowie begründen und sie über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen, informieren (Art. 12 Abs. 4 DS-GVO). Jedoch hat sich in manchen Fällen gezeigt, dass trotz bestätigter Löschung die Daten zum Teil noch vorhanden sind und die betroffenen Personen dennoch weitere Werbezusendungen erhalten.

Der LfDI hat im Jahr 2019 nicht nur in vielen Fällen Verwarnungen gegenüber Verantwortlichen aufgrund fehlerhafter Auskunft und Löschung aussprechen, sondern musste auch in einigen Fällen die Erteilung von Auskünften und Löschungen von Daten anordnen.

9. GESUNDHEIT

9.1 Auskunftsanspruch in der Heilbehandlung

Nach Wirksamwerden der Datenschutz-Grundverordnung im Mai 2018 wurde verstärkt die Frage aufgeworfen, ob sich der datenschutzrechtliche Auskunftsanspruch nach Art. 15 DS-GVO im Rahmen der Heilbehandlung auch auf die Bereitstellung einer vollständigen Kopie der Behandlungsdokumentation erstreckt. Die Angelegenheit hat für die Praxen hinsichtlich der dabei anfallenden Kosten eine praktische Relevanz: denn anders als nach § 630g Abs. 2 Satz BGB und den jeweiligen Berufsordnungen vorgesehen wäre eine auf Art. 15 Abs. 3 Satz 1 DS-GVO gestützte Kopie zumindest in der ersten Ausfertigung für die Betroffenen unentgeltlich.

Zum Hintergrund: das Einsichts- und Auskunftsrecht der an einer Heilbehandlung beteiligten Patienten ist an mehreren Stellen verankert: einerseits im Berufsrecht (vgl. § 10 Abs. 2 der Berufsordnung für Ärzte in Rheinland-Pfalz und § 11 der Berufsordnung für Psychotherapeuten in Rheinland-Pfalz), darüber hinaus im Vertragsrecht (§ 630g BGB) und im allgemeinen Datenschutzrecht (Art. 15 DS-GVO). Den Patienten steht danach ein einklagbarer Rechtsanspruch auf Einsicht in und Auskunft aus sämtlichen ihn betreffenden Krankenakten zu, ohne dass dies vor der Behandlung vereinbart werden muss. Der Rechtsanspruch gilt auch nach Abschluss der Behandlung. Der Patient kann zugleich die Anfertigung von Kopien verlangen. Lediglich hinsichtlich der Frage der Kostenerstattung unterscheiden sich die Vorgaben aus dem Berufs- und Vertragsrecht (Kopie mit Kostenerstattung) von denen aus dem Datenschutzrecht (erste Kopie unentgeltlich).

Im Ergebnis umfasst nach Ansicht des LfDI Rheinland-Pfalz aufgrund der besonderen Umstände im Bereich der Heilbehandlung der datenschutzrechtliche Auskunftsanspruch nach Art. 15 Abs. 3 DS-GVO ausnahmsweise das Recht auf Bereitstellung einer vollständigen Kopie der Behandlungsdokumentation, wenn dies dem Auskunftsbegehren des Patienten entspricht. Zwar ist grundsätzlich der Auskunftsanspruch nach Art. 15 DS-GVO nur auf die Erteilung einer allgemeinen Auskunft über das Ausmaß der Verarbeitung personenbezogener Daten beschränkt, so dass damit regelmäßig nicht die Ablichtung kompletter Dokumentationen oder Akten verlangt werden kann. Dies kann nur einzelfallbezogen und nach Prüfung des konkreten Anliegens bezogen auf einzelne Dokumente erforderlich sein. Im Bereich der Heilbehandlung durch Ärzte oder andere Gesundheitsberufe ist die Reichweite des datenschutzrechtlichen Auskunftsanspruchs dagegen weiter und erstreckt sich vorbehaltlich vorrangiger gesetzlicher Schranken, insbesondere aus dem BDSG, dem LDSG oder dem BGB, regelmäßig auf die Bereitstellung einer vollständigen Kopie der Behandlungsdokumentation, sofern der Patient dies verlangt.

Grund hierfür ist die Tatsache, dass es sich bei den in einer Patientenakte enthaltenen Daten fast ausschließlich um Gesundheitsinformationen und damit um personenbezogene Daten besonderer Kategorien im Sinne des Art. 9 Abs. 1 DS-GVO handelt. Diese sind nach Art. 15 Abs. 1 lit. b DS-GVO immer im Rahmen der Auskunftserteilung zu benennen. Nach Erwägungsgrund 63 zur DS-GVO umfasst das Recht der betroffenen Person auf Auskunft über ihre eigenen gesundheitsbezogenen Daten auch Informationen zu Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten. Nach Auffassung des Verordnungsgebers sollte mit dem Auskunftsanspruch zumindest die Möglichkeit

eines direkten Zugangs zu den Daten geschaffen werden.

Einschränkungen des Zugangsrechts ergeben sich nach der gegenwärtigen Rechtslage lediglich dann, wenn entweder erhebliche Persönlichkeitsrechte Dritter dagegen stehen oder aus therapeutischen Gründen eine Einsichtnahme für den Betroffenen zu einer erheblichen Gesundheitsgefahr führen würde. Begehrt der Patient Einsicht, muss im konkreten Fall auch bei den subjektiven Bestandteilen der Dokumentation geprüft werden, ob ein Verweigerungsgrund im Sinne von § 630g Abs. 1 Satz 1 BGB vorliegt. Grundsätzlich darf der Patient aber nicht vor der Kenntnis seiner gesundheitlichen Verfassung geschützt werden.

9.2 Wir schaffen das – Datenschutz und Datensicherheit im Krankenhaus

Die Krankenhäuser stehen täglich vor einer Vielzahl besonderer Herausforderungen. Dies wird der Gesellschaft und jedem Einzelnen gerade zu Anfang des Jahres 2020 sehr drastisch vor Augen geführt. Mit der Corona-Krise hat der bundesweite Stresstest der stationären Gesundheitsversorgung in Deutschland begonnen und es zeigt sich, dass wir trotz aller vor der Krise noch engagiert geführten Diskussionen über Form und Fortbestand der hiesigen Kliniklandschaft im Ergebnis von hohen Qualitätsstandards ausgehen können. Hiervon profitieren wir alle.

Dass dies auch im Hinblick auf den Schutz der Integrität und Vertraulichkeit stationärer Behandlungen von Patienten so gilt, ist erklärtes Ziel aller Beteiligten und entspricht auch dem gesetzlichen Auftrag, dem die Krankenhäuser unterliegen. In diesem Zusammenhang sei insbesondere auf die Regelungen aus dem Informationssicherheitsrecht (BSI-Gesetz sowie die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz) als auch auf die Bestimmungen aus dem Datenschutzrecht (DS-GVO und Landeskrankenhausgesetz) verwiesen.

Die Umsetzung der datenschutz- und informationssicherheitsrechtlichen Vorgaben in den einzelnen Krankenhäusern stellt im Klinikalltag dagegen immer noch eine große Herausforderung dar. Angesichts der Vielzahl der von den Einrichtungen zu erfüllenden Anforderungen, einer dauerhaft angespannten Finanz- und Personalsituation sowie der sich beschleunigenden Digitalisierung des Gesundheitssystems, die zu immer komplexer werdenden Datenverarbeitungsprozessen führt, ist dies zwar durchaus nachvollziehbar. Dennoch gibt es keine Alternative: Krankenhäuser gehören zur kritischen Infrastruktur einer Gesellschaft, deren Funktionieren für das Gemeinwohl elementar ist. Schon aus diesem Grund müssen sie zumindest ab einer bestimmten Größe effektive und umfassende sicherheitstechnische Vorkehrungen treffen, um ihre Funktionsfähigkeit dauerhaft zu garantieren. Zugleich gehören die im Rahmen stationärer Patientenbehandlungen verarbeiteten Daten zu den nach dem Datenschutzrecht schutzbedürftigsten Kategorien, die zwingend die Gewährleistung eines angemessenen Sicherheitsniveaus durch die einzelnen Verantwortlichen verlangen; unabhängig davon, wie groß die einzelne Einrichtung ist.

Dementsprechend hat die Datenschutzkonferenz auf ihrer Herbsttagung im November 2019 in einer Entschließung ausdrücklich darauf hingewiesen, dass der gesetzliche Auftrag der Gesundheitseinrichtungen zum effektiven Schutz der von ihnen verarbeiteten Patientendaten unabhängig von ihrer Größe gilt (**https://s.rlp.de/PatientendatenschutzGesundheitseinrichtungen**). Anlass waren verschiedene im Laufe des Jahres 2019 bundesweit aufgetretene Sicherheitsvorfälle, bei denen die Funktionsfähigkeit der betroffenen Krankenhäuser z.B.

durch den Befall mit Schadsoftware gefährdet wurde. Auch Einrichtungen in Rheinland-Pfalz waren hiervon betroffen (**https://s.rlp.de/SicherheitsvorfallKrankenhausIT**). Aus der Sicht der Datenschutzaufsichtsbehörden des Bundes und der Länder ist es unabdingbar, dass angesichts der zunehmenden Digitalisierung der Gesundheitsversorgung und der damit einhergehenden Gefährdungen alle Einrichtungen des Gesundheitswesens unabhängig von der Zahl der dort behandelten Patienten gerade auch in finanzieller Hinsicht so ausgestattet werden müssen, dass sie die zum Schutz der Patientendaten nach dem Stand der Technik gesetzlich gebotenen Vorkehrungen ergreifen können. Es bleibt zu hoffen, dass die benötigten Ressourcen auch tatsächlich den Häusern bereit gestellt werden. Aber auch dazu gibt es keine Alternative: eine Digitalisierung zum datenschutzrechtlichen Nulltarif, d.h. ohne Investitionen in Aufbau und Betrieb einer angemessenen Sicherheitsarchitektur zum Schutz der Gesundheitsdaten, wird es aufgrund der eindeutigen und zwingenden rechtlichen Rahmenbedingungen nicht geben können!

Im Berichtsjahr hat der LfDI in diversen Zusammenhängen versucht, Datenschutz und Datensicherheit bei den rheinland-pfälzischen Krankenhäusern zu stärken:

- So beteiligte er sich an dem von der Landesregierung aufgrund der im Sommer 2019 aufgetretenen Sicherheitsvorfälle kurzfristig gebildeten Runden Tisch zur IT-Sicherheit in Krankenhäusern. Dessen Empfehlungen wurden im März 2020 der Öffentlichkeit vorgestellt.

- Im Hinblick auf den im Klinikalltag zu beobachtenden verbreiteten Einsatz von WhatsApp zur Kommunikation zwischen Krankenhaus-Ärzten, um beispielsweise zeitkritische medizinische Entscheidungen treffen zu können, erarbeitete der LfDI im Rahmen einer bundesweiten Arbeitsgruppe der DSK federführend ein Papier mit technischen Anforderungen an den Einsatz von Messenger-Diensten im Krankenhausbetrieb.

