Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

TÄTIGKEITSBERICHT ZUM DATENSCHUTZ 2018

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

GESTALTUNG

LABOR - Agentur für moderne Kommunikation GmbH
Fischtorplatz 21
55116 Mainz, Germany
T. +49 (0) 6131 3046762
www.labor.digital

Februar 2020

INHALT

VORWORT

Prof. Dr. Dieter Kugelmann

Das Jahr 2018 stand ganz im Zeichen des Wirksamwerdens der Datenschutz-Grundverordnung. Dieses Datum nahm nahezu magischen Charakter an, weil sich in ihm die Bedeutung und Wahrnehmung des Datenschutzes in Europa, Deutschland und in Rheinland-Pfalz wie in einem Brennspiegel konzentrierte. Dementsprechend waren die seit 2016 durchgeführten inhaltlichen und organisatorischen Vorbereitungen der Behörde überaus ertragreich, um die dann erfolgten Anfragen, Eingaben, Beschwerden und Aufklärungsaktivitäten zu bewältigen.

Alle mussten sich umstellen, die Verantwortlichen wie die Auftragsverarbeiter. Diese Umstellungsprozesse waren teils aufwändig und schwierig, andererseits aber auch zukunftsorientiert und sinnhaft. Sie führten oftmals zur Anpassung von Prozessen und der Verbesserung von Abläufen in den Unternehmen und Verwaltungen. Der digitale Kassensturz hat viele positive Folgen gehabt. Dieser erfolgte vor dem Hintergrund des geänderten Rechtsrahmens.

Der Gesetzgeber im Lande Rheinland-Pfalz hat durch die Schaffung des Landesdatenschutzgesetzes auf Landesebene einen Rahmen für den Datenschutz bei der Wahrnehmung von Aufgaben öffentlicher Stellen geschaffen. Ich bin sehr dankbar, dass der LfDI bereits bei der Schaffung des Gesetzes Gehör fand und einen Beitrag leisten konnte. Eine Reihe weiterer Fachgesetze des Landes Rheinland-Pfalz wurden unter Begleitung des LfDI in einem großen Gesetzespaket angepasst, das im Dezember 2018 in Kraft trat.

Neben den Anpassungen des rheinland-pfälzischen Datenschutzrechtes an die Datenschutz-Grundverordnung standen auch für den polizeilichen und justiziellen Bereich datenschutzrechtliche Gesetzesänderungen an. Bis zum 6. Mai 2018 war es den Mitgliedsstaaten der Europäischen Union aufgetragen, die Richtlinie (EU) 2016/680 umzusetzen. Das Land Rheinland-Pfalz wurde dem Umsetzungsauftrag zunächst durch die Schaffung

des Teils 3 des Landesdatenschutzgesetzes (LDSG) gerecht. Konkretisierungen in den Fachgesetzen, wie dem Justizvollzugsdatenschutzgesetz oder dem Polizei- und Ordnungsbehördengesetz sollen sich 2019/2020 anschließen.

Darüber hinaus waren die Behörden und Verwaltungen aufgerufen, den geänderten rechtlichen Rahmen umzusetzen. Die behördlichen Datenschutzbeauftragten als erste Ansprechpartner des LfDI haben hier vielfach wichtige Anregungen gegeben und Umsetzungen begleitet. Der LfDI hat versucht, den daraus entstehenden Bedarf an Beratung durch Veranstaltungen, Hilfestellungen und Gespräche zu befriedigen.

Hervorzuheben ist, dass auch die Gerichte und Staatsanwaltschaften in Rheinland-Pfalz sich auf die geänderten rechtlichen Bedingungen eingestellt haben. Der LfDI findet hier immer ein offenes Ohr und interessierte und aufgeschlossene Gesprächspartner. Dies betrifft zum einen den Datenschutz bei den Gerichten und Staatsanwaltschaften selbst, zum anderen aber auch die Behandlung entsprechender Verfahren. Letztlich ist es die unabhängige Justiz, die über Rechtsfragen entscheidet.

Die privaten Unternehmen in Rheinland-Pfalz stehen gleichermaßen in Kontakt mit dem LfDI wie öffentliche Stellen. Hier sind die Industrie- und Handelskammern zu nennen, die für Kooperationen bereitstehen und mit denen eine Vielzahl von Aktivitäten verwirklicht werden konnte. Auch große Unternehmen selbst haben ein gesteigertes Interesse, den Datenschutz intern wie extern zu verwirklichen. Die Veranstaltungsreihe des LfDI gemeinsam mit BASF, Boehringer, Birkenstock und Schott ist ein prägendes Beispiel für die Kooperation. Betriebliche Datenschutzbeauftragte und andere Interessierte können sich auf diese Art und Weise gegenseitig austauschen und von den gemachten Erfahrungen berichten. Die Datenschutz-Grundverordnung hat hier neue Herausforderungen gestellt, denen die Verantwortlichen versuchen gerecht zu werden. Dies ist an vielen Stellen gelungen. Dennoch bleiben zum einen noch Fragen offen, zum anderen noch Herausforderungen unbewältigt. Der LfDI wird seine Aufgabe, hier zu begleiten, aber auch als Aufsichtsbehörde Verletzungen zu verfolgen, weiterhin verantwortungsvoll wahrnehmen.

Mitte des Jahres 2018 waren es insbesondere Ehrenamtliche und Vereine, die zutiefst verunsichert waren. Ungeachtet der bereits vorher geltenden Regeln des Datenschutzes gab es doch einige kleinere Neuerungen, die aufgegriffen wurden. Hier lag ein großer Schwerpunkt insbesondere in der telefonischen Beratung, aber auch in einer Vielzahl von Veranstaltungen vor Mitgliedern von Vereinen. Ziel des Datenschutzes ist es nicht, Ehrenamtliche von ihren Aktivitäten abzuhalten, sondern die Grundrechte von Bürgerinnen und Bürgern zu schützen, zu denen eben auch die Grundrechte der Mitglieder von Vereinen oder der Personen zählen, die mit Vereinen in Kontakt stehen. Dies hat der LfDI vielfach klargestellt und derart versucht, zur Beruhigung beizutragen. Dies hat nach und nach Erfolge gezeigt.

Die neuen rechtlichen Regeln hatten sich im Laufe des Jahres 2018 in der Anwendung zu bewähren. Für den LfDI bedeutete dies, dass nahezu jede Aktivität von der Datenschutz-Grundverordnung und den entsprechend angepassten Regelungen des innerstaatlichen Rechts geprägt war. Die Priorität, die abstrakten Regelungen der Datenschutz-Grundverordnung mit Leben zu füllen, überlagerte andere Aktivitäten. Dennoch sind darüber hinaus weitere Bemühungen des LfDI angestrengt worden, Datenschutz handhabbar und verstehbar umzusetzen. Dies betrifft etwa die ausgezeichnete Zusammenarbeit mit der Landesärztekammer, der Landespsychotherapeutenkammer oder der kassenärztlichen Vereinigung sowie die Unterstützung der kommunalen Datenschutzbeauftragten. Diese Tätigkeiten prägten insbesondere die letzten Monate des Jahres 2018. Sie setzen sich im Jahr 2019 fort und haben inzwischen dazu beigetragen, dass eine Stabilisierung der Durchsetzung von Datenschutz auf hohem Niveau eingetreten ist.

Im Jahr 2018 hat der Datenschutz ein neues, höheres Niveau der Wahrnehmung erreicht. Zugleich ging es darum, dies auch auf ein höheres Niveau der Verwirklichung des Datenschutzrechts und damit der effektiven Durchsetzung von Rechten der Bürgerinnen und Bürger zu heben. Zur Erreichung dieses Ziels ist der LfDI auf die Kooperation mit vielen öffentlichen und privaten Akteuren angewiesen. Diese sind als Verantwortliche dazu aufgerufen, die Verwirklichung des Datenschutzrechts sicherzustellen. Kooperationen und vielfältige Kommunikation haben zur Erreichung dieses Ziels erheblich beigetragen. Mein Dank gebührt all denen, die sich für derartige Kooperationen zur Verfügung gestellt haben. In Rheinland-Pfalz gelingt es, auch hochgesteckte Ziele nicht zuletzt durch eine offene Kommunikation und vertrauensvolle Zusammenarbeit zu erreichen. Diesen Weg wird der LfDI auch in Zukunft weiter verfolgen.

Ich danke auch nachdrücklich allen Mitarbeiterinnen und Mitarbeitern meiner Behörde. Ohne ihr großes Engagement und die Bereitschaft, neue Wege der Durchsetzung zu gehen, wäre die Leistung des Jahres 2018 nicht möglich gewesen. Die teilweise Vervierfachung der eingegangenen Beschwerden, die Verzwölffachung der gemeldeten Datenpannen und die Hunderte schriftlicher Beratungen und statistisch nicht erfasster telefonischer Beratungen verdeutlichen, dass die Behörde beeindruckende Leistungen erbracht hat. Die Vielzahl von Veranstaltungen, die der LfDI durchgeführt hat, die multiplen Zielgruppen, die angesprochen wurden und die schriftlichen und mündlichen Unterstützungsleistungen haben es ermöglicht, die Datenschutz-Grundverordnung mit Leben zu füllen. Dies geschah vor dem Hintergrund, dass auch in der Kooperation mit den anderen Datenschutzaufsichtsbehörden in Deutschland und Europa erhebliche Anstrengungen und neue Kooperationsformen erforderlich waren. Der LfDI Rheinland-Pfalz ist eine europäisierte Behörde, die im Land fest verwurzelt ist. Rheinland-Pfalz als Land im Herzen Europas hat auch im Datenschutz seine europäische Rolle aktiv gespielt.

Die Aktivitäten, die der Tätigkeitsbericht belegt, verdeutlichen, wie spannend und zugleich abwechslungsreich das Feld des Datenschutzes ist. Als Querschnittsmaterie berührt er eine Vielzahl von Sachgebieten unterschiedlichster Ausprägung. Eine weiterreichende Digitalisierung insbesondere durch den Einsatz von Algorithmen und KI-Systemen kann nur nach den Regeln erfolgen, die für Digitalisierung bereitstehen. Dazu zählen die Regeln des Datenschutzrechts. Ich werde weiter mit meinen Mitarbeiterinnen und Mitarbeitern den Weg gehen, diese Regeln konstruktiv im Sinne der Interessen der Bürgerinnen und Bürger von Rheinland-Pfalz auszulegen und anzuwenden.

Prof. Dr. Dieter Kugelmann

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

I.
GRUNDLINIEN DER ENTWICKLUNGEN DES DATEN-SCHUTZES UND DER BEHÖRDE

I. GRUNDLINIEN DER ENTWICKLUNGEN DES DATENSCHUTZES UND DER BEHÖRDE

1. DIE DS-GVO UND DER LFDI

Sowohl die Organisation der Behörde, als auch die Arbeit an sich änderten sich 2018 grundlegend. Zur Umstrukturierung der Behördenorganisation berichtete bereits der 26. Tätigkeitsbericht.

Die DS-GVO überträgt den Datenschutzaufsichtsbehörden deutlich stärkere Befugnisse. Damit ist auch der LfDI in der Verantwortung, seine Aufgaben effektiv wahrzunehmen und seine Befugnisse angemessen auszuüben. Aufgrund dessen wurde eine Neuorganisation der Behörde vorgenommen, die sich auch in der modifizierten Geschäftsverteilung konkretisiert. Alle materiellen Bereiche des Datenschutzes sind von übergreifenden Themen wie etwa Fragen der Auftragsverarbeitung, der Bestellung von Datenschutzbeauftragten, der Erweiterung von Betroffenenrechten oder der verstärkten Verhängung von Sanktionen betroffen. Die neu eingerichtete Stabstelle Europa koordiniert diese Bemühungen im Hinblick auf die DS-GVO und hält den Kontakt zu anderen Behörden und der europäischen Ebene. Der Bereich Querschnittsaufgaben umfasst größtenteils Technik, zunehmend aber auch Fragen des proaktiven Datenschutzes wie Akkreditierung, Zertifizierung oder Gütesiegel.

2. EUROPÄISIERUNG UND INTERNATIONALISIERUNG

Der LfDI vertritt seit 2017 die deutschen Länder im Beirat von Europol. Europol hat eine neue Rechtsgrundlage erhalten, mit der die Datenschutzkontrolle an den Europäischen Datenschutzbeauftragten (EDSB) übertragen wird. Dieser wird von einem Beirat unterstützt, der aus Vertreterinnen und Vertretern der Mitgliedsstaaten besteht.

Im Schnittfeld zwischen Europäisierung und Sicherheit liegt ohnehin ein Schwerpunkt der Tätigkeit des LfDI. Das Verhältnis von Freiheit und Sicherheit auf der Grundlage der grundrechtlichen Rahmenbedingungen zu konkretisieren, stellt sich ihm als eine wichtige Aufgabe in der Situation dar, die sich durch technische Entwicklungen und sicherheitspolitische Herausforderungen dynamisch weiterentwickelt.

2.1. Europäisierung - Neuordnung des Datenschutzes in Europa

Die DS-GVO wurde am 25. Mai 2018 geltendes Recht und entfaltete – als Verordnung des Europäischen Parlaments und des Rates im Sinne des Art. 288 AEUV – unmittelbare –Wirkung in den Mitgliedstaaten der Europäischen Union und damit für über 500 Millionen Bürgerinnen und Bürger.

Gleichzeitig trat das neu gefasste Bundesdatenschutzgesetz (BDSG) in Kraft. Auch das rheinland-pfälzische Landesdatenschutzgesetz (LDSG) wurde neu gefasst und wurde in dieser Neufassung im Mai 2018 geltendes Recht. Doch sowohl BDSG als auch das LDSG enthielten nicht nur Regelungen zur Anpassung des deutschen Rechts an die DS-GVO, sondern setzten gleichzeitig die Richtlinie für Polizei und Justiz in Teilen um. Deren Umsetzungsfrist endete am 6. Mai 2018.

Darüber hinaus wurden im Mai 2018 bereits einige bereichsspezifische Vorschriften auf Bundesebene an die DS-GVO angepasst. Weitere Gesetzentwürfe zur Anpassung weiterer bereichsspezifischer Regelungen sowohl auf Bundes- als auch auf Landesebene wurden im Jahre 2018 in den Gesetzgebungsgremien beraten.

2.2. Internationalisierung

Eine erfreuliche Entwicklung konnte hinsichtlich des zunehmenden Bewusstseins für internationale Datenschutzthemen verzeichnet werden. Dies wurde nicht nur durch den gestiegenen Beratungsbedarf bei rheinland-pfälzischen Unternehmern deutlich, sondern auch durch beim LfDI eingegangene Datenpannenmeldungen von Mutterkonzernen mit Sitz außerhalb der EU, bei denen rheinland-pfälzische Kunden betroffen waren.

2.2.1. Erweiterung des Informationsangebotes im Internet

Mit der DS-GVO wurden im Vergleich zur DSRL teilweise neue Möglichkeiten geschaffen, geeignete Garantien für den Schutz personenbezogener Daten im Drittland herzustellen, teilweise wurden die Anforderungen bestehender Rechtsinstrumente konkretisiert. Die richtige Wahl des Mittels und die korrekte Umsetzung sind nicht trivial und oftmals zeitaufwändig. Aufgrund des höheren Bußgeldrahmens bei Zuwiderhandlungen gegen das Datenschutzrecht, haben Verantwortliche und Auftragsverarbeiter nun ein gesteigertes Interesse daran gezeigt, sich rechtskonform zu verhalten.