- Aber auch aufsichtsrechtliche Maßnahmen wurden ergriffen: Im Herbst 2019 verhängte der LfDI die bislang seit dem Wirksamwerden der DS-GVO im Mai 2018 höchste Geldbuße seiner Geschichte in Höhe von 105.000 Euro gegen das größte Krankenhaus im Lande, nachdem die Einrichtung gleich in mehrfacher Hinsicht gegen Vorgaben der DS-GVO verstoßen hatte (**https://s.rlp.de/GeldbusseKrankenhaus**). Mit diesem Schritt unterstrich der LfDI neben der Sanktionierung des konkreten Vorfalls insbesondere seine Strategie, in Krankenhäusern bestehende strukturelle und dauerhafte Missstände bei der Beachtung datenschutzrechtlicher Vorgaben konsequent zu ahnden. Die seitdem durch die Einrichtung in Gang gebrachte Verbesserung des internen Datenschutzmanagements begleitete der LfDI konstruktiv. Über weitere Maßnahmen zur Fortentwicklung eines datenschutzgerechten Umgangs mit Patientendaten zum Zwecke der Gesundheitsversorgung und der wissenschaftlichen Forschung wird der LfDI regelmäßig unterrichtet.

Mit Blick auf die besondere Sensibilität der in den Krankenhäusern täglich verarbeiteten Daten und der elementaren Bedeutung der Einrichtungen für das Gemeinwohl ist es unumgänglich, dass die Erfüllung der datenschutz- und informationsrechtlichen Anforderungen von Anfang an zur Chefsache erklärt wird. Teilweise ist dies bei den rheinland-pfälzischen Krankenhäusern, die der Datenschutzaufsicht des LfDI unterliegen, bereits der Fall. Zur Gewährleistung eines angemessenen Datenschutz- und Datensicherheitsniveaus in den Häusern bedarf es überall einer schnellen und anhaltenden Bereitstellung der hierzu benötig-

ten Personal- und Sachmittel sowie der Schaffung effektiver interner Strukturen. Wird dies nicht beachtet, kann es teuer werden. Denn der LfDI wird auch künftig auf dem Feld des Umgangs mit Daten im Gesundheitswesen besonders wachsam sein.

9.3 Auf der Überholspur: die Digitalisierung des Gesundheitswesens

Anfang November 2019 hat der Deutsche Bundestag den Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitalen Versorgung-Gesetz) verabschiedet. Damit versucht die Bundesregierung der seit Jahren nicht vorankommenden Digitalisierung des deutschen Gesundheitswesens entscheidende Impulse zu geben. Dies ist verständlich und angesichts der seit Jahren erwarteten Chancen für eine Verbesserung der Gesundheitsversorgung der Bevölkerung auch überfällig.

Der Gesetzentwurf führt zu einem grundlegenden Wandel in der bisherigen Gesundheitsversorgung in Deutschland und ist auch aus datenschutzrechtlicher Sicht von besonderer Bedeutung. Mit der Schaffung eines Rechtsanspruchs der gesetzlich Versicherten auf Inanspruchnahme digitaler Gesundheitsanwendungen werden die gesetzlichen Voraussetzungen geschaffen, um z.B. den Einsatz von Medizin-Apps in die Behandlung von Patientinnen und Patienten zu forcieren.

Hiergegen ist aus Sicht des Datenschutzes generell nichts einzuwenden, sofern auch künftig die Vertraulichkeit der Heilbehandlung und der in diesem Zusammenhang verarbeiteten Patientendaten verlässlich gewahrt ist. Doch genau dies ist unklar. Zwar sollen die in der Behandlung eingesetzten digitalen Gesundheitsanwendungen nach dem Willen des Gesetzgebers nur dann erstattungsfähig sein, wenn sie in einem vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) zu erstellenden Verzeichnis gelistet sind. Damit dies erfolgt, müssen die Anwendungen u.a. den Anforderungen an den Datenschutz entsprechen und die Datensicherheit nach dem Stand der Technik gewährleisten. Nach welchen Kriterien, in welcher Prüftiefe und mit welcher Aussagekraft dies innerhalb von drei Monaten durch das BfArM geleistet werden kann, wird allerdings gesetzlich nicht geregelt.

Dies bleibt vielmehr eine Rechtsverordnung vorbehalten, deren erster Entwurf im Januar 2020 jedoch die grundlegenden Befürchtungen der Datenschutzbeauftragten des Bundes und der Länder in die datenschutzrechtlichen Risiken der Digitalisierung des Gesundheitswesens leider bestätigte. Solange sich der Nachweis über die Einhaltung grundlegender Anforderungen an den Schutz und die Sicherheit von Gesundheitsdaten bei der Nutzung digitaler Gesundheitsanwendungen auf eigene Erklärungen der Hersteller beschränkt kann zumindest aus Sicht des Datenschutzes nicht verlässlich von einer sicheren und vertraulichen Verarbeitung der Daten der Versicherten ausgegangen werden. Zugleich deutet der bislang vorgelegte Entwurf einer Rechtsverordnung darauf hin, dass den Herstellern digitaler Gesundheitsanwendungen massive Verarbeitungsbefugnisse z.B. zum Nachweis positiver Versorgungseffekte der von Ihnen auf den Markt gebrachten Produkte eingeräumt werden sollen, die sehr weitgehende Einblicke in die Gesundheit der Versicherten zulassen, ohne dass dem effektive Vorkehrungen zum Schutz dieser Daten wie z.B. die Schaffung einer strafrechtlich sanktionierbaren Schweigepflicht der Hersteller gegenüberstehen. Daran ändert auch die Tatsache nichts, dass solche Befugnisse von der Einwilligung der Versicherten abhängig gemacht werden sollen. Denn den Versicherten dürfte es allein schon aufgrund der Komplexität der einzelnen Anwendungen

und der zugrunde liegenden Verarbeitungsarchitektur regelmäßig kaum möglich sein, bestehende Risiken einer gegebenen Einwilligung mit angemessenem Aufwand zu erkennen und zu bewerten.

Auch die Ende 2019 aufgekommene Diskussion über sog. Analyse- und Tracker-Programme, die in verschiedenen Medizin-Apps integriert sind und teilweise sehr sensible Gesundheitsangaben der Nutzer an externe Stellen außerhalb der Gesundheitsversorgung wie z.B. facebook weitergegeben haben, zeigte, dass seitens des Gesetzgebers noch grundlegender Handlungsbedarf besteht. Nicht zuletzt aus diesem Grund hatte die 98. Datenschutzkonferenz auf ihrer Sitzung in Trier im November 2019 in diesem Zusammenhang eine Entschließung verabschiedet und u.a. den Gesetzgeber aufgefordert, den Schutz der Vertraulichkeit von Gesundheitsdaten mit der Einführung der digitalen Gesundheitsanwendungen in die Regelversorgung sicherzustellen.

Darüber hinaus enthält das Digitale-Versorgung-Gesetz noch weitere aus der Sicht des Datenschutzes klärungsbedürftige Punkte wie z.B. die Rolle der gesetzlichen Krankenkassen bei der Genehmigung digitaler Gesundheitsanwendungen, soweit diese der Patientenbehandlung dienen, oder die ihnen eingeräumte Befugnis zur Nutzung von Patientendaten zum Zwecke der Entwicklung digitaler Innovationen. Insoweit wie auch hinsichtlich der sonstigen seitens der Bundesregierung beabsichtigten gesetzgeberischen Impulse zum weiteren Vorantreiben der Digitalisierung im Gesundheitswesen, die für das Jahr 2020 geplant sind, kommt es nun auf eine enge inhaltliche Einbindung der Datenschutzaufsichtsbehörden und des BSI in die Ausgestaltung der künftigen Nutzung digitalen Instrumente in der Regelversorgung an. Bei allem Verständnis für die nun an den Tag gelegte Eile hängen der Erfolg und die Akzeptanz eines digitalen Versorgungssystems ganz entscheidend davon ab, ob alle Akteure einschließlich der betroffenen Patienten in dessen Sicherheit und Verlässlichkeit vertrauen dürfen. Künftig muss deshalb Sorgfalt vor Schnelligkeit gehen. Die Datenschutzbeauftragten des Bundes und der Länder sind in diesem Zusammenhang selbstverständlich bereit, ihre vorhandene Expertise konstruktiv und umfassend in den durchaus notwendigen Transformationsprozess einzubringen.

9.4 Einbindung von Inkassounternehmen durch Angehörige von Gesundheitsberufen

Im Rahmen einer Beschwerde wandte sich der Patient einer physiotherapeutischen Praxis gegen die Weitergabe seiner Identität einschließlich an ihn gerichteter Rechnungen bzgl. der Erstattung von Ausfallkosten nicht wahrgenommener Behandlungstermine an ein von dem Physiotherapeuten beauftragtes Inkassounternehmen. Zu Behandlungsbeginn hatte die Praxis gegenüber dem Betroffenen erklärt, dass bei einer nicht rechtzeitigen Absage von vereinbarten Behandlungsterminen Ausfallkosten zivilrechtlich geltend gemacht würden. Die Kenntnisnahme der Information hatte der Beschwerdeführer auch schriftlich quittiert. Allerdings wurde seitens der Praxis keine Einwilligung des Patienten in die mit der Einbindung des Inkassounternehmens verbundene Datenübermittlung eingeholt.

Der Fall warf die grundsätzliche Frage auf, ob und ggf. in welchem Rahmen es Angehörigen von Gesundheitsberufen datenschutzrechtlich gestattet ist, bei der Geltendmachung von Zahlungsforderungen Dritte einzubinden. Soweit es um die privatärztliche Abrechnung konkreter Behandlungsleistungen geht bestand bislang in Abstimmung mit den Heilberufskammern Konsens darüber, dass eine Einbeziehung externer Abrechnungsstellen oder Inkassounternehmen

nur auf der Basis einer von den Patienten erteilten Einwilligung zulässig ist. Lediglich die Beauftragung eines Rechtsanwalts zur Durchsetzung in eigenem Namen geltend gemachter Honorarforderungen wurde aus datenschutz- und berufsrechtlicher Sicht auch ohne Zustimmung der Patienten als zulässig angesehen.

Nach eingehender Prüfung hat der LfDI in dem der Beschwerde zugrunde liegenden Sachverhalt keinen Datenschutzverstoß der physiotherapeutischen Praxis feststellen können. Denn die Einschaltung von Inkassounternehmen durch Angehörige von Gesundheitsberufen zur Geltendmachung zivilrechtlicher Ausfallkosten nicht wahrgenommener Behandlungstermine ohne Einwilligung der Patienten ist auf der Basis von Art. 6 Abs. 1 lit. f, Art. 9 Abs. 2 lit. f DS-GVO zulässig, sofern der Schuldner trotz Mahnung zahlungssäumig ist und dem Inkassounternehmen lediglich die zur Eintreibung der Ausfallkosten erforderlichen personenbezogenen Daten zur Verfügung gestellt werden. Angesichts des nach Art. 5 Abs. 1 lit. a DS-GVO zu beachtenden Transparenz-Grundsatzes sollte den Patienten allerdings spätestens bei der Mahnung die beabsichtigte Einbindung der externen Stelle zur Geltendmachung der ausstehenden Forderung angekündigt werden.