Um der zunehmenden Anzahl an Beratungsanfragen und der wachsenden Bedeutung des internationalen Datentransfers Rechnung zu tragen, erweiterte der LfDI sein Informationsangebot im Internet um ein eigenes Themenfeld namens „Internationales“, welches sich mit allen Varianten des datenschutzkonformen Datentransfers in Drittländer befasst und auf weiterführende Informationsquellen, insbesondere bei der EU-Kommission und dem Europäischen Datenschutzausschuss (EDSA) und auf ggf. relevante Formulare verlinkt.

2.2.2. Entwicklungen in Bezug auf den Drittlandsstatus bestimmter Länder

Seit die Anwendung der DS-GVO mit Beschluss des Gemeinsamen EWR-Ausschusses vom 6. Juli 2018 (Nr. 154/2018) für die EWR-Staaten Island, Lichtenstein und Norwegen verbindlich ist, zählen diese Länder nicht mehr als Drittländer im Sinne der DS-GVO. Die Anforderungen des Kapitels V DS-GVO müssen daher für Datentransfers in diese Länder nicht erfüllt werden. Datentransfers innerhalb dieser Länder sowie zwischen diesen Ländern und den derzeit noch 28 EU-Mitgliedstaaten unterliegen nun wieder – wie bereits zur Zeit der DSRL – den gleichen Anforderungen wie Datentransfers innerhalb der EU-Mitgliedstaaten.

Die Irrungen und Wirrungen bezüglich des künftigen Status des Vereinigten Königreichs, Großbritannien und Nordirlands führten zur Überraschung des LfDI im Jahr 2018 kaum zu Beratungsanfragen in der Behörde. Nichtsdestotrotz befassten sich die Aufsichtsbehörden intensiv mit den datenschutzrechtlichen Folgen eines Austritts je nach Austrittsszenario. Auf seiner Webseite veröffentlichte der LfDI daraufhin im Januar 2019 als erste Aufsichtsbehörde in Deutschland umfassende Informationen zum Brexit für verantwortliche Stellen, um weiterhin einen datenschutzkonformen Datentransfer zwischen der EU und Großbritannien sicherzustellen.

2.2.3. Entwicklungen bei den Angemessenheitsfeststellungen der EU-Kommission in Bezug auf bestimmte Länder

Als 13. Land reihte sich Japan im Januar 2019 nach einem mehrmonatigen Verfahren in die Liste der Länder, denen die EU-Kommission ein angemessenes Datenschutzniveau bescheinigt. Dies war das erste Verfahren zur Annahme einer Angemessenheitsfeststellung, welches die EU-Kommission unter der neuen Vorschrift des Art. 45 DS-GVO durchführte.

Die zweite jährliche Überprüfung der Einhaltung der zwischen der EU-Kommission und der US-Regierung ausgehandelten Bedingungen für einen Transfer von personenbezogenen Daten aus der EU in die USA unter dem EU-U.S. Privacy Shield fand im Herbst 2018 statt. Verbesserungen der Umsetzung aufgrund der im Rahmen der ersten Überprüfung im Jahr 2017 festgestellten Mängel gingen in die richtige Richtung. Auch der Frist, die die EU-Kommission nach der zweiten Überprüfung zur Ernennung einer Ombudsperson gesetzt hatte, leistete die US-Regierung Folge. Dennoch bestehen einige der Kritikpunkte fort, die im Herbst 2019 Gegenstand der dritten Überprüfung sein werden. Der vollständige Bericht des EDSA vom 22. Januar 2019 ist in der entsprechenden Themenbox des Online-Informationsangebotes des LfDI abrufbar.

2.2.4. Herausforderung für die Aufsichtsbehörden

Eine besondere Herausforderung stellt für die Aufsichtsbehörden die Rechtsdurchsetzung im Drittland dar. Besonders verheißungsvoll klingt das seit der DS-GVO geltende Marktortprinzip, durch welches auch Verantwortliche der DS-GVO unterfallen, die keine Niederlassung in der EU haben, aber Waren oder Dienstleistungen gegenüber EU-Bürgern anbieten.

Hürden bei der Rechtsdurchsetzung ergaben sich für den LfDI gleich an mehreren Stellen. Solche tatsächlicher Art offenbarten sich zum Beispiel bei der Ermittlung des tatsächlich für die konkrete Datenverarbeitung Verantwortlichen, beim Zeitaufwand für die Übersetzung von Dokumenten oder wenn das ausländische Unternehmen nicht gemäß Art. 27 DS-GVO einen Vertreter in der EU benannt hatte. Zu den Hürden rechtlicher Art zählten etwa die ordnungsgemäße Zustellung behördlicher Dokumente im Ausland oder das generelle Nichtvorhandensein internationaler Rechtshilfeabkommen.

3. VERFÜGUNGSMACHT ÜBER DATEN UND KÜNSTLICHE INTELLIGENZ

Im Juni 2018 veröffentlichte die High Level Expert Group on AI der Europäischen Kommission einen Katalog von 33 Handlungsempfehlungen. Die Empfehlungen richtet sich an die EU-Mitgliedsstaaten und an EU-Institutionen und haben den Zweck, Maßnahmen er einer nachhaltigen, zukunftsfähigen Wirtschaftsentwicklung zu fördern. Dazu gehören die Bildung der EU-Bürger im Bereich künstlicher Intelligenz und der Schutz vor negativen Auswirkungen der Technologie.

Im November 2019 hat die Bundesregering die „Strategier Künstliche Intelligenz" beschlossen. Mit der Strategie verfolgt die Bundesregierung drei wesentliche Ziele:

1. Deutschland und Europa zu einem führenden Standort für die Entwicklung und Anwendung von KI-Technologien zu machen und die künftige Wettbewerbsfähigkeit Deutschlands zu sichern,

2. eine verantwortungsvolle und gemeinwohlorientierte Entwicklung und Nutzung von KI sicherzustellen, und

3. KI im Rahmen eines breiten gesellschaftlichen Dialogs und einer aktiven politischen Gestaltung ethisch, rechtlich, kulturell und institutionell in die Gesellschaft einzubetten.

Der LfDI hat sich mit den Handlungsempfehlungen und der Strategie intensiv beschäftigt als Vorbereitung für das Jahr 2019, in dem Rheinland-Pfalz den Vorsitz der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hatte.

4. RHEINLAND-PFALZ

4.1. Neues Datenschutzgesetz für Rheinland-Pfalz

Das Landesdatenschutzgesetz (LDSG) wurde vom Landtag Rheinland-Pfalz am 26. April 2018 verabschiedet. Bereits 1974 ist das erste Datenschutzgesetz des Landes Rheinland-Pfalz in Kraft getreten.

Durch die DS-GVO wurden einige Anpassungen notwendig. Die DS-GVO gilt in weiten Teilen unmittelbar, enthält jedoch Öffnungsklauseln, die es den nationalen Gesetzgebern erlauben, beispielsweise für den öffentlichen Bereich ergänzende Regelungen zu treffen. Darin wurden gleichzeitig auch die notwendigen Regelungen zur Umsetzung der EU-Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch Polizei- und Justizbehörden getroffen.

Im Gesetz wurden die notwendigen Anpassungen des Datenschutzes an die fortschreitende Digitalisierung vorgenommen damit die Verwaltungen in Rheinland-Pfalz, Rechtssicherheit bei der Anwendung datenschutzrechtlicher Vorschriften erhalten. Das Gesetz trägt auch der besonderen Unabhängigkeit von Kontroll- und Aufsichtsbehörden Rechnung, wie dem Landesrechnungshof und dem Datenschutzbeauftragten.

4.2. Anpassungen der Landesgesetze aufgrund der DS-GVO

Auch im besonderen Landesrecht, d. h. in allen fachbereichsspezifischen Datenschutzbestimmungen, mussten aufgrund der DS-GVO Anpassungen umgesetzt werden.

Es erfolgten Änderungen in 25 Landesgesetzen und 10 Landesverordnungen. Regelungsgegenstände sind insbesondere das Landestransparenzgesetz (Artikel 1), das Öffentliche Dienstrecht (Artikel 2, 3 und 26), das Gesundheitsrecht (Artikel 6- 12 und 28), das Brand- und Katastrophenschutzgesetz (Artikel 15), das Schulrecht (Artikel 19 und 27 und 32- 35), das Hochschulrecht (Artikel 20 und 21), das Landesstatistikgesetz (Artikel 23) und das Steuerberaterversorgungsgesetz (Artikel 24).

Regelungsinhalte sind jeweils insbesondere die Anpassung von Begriffsbestimmungen, die Aufhebung oder Schaffung von Regelungen und Verweisungen, Anpassungen und Schaffung von Rechtsgrundlagen für die Datenverarbeitung und die Schaffung von Regelungen zu den Rechten der betroffenen Person. Bei allen Änderungen werden – wie im neuen LDSG – Regelungsoptionen so genutzt, dass der bisherige Datenschutzstandard des Landes soweit wie möglich aufrechterhalten wird, insbesondere die materiellen Anforderungen an die Datenverarbeitung betreffend.

5. ÖFFENTLICHKEITSARBEIT UND VERANSTALTUNGEN

Das Berichtsjahr 2018 war geprägt von Informationsinitiativen seitens des LfDI im Hinblick auf die Änderungen im Datenschutzrecht für die rheinland-pfälzischen Stellen – eigeninitiativ, aber vielfach auch auf Anfrage rheinland-pfälzischer Verantwortlicher.

Das Online-Informationsangebot wurde stetig erweitert. Kern der Informationsinitiative bildeten allerdings die Veranstaltungen des LfDI zum Thema DS-GVO:

Aufgrund der Notwendigkeit, nach Wirksamwerden der DS-GVO frisch gekürte Datenschutzbeauftragte über die gesetzlichen Bestimmungen zu informieren, initiierte der LfDI im September 2018 die Reihenveranstaltung „125-Tage DSGVO“, die am 26. September 2018 und am 20. November 2018 in Kooperation mit der SCHOTT AG, Boehringer Ingelheim, Birkenstock bzw. BASF SE stattfand. Ziel der Veranstaltungen war ein Austausch der jüngsten Erfahrungen mit der DS-GVO zwischen Wirtschaft und Aufsichtsbehörde. Nach den Vorträgen der Kooperationspartner und des LfDI hatte das aus Datenschutzbeauftragten bestehende Publikum Gelegenheit, datenschutzrechtliche Fragen an das Podium zu stellen. Die Pressemitteilung zu „125 Tage DSGVO“ und „180 Tage DSGVO“ finden Sie unter folgenden Links:

- **https://s.rlp.de/125dsgvo**
- **https://s.rlp.de/180dsgvo**

Um auch ein junges Publikum für datenschutzrechtliche Aspekte zu begeistern und für einen bewussten Umgang mit Daten im Internet zu sensibilisieren, lud der LfDI 2018 ins Mainzer Kino „Ciné Mayence“ ein. Er zeigte beispielsweise am 8. Oktober 2018 den Film „The Cleaners“, um über die Hintergründe und Gefahren der Löschpolitiken von Unternehmen wie

Facebook zu informieren. Darauf folgte eine Diskussion zwischen LfDI mit einem interessierten Publikum. Die Pressemitteilung zur Filmvorstellung „The Cleaners“ finden Sie unter folgendem Link: **https://s.rlp.de/lfdikino**

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 11. September 2018 statt. Neben der Präsentation der interessantesten Datenschutzfälle wurden ebenfalls Angaben zu Statistiken vor der Presse gemacht, z.B. über die Anzahl der eingereichten Beschwerden und Beratungsanfragen, sowie die Anzahl der zunehmenden grenzüberschreitenden Fälle. Die Pressemitteilung finden Sie hier: **https://s.rlp.de/bestofdatenschutz2018**

Darüber hinaus fand im Berichtsjahr regelmäßig die Veranstaltungsreihe „Mainzer Vorträge“ in Kooperation mit der Johannes Gutenberg-Universität (JGU) Mainz statt, die regelmäßig Themen des IT-Rechts und des Sicherheits- und Informationsrechts aufgreifen. So fand beispielsweise die Veranstaltung „Dateneigentum, Datenschuldrecht, Datenschutz?“ am 7. Juni 2018 statt.

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.

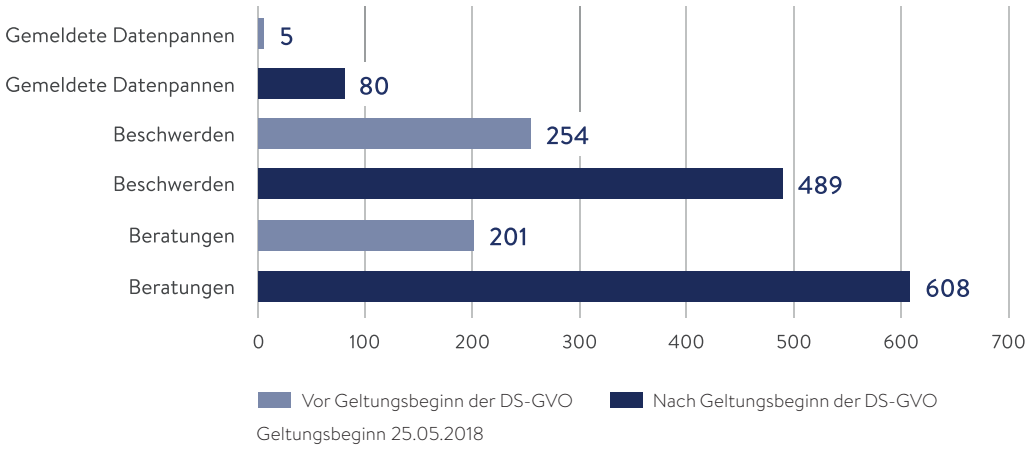
Zudem werden jeden zweiten Monat im Jahr Leserinnen und Leser über die Neuigkeiten im Datenschutz und die Tätigkeiten durch den Newsletter des LfDI informiert. Der Newsletter wurde dementsprechend im Februar, April, Juni, August, Oktober und Dezember 2018 versandt.