Die datenschutzrechtliche Bewertung basiert auf folgenden Erwägungen: Anders als im Falle der Geltendmachung von Honorarforderungen an Abrechnungsunternehmen, bei denen eine Übermittlung abrechnungsrelevanter Behandlungsinformationen unausweichlich ist, führt die Einbindung von Dritten wie z.B. Inkassounternehmen bei der Eintreibung von Ausfallkosten zu einem deutlich geringeren Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen. Denn hier werden lediglich Angaben über die Identität des Schuldners als Patient einer Praxis weitergegeben, ohne dass das Unternehmen weiterführende Kenntnisse über den konkreten Gesundheitszustand des Betroffenen erlangt. Eine derartige Informationsweitergabe hält das Datenschutzrecht im Rahmen des Art. 9 Abs. 2 lit. f DS-GVO für hinnehmbar, zumal es in der Hand des Betroffenen liegt zu entscheiden, ob er die an ihn gerichtete Forderung begleicht und damit die Einschaltung eines Dritten abwendet oder nicht. Schließlich ist es auch angesichts der geringen Eingriffstiefe in einer Gesamtschau rechtlich nicht begründbar, aus welchen Gründen in derartigen Fällen die Einbindung eines Rechtsanwalts und eines Inkassounternehmen datenschutzrechtlich differenziert bewertet werden sollte.

9.5 Datenschutzgerechter Einsatz von Messenger-Diensten im Krankenhausbereich

Der Einsatz von Messenger-Diensten ist mittlerweile in allen Lebensbereichen zu einer Selbstverständlichkeit geworden. Krankenhäuser oder andere Einrichtungen in der Gesundheitsversorgung bilden da keine Ausnahme. So ist die Nutzung von WhatsApp in der krankenhausinternen Kommunikation, aber auch einrichtungs- und sektorenübergreifend, leider keine Seltenheit. Soweit dabei patientenbezogene Gesundheitsdaten ausgetauscht werden, wirft die Nutzung von WhatsApp in Krankenhäusern aus verschiedenen Gründen datenschutzrechtliche Fragen auf.

Neben dem rechtlich problematischen Einsatz privater Endgeräte stehen insbesondere das Auslesen der auf dem Endgerät gespeicherten Adressbücher, die Nutzung von nicht näher lokalisierbaren Cloud-Speichern als Back-up-Speicherort sowie die Gefahr, dass vertrauliche Inhalte aus der ärztlichen Kommunikation wie z.B. Röntgen- oder MRT-Bilder in die Mediathek des genutzten (privaten) Smartphones gelangen, im Fokus der datenschutzrechtlichen Kritik. Hinzu kommen noch berufsrechtliche

Fragen z.B. hinsichtlich der Dokumentationspflicht, sofern therapierelevante Informationen über den Messenger ausgetauscht werden.

Angesichts der aufgezeigten Bedenken erklärte sich der LfDI Rheinland-Pfalz Ende 2018 in der von der Datenschutzkonferenz eingerichteten Arbeitsgruppe „Digitalisierung im Gesundheitswesen“ bereit, gemeinsam mit dem niedersächsischen Landesbeauftragten federführend ein Papier zu entwickeln, in dem die technischen Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich zusammengestellt werden. Dadurch soll die Entwicklung von Messenger-Lösungen unterstützt werden, mit denen aus technischer Sicht ein datenschutzgerechter Betrieb überhaupt nur möglich ist.

Angesichts der Komplexität der unterschiedlichen denkbaren Kommunikationsszenarien im ärztlichen Alltag (krankenhausintern, krankenhausübergreifend, sektorenübergreifend, praxisintern, praxisüberreifend, Arzt-Patienten-basiert) und der nur begrenzt zur Verfügung stehenden Ressourcen bei den Datenschutzaufsichtsbehörden fokussierte sich das im Laufe des Jahres 2019 erarbeitete Papier zunächst auf den Einsatz von Messenger-Diensten in der krankenhausinternen Kommunikation zwischen Ärzten. Ein erster Entwurf wurde mit Vertretern der Deutschen Krankenhausgesellschaft, dem Verband der Krankenhausdirektoren Deutschlands, dem Bundesverband der Krankenhaus IT-Leiterinnen /Leiter, der Bundesärztekammer und dem Bundesverband Gesundheit-IT erörtert. Dabei wurde der mit dem Papier verfolgte Ansatz, eine gemeinsam getragene Strategie bei der mobilen Messenger-Kommunikation im Krankenhausbereich zu erreichen, durchweg begrüßt. Es bestand zudem Einigkeit, über das Papier zu den technischen Anforderungen an Messenger-Dienste hinaus, das sich primär an die Hersteller richtet, auch den Krankenhäusern selbst konkrete Handlungsempfehlungen für die beim Einsatz von Messenger-Diensten gebotenen technischen und organisatorischen Vorkehrungen an die Hand zu geben. Diese sollten aus dem Krankenhausbereich selbst entwickelt und mit der Arbeitsgruppe abgestimmt werden.

Die 98. DSK verabschiedete im November 2019 auf der Grundlage des von der Arbeitsgruppe erstellten Entwurfs ein Whitepaper zu den technischen Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich. Zugleich beauftragte die Konferenz die Arbeitsgruppe, in einem sich anschließenden Konsultationsverfahren die bereits zuvor inhaltlich eingebundenen Institutionen zur Kommentierung des Papiers aufzufordern und auf dieser Grundlage Möglichkeiten auszuloten, eine zweite konsolidierte Version zu erstellen. Dabei wird neben den festzulegenden konkreten technischen Anforderungen an Messenger-Dienste insbesondere auch die Frage eine Rolle spielen, ob und ggf. unter welchen Rahmenbedingungen der Einsatz privater mobiler Endgeräte im Krankenhausbetrieb zulässig sein. Die staatlichen Datenschutzaufsichtsbehörden vertreten in diesem Zusammenhang die gleiche Rechtsauffassung: angesichts der hohen Schutzbedürftigkeit der im Krankenhausbetrieb verarbeiteten Daten und der mit einem Einsatz privater Endgeräte verbundenen Gefährdungen des informationellen Selbstbestimmungsrechts verstieße die Nutzung derartiger Geräte gegen die aus der DS-GVO resultierenden Anforderungen an ein von den Verantwortlichen sicherzustellendes angemessenes Datensicherheitsniveau. Vielmehr sind die Krankenhausträger aufgerufen, ihren Mitarbeitern, soweit diese auch Messenger-Dienste zur ärztlichen Kommunikation nutzen dürfen, dienstliche Endgeräte zur Verfügung zu stellen.

9.6 Projekt „Praxistest“ der Initiative „Mit-Sicherheit-gut-behandelt“

Die Umsetzung der aus dem Wirksamwerden der DS-GVO resultierenden datenschutzrechtlichen Vorgaben führte auch im Alltag der rheinland-pfälzischen Arzt- und Psychotherapiepraxen immer wieder zu praktischen Problemen und Handlungsunsicherheiten. Trotz der im Jahre 2018 sehr erfolgreich durchgeführten Informationsveranstaltungen und der permanent aktualisierten Website der Initiative häuften sich sowohl in diesem Zusammenhang stehende Beratungsanfragen als auch beim LfDI eingehende Beschwerden. Aus diesem Grund entschieden sich die Kooperationspartner – dies sind neben dem LfDI auch die Landesärztekammer, die Landespsychotherapeutenkammer sowie die Kassenärztliche Vereinigung Rheinland-Pfalz - Anfang 2019 dafür, zusammen mit zwei Pilotpraxen beispielhafte Musterlösungen im Sinne einer „Best Practice“ zu erarbeiten. Diese sollten sowohl den datenschutzrechtlichen Anforderungen gerecht werden als auch durch die Praxen mit einem angemessenen Aufwand und nachvollziehbar umgesetzt werden können. Ziel des Projektes „Praxistest“ war es, den Praxisinhaberinnen und Praxisinhabern mit unmittelbar von den praktizierenden Berufsangehörigen erstellten und im Praxisalltag erprobten Lösungsansätzen die Gewährleistung des Datenschutzes zu vereinfachen.

Das Projekt startete im März 2019 mit einer Analyse des Umsetzungsstands der DS-GVO in den beteiligten Pilotpraxen. Nach Besuchen der Kooperationspartner vor Ort wurden gemeinsam diverse Mustervorlagen beispielsweise zum Verzeichnis für Verarbeitungstätigkeiten, zu internen Arbeitsvorgaben und zu Einwilligungs- und Schweigepflichtentbindungserklärungen erarbeitet. Im Fokus stand dabei immer, den Praxen soweit wie möglich die Umsetzung des Datenschutzrechts zu erleichtern. Die erarbeiteten Muster wurden im 3. Quartal 2019 von den Pilotpraxen im Hinblick auf ihre Praxistauglichkeit getestet und mit zwei weiteren Arztpraxen inhaltlich abgestimmt. Die Muster wurden Anfang 2020 auf der Website der Initiative veröffentlicht (**http://www.mit-sicherheit-gut-behandelt.de/muster.html**). Es ist geplant, in zwei Veranstaltungen für Ärzte bzw. Psychotherapeuten Mitte 2020 den Einsatz der Muster, aber auch darüber hinausgehende Fragen rund um den Datenschutz im Praxisalltag zu erörtern.

9.7 Meldungen von Datenpannen - der Falschversand patientenbezogener Dokumente ist weit verbreitet

Nach Art. 33 Abs. 1 DS-GVO hat der Verantwortliche nach Bekanntwerden einer Datenschutzverletzung der für ihn zuständigen Aufsichtsbehörde einen Verstoß gegen datenschutzrechtliche Vorgaben zu melden, es sei denn, dieser führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen. Es ist im Kreise der staatlichen Datenschutzaufsichtsbehörden in Deutschland unstrittig, dass bei Verstößen gegen den Schutz von Patientendaten eine Meldepflicht nach Art. 33 Abs. 1 DS-GVO besteht. Denn regelmäßig handelt es sich um Daten nach Art. 9 DS-GVO, die aufgrund der hohen Sensibilität für den Betroffenen einem besonderen Schutzbedarf unterliegen. Für das Bestehen der Meldepflicht ist es deshalb auch unerheblich, ob die Datenschutzverletzung bei Berufsgeheimnisträgern, also z.B. Ärzten oder Psychotherapeuten, oder sonstigen Gesundheitsberufen wie z.B. Physiotherapeuten oder Optikern aufgetreten ist.