Das Archiv des Newsletter und die Anmeldung für den Newsletter finden Sie hier: **https://s.rlp.de/lfdinewsletter**

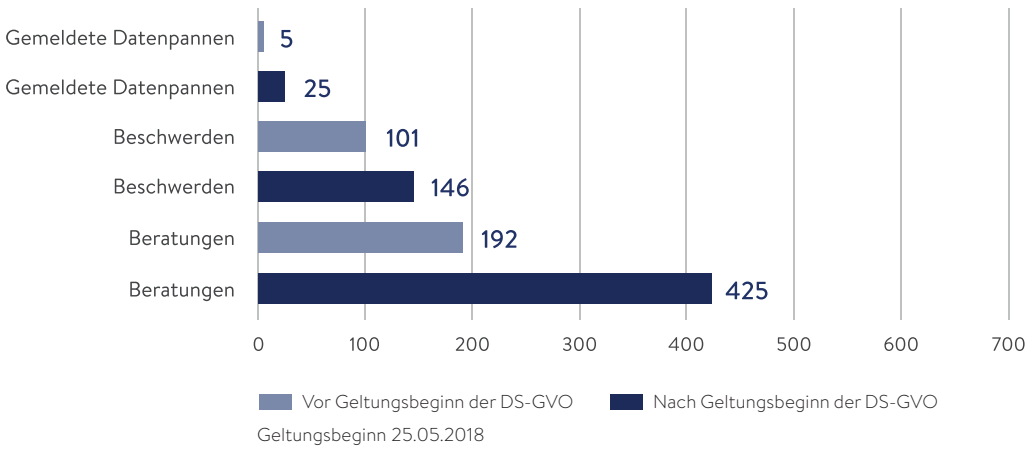
II.
ZAHLEN UND FAKTEN

II. ZAHLEN UND FAKTEN

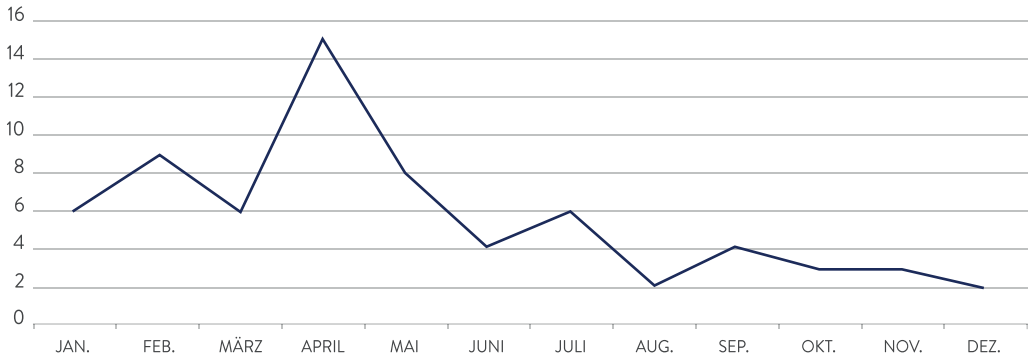
1. Geschäftsstatistik 2018: Privater Bereich



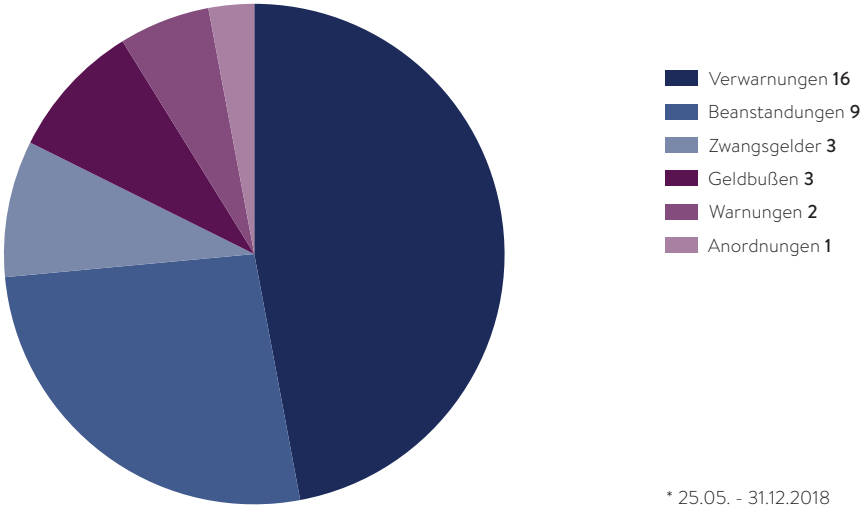
2. Geschäftsstatistik 2018: Öffentlicher Bereich



3. Beantwortete Pressefragen



4. Ausgeübte Befugnisse 2018*



* 25.05. - 31.12.2018

III.
SACHGEBIETE

III. SACHGEBIETE

1. EUROPÄISCHE ZUSAMMENARBEIT

Der LfDI hat im Berichtsjahr weiterhin die in Rheinland-Pfalz ansässigen Verantwortlichen verstärkt auf die Änderungen infolge der Europäischen Datenschutzreform vorbereitet und die Zusammenarbeit mit den anderen europäischen Aufsichtsbehörden und seinen Einsatz in den deutschen sowie europäischen Datenschutzgremien deutlich erweitert.

Bei der Bearbeitung von Beschwerden und sonstigen datenschutzrechtlich relevanten Vorgängen mit grenzüberschreitendem Bezug ist eine deutlich stärkere Zusammenarbeit mit den anderen europäischen Aufsichtsbehörden durch die DS-GVO notwendig geworden.

Die Kommunikation wird über die Web-Plattform „IMI“ (Internal Market Information System“ – zu deutsch „Binnenmarkt-Informationssystem) durchgeführt, die von allen europäischen Aufsichtsbehörden genutzt wird. Um diesem Zusammenarbeitsbedarf nachzukommen, hat der LfDI die Stabstelle Europa weiter personell verstärkt und eine „IMI-Stelle“ geschaffen, die sich um die Prüfung von grenzüberschreitenden Bezügen datenschutzrechtlicher Sachverhalte und die darauffolgende Kommunikation mit den anderen Aufsichtsbehörden kümmert.

1.1. Informationsinitiative des LfDI

Auch im Bereich Europa war das Berichtsjahr 2018 geprägt von Informationsinitiativen seitens des LfDI und das Online-Informationsangebot wurde stetig erweitert, z.B. zum EDSB **https://s.rlp.de/edsa** und zur Rolle der Aufsichtsbehörden **https://s.rlp.de/rollelfdi**.

1.2. Zusammenarbeit mit anderen Aufsichtsbehörden

Der LfDI hat im Berichtsjahr 2018 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.

Gemeinsam mit den anderen Aufsichtsbehörden des Bundes und Länder hat der LfDI auch im Jahr 2018 eine weitere Reihe von Kurzpapieren zu spezifischen datenschutzrechtlichen Themen erstellt und veröffentlicht, in denen die Neuerungen durch die DS-GVO themenspezifisch für die Verantwortlichen und die betroffenen Personen aufbereitet werden und die die gemeinsame Auffassung der Datenschutzkonferenz zur DS-GVO wiedergeben. Eine Zusammenstellung der Kurzpapiere ist unter den Themenfeldern einsehbar oder im Internetangebot abrufbar: **https://s.rlp.de/kurzpapieredsgvo**

Auf europäischer Ebene kam es zum Wechsel von der sog. Art. 29-Gruppe zum Europäischen Datenschutzausschuss (EDSA).

Bereits nach der Datenschutz-Richtlinie 95/46/EG (DSRL) wurde gem. Art. 29 DSRL eine sog. Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten etabliert. Diese hatte unter Geltung der DSRL die Aufgabe, die einheitliche Anwendung der unionsrechtlichen Datenschutzregeln zu gewährleisten. Die Gruppe wurde passend zu dem zu ihr geschaffenen Artikel „Art. 29-Gruppe“ genannt.

Mit Geltung der DS-GVO hat der nach Art. 68 DS-GVO gebildete EDSA die bisherige Artikel 29-Gruppe abgelöst. Dieser ist eine unabhängige europäische Einrichtung mit der Aufgabe, die einheitliche Anwendung der europäischen Datenschutzregelungen innerhalb der EU sicherzustellen und die Zusammenarbeit zwischen den EU-Datenschutzbehörden zu fördern. Hierzu weist die DS-GVO dem EDSA eine Reihe von Aufgaben und Befugnissen zu, z.B. Stellungnahmen und Beschlüsse im Rahmen der Kohärenzverfahren nach Art. 63 ff. DS-GVO und die Herausgabe von Leitlinien zur Unterstützung einer einheitlichen Auslegung der DS-GVO und der EU-DSRL für den Bereich Justiz und Inneres. Der EDSA hat seinen Sitz in Brüssel und besteht aus Vertreterinnen und Vertretern der nationalen Datenschutzaufsichtsbehörden und dem EDSB. Die Europäische Kommission ist berechtigt, an den Aktivitäten und Sitzungen des Ausschusses teilzunehmen, hat jedoch kein Stimmrecht.

Gemeinsamer Vertreter für die deutschen Datenschutzbehörden im EDSA ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Er wird von einem/einer Stellvertreter/in begleitet, den bzw. die der Bundesrat aus dem Kreise der Leiter und Leiterinnen der Aufsichtsbehörden der Länder wählt. In Angelegenheiten, für die die Länder das alleinige Recht zur Gesetzgebung haben oder die die Einrichtung oder das Verfahren von Landesbehörden betreffen, überträgt ihm/ihr der BfDI auf Verlangen das Stimmrecht im EDSA.

In seiner konstituierenden Sitzung am 25. Mai 2018 hat der Ausschuss von der bisherigen Art. 29-Gruppe zur DS-GVO erlassene Leitlinien übernommen. Darüber hinaus hat der EDSA im Laufe des Jahres 2018 auch seine ersten eigenen Leitlinien veröffentlicht. Die Leitlinien können im Internetangebot abgerufen **https://s.rlp.de/leitliniendsgvo** oder unter den Themenfeldern eingesehen werden sowohl in englischer als auch – soweit übersetzt und veröffentlicht – in deutscher Sprache.

Der EDSA verfügt über Unterarbeitsgruppen, die themenbezogen die Stellungnahmen und Entscheidungen des Ausschusses vorbereiten, die sog. Expertengruppen. Der LfDI wirkt in diesen mit, d.h. er teilt seine Auffassung zu verschiedenen in den Expertengruppen besprochenen Sachthemen den jeweiligen Ländervertretern mit, die dann wiederrum eine die deutsche Auffassung in Brüssel vertreten. Seit dem Berichtsjahr ist der LfDI auch in einer dieser Expertengruppen sog. Ländervertreter, d.h. Vertreter für die Aufsichtsbehörden der Bundesländer in diesem europäischen Gremium. Diese Expertengruppe wird namentlich als „IT-User-Subgroup“ bezeichnet und beschäftigt sich primär mit praktischen Anwendungsfragen des Binneninformationssystems „IMI“ („Internal Market Information System“) und mit der Abbildung weiterer in der DS-GVO vorgesehener Verfahren, wie z.B. dem Verfahren nach Art. 70. Darüber hinaus beschäftigt sich die IT-User-Subgroup mit der Einsetzung anderer IT-Tools, wie z.B. dem neu eingeführten Wissensmanagementsystem „Confluence“ und dem Videokonferenzsystem. Am 10. Oktober 2018 fand die erste Sitzung der IT-User-Subgroup in Brüssel in den Räumen des EDSB statt und am 7. November 2018 tagte eine Telefonkonferenz, in der man sich mit den europäischen Datenschutzaufsichtsbehörden auf eine Lösung eines Videokonferenzsystems einigte. An beiden Sitzungen nahm die ernannte Ländervertreterin des LfDI teil.

Die Aufgaben, die hinsichtlich der Hauptländervertretung anfallen, schließen u.a. eine kontinuierliche Unterrichtung der deutschen Datenschutzaufsichtsbehörden über die in der Expertengruppe gefassten Entscheidungen ein. Deshalb wird nach einer jeden Sitzung regelmäßig ein mit der ZAST gemeinsam

erstelltes Protokoll an alle Datenschutzaufsichtsbehörden gesandt, ggfs. mit der Möglichkeit dieser zur Kommentierung. Zudem werden vor einer jeden Sitzung der IT-User-Subgroup die Tagesordnung sowie weitere Dokumente an die Aufsichtsbehörden geschickt und ggfs. ein Meinungsbild zu unterschiedlichen Themen abgefragt.

1.3. Internationaler Datenschutz; ICDPPC

Neben seinem europäischen Engagement ist der LfDI Mitglied in der Internationalen Datenschutzkonferenz „International Conference of Data Protection and Privacy Commissioners", die jährlich stattfindet und Resolutionen in Expertengruppen vorbereitet. Vom 21. bis 26. Oktober 2019 fand die 40. Internationale Datenschutzkonferenz in Brüssel statt, an der der LfDI teilnahm und teilweise auch Änderungsvorschläge zu den Resolutionen vor Ort oder vorab einbrachte oder diskutierte.

Auf der 40. Internationalen Datenschutzkonferenz wurden folgende Resolutionen bzw. Erklärungen verabschiedet:

- Erklärung über Ethik und Datenschutz in der künstlichen Intelligenz **https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf**,
- Resolution über die Zusammenarbeit zwischen Datenschutzbehörden und Verbraucherzentralen für einen besseren Schutz von Bürgern und Verbrauchern in der Digitalen Wirtschaft **https://icdppc.org/wp-content/uploads/2018/10/20180918_ICDPPC-40th_DCCW-Resolution_ADOPTED.pdf**
- Resolution über E-Learning-Plattformen **https://www.privacyconference2018.org/system/files/2018-10/20180918_ICDPPC-40th_DEWG-Resolution_ADOPTED.pdf**

2. SICHERHEIT

2.1. Zuverlässigkeitsüberprüfungen bei Großveranstaltungen/Fußballspielen

Bereits im vergangenen Tätigkeitsbericht hat der LfDI zu der Thematik berichtet **https://s.rlp.de/datenschutzttigkeitsberichte**. Besondere Aufmerksamkeit erlangte die Thematik in diesem Jahr zudem aufgrund des G-20-Gipfels in Hamburg. Dort wurden zahlreichen Pressevertretern aufgrund von Sicherheitsbedenken die Akkreditierung versagt. Dies führte zu einer Auseinandersetzung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder mit der Thematik.

Nachdem bereits im Zuge der WM 2006 sich mit der Entschließung „Zuverlässigkeitsüberprüfungen bei Großveranstaltungen" der 74. Datenschutzkonferenz gegen die eingriffsintensiven polizeilichen Überprüfungen – ohne Rechtsgrundlage – ausgesprochen wurde, bestand in diesem Jahr das Erfordernis diesem Anliegen erneut und konkretisiert Ausdruck zu verleihen: Mit der Entschließung „Zuverlässigkeitsüberprüfungen bei öffentlichen und privaten Veranstaltungen nur im erforderlichen Maß und nach einem rechtsstaatlichen und transparenten Verfahren" wird von den Gesetzgebern und den Verantwortlichen erneut nachdrücklich gefordert, durch ein rechtsstaatliches und transparentes Verfahren solcher Zuverlässigkeitsüberprüfungen dafür zu sorgen, dass diese auf das absolut erforderliche Maß beschränkt bleiben, sowohl was den Umfang der Überprüfung als auch den betroffenen Personenkreis betrifft.

Dabei sind drei Forderungen besonders gewichtig. Zum einen sollten Zuverlässigkeitsüberprüfungen nur aufgrund einer spezifischen Rechtsgrundlage erfolgen. Dazu sind die Gesetzgeber aufgefordert, bereichsspezifische

Rechtsgrundlagen zu schaffen, die den Grundsatz der Verhältnismäßigkeit beachten und aus denen die Voraussetzungen und der Umfang der Überprüfungen klar und für die Bürgerinnen und Bürger erkennbar ersichtlich sind.

Anwendung, Umfang, Kreis der betroffenen Personen und die Datenverarbeitung sind auf das erforderliche Maß zu beschränken. Zuverlässigkeitsüberprüfungen dürfen nur bei Veranstaltungen eingesetzt werden, die infolge einer belastbaren Gefahrenprognose als besonders gefährdet bewertet werden. Entsprechend müssen die personenbezogenen Daten, die in den zum Abgleich herangezogenen Dateien und Informationssystemen gespeichert sind, nicht nur eine ausreichende Qualität haben, sondern es dürfen auch nur hinreichend gewichtige Delikte in die Überprüfung einbezogen werden, die einen konkreten Bezug zu den abzuwehrenden Gefahren haben.

Durch ein transparentes Verfahren müssen die Rechte und Freiheiten der betroffenen Personen gewährleistet werden. Mittel dazu sind Anhörungsrechte, unabhängige und verfahrenssichernde Instanzen, wie Clearingstellen und die Konsultation der Datenschutzaufsichtsbehörden.

Der LfDI steht mit dem Ministerium des Innern und für Sport des Landes Rheinland-Pfalz sowohl zu Schaffung einer geeigneten Rechtsgrundlage als auch der Etablierung eines rechtsstaatlichen Verfahrens bereits seit 2017 in Korrespondenz und nutze die Entschließung, um den Forderungen Nachdruck zu verleihen.