Etwa ein Viertel der im Jahre 2019 dem LfDI nach Art. 33 DS-GVO gemeldeten Datenschutzverstöße betrafen den Bereich Gesundheit. Überwiegend lagen den Datenpannen technisch-organisatorische Defizite bei der

Datenverarbeitung wie z.B. die unzureichende Adressierung von Briefen und Telefaxen, Fehler bei der Kuvertierung, der unverschlüsselter Versand elektronischer Nachrichten oder der Verlust von Datenträgern zugrunde. In Krankenhäusern fehlten wiederholt ausreichende organisatorische Vorkehrungen, die derartige Vorkommnisse im Regelfall vermeiden sollten.

Welche Erkenntnisse können aus den gemeldeten Verstößen hinaus generell gezogen werden? Nach Art. 32 DS-GVO obliegt es den Verantwortlichen, geeignete technische sowie organisatorische Maßnahmen zu ergreifen, um denkbaren Datenschutzverletzungen präventiv entgegenzuwirken. Zumindest nach Eintritt einer Datenschutzverletzung müssen derartige Maßnahmen ergriffen oder an bislang nicht berücksichtigte Gefährdungsszenarien angepasst werden. Gerade im Bereich der Übermittlung von Telefaxen, der Kuvertierung ausgehender Post und deren Versand empfiehlt es sich, technische Lösungen wie bspw. die Speicherung von Faxnummern oder eine vollautomatisierte Adressierung zurückzugreifen.

Im Interesse eines funktionierenden Datenschutz-Managements sollten daher die in einem bestimmten Zeitintervall aufgelaufenen Meldungen einrichtungsintern mit dem Ziel ausgewertet werden, ggf. daraus ersichtliches Verbesserungspotential für technisch-organisatorische Maßnahmen zum Schutz der Daten auch tatsächlich zu nutzen. Nachdem die Presse Umfang und Inhalte der seit dem Wirksamwerden der DS-GVO bundesweit gemeldeten Datenschutz-Verstöße bei Einrichtungen des Gesundheitswesens recherchiert und veröffentlicht hatte, nahm der LfDI dies zum Anlass, die Akteure im Gesundheitsbereich zu einem noch sorgfältigeren Umgang mit Patientendaten aufzufordern. Siehe hierzu **https://s.rlp.de/falschversand**

10. SOZIALES

Welche Unterlagen zum Nachweis der Voraussetzungen von Sozialleistungen vorgelegt werden müssen beschäftigt den LfDI bereits seit vielen Jahren (vgl. 25. Tätigkeitsbericht, Tz. 6.2). Datenschutzrechtlich ist dabei zu differenzieren zwischen dem Inhalt und Umfang der gesetzlichen Mitwirkungspflicht der Antragsteller im Rahmen ihrer Beantragung und den der Sozialverwaltung zur Verfügung stehenden Möglichkeiten, für die Antragsbearbeitung erforderliche Unterlagen auch von anderen Stellen der Verwaltung oder von Dritten zu beziehen. Auch im Berichtsjahr erreichten den LfDI immer noch Beschwerden über das Vorgehen einzelner Sozialverwaltungen.

Die datenschutzrechtlichen Rahmenbedingungen sind im Grunde gar nicht so kompliziert: Wer Sozialleistungen beantragt, hat das Vorliegen der Bewilligungsvoraussetzungen darzulegen und in einem angemessenen Umfang nachzuweisen. Dies umfasst auch die Zustimmung zur Erteilung von Auskünften durch Dritte, sofern die Leistungsträger dies verlangen (§ 60 Abs. 1 SGB I). Allerdings ist diese Mitwirkungspflicht der Antragsteller begrenzt: Sie besteht u.a. dann nicht, soweit ihre Erfüllung nicht in einem angemessenen Verhältnis zu der in Anspruch genommenen Sozialleistung steht, ihre Erfüllung dem Betroffenen aus einem wichtigen Grund nicht zugemutet werden kann oder der Leistungsträger sich durch einen geringeren Aufwand als der Antragsteller oder Leistungsberechtigte die erforderlichen Kenntnisse selbst beschaffen kann (§ 65 SGB I). Und nicht zu vergessen: die Sozialbehörden müssen dabei selbstverständlich die Vorgaben des Sozialdatenschutzes, insbesondere die Wahrung des Sozialgeheimnisses (§ 35 SGB I), beachten. Das bedeutet, dass im Rahmen der Bearbeitung von Sozialleistungsanträgen die hierfür erforderlichen Angaben nur auf der Grundlage der gesetzlichen Vorgaben (Art. 6 Abs. 1 lit. e, ggf. Art. 9 DS-GVO i.V.m. §§ 67 ff. SGB X) verarbeitet werden dürfen. Im Ergebnis sollen personenbezogene Informationen über einen möglichen Bezug von Sozialleistungen durch Dritte nur zur Kenntnis genommen werden dürfen, wenn gesetzliche Regelungen dies erlauben oder die Antragsteller damit einverstanden sind.

In der Vergangenheit haben sowohl die Datenschutzaufsichtsbehörden des Bundes und der Länder als auch die Gerichte klargestellt, dass bei der Beantragung von Sozialleistungen sowohl die Mitwirkungspflichten der Antragsteller als auch die Ermittlungsbefugnisse der Sozialbehörden begrenzt sind (vgl. 25. Tätigkeitsbericht, a.a.O. mit weiteren Nachweisen). Dies wird mittlerweile auch von den meisten Sozialverwaltungen in Rheinland-Pfalz beachtet. Klärungsbedarf im Hinblick auf ein datenschutzgerechtes Vorgehen bestand im Berichtszeitraum immer noch bezüglich der Anforderung von Mietbescheinigungen oder Personalausweiskopien sowie der Befugnisse der Sozialbehörden, antragsrelevante Informationen unmittelbar bei Dritten einzuholen.

Mit den Vorgaben des Datenschutzes ist es selbstverständlich vereinbar, wenn die für die einzelnen Sozialleistungen erforderlichen Nachweise wie z.B. ein vollständiger Mietvertrag, aktuelle Verbrauchsabrechnungen, Kontoauszüge, Leistungsbescheide und sonstige Einkommensbelege unmittelbar von den Antragstellern angefordert werden. Dies entspricht dem im Sozialdatenschutzrecht verankerten Grundsatz der direkten Erhebung bei der betroffenen Person (§ 67a Abs. 2 Satz 1 SGB X). Dabei sind die rechtlichen Grenzen der Mitwirkung wie z.B. zeitliche Schranken für die Vorlage von Kontoauszüge oder Schwärzungsrechte zu beachten. Teilweise kann es gesetz-

lich zulässig sein, für die Leistungsgewährung relevante Angaben unmittelbar von Dritten beizuziehen (vgl. u.a. § 60 SGB II, § 117 SGB XII und allgemein § 67a Abs. 2 Satz 2 SGB X). Bei der bloßen Anforderung von Nachweisen ist dagegen § 60 Abs. 1 SGB I zu beachten, d.h. hier bedarf es regelmäßig einer Zustimmung durch den Antragsteller, wenn die Unterlagen unmittelbar von Dritten eingeholt werden sollen.

Den Antragstellern sollte zu Beginn des Verfahrens erläutert werden, welche Angaben und Unterlagen zur Bearbeitung des Leistungsantrags erforderlich sind. Dabei kann es den Betroffenen freigestellt werden, entweder die benötigten Unterlagen selbst beizubringen oder der Sozialbehörde die Einholung von Auskünften oder Nachweisen bei Dritten zu gestatten. Die seitens der Antragsteller zu diesem Zweck zu erteilende Einwilligung muss freiwillig sein, d.h. deren Nichterteilung darf nicht automatisch zur Ablehnung des Leistungsantrags führen. Es empfiehlt sich, zu diesem Zweck Vordrucke einzusetzen, in denen sowohl die erforderlichen Unterlagen benannt als auch die von den Antragstellern möglichen Zustimmungen zur direkten Vorlage durch konkret benannte Dritte erklärt werden. Es empfiehlt sich vor dem Hintergrund der allgemeinen datenschutzrechtlichen Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO, ein solches Vorgehen über eine intern verbindliche Handlungsanweisung dokumentiert vorzugeben.

Mietbescheinigungen, die von Vermietern unterschrieben sind, sollten nur in begründeten Ausnahmefällen angefordert werden, wenn sich aufgrund der bisherigen Angaben und vorgelegten Unterlagen nicht ausräumbare, für die Gewährung der beantragten Sozialleistung aber relevante Unklarheiten ergeben. Denn mit der Unterzeichnung der Bescheinigung wird den Vermietern automatisch der Sozialleistungsbezug ihrer Mieter offenbart. Dies kann den Betroffenen aber im Regelfall nicht zugemutet werden. Die Aufforderung zur Vorlage von Ausweiskopien wie z.B. Personalausweisen ist datenschutzrechtlich zulässig, nicht dagegen die standardmäßige Anforderung von Kopien und deren Ablage in die Verfahrensakte. Diese ist ohne im Einzelfall vorliegende besondere Anhaltspunkte, die zu dokumentieren wären, nicht erforderlich und sollte auch nicht über den Umweg einer Einwilligung erfolgen.

11. KOMMUNALES

11.1 Datenverarbeitung zur Erstellung von Mietspiegeln

Die Aufstellung eines Mietspiegels ist entsprechend § 558 c Abs. 4 S. 1 BGB eine im öffentlichen Interesse liegende Aufgabe bzw. eine Aufgabe der Daseinsvorsorge, die den Kommunen obliegt.

Nach § 22c Sozialgesetzbuch – Zweites Buch sollen die Kreise und kreisfreien Städte zur Bestimmung der angemessenen Aufwendungen für Unterkunft und Heizung insbesondere auch Mietspiegel berücksichtigen.

Mit der Anwendung der DS-GVO sowie der Neufassung des LDSG stellte sich für den LfDI die Frage, ob es zulässig ist, wenn Kreisverwaltungen zur Erfüllung dieser Aufgabe insbesondere auf den Adressbestand von Vermieterinnen und Vermietern des Abfallwirtschaftsbetriebes des Landkreises zurückgreifen und diese Daten zur Durchführung von Befragungen gegebenenfalls auch einem Dienstleister zur Verfügung stellen.

Da diese Daten einem Abfallwirtschaftsbetrieb von den Meldebehörden zweckgebunden lediglich „zur Veranlagung von Abfallentsorgungsgebühren“ zur Verfügung gestellt werden (§ 7 der Meldedatenlandesverordnung, MDLVO), stellt die Erstellung eines Mietspiegels durch die Kreisverwaltung eine Zweckänderung dar, für die entweder einer Einwilligung der betroffenen Personen oder eine Rechtsgrundlage vorhanden sein muss.

Diesbezüglich wurden in der Vergangenheit keine datenschutzrechtlichen Bedenken geäußert, weil das LDSG a.F. eine Zweckänderungsregelung vorsah. Auf der Grundlage von § 32 LDSG aF. war eine Zweckänderung der für die Aufgabenerledigung des Abfallwirtschaftsbetriebes erhobenen Daten gemäß § 13 Abs. 2 LDSG für die Erstellung eines Mietspiegels zulässig.

Da eine vergleichbare Vorschrift im LDSG RP n.F. nicht mehr vorhanden ist, steht einem solchen Anliegen nun § 41 BMG entgegenstehen. Nach dieser Vorschrift dürfen Datenempfänger (also die Abfallwirtschaftsbetriebe) die Daten und Hinweise, soweit gesetzlich nichts anderes bestimmt ist, nur für die Zwecke verarbeiten oder nutzen, zu deren Erfüllung sie ihnen übermittelt oder weitergegeben wurden.

Auch eine sog. Vereinbarkeitsprüfung gemäß Art. 6 Abs. 4 DS-GVO im Hinblick auf die Recht-fertigung einer zweckändernden Weiterverarbeitung führt zu keinem anderen Ergebnis (vgl. Datenschutzbericht 2018, III-13.2, S. 62).

Gegenüber verschiedenen Kreisverwaltungen, die den LfDI in diesem Zusammenhang um Beratung bzw. Stellungnahme gebeten hatten, erging dann folgender Hinweis gemäß Art. 58 Abs. 1 lit. d DS-GVO:

Unter Beachtung des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) können zur Erfüllung der oben genannten Aufgabe die Grundsteuerstellen kreisangehöriger Gemeinden gem. Art. 6 Abs. 1 lit. e, Abs. 2 und Abs. 3 DS-GVO i.V.m. § 3 LDSG um die Übermittlung von entsprechenden personenbezogenen Daten privater Vermieterinnen und Vermieter (§ 31 Abs. 3 AO) zusätzlich zu institutionellen Vermietern ersucht werden. Gegebenenfalls ist eine Stichprobe ausreichend. Auf § 5 Abs. 1 S. 2, 3 LDSG wird verwiesen.

Mit diesen Daten verschickt die Kreisverwaltung das Informationsmaterial zur Erstellung

eines Mietspiegels mitsamt den Fragebögen an die Vermieterinnen und Vermieter, die wiederum die – ohne personenbezogene Daten - ausgefüllten Fragebögen an ein beauftragtes Unternehmen oder die Behörde senden. Andere Vorgehensweisen sind möglich.

Sofern zu dem oben genannten Zweck zusätzlich noch eine Befragung von Mieterinnen und Mietern, die unter den Anschriften der in eine Stichprobe aufgenommenen Objekte gemeldet sind, notwendig und seitens der Kreisverwaltung dafür die Erhebung von personenbezogenen Daten erforderlich sein sollte, könnte unter Beachtung des Grundsatzes der Datenminimierung eine Gruppenauskunft gemäß § 34 Abs. 2 BMG oder eine Gruppenabfrage im automatisierten Abruf gemäß § 14 Abs. 7 MDLVO in Frage kommen. Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt die abrufende Stelle (§ 14 Abs. 4 S. 2 MDLVO).

11.2 Örtliche Datenschutzprüfungen in Kommunalverwaltungen des Landes Rheinland-Pfalz

Der LfDI ist Aufsichtsbehörde und kontrolliert in dieser Funktion die Einhaltung der Vorschriften der Datenschutz-Grundverordnung, des Bundesdatenschutzgesetzes, des Landesdatenschutzgesetzes Rheinland-Pfalz und anderer datenschutzrechtlicher Bestimmungen.

Er kann bei Verstößen gegen datenschutzrechtliche Bestimmungen unter anderem Verwarnungen aussprechen, Anweisungen verschiedener Art erteilen und dabei letztlich auch den Einsatz einzelner Verfahren gänzlich untersagen.

Um seine Aufgaben erfüllen zu können, verfügt der LfDI über verschiedene Befugnisse. Neben weiteren ihm zustehenden Untersuchungsbefugnissen kann er örtliche Kontrollen auf der Grundlage von § 16 Abs. 1 und § 17 Abs. 3 LDSG i.V.m. den Art. 57 und 58 DS-GVO durchführen.

Im Herbst 2019 hat der LfDI mit einer umfangreichen Prüfphase von Kommunalverwaltungen begonnen. In 2019 wurden zwei Verbandsgemeindeverwaltungen geprüft, weitere zehn Prüfungen (hierunter auch mehrere Kreisverwaltungen) sind für das Kalenderjahr 2020 vorgesehen. Etwa vier Wochen vor einem Prüfungstermin werden die betreffenden Kommunen angeschrieben und – neben der Mitteilung des Prüfungstermins – um die Übersendung verschiedener Unterlagen gebeten.

Dies sind unter anderem:

- alle Dienstanweisungen bzw. –vereinbarungen dieser Verwaltung zum Datenschutz.
- Verzeichnis von Verarbeitungstätigkeiten
- Übersicht zu den Verarbeitungstätigkeiten, zu denen Informationen nach Art. 13 DS-GVO vorhanden sind.
- Aufstellung der Verträge zur Auftragsdatenverarbeitung (Artikel 28 Abs. 3 DS-GVO)
- Übersicht über die eingesetzten IT-Verfahren inklusive eines Netzwerkplans

Die bisherigen Prüfungen waren für alle Beteiligten sehr aufschlussreich. Gerade in den Vorstellungs- und Abschlussgesprächen mit der jeweiligen Behördenleitung konnten die Mitarbeiter des LfDI hilfreich beraten und individuelle Fragen beantworten und somit wirksam aufklären.

Es hat sich deutlich gezeigt, dass noch große Schwierigkeiten in der Umsetzung der Daten-

schutz-Grundverordnung in den Bereichen des technisch-organisatorischen Datenschutzes und der Datenschutz-Folgenabschätzung liegen. Ergebnisse der Prüfungen und daraus gezogene Schlüsse wird der Datenschutzbericht 2020 enthalten

11.3 Zweckverbände als Verantwortliche im öffentlichen Bereich identifiziert – nächster Schritt: Benennung eines/einer Datenschutzbeauftragten

Im September 2019 wurden erstmals die in Rheinland-Pfalz bestehenden Zweckverbände angeschrieben. Nach dem Landesgesetz über die kommunale Zusammenarbeit (KomZG) ist ein Zweckverband eine Körperschaft des öffentlichen Rechts und somit eine öffentliche Stelle (§ 2 Abs. 1 LDSG). Ein Zweckverband ist berechtigt, Beamte zu haben und darf Aufgaben für kommunale Gebietskörperschaften wahrnehmen.

Vorrangig ging es bei der Umfrage darum, inwiefern die Pflicht aus Art. 37 Abs. 1 lit. a DS-GVO erfüllt wurde, eine bzw. einen Datenschutzbeauftragte/n zu benennen.

Die 363 angeschriebenen Zweckverbände in Rheinland-Pfalz können insbesondere folgenden Bereichen zugeordnet werden:

1. Kindergarten	85
2. Wasser/Abwasser	70
3. Forst	61
4. Entwicklung/Planung	60
5. Fremdenverkehr	33

Erst 10 Zweckverbände hatten bis zur Umfrage einen Datenschutzbeauftragten gemeldet. Anlässlich dieser Umfrage haben 203 Zweckverbände erstmalig den Datenschutzbeauftragten gemeldet.

Weitere Verantwortliche teilten mit, die Pflicht zur Benennung erst rechtlich prüfen zu wollen.

Hauptargumente der Zweckverbände, die keine Pflicht zur Benennung eines Datenschutzbeauftragten erkennen wollten, sind, dass sie keine eigenen Aufgaben wahrnehmen und/oder dass sie kein eigenes Personal beschäftigen. So wurde auch öfters angemerkt, dass man nur ein Gebäude z.B. eines Kindergarten verwaltet. Die Ausstattung mit Personal spielt in diesem Zusammenhang aber nur eine untergeordnete Rolle. Maßgeblich ist dagegen, dass überhaupt personenbezogene Daten verarbeitet werden.

Selbstverständlich ist dem LfDI auch bewusst, dass bei einem Zweckverband, der weder eigene Aufgaben wahrnimmt noch eigenes Personal beschäftigt, die Aufgaben eines behördlichen Datenschutzbeauftragten sich im überschaubaren Rahmen halten. In diesen Fällen bietet es sich an, die gesetzliche Notwendigkeit zur Benennung eines Datenschutzbeauftragten über verschiedene Möglichkeiten der Kooperation zwischen öffentlichen Stellen zu erfüllen (Art. 37 Abs. 3 DS-GVO).

Von zahlreichen Zweckverbänden steht eine Benennung noch aus, d.h. die Maßnahme ist noch nicht abgeschlossen.

11.4 Regionaltreffen mit den behördlichen Datenschutzbeauftragten

Die Reihe an Informationsveranstaltungen wird fortgesetzt (siehe 26. Datenschutzbericht

2016/2017, S. 111). So lud der LfDI am 22. Oktober 2019 in den historischen Rathaussaal der Stadtverwaltung Koblenz ein.

Über 70 Datenschutzbeauftragte aus den rheinland-pfälzischen Gemeinden, Städten und Landkreisen waren der Einladung gefolgt und zu einer Schulung sowie einem regen Gedankenaustausch über den kommunalen Datenschutz zusammengekommen.

Vielfältige Themengebiete, die die behördlichen Datenschutzbeauftragten in der Praxis beschäftigen, wurden angesprochen wie die Vorgehensweise bei Auskunftsanträgen nach Art. 15 DS–GVO und die Erstellung von Verarbeitungsverzeichnissen nach Art. 30 DS-GVO. Den Teilnehmer wurde der Ablauf von Beschwerdeverfahren beim LfDI bis hin zur Ausübung der Befugnisse anhand von Beispielen aus der täglichen Arbeit geschildert.

Die Veranstaltung gab den Teilnehmer Gelegenheit, Erfahrungen mit verschiedenen datenschutzrechtlichen Sachverhalten aus der Praxis auszutauschen. Mit dieser Veranstaltung wurden die guten Kontakte zu den kommunalen Datenschutzbeauftragten gepflegt und weiter ausgebaut. Der Austausch wird von den kommunalen Datenschutzbeauftragten begrüßt und vom LfDI auch in Zukunft weiter regelmäßig angeboten.

Weitere Informationsveranstaltungen in 2020 werden folgen. Thematisch wird der Schwerpunkt dann noch stärker auf Informationen zur praktischen Anwendung der DS-GVO liegen.

12. MEDIENBILDUNG UND SCHULE

12.1 Digitalpakt

Im Berichtszeitraum war die Verteilung der Gelder aus dem Digitalpakt Gegenstand bildungspolitischer Diskussion. Der LfDI hat sich wiederholt gegenüber dem Ministerium für Bildung dafür ausgesprochen, dass in den Förderrichtlinien für die Verteilung der Gelder aus dem Digitalpakt (rund 240 Mio. Euro für Rheinland-Pfalz) auch Konzepte zur Förderung von Medien- und Datenschutzkompetenzen berücksichtigt werden sollten und nicht nur eine bessere Hardware-Ausstattung der Schulen im Vordergrund steht. Am 26. Juli 2019 veröffentlichte das Ministerium für Bildung die Richtlinie zur Umsetzung des Digitalpaktes Schule. Unter Ziff. 7.2 wird die Förderung u.a. von der Vorlage eines Medienbildungskonzeptes sowie einer bedarfsgerechten Fortbildungsplanung abhängig gemacht. Dies ist aus datenschutz- und medienpädagogischer Sicht zu unterstützen. Die Leiterinnen und Leiter kommunaler Medienzentren können die Schulen bei der Erarbeitung der geforderten Medienkonzepte unterstützen.