2.2. Polizeiliche Videoüberwachung nach der Richtlinie (EU) 2016/680

Bis zum 6. Mai 2018 sollte die Richtlinie (EU) 2016/680 in nationales Recht umgesetzt werden. In Rheinland-Pfalz wurde dies zunächst im Rahmen der Schaffung des Teils 3 des LDSG verwirklicht. Da das Polizei- und Ordnungsbehördengesetz die Richtlinie (EU) 2016/680 dagegen noch nicht umgesetzt hat, sind die Regelungen des Teils 3 des LDSG ergänzend zu den bestehenden anwendbar. Dies betrifft insbesondere die Pflichten der Verantwortlichen, die mit der Durchführung von Datenverarbeitungsvorgängen erfüllt werden müssen, wie das Führen eines Verzeichnis von Verarbeitungstätigkeiten und die Durchführung einer Datenschutz-Folgenabschätzung (DSFA). Zahlreiche Befugnisse der Polizei des Landes Rheinland-Pfalz bedürfen in der Praxis deswegen Anpassungsbedarfs. Einen Anwendungsfall stellt die polizeiliche Videoüberwachung nach § 27 POG dar. Dabei beschäftigte den LfDI die Frage, wann im Vorfeld einer Videoüberwachungsmaßnahme eine DSFA durchzuführen ist.

Gem. § 56 Abs. 1 LDSG muss eine DSFA dann durchgeführt werden, wenn die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechtsgüter betroffener Personen zur Folge hat.

§ 27 POG regelt die Befugnis zur Videoüberwachung durch die Polizei- und Ordnungsbehörden. Obwohl die systematische Überwachung betroffener Personen im öffentlichen Raum grundsätzlich nach der DS-GVO (Art. 35 Abs. 3 lit. c DS-GVO) ein besonders hohes Risiko darstellen kann, ist dieses Szenario im Rahmen der Richtlinie (EU) 2016/680 nicht hervorgehoben.

Da in § 27 POG selbst bereits neben den Eingriffsschwellen durch Verfahrensvoraussetzungen, wie z.B. die Meldepflicht gegenüber dem LfDI (§ 27 Abs. 7 POG) die Risiken für die Rechte und Freiheit der betroffenen Personen

eingedämmt werden, ist der LfDI zu der Auffassung gelangt, dass nicht per se bei jeder polizeilichen Videoüberwachungsmaßnahme eine DSFA durchzuführen ist. Vielmehr ist in einem gestuften Ansatz dann die Durchführung einer DSFA erforderlich, wenn über die systematische Überwachung hinaus Merkmale bestehen, aufgrund derer sich die Videoüberwachung besonders eingriffsintensiv auf die betroffenen Personen auswirkt.

Besonders eingriffsintensive Ausgestaltungen sind beispielsweise:

- Videoüberwachung mittels Drohnen
- Videoüberwachung unter Nutzung biometrischer Gesichtserkennung
- Videoüberwachung besonders schutzwürdiger betroffener Personen (z.B. Kinder)

Über die Videoüberwachung ist gem. § 43 LDSG in allgemeiner Form zu informieren. Dazu hat der LfDI mit dem MdI ein entsprechendes Informationsblatt erarbeitet, welches z.B. bei der Videoüberwachung bei Großveranstaltungen genutzt wird.

2.3. Neue Anforderungen an die Auskunftsrechte der betroffenen Personen nach der Richtlinie (EU) 2016/680

Durch die Richtlinie (EU) 2016/680 sollen insbesondere die Rechte der betroffenen Personen gestärkt und innerhalb der Europäischen Union harmonisiert werden. Die Anforderungen sind hoch, was angesichts der Sensibilität der personenbezogenen Daten, die im polizeilichen und justiziellen Kontext verarbeitet werden und den Konsequenzen, die die Verarbeitungen nach sich ziehen nachvollziehbar ist.

Das Auskunftsrecht ist seit jeher ein wichtiges Recht der von polizeilicher Datenverarbeitung betroffenen Personen, da mit fortschreitender Digitalisierung die polizeiliche Aufgabenerfüllung ohne Datenverarbeitung nicht denkbar ist. Das Ausmaß der Datenverarbeitung ist für die betroffenen Personen jedoch häufig nicht erkennbar. Benachrichtigungspflichten sind sehr restriktiv geregelt. Deswegen ist es nach vorheriger Rechtslage nur durch Ausübung des Auskunftsrechts möglich, Transparenz zu erlangen und die seine personenbezogenen Daten betreffende Datenverarbeitung nachvollziehen zu können.

Durch die Informationspflichten gem. § 43 LDSG wird bereits ein höheres Maß an Transparenz der Datenverarbeitung geschaffen, darüber hinaus wurde jedoch auch das Auskunftsrecht modifiziert und ausgeweitet. Mangels Umsetzung der Anforderungen aus Art. Art. 15 Richtlinie (EU) 2016/680 im Polizei- und Ordnungsbehördengesetz richtet sich das Auskunftsrecht nun nach § 40 POG i.V.m. § 45 LDSG. Konsequenz ist, dass neben den Voraussetzungen des § 40 Abs. 1 POG nach § 45 LDSG den betroffenen Personen auf Antrag Auskunft darüber zu erteilen ist, ob der Verantwortliche sie betreffende Daten verarbeitet. Betroffene Personen haben darüber hinaus das Recht, Informationen zu erhalten über

1. die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, und die Kategorie, zu der sie gehören,
2. die verfügbaren Informationen über die Herkunft der Daten,
3. die Zwecke der Verarbeitung und deren Rechtsgrundlage,
4. die Empfänger oder die Kategorien von Empfängern, gegenüber denen die Daten

offengelegt worden sind, insbesondere bei Empfängern in Drittstaaten oder bei internationalen Organisationen,

5. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,

6. das Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten durch den Verantwortlichen,

7. das Recht, nach § 48 die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit anzurufen sowie

8. Angaben zur Erreichbarkeit der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit.

Wie auch in der vorherigen Regelungen kann sich die betroffene Person an den LfDI wenden, soweit ihrem Antrag nicht nachgekommen wurde, ihr die Auskunft verweigert wurde oder nur unzureichende Informationen zu Verfügung gestellt wurde. Im Rahmen seiner Untersuchungsbefugnisse gem. § 42 Abs. 3 LDSG geht der LfDI diesen Beschwerden dann nach und verhilft der betroffenen Person dazu, Nachvollziehbarkeit über die Verarbeitung ihrer personenbezogenen Daten zu erlangen.

2.4. Präventiv-Polizeiliche automatisierte Kennzeichenerfassung

Bereits in der Novellierung des Polizei- und Ordnungsbehördengesetzes im Jahre 2012 wurde eine Rechtsgrundlage zur automatisierten Kennzeichenerfassung geschaffen, die jedoch den Anforderungen des Bundesverfassungsgerichts und des Bundesverwaltungsgerichts nicht standhielt. Durch Rechtsprechung wurde diese besonders eingriffsintensive, weil eine Vielzahl von Unbeteiligten betreffende, Datenverarbeitung verfassungskonform eingehegt.

Nach den Anforderungen des Bundesverfassungsgerichts (BVerfG, Urteil v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07, NJW 2008, 1505 [1507 Rn. 62]) begründen solche automatisierte Datenerfassungen dann keinen Gefährdungstatbestand, soweit die Daten unmittelbar nach der Erfassung technisch wieder spurlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert werden. Konkretisiert wurden die Anforderungen durch die Entscheidung des Bundesverwaltungsgerichts aus dem Jahr 2014 (BVerwG, Urteil v. 22.10.2014 – 6 C 7/13, NVwZ 2015, 906).

Diese Anforderungen wurden im Rahmen des § 27b POG im Polizei- und Ordnungsbehördengesetz konkret umgesetzt, was durch den LfDI in seiner Stellungnahme im Rahmen der Anhörung (LT-Drs. 17/1541) zu dem Entwurf des Landesgesetzes zur Änderung des Polizei- und Ordnungsbehördengesetzes (POG) (LT-Drs. 17/2895) ausdrücklich begrüßt wurde.

Nachdem der gesetzliche Rahmen in verfassungskonformer Weise geschaffen wurde, war es nicht zuletzt aufgrund seiner Prüfpflichten gem. § 41b POG ein Anliegen des LfDI, der Polizei des Landes Rheinland-Pfalz bei der Anschaffung der Kennzeichenlesegeräte beratend zur Seite zu stehen, damit die anzuschaffende Technik auch den gesetzlichen Anforderungen entspricht und eine verfassungskonforme Praxis ermöglicht.

Sobald die Anschaffungen getätigt werden, wird die Praxis zeigen, wie hoch der Bedarf zur Nutzung der Befugnis aus präventiv-polizeilicher Perspektive ist. Auch diesen Prozess wird der LfDI weiter begleiten.

2.5. Prüfung der Rechtsextremismus-Datei beim Landeskriminalamt

Zweck der Rechtsextremismus-Datei (RED) ist es, die Sicherheitsbehörden bei der Bekämpfung und Verhinderung von rechtsextremistischen Gewaltdaten sowie der Verfolgung der selbigen zu unterstützen (§ 1 Rechtsextremismus-Datei-Gesetz (RED-G)).

Gem. § 11 Abs. 1 S. 2 und Abs. 2 RED-G besteht im Abstand von zwei Jahren eine Überprüfungspflicht der Datei seitens der Datenschutzaufsichtsbehörden.

In der RED werden keine Kontaktpersonen gespeichert. Ebenso waren zum Prüfzeitpunkt keine Personen beschränkt oder verdeckt gespeichert.

Das Bundeskriminalamt protokolliert gem. § 10 RED-G bei jedem Zugriff den Zeitpunkt, die Angaben, die die Feststellung der aufgerufenen Datensätze, sowie die für den Zugriff verantwortliche Behörde und den Zugriffszweck nach § 5 Abs. 4 oder § 7 RED-G. Eine Protokolldatenauswertung wurde über das Landeskriminalamt (LKA) angefordert. Die Einsichtnahme in die Protokolldaten ist als eigener Kontrolltermin beim LKA geplant.

Der LfDI hat im Oktober eine Kontrolle der RED beim LKA Rheinland-Pfalz vorgenommen. Gegenstand der örtlichen Feststellung war vor allem die Darstellung der Verfahrensabläufe bis zur Speicherung bzw. Löschung der personenbezogenen Daten in der RED. Weiterhin wurde eine stichprobenartige Festlegung der Speicherungen vorgenommen, deren Erkenntnisse nach Aktenlage zur Speicherung in der RED geführt haben. Zudem wurde ein Zugriff auf die RED am Kontrolltag initiiert, um im Rahmen der noch zu erfolgenden Protokolldatenauswertung diesen Zugriff als protokolliert nachzuweisen.

2.6. Inbetriebnahme einer Online-Wache bei der Polizei Rheinland-Pfalz

Die Onlinewache der Polizei Rheinland-Pfalz ging als gemeinsames Projekt mit dem Saarland am 06.Dezember 2018 an den Start.

Die Bürger haben seitdem Gelegenheit, Strafanzeigen und Hinweise über das Portal der Onlinewache an den Lagedauerdienst des LKAs Rheinland-Pfalz zu übersenden. Von dort erfolgt nach erster Sichtung die Verteilung an die zuständigen Dienststellen. Der LfDI war zusammen mit dem Unabhängigen Datenschutzzentrum des Saarlandes in die datenschutzrechtliche Bewertung der Inbetriebnahme eingebunden.

Dabei wurde die Dauer der Speicherung der IP-Adressen problematisiert. Im Rahmen der Gestaltung der Zugriffsrechte wurde letztlich nur dem Lagedauerdienst in seiner „Back-Office-Funktion“ eine direkte Offenlegung der IP-Adresse zur Verfügung gestellt, um bei Gefahrenlagen oder in Fällen, in denen die Anzeige selbst erkennbar bereits eine Straftat darstellt, sofort reagieren zu können. Diese Verfahrensweise soll zunächst für den Zeitraum eines Jahres erprobt und im Anschluss evaluiert werden.

3. JUSTIZ

Am 25. September 2018 fand eine Veranstaltung des LfDI unter dem Titel „Datenschutz und Justiz – Herausforderungen an Rechtsprechung und Gerichtsverwaltung“ im Plenarsaal des Landtags Rheinland-Pfalz im Landesmuseum in Mainz statt. Vertreter der Wissenschaft, der aufsichtsbehördlichen Praxis, der rheinland-pfälzischen Justiz und der Anwaltschaft diskutierten zu den Auswirkungen der Datenschutzreform auf die rheinland-pfälzische Justiz.

Privatdozent Dr. Nikolaus Marsch vom Karlsruher Institut für Technologie (KIT) erörterte zu Beginn der Veranstaltung in seinem Impulsvortrag die Möglichkeiten der gerichtlichen Durchsetzung der DS-GVO und nahm dabei besonders das Vorabentscheidungsverfahren, das auch nationalen Instanzgerichten die Vorlage von Fragen an den EuGH bezüglich der Auslegung und Gültigkeit von Europarecht ermöglicht, in den Blick. Maria Christina Rost – persönliche Referentin des Hessischen Beauftragten für Datenschutz und Informationsfreiheit – schloss mit einem Vortrag zu den Bußgeldverfahren unter der DS-GVO an – unter besonderer Berücksichtigung des europäischen Einflusses auf das nationale Ordnungswidrigkeitenrecht.

Im Anschluss an diese beiden Vorträge diskutierten die Referenten der Impulsvorträge gemeinsam mit dem Staatssekretär im Ministerium der Justiz Philipp Fernis, dem Leitenden Oberstaatsanwalt Mario Mannweiler und den Rechtsanwälten Dr. Carlo Piltz und Tim Wybitul zu den Auswirkungen der Datenschutzreform auf die Gerichtsverwaltung und die Justiz und nahmen dabei unter anderem folgende Fragen in den Fokus ihrer Diskussion: Welche Auswirkungen hat die DS-GVO auf die Organisation der Gerichtsbarkeiten und auf die Rechtsprechung? Wie sind Ordnungswidrigkeitenverfahren unter Geltung der DS-GVO durchzuführen? Was hat die Gerichtsverwaltung beim Umgang mit personenbezogenen Daten zu berücksichtigen? Wie beeinflusst das neue Datenschutzrecht die Zivil- und die Verwaltungsgerichtsbarkeit? Welche Aspekte müssen auch in der rechtsprechenden Tätigkeit berücksichtigt werden? Wie ist das Datenschutzrecht in der Anwendung fortzuentwickeln?

Nähere Informationen dazu sind zu finden unter: **https://s.rlp.de/GvQ94**

3.1 Veröffentlichung von Vorschlagslisten für die Wahl von Schöffen

Im Zusammenhang mit einer Beschwerde hat der LfDI sich auch wieder mit der Frage der Zulässigkeit der Veröffentlichung von Vorschlagslisten für die Wahl von Schöffen im Internet beschäftigt.

§ 36 Abs. 2 Satz 2 Gerichtsverfassungsgesetz (GVG) legt fest, dass die Vorschlagsliste für die Wahl der Schöffen Geburtsnamen, Familiennamen, Vornamen, Tag und Ort der Geburt, Wohnanschrift und Beruf der vorgeschlagenen Person enthalten muss.

Im Hinblick auf die Veröffentlichung der Listen zu beachten, dass gemäß § 36 Abs. 3 Satz 1 GVG lediglich vorgesehen ist, die Vorschlagsliste für die Schöffen in der Gemeinde eine Woche lang zu jedermanns Einsicht aufzulegen ist. Der Zeitpunkt der Auflegung ist vorher öffentlich bekanntzumachen (§ 36 Abs. 3 Satz 2 GVG). Die Veröffentlichung ist durch die Formulierung „in der Gemeinde“ lokal begrenzt. Eine Veröffentlichung z.B. im Internet ist aufgrund der weltweiten Zugriffsmöglichkeit und des damit zusammenhängenden grundsätzlichen Gefährdungspotentials von dieser Rechtsgrundlage

nicht mehr gedeckt. Eine Veröffentlichung dieser Daten im Internet ist somit nur über eine Einwilligung der betroffenen Personen zulässig.