12.2 Auswirkungen der DS-GVO

Den Schulen und Kindertagesstätten im Land wurde „der Übergang“ in die DS-GVO mit zahlreichen Informationen, Mustertexten und Handreichungen erleichtert, die gemeinsam mit dem Bildungsministerium erstellt und pünktlich mit Wirksamwerden der DS-GVO zur Verfügung gestellt wurden. In keinem anderen Bundesland wurde ein derartiges umfangreiches und praxisnahes „Rund-um-sorglos-Paket“ von Seiten einer Datenschutz-Aufsichts-

behörde für Schulen und Kitas geschnürt, wie dies in Rheinland-Pfalz der Fall war.

Mit Blick auf die erweiterten Sanktionsmöglichkeiten des LfDI ist gleichwohl der Beratungsbedarf von Bildungseinrichtungen deutlich angestiegen. Zu nahezu jeder am Markt erhältlichen (Bildungs-)Software gehen Anfragen ein, ob gegen deren Anschaffung datenschutzrechtliche Bedenken bestünden. Aus tatsächlichen und rechtlichen Gründen ist es dem LfDI jedoch grundsätzlich nicht möglich, Softwareanwendungen auf ihre Datenschutzkonformität hin zu überprüfen. Denn zum einen kommt es stets auf das tatsächliche Einsatzszenario an, zum anderen kann mit einem einzigen Software-Update eine datenschutzrechtliche Einschätzung wieder obsolet werden. Der LfDI beschränkt sich daher auf allgemeine Datenschutzhinweise, die es dem Verantwortlichen (hier also der Schule) ermöglichen sollen, über die Zulässigkeit einer Verwendung von Software-Produkten selbst zu entscheiden.

Einen weiteren Schwerpunkt der Anfragen bildet das Thema „Recht am eignen Bild“. Auch hierzu wurde umfangreiches Material veröffentlicht. Hervorzuheben ist das Erklärvideo (https://s.rlp.de/rechtameigenenbild), in dem die Thematik anschaulich vermittelt wird. Ein Flyer, der sich an die Zielgruppe „Jugendliche“ richtet, wird im kommenden Jahr veröffentlicht.

Auf der Basis seiner neuen sanktionsrechtlichen Möglichkeiten musste der LfDI erstmals eine Anordnung zur Löschung von Videoaufnahmen treffen: Eine Kita hatte ohne die erforderliche Einwilligung der Eltern Videoaufnahmen für die Bildungs- und Lerndokumentation der Kinder (sogenannte Portfolio-Arbeit) gemacht. Die Kita kam der Anordnung nach, was jedoch mit einem erheblichen Aufwand verbunden war.

12.3 Schüler-Workshop-Projekt

Mit über 500 Workshops konnte auch im Jahr 2019 das hohe Niveau der Vorjahre gehalten werden. Seit Beginn des Projekts im Jahr 2010 wurden damit insgesamt 4.605 Workshops mit einem jährlichen Gesamtvolumen von über 100.000 Euro erfolgreich durchgeführt. Dank der großzügigen Unterstützung des Verbraucherschutzministeriums war es auch im Berichtsjahr möglich, diesen wichtigen Beitrag zur Digitalen Bildung fortzuführen und weiterzuentwickeln. Anlässlich des 4000. Schüler-Workshops besuchten am 10.1.2019 Frau Verbraucherschutzstaatssekretärin Dr. Christiane Rohleder und der LfDI die 3. Klasse einer Mainzer Grundschule und zeigten sich überrascht, welche technischen Kenntnisse bei den jüngsten Onlinern bereits vorhanden waren. Gerade hier setzen die Schüler-Workshops an und vermitteln mit den eigens geschulten Referentinnen und Referenten aus erster Hand eine digitale Grundbildung, die die Risiken und Gefahren der Internetnutzung verdeutlicht. Die Themen werden kontinuierlich an die aktuellen Entwicklungen angepasst; beispielsweise wurden digitale Sprachassistenten, das Recht am eigenen Bild, sichere Handynutzung und die Überwachungsmethoden in China als neue Workshop-Themen aufgenommen. Dadurch, dass es zwischenzeitlich gelungen ist, eine medienpädagogische Stelle im Haushalt des LfDI zu verankern, ist die Kontinuität der zahlreichen Bildungsaktivitäten des LfDI auch künftig sichergestellt.

12.4 Elternabende für Kitas

Um den Beratungsbedarf von Kitas und Eltern besser bewältigen zu können, werden seit 2019 auch Elternabende angeboten, die von den Referentinnen und Referenten der Schüler-Workshops durchgeführt werden. Für die ca. 2.500

Kitas im Land besteht nunmehr die Möglichkeit, sich gemeinsam mit den Eltern zu ausgewählten Themen der Medienkompetenz informieren zu lassen. Gemeinsam mit dem Verbraucherschutzministerium und der Verbraucherzentrale Rheinland-Pfalz gelang es, Elternthemenabende auf der Basis eines pädagogischen Konzeptes zu entwickeln. Unter dem Motto „Kinder im Netz begleiten“ können Eltern bzw. Kitas je nach Bedarf zwischen verschiedenen Themen des Verbraucherschutzes (z.B. Smartphones und Apps als Kostenfallen) und Datenschutzthemen (z.B. GPS-Ortung von Kindern, Veröffentlichung von Kinderfotos im Internet) wählen und bequem mithilfe eines Online-Formulars beantragen. Ein entsprechendes Formular sowie weiteres Informationsmaterial ist auf der Homepage des LfDI unter https://s.rlp.de/kitaelternabende veröffentlicht.

12.5 Neue Regelungen im Schulgesetz

Die im künftigen Schulgesetz vorgesehene verpflichtende Nutzung einer neuen zentralen Schulverwaltungssoftware für alle Schulen im Land hat bereits im Vorfeld für zahlreiche Anfragen gesorgt. Mit den Verantwortlichen des Bildungsministeriums wurde eine Datenschutz-Folgenabschätzung, wie sie die DS-GVO für Verfahren dieser Art fordert, gemeinsam durchgeführt. Die Schulen müssen diese umfangreiche Prüfung der rechtlichen und technischen Gegebenheiten somit nicht mehr vornehmen.

Zu begrüßen ist eine neue Regelung im Schulgesetz, wonach bei Bild- und Tonaufnahmen des Unterrichts die bisherige Widerspruchsmöglichkeit der Eltern durch ein Einwilligungserfordernis ersetzt wird (§ 67 Abs. 4 n.F. SchulG). Dies entspricht den Regelungen der DS-GVO, wonach bei Einwilligungen eine „eindeutige bestätigende Handlung“ zu fordern ist (EG 32).

Was Regelungen zu digitalen Lehr- und Lernmittel angeht, ist auf die Beschlüsse der Kultusministerkonferenz aus dem Jahr 2016 zur „Bildung in der digitalen Welt“ (s. 26. Tätigkeitsbericht 2016/2017, Tz. 8.2) einerseits und der Datenschutzkonferenz vom Dezember 2018 andererseits zu verweisen, in dem den Kultusministerien ein Formulierungsvorschlag für etwaige gesetzliche Ausgestaltungen von digitalen Lehr- und Lernmitteln gemacht wird. Dieser lautet:

„Die Schule darf für den Einsatz digitaler Lehr- und Lernmittel personenbezogene Daten der Schülerinnen und Schüler, der Lehrkräfte und der Erziehungsberechtigten verarbeiten, soweit dies für die Aufgaben der Schule erforderlich ist. Besonders sind dabei die Anforderungen der Art. 5, 24, 25 und 32 DS-GVO zu beachten.“

Im neuen Schulgesetz findet sich eine etwas andere Formulierung, die aus Sicht des LfDI aber ebenfalls akzeptabel ist. Hiernach sind digitale Lehr- und Lernsysteme sowie Netzwerke „regulärer Bestandteil der Erziehungs- und Unterrichtsarbeit“ (§ 1 Abs. 6 SchulG n.F.). In § 67 Abs. 8 n.F. soll eine Verordnungsermächtigung aufgenommen werden, so dass insb. die Frage der Freiwilligkeit, der Nutzung privater Endgeräte durch Schülerinnen und Schüler sowie technisch-organisatorischer Datenschutzfragen untergesetzlich konkretisiert werden können.

In diesem Kontext war auch die neu aufgesetzte Lernplattform „Moodle@RLP“ Gegenstand von Beratungen durch den LfDI. Im Gegensatz zu früheren Versionen unterstützt das neue Moodle die Bedienung über eine App und kann ortsunabhängig auf mobilen Endgeräten genutzt werden. Virtuelle Lehrerzimmer, virtuelle Klassenzimmer, elektronische Vertretungspläne u.v.m. sollen die schulische Kommunikation sowie die Schul- und Unterrichtsorganisation

erleichtern. Moodle soll auch integraler Bestandteil des Schulcampus als künftige Bildungscloud für rheinland-pfälzische Schulen sein. Schwerpunktmäßig ging es bei der datenschutzrechtlichen Beratung um die Frage der freiwilligen Nutzung, um Verantwortlichkeiten nach der DS-GVO sowie um technisch-organisatorischer Fragen zur Datensicherheit, insb. zur Trennung zwischen Schulverwaltungsdaten und pädagogischem Netzwerk. Grundlage der Beratung waren dabei die Anforderungen, die der LfDI in seinem 26. Tätigkeitsbericht 2017/2017 unter Tz. 7.1.1 veröffentlicht hat.

12.6 Zusammenarbeit mit dem zentralen schulischen Datenschutzbeauftragten der Grundschulen

Bereits im 27. Tätigkeitsbericht 2018 wurde unter Tz. 12.2 über die neue Stelle eines zentralen schulischen Datenschutzbeauftragten für kleinere Grundschulen bei der ADD berichtet. Die Zusammenarbeit mit diesem gestaltete sich im Berichtszeitraum sehr erfolgreich: Handreichungen zu technisch-organisatorischen Datensicherheitsmaßnahmen, zum Verzeichnis der Verarbeitungstätigkeiten, zur Schulhomepage sowie zur Nutzung privater Endgeräte durch Lehrkräfte wurden nach Abstimmung mit dem LfDI den Grundschulen, aber auch sonstigen anfragenden Schulen vom zentralen schulischen Datenschutzbeauftragten zur Verfügung gestellt. Gleichzeitig trat in Bezug auf die Beratungstätigkeit des LfDI die erhoffte Entlastung von Anfragen aus dem schulischen Kontext ein.