Eine Einwilligung der betroffenen Personen muss auch dafür vorliegen, wenn mit der Vorschlagsliste über die gesetzlichen Vorgaben hinaus zusätzliche Daten, wie z.B. „Begründung der Bewerbung", erhoben und veröffentlicht werden sollen. Vergleichbares gilt für die Veröffentlichung der Vorschlagslisten für die Wahl der ehrenamtlichen Richter in der Verwaltungsgerichtsbarkeit (§ 28 Satz 6 Verwaltungsgerichtsordnung).

3.2. Gefangeneneinkauf – Einkaufsscheine mit Eindruck der Haftart

Daneben wandten sich mehrere Gefangene im Berichtsjahr an den LfDI, da auf den Einkaufsscheinen der Gefangenen der Justizvollzugsanstalten in Rheinland-Pfalz plötzlich die aktuelle Haftart angegeben wurde. Dabei handelt es sich um eine besonders sensible Information.

Die Angabe der Haftart erfolgte vor dem folgenden Hintergrund: Gemäß § 62 Abs. 2 LJVollzG können Strafgefangene und Jugendstrafgefangene Nahrungs-, Genuss und Körperpflegemittel nur vom Haus- und Taschengeld, andere Gegenstände in angemessenem Umfang auch von Eigengeld einkaufen. Untersuchungsgefangene können hingegen auch Nahrungs-, Genuss- und Körperpflegemittel vom Eigengeld einkaufen.

Die Anstaltskaufleute müssen folglich wissen, ob es sich bei dem jeweiligen Gefangenen um einen Untersuchungsgefangenen handelt oder nicht, um feststellen zu können, welche Ware an wen gegen Eigengeld herausgegeben werden kann.

Die Angaben auf den Einkaufsscheinen, die vor jedem Einkauf erstellt werden, wurden aus dem Programm BASIS-Web importiert; dabei wurde nicht der Name, sondern die Gefangenenbuchnummer als Pseudonym aufgedruckt. Für die Angabe der Haftart wurde auf die in der Strafzeitberechnung eingegebene Haftart zugegriffen, da keine andere Datenquelle für die Angabe, ob es sich um einen Untersuchungsgefangenen handelt oder nicht, vorhanden war. Bei der Strafzeitberechnung wird jedoch nicht nur zwischen Straf-, Jugend- und Untersuchungshaft differenziert, sondern die genaue für den Gefangenen zutreffende Haftart angegeben.

Dies war aus datenschutzrechtlicher Sicht allerdings unzulässig – trotz Pseudonymisierung der personenbezogenen Daten auf dem Einkaufsschein mithilfe der Gefangenenbuchnummer.

Nach § 10 Abs. 1 und 2 Nr. 2c Landesjustizvollzugsdatenschutzgesetz (LJVollzDSG RP) dürfen personenbezogene Daten von den Justizvollzugsbehörden übermittelt werden, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, wobei eine solche Übermittlung regelmäßig dann erforderlich ist, wenn sie dazu dient, Gefangenen den Einkauf zu ermöglichen. Allerdings sind die Daten dabei gemäß § 12 Abs. 2 LJVollzDSG RP zwingend zu pseudonymisieren, wobei grundsätzlich die Gefangenenbuchnummer als Pseudonym zu verwenden ist, wenn nicht besondere Gründe entgegenstehen (§ 12 Abs. 1 S. 2 LJVollzDSG RP). Des Weiteren dürfen personenbezogene Daten selbstverständlich nur insoweit übermittelt werden, als dies für den jeweils zu erreichenden Zweck – hier der ordnungsgemäßen Abwicklung des Gefangeneneinkaufs – erforderlich ist.

Die Übermittlung der Information, ob es sich um einen Untersuchungsgefangenen

handelt, an die Anstaltskaufleute ist gemäß § 10 Abs. 2 Nr. 2 c) LJVollzDSG RP erforderlich, um eine ordnungsgemäße Abwicklung der Einkäufe zu gewährleisten. Allerdings ist es zur ordnungsgemäßen Abwicklung der Einkäufe nicht erforderlich auf dem Einkaufsschein die genaue Haftart anzugeben. Es genügt ein Hinweis, ob es sich um einen Untersuchungsgefangenen handelt oder nicht.

Dass es aufgrund des Erstellens der Einkaufsscheine mithilfe des Programms BASIS-Web zu der Angabe der genauen Haftart kam, weil keine andere Datenquelle für die Angabe „Untersuchungsgefangener ja/nein“ vorhanden war, ist keine ausreichende Rechtfertigung.

Der LfDI hat auf die Unzulässigkeit hingewiesen. Daraufhin wurde von dem Aufdruck der Haftart (mit Ausnahme der Untersuchungshaft) auf den Einkaufsscheinen abgesehen.

3.3. Inanspruchnahme von Mediendiensten durch Gefangene

Der LfDI hat sich im Berichtszeitraum aufgrund einer Anfrage auch mit der Zulässigkeit der Übermittlung personenbezogener Daten zur Inanspruchnahme von Mediendiensten durch Gefangene beschäftigt.

Personenbezogene Daten Gefangener dürfen von den Justizvollzugsbehörden an nicht-öffentliche Stellen grundsätzlich nur übermittelt werden, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, wobei eine solche Übermittlung regelmäßig dann erforderlich ist, wenn sie dazu dient, Gefangenen den Einkauf oder die Inanspruchnahme von Telekommunikations- und Mediendienstleistungen zu ermöglichen (§ 10 Abs. 1 und 2 Nr. 2 c) und d) LJVollzDSG RP.

Die personenbezogenen Daten sind dabei gemäß § 12 Abs. 2 LJVollzDSG RP zwingend zu pseudonymisieren, wobei grundsätzlich die Gefangenenbuchnummer als Pseudonym zu verwenden ist, wenn nicht besondere Gründe entgegenstehen (§ 12 Abs. 1 S. 2 LJVollzDSG RP). Des Weiteren dürfen personenbezogene Daten selbstverständlich nur insoweit übermittelt werden, als dies für den jeweils zu erreichenden Zweck erforderlich ist.

Daraus folgt, dass keine personenbezogenen Daten von Gefangenen in nicht pseudonymisierter Form von der Justizvollzugsanstalt zum Zwecke des Gefangeneneinkaufs oder zur Ermöglichung der Inanspruchnahme von Telekommunikations- und Mediendienstleistungen an externe Stellen übermittelt werden dürfen.

3.4. Musterentwurf für ein Landesjustizvollzugsdatenschutzgesetz

Rheinland-Pfalz hat bereits seit geraumer Zeit ein Landesjustizvollzugsdatenschutzgesetz (LJVollzDSG). Dieses bedarf allerdings im Zuge der Umsetzung der Richtlinie für Polizei und Justiz einiger Änderungen.

Dazu haben die Justizvollzugsdatenschutzreferenten der Länder einen Musterentwurf erarbeitet, der nun den Ländern als Grundlage für eigene Gesetzgebungstätigkeiten dahingehend dienen soll, die Richtlinie für Polizei und Justiz im Justizvollzugsbereich umzusetzen. Zu diesem Musterentwurf hat der LfDI bereits eine Stellungnahme abgegeben.

3.5. Auskunftsanspruch nach Art. 15 DS-GVO gegenüber Rechtsanwälten

Mehrfach hat sich der LfDI aufgrund von Beschwerden auch mit dem Auskunftsanspruch

nach Art. 15 DS-GVO gegenüber Rechtsanwälten beschäftigt.

Ein Auskunftsanspruch einer betroffenen Person ergibt sich grundsätzlich aus Art. 15 DS-GVO, wobei § 29 Abs. 1 S. 2 BDSG diesen gegenüber Berufsgeheimnisträgern einschränkt. Das Recht auf Auskunft der betroffenen Person besteht nach § 29 Abs. 1 S. 2 BDSG nicht, soweit durch die Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

Die Regelung des § 29 Abs. 1 S. 2 BDSG schließt den Auskunftsanspruch der betroffenen Person gegenüber Berufsgeheimnisträgern folglich nicht generell aus, sondern nur soweit durch eine Auskunft geheimhaltungsbedürftige Informationen offenbart würden.

Der Auskunftsanspruch besteht gegenüber Rechtsanwälten daher in Gänze in Fällen, in denen personenbezogene Daten betroffen sind, die nicht im Rahmen eines Mandatsverhältnisses erhoben wurden. Sind allerdings Daten betroffen, die der Rechtsanwalt in seiner Eigenschaft als Berufsgeheimnisträger d.h. in einem Mandatsverhältnis erhalten hat, ist von einem vollständigen Ausschluss des Auskunftsanspruchs auszugehen – jedenfalls dann, wenn der Auskunft-begehrende nicht der Mandant des Rechtsanwalts ist, von dem er Auskunft begehrt. Denn gemäß § 43a Abs. 2 S. 1 BRAO ist der Rechtsanwalt zur besonderen Verschwiegenheit verpflichtet. Eine Differenzierung und Einzelfallwürdigung der jeweiligen Informationen dahingehend, ob diese der betroffenen Person offenbart werden dürfen oder nicht, ist nicht praxisgerecht und auch vom Sinn und Zweck des § 29 Abs. 1 S. 2 BDSG nicht geboten.

4. VIDEOÜBERWACHUNG

Die private und die öffentliche Videoüberwachung bleibt ein rechtlich und gesellschaftlich umstrittenes Feld. Bereits die Rechtsgrundlage einer privaten Videoüberwachung war umstritten, da § 4 BDSG hierzu Regelungen trifft, ohne dass der nationale Gesetzgeber sich hierfür auf eine Öffnungsklausel in der DS-GVO berufen konnte. Zwischenzeitlich liegt mit dem Urteil des Bundesverwaltungsgerichts vom 27. März 2019, Az. 6 C 2.18 eine bundesgerichtliche Entscheidung vor, die bestätigt, dass sich die Zulässigkeit einer privaten Videoüberwachung nach Art. 6 Abs. 1 lit. f DS-GVO bestimmt. Eine abschließende Klärung dürfte jedoch erst der Europäische Gerichtshof bringen.

Auch mit diesem wichtigen Meilenstein für mehr Rechtsklarheit und –sicherheit bleiben jedoch viele ungeklärte Fragen. Bei der Beurteilung der Rechtmäßigkeit einer Videoüberwachung wird es weiterhin stark auf den Einzelfall ankommen. Zu begrüßen ist, dass sich die materiell rechtliche Zulässigkeit einer Videoüberwachung mit Anwendbarkeit der DS-GVO in den meisten Fällen nicht substantiell verändert hat. Die Erfüllung der Informations- und Dokumentationspflichten wirft dagegen zahlreiche ungelöste Fragen auf, deren praxistaugliche, einheitliche, rechtlich saubere und nicht zuletzt zeitnahe Beantwortung wenig aussichtsreicher als die sprichwörtliche Quadratur des Kreises sein dürfte. Hierbei dürfen die eigentlichen Ziele der DS-GVO nicht aus den Augen verloren werden. Diese Aufsichtsbehörde bekennt sich zu einer praxistauglichen Anwendung der DS-GVO, die ein hohes Datenschutzniveau gewährleistet. Neben den rechtlichen Schwierigkeiten, die eine datenschutzrechtliche Zeitenwende mit sich bringt, bleibt die unzureichende Ausstattung der Aufsichtsbehörden gerade im Bereich der Videoüberwachung ein Problem. Die digitale Gesellschaft ist geprägt

von der flächendeckenden Verfügbarkeit und dem weitverbreiteten Einsatz opto-elektronischer Datenverarbeitung. Smartphones, elektronische Türspione, Webcams, Dashcams, Videodrohnen und nicht zuletzt „klassische" Überwachungskameras mit WLAN-Verbindung und eigener Solarstromversorgung gehören zum Alltag. Im Bereich des autonomen Fahrens wird eine umfassende und von künstlicher Intelligenz gestützte opto-elektronische Datenverarbeitung unabdingbar sein. Diese Entwicklung führt in Verbindung mit der durch die sog. Rynes-Entscheidung des Europäischen Gerichtshofs (EuGH, Urteil vom 11.12.2014, Az. C-212/13) vorgegebenen engen Auslegung der so genannten Haushaltsausnahme, der Nichtanwendbarkeit der DS-GVO im privaten und familiären Bereich (Art. 2 Abs. 2 lit. c DS-GVO) zu einer strukturellen Überdehnung der Zuständigkeit der Datenschutzaufsicht. Selbst bei einer Vervielfachung der zur Verfügung stehenden Mittel würden diese möglicherweise keinen flächendeckenden Schutz des Grundrechtes auf informationelle Selbstbestimmung gewährleisten können. Dies ist auch darin angelegt, dass auf Grundlage der Rynes-Entscheidung zwar der Anwendungsbereich der DS-GVO bei der Überwachung des öffentlichen Raumes eröffnet wird. Die DS-GVO eröffnet den Aufsichtsbehörden allerdings keine effektiven Möglichkeiten, Datenschutzverstöße in privaten Wohnungen zu ermitteln. Dies ist mit Blick auf die Unverletzlichkeit der Wohnung zu begrüßen, zeigt aber einen Bruch zwischen dem Anwendungsbereich der DS-GVO und den Ermittlungsbefugnissen der Aufsichtsbehörden auf. Es liegt weiterhin nahe, dass sich mit Blick auf das Grundrecht der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ähnliche Probleme bei den genutzten, ggf. mobilen, Geräten stellen werden. Es scheint vor diesem Hintergrund zweifelhaft, ob die Rynes-Entscheidung auf Dauer Bestand haben kann. Die Entscheidung basiert auf einer Grundrechtsabwägung, die nicht Eins-zu-eins auf die DS-GVO übertragen werden kann. Der Anwendungsbereich der DS-GVO bringt nicht erst hinsichtlich der Ermittlungs- und Sanktionsbefugnisse der Aufsichtsbehörden substantielle Grundrechtseingriffe mit sich. Die umfangreichen Dokumentations- und Meldepflichten beeinträchtigen selbst diejenigen, die bereits über die notwendige Sachkenntnis verfügen. De lege ferenda wären daher Möglichkeiten zu schaffen, die die Datenverarbeitung im halb-privaten und nachbarschaftlichen Kontext wieder den jeweils zuständigen Ordnungsbehörden und den auch sonst mit nachbarschaftlichen Streitigkeiten belasteten Zivilgerichten zuweisen. Die umfassend ausgestalteten Betroffenenrechte der DS-GVO sind zu begrüßen. Sie bedeuten aber auch, dass die DS-GVO als Regelungswerk für nachbarschaftliche Konflikte nicht nur nicht geeignet, sondern hochgradig missbrauchsgefährdet ist.

4.1. Dashcams vs. Crashcams

Der Bundesgerichtshof (BGH) beschäftigte sich in seinem Urteil v. 15. Mai 2018 – VI ZR 233/17 mit der Verwertbarkeit von permanenten Dashcam-Aufzeichnungen als Beweismittel in einem Unfallhaftpflichtprozess und stellte fest, dass die im Verfahren vorgelegte permanente anlasslose Videoaufzeichnung nach den (zum Urteilszeitpunkt noch) geltenden datenschutzrechtlichen Bestimmungen unzulässig sind.

Im Ausgangsfall ging es um die Verwertbarkeit solcher Aufzeichnungen als Beweismittel in einem Verkehrsunfall, bei dem zwei Autofahrer beim Linksabbiegen auf zwei nebeneinander verlaufenden Linksabbiegespuren seitlich zusammenstießen. Der Kläger, Fahrer eines Wagens mit Dashcam, wollte mit Aufnahmen seiner Videokamera beweisen, dass der

Unfallgegner seine Spur verlassen und seitlich auf ihn aufgefahren sei.

Zwar lässt der BGH eine Verwertung der Aufnahmen im Zivilprozess nach einer Interessen- und Güterabwägung nach den im Einzelfall gegebenen Umständen zu, jedoch wird die Auffassung des LfDI Rheinland-Pfalz, dass die dauerhafte Aufzeichnung mit Dashcams unzulässig ist, bestätigt.

Eine dauerhafte Aufzeichnung verstößt gegen Art. 5, 6 DS-GVO, da die Aufnahmen ohne Einwilligung der Betroffenen erfolgten. Berechtigte Interessen des Verantwortlichen im Sinne des Art. 6 Abs. 1 lit. f bestehen wenn dann nur in einem zeitlich geringen Umfang. Eine anlasslose permanente Aufzeichnung des gesamten Geschehens sei zur Wahrnehmung der Beweissicherungsinteressen nicht erforderlich, denn es sei technisch möglich, eine kurze, anlassbezogene Aufzeichnung des unmittelbaren Unfallgeschehens zu gestalten. Dies könne beispielsweise durch ein dauerndes Überschreiben der Aufzeichnung in kurzen Abständen und Auslösen der dauerhaften Speicherung erst bei Kollision oder starker Verzögerung des Fahrzeuges geschehen.

Das Urteil ist kein Freibrief für den grundlosen und flächendeckenden Einsatz von Dashcams. Der Betrieb einer Dashcam ist in der Regel unzulässig. Auch der Betrieb von so genannten CrashCams, der nicht zwangsläufig rechtswidrig sein muss, birgt erhebliche datenschutzrechtliche Risiken.

Verstöße gegen die am 25. Mai 2018 wirksam gewordene DS-GVO können sowohl Anordnungen als auch die Verhängung von Geldbußen durch die Aufsichtsbehörde nach sich ziehen. Im kommenden Jahr erwartet der LfDI, aufgrund eines eigenen Ordnungswidrigkeitenverfahrens mehr Rechtsklarheit in der Sache zu erlangen.

4.2. Big Brother oder Neighbourhoodwatch – FAQ zur Videoüberwachung im Nachbarschaftsverhältnis

Videoüberwachung im Nachbarschaftskontext führt häufig zu Beschwerden, Streitigkeiten und im schlimmsten Fall gerichtlichen Verfahren. Auch wenn die Beobachtung des angrenzenden Nachbargrundstücks oder des öffentlichen Verkehrsraums häufig nicht gewollt ist, so fühlen sich mögliche betroffene Personen allein vom Vorhandensein einer Kamera in der Nähe ihres privaten Umfeldes gestört. Es ist für diese oft nicht ohne weiteres ersichtlich, welche Bereiche von der Kamera erfasst werden.

Da Fragen im Zusammenhang mit Videoüberwachung durch Privatpersonen einen großen Anteil an der täglichen Arbeit des LfDI haben, soll die folgende Fragen-Antwort-Zusammenstellung dazu beitragen, auf diesem Gebiet etwas mehr Klarheit für Verantwortliche und betroffene Personen zu schaffen. Der LfDI stößt hier aufgrund der Vielzahl der eingehenden Beratungsanfragen und Beschwerden oft an seine Grenzen.

„Darf ich mein vor meinem Haus auf öffentlicher Straße parkendes Fahrzeug von meinem Grundstück aus überwachen?“, „Ist die Nutzung einer Kamera-Attrappe erlaubt?“, „Welche Anforderungen an eine Hinweisbeschilderung stellen sich?“. Solche und andere Fragen und deren Antworten sind im Internetangebot des LfDI abrufbar.

Bezüglich der rechtlichen und tatsächlichen Schwierigkeiten bei der Videoüberwachung im nachbarschaftlichen Kontext wird auf die Ausführungen zu Beginn des Abschnitts Videoüberwachung verwiesen.

5. WIRTSCHAFT

5.1. Ist Werbung nach der DS-GVO zulässig?

Mit der DS-GVO sind alle detaillierten Regelungen des bisherigen BDSG zur Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung weggefallen.

Grundlage für die Beurteilung der Zulässigkeit einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung ist in der DS-GVO, abgesehen von einer Einwilligung der betroffenen Person oder einer vertraglichen Vereinbarung mit dieser Person, eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO. Anhaltspunkte für die zu treffende Abwägungsentscheidung enthält Erwägungsgrund 47 DS-GVO, der u. a. ausführt: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden."

Direktwerbung kann also nach der DS-GVO durchaus zulässig sein. Jede betroffene Person hat aber weiterhin das Recht, dieser Werbung zu widersprechen und muss auf dieses Widerspruchsrecht hingewiesen werden.

Neben den datenschutzrechtlichen Bestimmungen ist bei Werbung immer auch das Wettbewerbsrecht zu beachten. Werbemaßnahmen sind nur rechtskonform, wenn sie sowohl nach Datenschutzrecht als auch nach Wettbewerbsrecht rechtskonform sind. Zu beachten sind dabei auch medien- und telekommunikationsrechtliche Regelungen wie das Telemediengesetz und das Telekommunikationsgesetz.

Grundsätzlich kann eine Werbemaßnahme datenschutzkonform sein, dennoch aber gegen Wettbewerbsrecht verstoßen. So bedarf es nach der DS-GVO in vielen Fällen der Direktwerbung keiner ausdrücklichen Einwilligung der betroffenen Personen, da sich die Werbenden in der Regel auf ein berechtigtes Interesse stützen dürfen. Richtet sich die Werbung an sog. Marktteilnehmer, also Personen, die als Anbieter oder Nachfrager von Waren oder Dienstleistungen tätig sind, bedarf es hierzu in bestimmten Fällen der Einwilligung. Dies bestimmt sich nach § 7 UWG. Danach ist eine geschäftliche Handlung, durch die ein Marktteilnehmer in unzumutbarer Weise belästigt wird, unzulässig. Dies gilt insbesondere für Werbung, obwohl erkennbar ist, dass der angesprochene Marktteilnehmer diese Werbung nicht wünscht (§ 7 Abs. 1 UWG). Wann eine unzumutbare Belästigung anzunehmen ist, bestimmt § 7 Abs. 2 UWG.

Die Einhaltung des Wettbewerbsrechts unterliegt allerdings nicht der Kontrolle des LfDI. Er darf zu diesem Rechtsgebiet auch nicht beraten. Es handelt sich um ein rein zivilrechtliches Themengebiet.

Als Vorsorgemaßnahme rät der LfDI daher immer wieder, mit dem Umgang der eigenen personenbezogenen Daten im Internet sorgsam umzugehen und auch bei Gewinnspielaktionen und vermeintlich kostenlosen Gutscheinen wachsam zu sein und das Kleingedruckte sorgfältig zu lesen, damit die eigenen Daten erst gar nicht in die falschen Hände geraten. Hinweise zum Selbstdatenschutz finden Sie unter: **https://s.rlp.de/selbstds**

5.2. Steuerberaterinnen und –berater und die Auftragsverarbeitung

Bereits im 26. Tätigkeitsbericht hatte sich der LfDI zur Frage geäußert, ob Steuerberaterinnen und –berater Auftragsverarbeitung

durchführen. Auch wenn sich nach Wirksamwerden der DS-GVO bei der Bewertung, ob eine Auftragsverarbeitung vorliegt, kaum etwas geändert hat, treibt die Vertreter der steuerberatenden Berufe diese Frage weiter um. So erreichen den LfDI weiterhin zahlreiche Anfragen von einzelnen Steuerberatungskanzleien, aber auch von deren berufsständischen Organisationen. Der LfDI kann insoweit nur auf seine öffentlich vertretene Rechtsauffassung verweisen.

Die Datenschutzkonferenz hat sich in ihrem Kurzpapier Nr. 13 zur Auftragsverarbeitung hierzu bereits positioniert. Dazu heißt es im Anhang B, dass keine Auftragsverarbeitung, sondern die Inanspruchnahme fremder Fachleistung bei einem eigenständigen Verantwortlichen, für die bei der Verarbeitung einschließlich Übermittlung personenbezogener Daten eine Rechtsgrundlage gem. Art. 6 DS-GVO gegeben sein muss, beispielsweise dann vorliegt, wenn ein Berufsgeheimnisträger (Steuerberater) einbezogen wird. Folglich bezieht sich dies aber nur auf Arbeiten der Steuerberaterinnen und -berater, die sie im Rahmen des Steuerberatungsgesetzes durchführen. Dieses Gesetz trifft hier spezielle berufsrechtliche Regelungen. Die getroffene Regelung in § 6 Nr. 4 StBerG (Steuerberatungsgesetz) spricht ebenfalls hierfür: Danach ist davon auszugehen, dass es sich bei der reinen Lohnbuchhaltung um Verarbeitungsvorgänge handelt, die nicht die besonderen Qualifikationen von Steuerberaterinnen und -beratern erfordern (**https://s.rlp.de/steuerberatung**).

5.3. Einschaltung von Inkassobüros – Was gilt aus datenschutzrechtlicher Sicht?

Bei der Einschaltung von Inkassounternehmen bei (vermeintlich) offenen Forderungen stellen sich auch datenschutzrechtliche Fragen. So wenden sich viele betroffene Personen an den LfDI, weil sie die Übermittlung ihrer personenbezogenen Daten durch ihren Vertragspartner an ein Inkassounternehmen für unzulässig halten und die Löschung beim Inkassounternehmen fordern. Weiterhin ist oft fraglich, unter welchen Voraussetzungen das Inkassounternehmen (vermeintlich) offene Forderungen an Wirtschaftsauskunfteien melden darf.

Übermittlung personenbezogener Daten an ein Inkassounternehmen: Die Zulässigkeit der Übermittlung personenbezogener Daten an ein Inkassounternehmen richtet sich nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO. Nach dieser Vorschrift ist das Übermitteln personenbezogener Daten rechtmäßig, wenn die Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Das berechtigte Interesse des übermittelnden Unternehmens besteht darin, dass die (vermeintlich) offene Forderung vom Schuldner beglichen wird. Hierzu kann es sich der Hilfe Dritter, nämlich eines Inkassounternehmens bedienen. Dann ist es aber auch erforderlich, dass das Inkassounternehmen die Informationen erhält, die die Forderung begründen und die einen Einzug durch das Inkassounternehmen ermöglichen. Dies gilt auch dann, wenn das Bestehen oder die Höhe der Forderung zwischen den Parteien strittig ist.

Wenn also mit einem Unternehmen vereinbart wurde, dass dieses gegen Bezahlung entsprechender Entgelte seine Leistungen zur Verfügung stellt und die Forderung nicht beglichen bzw. nicht vollständig beglichen wurde, ist das Unternehmen berechtigt, die Vertragsdaten an ein Inkassounternehmen weiterzugeben.

Da die Datenübermittlung der Forderungsbegleichung dienen soll, ist grundsätzlich nicht davon auszugehen, dass Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Vor einer zivilrechtlichen Klärung, ob und ggf. in welcher Höhe tatsächlich eine Forderung besteht, kann aus datenschutzrechtlicher Sicht keine Löschung der personenbezogenen Daten beim Inkassounternehmen veranlasst werden.

5.4. Übermittlung personenbezogener Daten durch Inkassounternehmen an Wirtschaftsauskunfteien

Unter bestimmten Voraussetzungen dürfen auch Inkassounternehmen Informationen über offene Forderungen an Wirtschaftsauskunfteien melden. Die Zulässigkeit einer solchen Einmeldung beurteilt sich ebenfalls nach Art. 6 Abs. 1 lit. f DS-GVO. Hierzu ist es notwendig, dass die Einmeldung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Das können die Interessen des Inkassounternehmens selbst sein oder die des (ursprünglichen) Gläubigers. Zudem dürfen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen. Das bedeutet, dass eine Abwägung unter Berücksichtigung dieser Kriterien im Einzelfall vorzunehmen ist.

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

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

Zusätzliche Anhaltspunkte oder Hinweise können ggf. zu einer anderen Abwägung führen.

Darüber hinaus muss eine Kompatibilitätsprüfung nach Art. 6 Abs. 4 DS-GVO erfolgen, weil die personenbezogenen Daten zunächst für einen anderen Zweck – zur Durchführung eines Rechtsgeschäfts und nicht zur Einmeldung bei einer Auskunftei – verarbeitet wurden. Die betroffene Person muss also zuvor durch die Auskunftei-Vertragspartner (also ursprünglicher Gläubiger oder Inkassounternehmen) über die Möglichkeit der Einmeldung unterrichtet worden sein, denn es darf nur das eingemeldet werden, womit die betroffene Person vernünftigerweise rechnen muss (Erwägungsgrund 47 DS-GVO).

Es ist daher in strittigen Fällen zu empfehlen, der Forderung auch gegenüber dem Inkassounternehmen zu widersprechen. Damit wird in

der Regel verhindert, dass entsprechende Inkassoinformationen bereits vor einer weiteren zivilrechtlichen Klärung an eine Wirtschaftsauskunftei übermittelt werden.

5.5. Immobilienverwaltungen und Auftragsverarbeitung

Aus dem Bereich der Immobilienverwaltungen wurden vermehrt Anfragen an den LfDI herangetragen, ob Tätigkeiten nach dem Wohnungseigentumsgesetz durch Immobilienverwaltungen für Wohnungseigentumsgemeinschaften eine Auftragsverarbeitung darstellen. Auch wenn sich nach Wirksamwerden der DS-GVO bei der Bewertung, ob eine Auftragsverarbeitung vorliegt, kaum etwas geändert hat, wollten einige Immobilienverwaltungen aufgrund der neuen europäischen Rechtsgrundlage entsprechende Verträge mit Wohnungseigentumsgemeinschaften abschließen.

Der LfDI teilt diese Auffassung, dass die Verwaltung für Wohnungseigentumsgemeinschaften grundsätzlich eine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO darstelle, nicht. Die Verwaltung verarbeitet personenbezogene Daten in eigener Verantwortung. Sie ist mithin Verantwortlicher im Sinne der DS-GVO. Verantwortlicher ist u.a. die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DS-GVO). Die Wohnungseigentümergemeinschaft hat mit der Verwaltung einen Vertrag abgeschlossen, der die Hausverwaltung zum Gegenstand hat.

Die Verwaltung will ihre Pflichten aus dem Verwaltervertrag ordnungsgemäß erfüllen. Dazu muss sie personenbezogene Daten verarbeiten. Diese Datenverarbeitung ist über Art. 6 Abs. 1 Satz 1 lit. b (Vertragserfüllung) und lit. f (berechtigtes Interesse) DS-GVO legitimiert. Zu diesem Zweck verarbeitet sie personenbezogene Daten von Eigentümerinnen und Eigentümern und Mieterinnen und Mietern in eigener Verantwortung. Sie ist damit Verantwortlicher innerhalb der Datenverarbeitung ihres Geschäftsbereichs. Die Verwaltung entscheidet überwiegend autark, welche Daten sie zur Erfüllung ihrer Aufgabe verarbeitet und wie sie das tut. Ein Auftragsverarbeitungsverhältnis liegt daher nicht vor.

Der Verband der Immobilienverwalter Rheinland-Pfalz/Saarland e.V. wurde gebeten, bei der Beratung seiner Mitglieder diese Rechtsauffassung zu berücksichtigen.