13. MELDEWESEN

13.1 Übermittlung von Gesamteinwohnerlisten an Ortsbürgermeisterinnen und Ortsbürgermeister

Immer wieder beschweren sich Ortsbürgermeisterinnen und Ortsbürgermeister beim LfDI darüber, dass sie seitens der Meldeämter keine regelmäßigen Einwohnerlisten (mehr) erhalten. Im Rahmen einer datenschutzrechtlichen Bewertung ist zu unterscheiden, ob die Daten einmalig oder regelmäßig übermittelt werden sollen. In meinem 26. Datenschutzbericht 2016/2017 habe ich mich unter Tz. 9.2.2 bereits in diesem Sinne zu entsprechenden Datenweitergaben an Ortsvorsteherinnen und Ortsvorsteher geäußert.

Sollen die Daten nur einmalig übermittelt werden, sind die Voraussetzungen des § 34 BMG zu prüfen. Hierbei spielt insbesondere eine Rolle, inwieweit die von den Ortsbürgermeisterinnen und Ortsbürgermeister vorgetragenen Gründe einer Aufgabenerfüllung im Bereich der freiwilligen kommunalen Selbstverwaltung entsprechen und die erbetene Datenübermittlung zur Erfüllung dieser Aufgaben auch erforderlich ist. Soweit dies bejaht werden kann, ist zudem zu prüfen und abzuwägen, ob die schutzwürdigen Interessen der betroffenen Personen durch die Datenübermittlung beeinträchtigt würden (§ 8 BMG). Dies wäre zum Beispiel grundsätzlich der Fall, wenn für die betroffene Person eine Auskunftssperre nach § 51 BMG im Melderegister eingetragen wäre. Wurde hinsichtlich der Übermittlung von Alters- oder Ehejubiläumsdaten widersprochen (§ 50 Abs. 2 und Abs. 4 BMG), müsste dieser Widerspruch auch bei einer Übermittlung nach § 34 BMG beachtet werden.

Handelt es sich hingegen um regelmäßige Datenübermittlungen, die ohne Ersuchen in allgemein bestimmten Fällen regelmäßig wiederkehrend durchgeführt werden, ist § 36 BMG einschlägig. Dies bedeutet, dass für regelmäßige Datenübermittlungen eine Rechtsgrundlage vorhanden sein muss. Diese besteht ausschließlich im Rahmen des § 10 Meldedatenlandesverordnung (MDLVO). Hier findet sich in § 10 Abs. 1 MDLVO eine abschließende Regelung zur regelmäßigen Übermittlung von Daten anlässlich von Alters- und Ehejubiläen an die Ortsgemeinden.

Eine regelmäßige Datenübermittlung anlässlich von Zuzügen (Anmeldungen) an die Ortsgemeinden ist in § 10 Abs. 3 MDLVO geregelt. Diese Regelung erfasst allerdings keine Wegzüge (Abmeldungen).

Bezüglich der begehrten Übermittlungen von Gesamteinwohnerlisten, die ohne Ersuchen regelmäßig wiederkehrend durchgeführt werden sollen, ist demnach eine rechtliche Grundlage weder in der MDLVO noch im BMG ersichtlich.

Für eine regelmäßige Übermittlung von gesamten aktuellen Einwohnerlisten müsste daher eine gesonderte Rechtsgrundlage erst noch geschaffen werden. Diesbezüglich bestehen jedoch Zweifel an einer Erforderlichkeit für die Aufgabenerfüllung der Ortsgemeinden.

Die Datenschutzkonferenz hat derzeit keinen Arbeitskreis für melderechtliche Fragen gebildet, so dass diese und andere praxisrelevante Fragen im Kollegenkreis leider nicht erörtert werden können. Da es in erster Linie um die Anwendung eines Bundesgesetzes geht, wären hier einheitliche Positionen sicherlich leichter zu erreichen, als dies bei der Anwendung unterschiedlicher landesrechtlicher Regelungen der Fall ist.

13.2 „Ich weiß, wo du wohnst“ - einfach so zulässig?

Viele Beschwerdeführer/-Innen verstehen die Welt nicht mehr, wenn sie erfahren, dass im Wege einer sogenannten einfachen Melderegisterauskunft nach § 44 Abs. 1 BMG ihre Adressdaten an anfragende Personen oder Stellen „einfach so“ herausgegeben werden dürfen, und zwar ohne dass hierfür besondere Voraussetzungen, wie etwa eine Einwilligungserklärung, erfüllt sein müssen. Tatsächlich können sogar eine Vielzahl namentlich bezeichneter Personen angefragt werden (§ 44 Abs. 2 BMG). Lediglich dann, wenn die Meldedaten für Werbezwecke oder den Adresshandel verwendet werden sollen, ist eine Einwilligung der betroffenen Personen erforderlich. Eine kleine Hürde stellt allenfalls § 8 BMG für eine Beauskunftung dar. Hiernach dürfen schutzwürdige Interessen einer betroffenen Person durch eine Datenübermittlung durch das Meldeamt nicht beeinträchtigt werden. Hat die Behörde aber keine Hinweise, dass dies der Fall sein könnte, kann sie – ohne Nachfrage bei der betroffenen Person – die Auskunft gegen eine Gebühr erteilen. Ob man diese Praxis im Ergebnis als „gebührenpflichtige Amtshandlung“ oder als „Verkauf von Meldedaten“ bezeichnet, liegt im Auge des Betrachters.

Die Kritik der Beschwerdeführer/-innen, was die Zulässigkeit einer diesbezüglichen Auskunftserteilung durch Meldebehörden angeht, ist für den LfDI gut nachzuvollziehen. Die Datenschutzkonferenz hat sich in den vergangenen Jahren wiederholt gegenüber dem Gesetzgeber für restriktivere Bestimmungen im Bereich des Meldewesens eingesetzt (Entschließung vom 22.8.2012: **https://s.rlp.de/entschliessungdsk2012**).

Tatsächlich wurden die Abrufmöglichkeiten im Wege eines Online-Zugriffs für öffentliche und private Stellen jedoch erheblich ausgeweitet,

auch was überregionale Auskünfte über die Landesgrenzen hinaus angeht.

Ebenfalls wurde die Forderung der Datenschutzaufsichtsbehörden nicht aufgegriffen, die Weitergabe von Alters- und Ehejubiläumsdaten an die Presse einschließlich deren Veröffentlichung im Internet von einer ausdrücklichen Einwilligungserklärung des Betroffenen abhängig zu machen. Gegenwärtig können Betroffene einer diesbezüglichen Datenweitergabe lediglich widersprechen. Eine Nichtausübung des Widerspruchs führt hier zu einer Datenübermittlung, auch wenn die betroffenen Personen gar keine Kenntnis über ihre Widerspruchsmöglichkeit haben. Auch bei anderen Datenweitergaben der Meldeämter besteht lediglich eine Widerspruchsmöglichkeit (bspw. im Zusammenhang mit Wahlwerbung, Werbung für die Bundeswehr, Adressbuchverlagen oder Religionsgesellschaften).

Im Berichtszeitraum haben nicht zuletzt politisch motivierte Anschläge auf Kommunalpolitiker dazu geführt, dass zumindest im Zusammenhang mit der Erteilung einfacher Melderegisterauskünfte die Anforderungen verschärft werden sollen. Das rheinland-pfälzische Innenministerium stellte Überlegungen an, im Bundesrat einen entsprechenden Änderungsentwurf zum Bundesmeldegesetz einzubringen. Das Bundesministerium des Innern, für Bau und Heimat hatte dann jedoch eine Änderung von § 51 Bundesmeldegesetz (BMG) angekündigt und daraufhin das Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität auf den Weg gebracht. Damit wird § 51 Abs. 1 BMG dahingehend erweitert, dass ein schutzwürdiges Interesse insbesondere der Schutz der betroffenen oder einer anderen Person vor Bedrohungen, Beleidigungen sowie unbefugten Nachstellungen ist. Bei der Feststellung, ob Tatsachen im Sinne des § 51 Abs. 1 Satzes 1 BMG vorliegen, ist auch zu berücksichtigen, ob die betroffene oder eine andere Person einem Personenkreis angehört, der sich auf Grund seiner beruflichen oder ehrenamtlich ausgeübten Tätigkeit allgemein in verstärktem Maße Anfeindungen oder sonstigen Angriffen ausgesetzt sieht. Der LfDI hält die gegenwärtigen Regelungen für die Weitergabe von Adressdaten für dringend korrekturbedürftig. Es kann nicht sein, dass man für Auskünfte aus öffentlichen Registern regelmäßig zumindest ein „berechtigtes Interesse“ oder gar ein „rechtliches Interesse“ darlegen muss (z.B. Gewerberegister, Handelsregister, Fahrzeugregister) und bei so schützenswerten Daten, wie der Wohnanschrift, aber nahezu voraussetzungslos eine Auskunft erhält.

14. VERWALTUNG DIGITAL

Das Landeshauptarchiv trat 2017 mit der Erwägung an den LfDI heran, die in der Benutzung stark nachgefragten Zweitschriften des Personenstandsarchivs zu digitalisieren und damit zu schonen und beabsichtigte, mit dieser Tätigkeit einen externen bzw. kommerziellen Dienstleister zu beauftragen. Im Datenschutzbericht 2016/2017 (IV-14.3) wurde die datenschutzrechtliche Bewertung der damals beabsichtigten Vorgehensweise wiedergegeben.

Der LfDI kam zu dem Ergebnis, dass dies mit der aktuellen Rechtslage nicht vereinbar wäre, insbesondere weil auch für die Nutzung von Archivgut nach Ablauf der Sperrfrist ein berechtigtes Interesse dargelegt werden muss (§ 3 Abs. 1 S. 1 LArchG) und eine Nutzung von der Archivverwaltung im Einzelfall einzuschränken oder zu versagen ist, wenn u.a. Grund zu der Annahme besteht, dass schutzwürdige Belange Betroffener oder Dritter entgegenstehen (§ 3 Abs. 2 Nr. 2 LArchG). Denn in solchen Registern können auch nach Ablauf der Sperrfrist noch Daten von lebenden, natürlichen Personen enthalten sein und es können aus bestimmten Merkmalen zusätzlich familiäre Zusammenhänge erschlossen werden.

Das Landeshauptarchiv trat nach diesem negativen Votum mit einer veränderten Vorgehensweise an den LfDI heran. Im Gegensatz zu der 2017 skizzierten Vorgehensweise ist nun geplant, dass Personenstandsunterlagen, für die die Sperrfristen abgelaufen sind, von Hilfskräften in den Räumlichkeiten des Landeshauptarchiv gescannt und die hergestellten Digitalisate bzw. Indices vor der Nutzung von qualifizierten Mitarbeitern des Landeshauptarchives komplett gesichtet und soweit notwendig „geschwärzt“ werden im Sinne einer irreversiblen Tilgung bzw. anonymisiert werden. Die zur Herstellung der Digitalisate auf diese Weise anfallenden Kosten sollen von dem externen bzw. kommerziell tätigen Unternehmen (mit)finanziert werden, bevor eine Nutzung der Digitalisate im Rahmen eines Geschäftsmodells erfolgen kann.

Eine erneute datenschutzrechtliche Beurteilung durch den LfDI ergab gerade im Hinblick auf den oben zu § 3 Abs. 1 S. 1, Abs. 2 Nr. 2 LArchG geltend gemachten Einwand, dass in der „körperlichen“ Herstellung der Digitalisate in den Räumlichkeiten des Landeshauptarchivs, verbunden mit einer inhaltlichen Sichtung und gegebenenfalls einer Schwärzung von Daten, eine Einzelfallprüfung im Sinne von § 3 Abs. 2 Nr. 2 LArchG vor einer Nutzung digitalisierter Personenstandsunterlagen gesehen werden kann.

Zusätzlich zu erfolgten Schwärzungen wird der Schutz von Persönlichkeitsrechten durch die Herausgabe von Personenstandsregistern erst nach Ablauf der gesetzlichen Sperrfrist zuzüglich eines „Zeit-Puffers“ gestärkt.

Außerdem war im Rahmen der datenschutzrechtlichen Bewertung zu berücksichtigen, dass die Gewichtung der gegenüberstehenden Interessen in der Abwägung vor und nach Ablauf der Sperrfristen unterschiedlich ist. Vor Ablauf der Schutzfrist überwiegt das Geheimhaltungsinteresse des Staates, d.h., die schutzwürdigen Interessen betroffener Personen gehen dem Interesse der Allgemeinheit auf Informationszugang im Zweifel vor. Nach diesem Zeitpunkt erhält jedoch das Interesse auf Einsichtnahme ein höheres Gewicht.

Das jetzt positiv ausfallende Votum des LfDI beinhaltete auch ergänzende Empfehlungen, vertraglich wenn möglich einen Abgleich der Digitalisate mit anderen Datenbeständen auszuschließen oder eine Befristung der Laufzeit vorzusehen. Eine solche Vertragsregelung kann

als Maßnahme zur Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen gesehen werden.

15. ZERTIFIZIERUNG

15.1 Entwurf einer Kooperationsvereibarung

Der LfDI hat auch im Jahr 2019 am Arbeitskreis Zertifizierung (AK Zertifizierung) teilgenommen. Im Jahr 2019 war es dessen Kernaufgabe, die Grundlagen der Zusammenarbeit zwischen den deutschen Datenschutzaufsichtsbehörden und der Deutschen Akkreditierungsstelle GmbH (DAkkS) gemäß Art. 42 und 43 DS-GVO zu erarbeiten. Hierzu hat der Arbeitskreis zusammen der DAkkS eine Kooperationsvereinbarung über die Akkreditierung von Zertifizierungsstellen nach Art. 43 DS-GVO entworfen. Mit der Kooperationsvereinbarung wird im Wesentlichen festgelegt, dass die DAkkS die Akkreditierung von Zertifizierungsstellen im Einvernehmen mit den Aufsichtsbehörden durchführt, die Aufsichtsbehörden im Rahmen der Akkreditierung die Begutachtung gemeinsam mit der DAkkS durchführen, an der Akkreditierungsentscheidung mitwirken, Mitglieder für den Akkreditierungsausschuss stellen sowie Vertreter in das relevante Sektorkomitee der DAkkS entsenden können, um die Fachkunde sicherzustellen. Die Vereinbarung enthält auch grundsätzliche Regelungen für die Zusammenarbeit zwischen der DAkkS und den Aufsichtsbehörden und stellt klar, dass Genehmigungen von Zertifizierungskriterien nach Art. 42 Abs. 5 DS-GVO deutschlandweit gelten. Sie enthält auch die Möglichkeit des freiwilligen Austausches von Begutachtern, wenn aufgrund erhöhter Antragszahlen personelle Engpässe entstünden.

15.2 Einreichung von Akkreditierungskriterien

Die durch den Arbeitskreis erarbeiteten Akkreditierungskriterien, welche im August 2018 von der Datenschutzkonferenz angenommen wurden, waren nach Art. 64 Abs. 1 lit. c DS-GVO dem Europäischen Datenschutzausschuss zur Stellungnahme zu übermitteln. Ein entsprechender Antrag war im Jahr 2019 leider noch nicht erfolgreich. Aufgrund fehlender Grundlagenpapiere auf europäischer Ebene wurden die deutschen Datenschutzaufsichtsbehörden mehrfach vom Sekretariat des Ausschusses gebeten, ihren Antrag zurückzunehmen bzw. ruhen zu lassen. Als im Herbst 2019 die vollständigen Unterlagen des Ausschusses vorlagen, ergab sich ein Änderungsbedarf an den Akkreditierungskriterien in kleinerem Umfang. Die Datenschutzkonferenz gab daher dem Arbeitskreis den Auftrag, diese Änderungen vorzunehmen.

15.3 Grafik für den Akkreditierungsprozess

Der AK Zertifizierung hat eine Grafik für den Akkreditierungsprozess für den Bereich Datenschutz gem. Art. 42, 43 DS-GVO entworfen. Diese gibt einen ersten, nicht abschließenden Überblick über den Ablauf eines reibungslosen Akkreditierungsprozesses. Zu dessen Durchführung sind insgesamt sechs Phasen vorgesehen:

1. Antragsphase – Programmprüfung
2. Programmprüfung und Genehmigung der Kriterien
3. Antragsphase Akkreditierung / Befugniserteilung
4. Begutachtungsphase
5. Akkreditierungsphase / Befugniserteilung
6. Überwachungsphase

Die Grafik ist abrufbar unter **https://s.rlp.de/ohakk**

16. RECHTSDRUCHSETZUNG

Nachdem das Jahr 2018 bei Unternehmen, staatlichen Einrichtungen, Privatpersonen und auch den Aufsichtsbehörden durch die Anpassung an die DS-GVO geprägt war, stand das Jahr 2019 im Zeichen einer effektiven Rechtsdurchsetzung. Hierzu machte der LfDI von seinen Befugnissen umfassend Gebrauch.

Verantwortliche und Auftragsverarbeiter sind grundsätzlich verpflichtet, auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen zu arbeiten. Informationsersuchen sind unabdingbar, um die Sachverhalte zu ermitteln und dem Anliegen der Beschwerdeführer gerecht zu werden. Da jedoch nicht alle Verantwortlichen sofort ihren Mitwirkungspflichten nachkamen, wurde in 28 Fällen ein Zwangsgeld von durchschnittlich 500,00 € angedroht. In neun Fällen kam es auch zur Festsetzung der Zwangsgelder.

Der LfDI erließ zwei Warnungen. In 7 Fällen wurde gegenüber Verantwortlichen eine Anweisung erlassen und in 33 Fällen eine Verwarnung ausgesprochen. Besonderes Augenmerk wurde hier auf die datenschutzkonforme Gestaltung von Webseiten gelegt. Im öffentlichen Sektor kam es in 20 Fällen zu einer Beanstandung. Meistens ging es dabei um eine unberechtigte Weitergabe personenbezogener Daten.

Nach der neuen Rechtslage wurden verstärkt Bußgeldverfahren eingeleitet. Dies führte zum Erlass von 8 Bußgeldbescheiden. Dabei reichten die Vorwürfe vom unzureichenden Schutz von Patientendaten über die Videoüberwachung Beschäftigter bis hin zu unberechtigten Datenbankabrufen durch Beamte oder dem unzulässigen Einsatz von Dashcams.

Auch an der bundesweiten Vereinheitlichung der Bußgeldverfahren wurde weitergearbeitet. Dies führte im Oktober 2019 zur Präsentation eines ersten Bußgeldkonzeptes durch die Datenschutzkonferenz. Dieser Bereich wird auf nationaler wie auch auf europäischer Ebene weiter intensiv diskutiert und weiterentwickelt.

Mit dem zunehmenden Erlass von Maßnahmen gegenüber den Verantwortlichen und der großen Zahl der überprüften Beschwerden ging es einher, dass der LfDI Beklagter in zahlreichen Verfahren wurde. Im Jahr 2019 wurde der LfDI in 22 Fällen verklagt. Gerade diejenigen Verfahren, in denen ein Beschwerdeführer sich gegen die Beendigung des Verfahrens wendete (da ein Datenschutzverstoß nicht festgestellt werden konnte), hat der LfDI für sich entschieden. Die Gerichte billigen hier den Aufsichtsbehörden einen Ermessensspielraum zu. Eine angemessene Prüfung des Beschwerdeanliegens unter Berücksichtigung auch der vorhandenen Ressourcen ist ausreichend, um die Rechte des Beschwerdeführers aus Art. 77, 78 DS-GVO zu wahren. Ein Anspruch auf eine konkrete Maßnahme besteht indes nicht.

ABKÜRZUNGSVERZEICHNIS

AEO	Authorized Economic Operator
AK	Arbeitskreis
ANBest-P	Allgemeine Nebenbestimmungen für Zuwendungen zur Projektförderung
ASP	Arbeitskreis Strafprozessrecht und Polizeirecht
AWG	Außenwirtschaftsgesetz
BDSG	Bundesdatenschutzgesetz
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BMG	Bundesmeldegesetz
BSI-Gesetz	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
DAkkS	Deutsche Akkreditierungsstelle GmbH
DS-GVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
EDSA	Europäischer Datenschutzausschuss
EG	Erwägungsgrund
EU	Europäische Union
EuGH	Europäischer Gerichtshof
GGO	Gemeinsame Geschäftsordnung
ICDPPC	International Conference of Data Protection & Privacy Commissioners
IMI	Binnenmarkt-Informationssystem
JVA	Justizvollzugsanstalt
KI	Künstliche Intelligenz
KomZG	Landesgesetz über die kommunale Zusammenarbeit
LAG	Landesarbeitsgericht
LArchG	Landesarchivgesetz Rheinland-Pfalz

LDSG	Landesdatenschutzgesetz Rheinland-Pfalz
LfDI	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
LG	Landgericht
LHO	Landeshaushaltsordnung
MDLVO	Meldedatenlandesverordnung Rheinland-Pfalz
POG	Polizei- und Ordnungsbehördengesetz
RED	Rechtsextremismusdatei
SchulG	Schulgesetz Rheinland-Pfalz
SGB	Sozialgesetzbuch
TMG	Telemediengesetz
TV-L	Tarifvertrag für den Öffentlichen Dienst der Länder
TVöD	Tarifvertrag für den Öffentlichen Dienst
UZK	Unionszollkodex
VV	Verwaltungsvorschrift
ZBS	Zentrale Bußgeldstelle

Hintere Bleiche 34 | 55116 Mainz
Postfach 3040 | 55020 Mainz

Telefon +49 (0) 6131 208-2449
Telefax +49 (0) 6131 208-2497

poststelle@datenschutz.rlp.de