6. LEBEN DIGITAL

6.1. Vereine

Nicht nur Unternehmen, Behörden und Institutionen sind verpflichtet, die Regelungen der DS-GVO und des neuen BDSG umzusetzen, sondern auch alle Vereine, einschließlich der gemeinnützigen, nicht eingetragenen oder nicht rechtsfähigen Vereine. Angefangen vom Mitgliedsantrag über Einladungen zu Veranstaltungen oder Mitgliederversammlungen bis hin zum Internetauftritt eines Vereins – im Vereinsleben gibt es viele Szenarien, in denen personenbezogene Daten, wie Name, Anschrift, E-Mail-Adresse, Geburtsdatum oder Geschlecht verarbeitet werden. Die Auseinandersetzung mit der neuen Rechtslage ist daher unverzichtbar.

6.1.1. An der Belastungsgrenze

Unzählige schriftliche und telefonische Anfragen von Vereinsaktiven zur Umsetzung der DS-GVO erreichten den LfDI seit Anfang des Jahres mit steigender Tendenz und gingen weit über die Beratungskapazitäten der Behörde hinaus. Zwar galten datenschutzrechtliche Vorgaben für Vereine auch bereits vor dem 25. Mai 2018 und es gab zum Teil umfangreiche Informationsbroschüren anderer Datenschutzaufsichtsbehörden für Vereine, auf die der LfDI auf seiner Internetseite verlinkt hatte. Es stellte sich jedoch heraus, dass viele Vereine dem Thema Datenschutz bisher nicht viel Beachtung geschenkt hatten und dass sie sich nun oftmals mit der Fülle an Informationen überfordert sahen. Teilweise fanden sie dort dennoch ihre konkrete Fragestellung nicht beantwortet.

6.1.2. Datenschutz kompakt

Um kleineren Vereinen und ehrenamtlich Engagierten bei der Umsetzung der Anforderungen der DS-GVO mit praxisorientierten Informationen eine Hilfestellung zu geben, reagierte der LfDI darauf mit der Veröffentlichung einer Handreichung für Vereinsvorstände und ehrenamtlich Tätige, die kurz und prägnant darstellt, welche datenschutzrechtlichen Rechte und Pflichten im Rahmen der Vereinsarbeit mit Geltung der DS-GVO zu berücksichtigen sind. Auf weiterführende Informationen wird darin lediglich an den entsprechenden Stellen verwiesen. Diese Art der Darstellung stieß auf sehr positive Resonanz. Die Handreichung ist unter dem folgenden Link abrufbar: **https://s.rlp.de/dsgvoverein**

6.1.3. Zielgruppenorientierter Fragenkatalog schafft schnelle Abhilfe

Die zielgruppenorientierte Bereitstellung von Datenschutzinformationen wurde zudem durch eine umfangreiche Liste von Fragen, die typischerweise im Rahmen der Vereinstätigkeit aufkommen, und den entsprechenden Antworten und Empfehlungen des LfDI zur praktischen Umsetzung sowie durch passende Vordrucke ergänzt. So konnten zumindest die häufigsten Fragen einer zügigen Beantwortung zugeführt werden. Der Fragenkatalog wurde kontinuierlich erweitert und ist unter dem folgenden Link abrufbar: **https://s.rlp.de/vereine**

6.1.4. Informationsveranstaltungen

Darüber hinaus stand der LfDI selbst und vertreten durch seine Mitarbeiterinnen und Mitarbeiter in einer Reihe von Informationsveranstaltungen für Vereine zur Beantwortung

der konkreten Fragen der Vereinsaktiven zur Verfügung und kam dabei sehr schnell an seine Belastungsgrenzen. Viele Anfragen zur Durchführung weiterer Veranstaltungen mussten aus Kapazitätsgründen daher leider abgelehnt werden.

6.1.5. Die häufigsten Umsetzungsfragen der Vereine

Die häufigsten Fragen gingen ein zum Umgang mit und zur Veröffentlichung von Vereinsfotos, zur Rechtsgrundlage für die Verarbeitung personenbezogener Daten von Mitgliedern, Vorständen, Newsletterempfängern und Veranstaltungsgästen, zur Umsetzung der Informationspflicht nach Art. 13 DS-GVO, zur Bestellpflicht eines Datenschutzbeauftragten im Verein, zu Löschpflichten und zur datenschutzkonformen Gestaltung der Vereins-Webseite.

Im Rahmen der zeitlichen Möglichkeiten befasste sich der LfDI auch mit schwierigeren Fragen des Einzelfalles, wie etwa der Verteilung der Verantwortlichkeiten in Vereinen oder Verbänden mit komplexer Organisationsstruktur, der Sicherstellung der rechtmäßigen Verarbeitung besonders sensibler Daten bei Vereinen z.B. aus dem Bereich der Pflege, Gesundheit, der sozialen Unterstützung oder mit vornehmlich minderjährigen Mitgliedern oder mit Fragen zur Rechtmäßigkeit der Datenverarbeitung, wenn der Vereinszweck die regelmäßige oder auch unregelmäßige Kommunikation mit Stellen in Ländern außerhalb der Europäischen Union umfasst und dabei nicht nur personenbezogene Daten von Vereinsmitgliedern, sondern auch die von Dritten verarbeitet werden.

Diese Fragen stellen nur einen Ausschnitt des sehr breiten Spektrums des Beratungsbedarfs dar. Auch bis zum Jahresende ließ die hohe Anzahl eingehender Beratungsanfragen nicht nach, die aus Kapazitätsgründen bis zum heutigen Tag nicht vollständig abgearbeitet werden konnten.

6.2. Verbraucher

Bereits vor Geltungsbeginn der DS-GVO stieg die Zahl der Beschwerden gegen Unternehmen wegen mutmaßlicher Datenschutzverstöße an. Dies zeigte, dass das neue Regelwerk und die damit verbundene Berichterstattung in den Medien die Bürgerinnen und Bürger nicht nur in Datenschutzfragen sensibilisierte, sondern sie auch darin motivierte, ihre Rechte tatsächlich geltend zu machen. Dies ist eine erfreuliche Entwicklung und dient der gezielten Verbesserung des Datenschutzes in den einzelnen Unternehmen.

6.2.1. Geltendmachung des Auskunftsanspruchs

Ein Schwerpunkt der eingegangenen Beschwerden beim LfDI gegen nicht-öffentliche Stellen betraf die ausgebliebene oder unzureichende Erfüllung des von betroffenen Personen geltend gemachten Auskunftsanspruchs durch den Verantwortlichen. Bereits nach altem Recht hatte jedermann das Recht auf Auskunft hinsichtlich der Verarbeitung der ihn oder sie betreffenden personenbezogenen Daten. Dieses Recht findet sich in Art. 15 DS-GVO wieder. Diese Vorschrift gewährt ein nun noch umfangreicheres Auskunftsrecht. Gerade in der konkreten Reichweite des Auskunftsanspruchs jedoch bestand und besteht weiterhin noch Klärungsbedarf.

Inzwischen entschied das Landgericht Köln in seinem Urteil vom 18. März 2019 (Az. 26 O 25/18), dass der Auskunftsanspruch dahingehend begrenzt sei, dass z.B. interne Vermerke

des Verantwortlichen und Kopien bereits übersendeten Schriftverkehrs nicht vom Recht auf Auskunft nach Art. 15 DS-GVO umfasst seien. Zudem stellten rechtliche Bewertungen oder Analysen keine personenbezogenen Daten in diesem Sinne dar. Das Auskunftsrecht diene nicht zur Erleichterung der Buchführung des Einzelnen, sondern der Überprüfung der Rechtmäßigkeit der Verarbeitungen des Verantwortlichen. Ob sich aber diese Rechtsprechung in allen Teilen durchsetzen wird, bleibt abzuwarten. Dennoch gibt das Urteil zumindest eine Richtung vor, die der Sicherheit bei der Rechtsanwendung zuträglich ist.

6.2.2. Ausnutzung der Zwangslage von Mietinteressenten

Frustriert sind oftmals auch Mietinteressenten, die, um einen Besichtigungstermin in einer begehrten Wohnung zu erlangen, sensibelste Daten wie Gehaltsabrechnungen und Ausweiskopien an potentielle Vermieter senden, wohlweißlich, dass diese – zumindest in diesem frühen Stadium – rechtswidrig verlangt werden. Vermieter und Makler nutzen die Zwangslage der betroffenen Personen aus, um selbst Zeit und Kosten zu sparen, indem bestimmte Bewerber schon frühzeitig aussortiert werden können.

Wenn auch betroffene Personen in der Regel erst nach erfolgloser Wohnungsbewerbung bei der Aufsichtsbehörde Beschwerde einlegen, also erst dann, wenn es schon zum Datenschutzverstoß im konkreten Fall gekommen ist, helfen sie dadurch dennoch, den Datenschutz im Wohnungs- und Immobilienmarkt insgesamt für alle nachhaltig zu verbessern.

Die DSK hat die Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressenten Anfang 2018 aktualisiert. Sie dient nicht nur den Verantwortlichen zur Überprüfung und ggf. Anpassung der eigenen Vorgehensweise, um sich datenschutzkonform zu verhalten. Sie ist auch eine Hilfestellung für betroffene Personen, um einschätzen zu können, ob ein Datenschutzverstoß in ihrem Fall vorliegen könnte. Die Orientierungshilfe ist unter dem folgenden Link abrufbar: **https://s.rlp.de/mietauskunft**

6.2.3. Datenschutzbeschwerde als Mittel zum Zweck

Gerne möchten Beschwerdeführer das Beschwerderecht bei der Datenschutzaufsichtsbehörde unterstützend zur Geltendmachung zivilrechtlicher Ansprüche nutzen – jedoch nicht immer mit Recht. Entspricht etwa die Versicherung nicht dem Leistungsantrag des Versicherungsnehmers, handelt es sich um einen rein zivilrechtlichen Streit, der nicht im Verwaltungsrechtsweg über die Aufsichtsbehörde beigelegt werden kann. Ebenso wenig kann diese bei nicht gelieferten Waren oder verschollenem Eigentum Abhilfe schaffen.

Bekannt wurden allerdings auch umgekehrte Fälle, in denen Mitarbeiter von Verantwortlichen den Auskunftssuchenden mitteilten, dass sie aus Datenschutzgründen keine Auskunft erteilen dürften. Diese Aussage mutet auf den ersten Blick an wie eine Posse, war in begründeten Einzelfällen dann aber doch gerechtfertigt, z.B. wenn das Auskunftsgesuch den erforderlichen Umfang des Auskunftsrechts überschritt.

6.2.4. Informationsveranstaltung für Verbraucher zum neuen Datenschutzrecht

Das neue Datenschutzrecht will einen modernen Rechtsrahmen für das Recht auf informationelle Selbstbestimmung in der Europäischen

Union setzen und verspricht einen besseren Schutz durch mehr Kontrolle der Verbraucherinnen und Verbraucher über die Datenverarbeitung und durch einen höheren Bußgeldrahmen bei Rechtsverstößen.

In einer gemeinsamen Diskussionsveranstaltung des LfDI und der Verbraucherzentrale Rheinland-Pfalz e.V. kamen am 16. April 2018 in Mainz folgende fachkundige Podiumsteilnehmer aus Wirtschaft sowie Daten- und Verbraucherschutz zusammen. Unter dem Titel „Das neue Datenschutzrecht unter der Lupe - Diskussion zur DS-GVO“ beleuchteten sie die Vor- und Nachteile der ab dem 25. Mai 2018 geltenden Regelungen aus Verbrauchersicht sowie die Herausforderungen, aber auch die Chancen für Unternehmen bei der Umsetzung der DS-GVO.

Der LfDI sieht vor allem die erheblichen Verbesserungen, die die DS-GVO für die Rechte der Bürgerinnen und Bürger bringt. Neben bestehenden Rechten wie demjenigen auf Auskunft, wird nun das Recht auf Vergessenwerden festgeschrieben. Auch das neu eingeführte Recht auf Datenübertragbarkeit, also die einfache Möglichkeit, die eigenen Informationen von einem alten zu einem neuen Anbieter als „Datenpaket“ mitzunehmen, bedeutet eine große Erleichterung im Alltag. Und der Einzelne kann seine Rechte mit Hilfe der Datenschutzbeauftragten einfacher durchsetzen.

Die Veranstaltung im Plenarsaal des rheinland-pfälzischen Landtags erfreute sich einer großen Besucherzahl. Das Publikum erlebte eine spannende Diskussionsrunde. Die Abendveranstaltung war Teil einer Veranstaltungsreihe des LfDI in bewährter Kooperation mit der Verbraucherzentrale Rheinland-Pfalz e.V. Sie diente der datenschutzrechtlichen Sensibilisierung und Information der Verbraucherinnen und Verbraucher und Unternehmerinnen und Unternehmer gleichermaßen.

6.2.5. Fünfter Verbraucherdialog „Wearables: Fitnessarmbänder & Co.“

Schritte zählen, Schlafgewohnheiten beobachten, den Blutdruck oder die Blutwerte messen – sogenannte Wearables, wie zum Beispiel Fitnesstracker, aber auch smarte Kleidung machen es möglich und werden von immer mehr Menschen genutzt. Wearables sind am Körper tragbare Computertechnologien, die körperliche Aktivitäten und Abläufe messen und Aussagen über Fitness, Gesundheit und Wohlbefinden ermöglichen.

Mit den Vor- und Nachteilen dieser technischen Möglichkeiten befasste sich der 5. Verbraucherdialog, der am 12. September 2017 in Mainz startete und mit der Pressekonferenz am 12. April 2018 endete. Im Austausch mit Expertinnen und Experten aus Wirtschaft und Wissenschaft sowie von Behörden und Organisationen wurden im Rahmen mehrerer Arbeitstreffen praxisorientierte Empfehlungen für Anbieter erarbeitet, wie Wearables verbraucher- und datenschutzfreundlich angeboten werden können und welche besonderen Anforderungen zu beachten sind. Dabei standen Datenschutzgrundsätze wie die Transparenz der Datenübermittlungen, Datensparsamkeit, Datensicherheit sowie der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen im Fokus.

Der Verbraucherdialog ist eine Initiative des Verbraucherschutzministeriums in Kooperation mit der Verbraucherzentrale Rheinland-Pfalz e.V. und dem LfDI. Die Empfehlungen sollen dazu beitragen, dass Verbraucherinnen und Verbraucher neue Technologien unter Wahrung ihres Rechts auf informationelle Selbstbestimmung mit Vertrauen und Mehrwert nutzen können. Sie sind auf der folgenden Internetseite abrufbar: **https://verbraucherdialog.rlp.de**

7. BESCHÄFTIGTENDATEN-SCHUTZ

7.1. Bußgelder gegenüber öffentlich Bediensteten

Der LfDI musste sich in der Vergangenheit vermehrt mit Fällen auseinandersetzen, in denen Polizeibeamte zu privaten Zwecken Personenabfragen in polizeilichen Informationssystemen vorgenommen hatten. Dabei kam es zu Abfragen von ehemaligen Lebensgefährten, Nachforschungen im Auftrag von Verwandten oder zur Nutzung der Telefonnummer einer Zeugin, um dieser über WhatsApp Avancen zu machen.

Der rheinland-pfälzische Gesetzgeber hat sich im Rahmen der Neufassung des LDSG dagegen entschieden, Bußgelder gegenüber öffentlichen Stellen zu ermöglichen. § 24 Abs. 3 LDSG verbietet dies sogar ausdrücklich. Mit § 24 Abs. 1 LDSG ist allerdings eine Vorschrift über bußgeldbewehrte Ordnungswidrigkeiten in Bezug auf einzelne Beschäftigte aufgenommen worden. Hiernach handelt ordnungswidrig, wer entgegen den Bestimmungen der DS-GVO, des LDSG oder einer anderen Rechtsvorschrift über den Schutz personenbezogener Daten, personenbezogene Daten, die nicht offenkundig sind, abruft, übermittelt oder weitergibt. Dieses Verhalten sanktioniert § 24 Abs. 2 LDSG mit einem Bußgeld bis zu 50.000 EUR.

Kommt es zu einer unzulässigen Datenverarbeitung, liegt die datenschutzrechtliche Verantwortlichkeit zunächst beim Dienstherrn/Arbeitgeber und nicht bei dem einzelnen Beschäftigten, der pflichtwidrig Daten verarbeitet hat. Der Anwendungsbereich des § 24 LDSG ist nach Auffassung des LfDI aber in den Fällen eröffnet, in denen ein Beschäftigter dermaßen pflichtwidrig von den datenschutzrechtlichen Vorgaben abweicht, dass er sich gewissermaßen zum Verantwortlichen „aufschwingt". Dies ist insbesondere bei ausschließlich privat motivierten Datenabfragen und –nutzungen - wie in den eingangs genannten Beispielen - der Fall. Der Beschäftigte handelt dann weder auf Weisung noch mit Kenntnis oder Billigung des Arbeitgebers, sondern entscheidet selbst über die Mittel und die Zwecke der Datenverarbeitung. Seine Tätigkeit kann dem Arbeitgeber dann nicht mehr zugerechnet werden. Im Falle eines solches „Exzesses" besteht nach § 24 LDSG ausnahmsweise die Möglichkeit, gegenüber dem einzelnen öffentlich Bediensteten ein Bußgeld zu verhängen.

Von einem Exzess kann indes nicht ausgegangen werden, wenn dienstlich gebotene Datenabfragen lediglich unter Verstoß gegen Zuständigkeitsregelungen erfolgen oder ein Mitarbeiter seine eigenen Daten abfragt.

7.2. Betriebs- und Personalräte sind und bleiben Teil des „Verantwortlichen"!

Unter Anwendung des bis zum 25. Mai 2018 geltenden BDSG gingen sowohl die Datenschutzaufsichtsbehörden in ihrer Praxis als auch das Bundesarbeitsgericht in ständiger Rechtsprechung davon aus, dass der Betriebsrat oder andere Interessenvertretungen als Teil der für die Datenverarbeitung verantwortlichen Stelle anzusehen sei. Begründet wurde dies damit, dass nur natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts verantwortliche Stelle sein konnten (§ 3 Abs. 7 i. V. m. § 2 Abs. 4 BDSG a. F.).

Durch das Inkrafttreten der DS-GVO sahen sich die Aufsichtsbehörden einiger Länder dazu veranlasst, dies einer Neubewertung zu unterziehen. Grund dafür ist der Wortlaut des Art. 4 Nr. 7 DS-GVO, welcher bestimmt, dass der für

die Datenverarbeitung Verantwortliche „die natürliche oder juristische Person, Behörde oder Einrichtung oder andere Stelle“ ist, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Seither herrscht Uneinigkeit im Hinblick auf die Frage, ob auch der Personal- bzw. Betriebsrat eines Verantwortlichen als eigenverantwortliche Stelle anzusehen ist. Bejaht man dies, müssten Personal- und Betriebsräte eigene Datenschutzbeauftragte bestellen und auch die übrigen formellen Verpflichtungen eines Verantwortlichen nach der DS-GVO erfüllen, also etwa ein Verzeichnis der Verarbeitungstätigkeiten führen, die Beschäftigten gem. Art. 13 DS-GVO bei erstmaliger Datenerhebung informieren und bei besonders risikobehafteten Verfahren eine DSFA durchführen. Auch Bußgelder der Datenschutzaufsichtsbehörden gegenüber einem Betriebsrat wären möglich.

Nach Auffassung des LfDI sind Betriebs- und Personalräte nicht selbst „Verantwortlicher“, sondern lediglich Teil des Verantwortlichen. Die Gründe dafür sind vielfältig:

Zur Bestimmung der Eigenschaft als Verantwortlicher ist nach der o.g. Definition maßgeblich, wer über die Mittel und Zwecke der Verarbeitung personenbezogener Daten bestimmt. Damit ein Personal- bzw. Betriebsrat „Verantwortlicher“ im Sinne der DS-GVO sein kann, wäre es also notwendig, dass diesem bei der Datenverarbeitung ein erheblicher Entscheidungsspielraum unabhängig vom Arbeitgeber zusteht.

In Bezug auf Betriebsräte ergibt sich zwar aus dem Strukturprinzip der Betriebsverfassung und aus einzelnen Regelungen des Betriebsverfassungsgesetzes, dass der Betriebsrat hinsichtlich seiner Aufgabenerfüllung eine vom Arbeitgeber unabhängige Stelle ist. Die autonome Interessenwahrnehmung mit dem Ziel eines angemessenen Ausgleichs ist nur möglich, wenn Arbeitgeber und Betriebsrat unabhängig voneinander ihre Meinung bilden, also insbesondere Verhandlungsziele und mögliche Kompromisslinien bestimmen können. Jedoch ist zu beachten, dass der Betriebsrat keine juristische oder natürliche Person ist und nicht über eine generelle Rechts- und Vermögensfähigkeit verfügt, die ihn befugt, am allgemeinen Rechtsverkehr teilzunehmen. Es besteht lediglich eine partielle Vermögensfähigkeit insoweit, als das Betriebsverfassungsgesetz rechtliche Ansprüche zur Erstattung von erforderlichen Kosten der Betriebsratsarbeit und zur Deckung des Sachaufwands im erforderlichen Umfang vorsieht, wie z. B. in § 40 Abs. 1 und 2 BetrVG. Aus dieser Vorschrift ergibt sich zugleich, dass die vom Betriebsrat genutzte Informations- und Kommunikationstechnik vom Arbeitgeber bereitgestellt wird. Dies erfolgt gemäß § 40 Abs. 2 BetrVG jedoch nur zur Ermöglichung der laufenden Geschäftsführung. Welche Aufgaben diese laufende Geschäftsführung umfasst, sind klar durch das Gesetz vorgegeben. Mittel und Zwecke der Datenverarbeitung sind demnach bereits derart festgelegt, dass dem Betriebsrat insoweit keine eigene Entscheidungsbefugnis zukommt.

Hinzu kommt, dass aufgrund der Vermögenslosigkeit des Betriebsrates Bußgelder gegen diesen nicht vollstreckbar wären und daher ins Leere laufen würden. Dies schließt nicht aus, dass gegen einzelne Betriebsratsmitglieder bei einem so genannten „Exzess“, also einer pflichtwidrigen Datenverarbeitung für eigene Zwecke, ein Bußgeldverfahren eingeleitet werden kann.Grobe Verstöße des Betriebsrates als Gremium können den Arbeitgeber dazu berechtigen, beim Arbeitsgericht die Auflösung des Betriebsrates zu beantragen (§ 23 Abs. 1 S. 1 BetrVG). Dies zeigt, dass sich der Betriebs-

rat in einer im Vergleich zum Arbeitgeber erheblich schwächeren Position befindet, was eindeutig gegen die Stellung des Betriebsrates als Verantwortlicher spricht. Neben diese Überlegungen tritt auch ein systematisches Argument. Art. 4 Ziff. 7 DS-GVO enthält eine Öffnungsklausel für die Mitgliedstaaten in Bezug auf Regelungen zum Verantwortlichen. Der deutsche Gesetzgeber hat mit § 26 BDSG neu eine Hervorhebung der Interessenvertretung vorgenommen, ohne deren eigenständige Verantwortlichkeit zu regeln. Im Hinblick auf die Personalräte öffentlicher Stellen kann nichts anderes gelten. Hier kommt hinzu, dass die Bestellung und Abberufung des behördlichen Datenschutzbeauftragten nach dem Landespersonalvertretungsgesetz mitbestimmungspflichtig ist (§ 80 Abs. 2 Nr. 8 LPersVG). Wäre der Personalrat selbst „Verantwortlicher" müsste er somit bei der Bestellung/Abberufung seines eigenen Datenschutzbeauftragten zustimmen, was wiederum zu Wertungswidersprüchen führen würde. Auch nach Wirksamwerden der DS-GVO haben sich die datenschutzrechtlichen Verpflichtungen der Betriebs- und Personalräte daher nicht wesentlich verändert. Als Teil des Betriebs bzw. der Behörde müssen sie nicht die Pflichten eines Verantwortlichen nach der DS-GVO erfüllen.

7.3. Unzulässige Fragen im Bewerbungsverfahren

Aufgrund einer Beschwerde hatte der LfDI einen Fragebogen datenschutzrechtlich zu bewerten, welcher auf der Internetseite eines Unternehmens für Bewerber abrufbar und von diesen ausgefüllt zu den Bewerbungsunterlagen zu reichen war. In diesem Fragebogen wurde unter anderem nach Angaben zum derzeitigen Bruttoverdienst, zu Namen und Geburtsdatum eines gegebenenfalls vorhandenen Ehepartners, zu einer eventuellen Ausmusterung, zu Schulden, der Raucher-eigenschaft sowie dem Vorliegen einer Schwangerschaft verlangt. Abschließend erfolgte der Hinweis, dass die wissentliche Falschbeantwortung der Fragen zur Beendigung des Arbeitsverhältnisses führen könne. Ausgangspunkt der rechtlichen Bewertung ist § 26 Abs. 1 BDSG. Danach dürfen personenbezogene Daten von Beschäftigten für die Zwecke des Beschäftigungsverhältnisses unter anderem dann verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist. Bei der Erhebung von Bewerberdaten sind die von der Rechtsprechung entwickelten Grundsätze zum Fragerecht des Arbeitgebers einzubeziehen. Hiernach ist zu prüfen, ob ein berechtigtes, billigenswertes und schutzwürdiges Interesse des Arbeitgebers an der Beantwortung seiner Fragen bzw. der sonstigen Informationsbeschaffung besteht, welches das Interesse des Arbeitnehmers an der Geheimhaltung seiner Daten überwiegt. Der o.g. Bewerbungsbogen genügt in weiten Teilen nicht diesen Anforderungen. Die begehrten Informationen sind nicht notwendig, um die Fähigkeiten des Bewerbers im Hinblick auf die zu besetzende Stelle zu beurteilen. In diesem Zusammenhang ist zu beachten, dass im Bewerbungsverfahren der Rückgriff auf eine Einwilligung regelmäßig ausscheidet. Aufgrund der faktischen Zwangslage kann nicht von einer Freiwilligkeit der Einwilligung ausgegangen werden (vgl. § 26 Abs. 2 BDSG). Werden im Bewerbungsverfahren unzulässige Fragen durch den Arbeitgeber gestellt, steht dem Bewerber das sog. „Recht zur Lüge" zu, was dazu führt, dass der Arbeitgeber den Vertrag auch bei wissentlicher Falschbeantwortung nicht wegen arglistiger Täuschung anfechten kann. Nachdem der LfDI den Umfang des Datakataloges gegenüber dem Unternehmen problematisierte, wurde der Fragebogen umgehend von der Webseite genommen.

7.4. Übermittlung von Beschäftigtendaten nach China

In der heutigen globalisierten Welt gehört es vielerorts zur beruflichen Tätigkeit, Geschäftsreisen ins Ausland zu unternehmen. Wo bei Reisen innerhalb der Europäischen Union beim Grenzübertritt das Vorzeigen eines Dokumentes, das den Inhaber als Unionsbürger ausweist, ausreichend ist, bedarf es an anderer Stelle zuvor der Erteilung eines Visums.

Der LfDI wurde um Rat ersucht, welche Regelungen in Bezug auf den Mitarbeiterdatenschutz gelten, wenn ein wesentlicher Teil der unternehmerischen Tätigkeit mit Dienstreisen nach China verbunden ist. Das Antragsformular für ein entsprechendes Visum beinhalte dabei u.a. die Verpflichtung, Angaben über erteilte Visa anderer Staaten, psychische Störungen oder private Reisen zu machen; auch personenbezogene Daten Dritter, wie beispielsweise solche von Ehegatten, Kindern und Eltern sollten angegeben werden. Klärungsbedürftig war, ob ein Arbeitgeber die im Rahmen des Antragsverfahrens verlangten personenbezogenen Daten seiner Beschäftigten an die visumsausstellende Behörde übermitteln darf.

Bei der Bewertung dieser Frage spielen verschiedene Aspekte eine Rolle:

Zunächst ist es selbstverständlich jedem Land unbenommen, seine Einreiseregelungen zu gestalten. Dies gilt auch für Länder, deren Datenschutzniveau hinter dem der Europäischen Union zurückbleibt. So ist es einer Privatperson möglich, von Reisen in solche Länder Abstand zu nehmen, wenn sie nicht damit einverstanden ist, dass in einem kaum zu überblickenden Umfang personenbezogene Daten über sie gespeichert werden. Anders ist die Situation im Beschäftigungsverhältnis, wenn Geschäftsreisen in Drittländer zur vertraglich geschuldeten Leistung gehören. Im Ausgangspunkt handelt es sich bei der Weitergabe personenbezogener Daten von Mitarbeitern zu Zwecken der Visumserteilung um eine Datenverarbeitung im Beschäftigungsverhältnis, welche sich an den Maßstäben des § 26 BDSG (BDSG) messen lassen muss. Gemäß § 26 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten von Beschäftigten unter anderem nur dann verarbeitet werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Erforderlich ist die Datenverarbeitung insbesondere, wenn der Arbeitgeber diese zur Erfüllung seiner – gegenüber dem Beschäftigten oder Dritten – bestehenden gesetzlichen Pflichten, für die Erfüllung seiner vertraglichen Pflichten oder zur Wahrnehmung seiner gesetzlichen oder vertraglichen Rechte benötigt. Für die Bestimmung der Erforderlichkeit kommt es auf die berechtigten Interessen und Zwecke des Arbeitgebers an. Hierbei ist grundsätzlich in Rechnung zu stellen, dass dem Arbeitgeber die nach Art. 12 GG verbriefte unternehmerische Freiheit zusteht, zu entscheiden, wie er seinen Betrieb organisiert (vgl. BeckOK DatenschutzR/Riesenhuber, 26. Ed. 1.11.2018, BDSG § 26 Rn. 114). Klassischerweise muss die Beurteilung, ob eine Erforderlichkeit vorliegt, vor dem Hintergrund erfolgen, dass die Datenverarbeitung nur innerhalb Deutschlands oder auch der Grenzen der EU vorgenommen wird. Kommt es zu einer Datenübermittlung in ein o. g. Drittland, hat der Verantwortliche zunächst die Grundsätze bezüglich der Übermittlung personenbezogener Daten an Drittländer gemäß Art. 44 ff. DS-GVO einzuhalten. Allerdings handelt es sich bei den dort betroffenen personenbezogenen Daten in der Regel um solche, die mit dem Beschäftigungsverhältnis in Zusammenhang stehen, beispielsweise Daten zu Zwecken der Personalverwaltung bei international tätigen Konzernen mit Hauptsitz in einem Drittland.

Problematisch bei Datenübermittlungen zu Zwecken der Visumserteilung ist jedoch, dass diese regelmäßig auch Informationen über private Verhältnisse einer Person beinhalten, die diese im Beschäftigungsverhältnis nicht angeben müsste. Sollte sich erst während eines bestehenden Beschäftigungsverhältnisses zeigen, dass Geschäftsreisen in Drittstaaten notwendig werden, kann der Beschäftigte aus Sicht des LfDI nicht auf der Grundlage des § 26 Abs. 1 S. 1 BDSG dazu gezwungen werden, weitergehende Eingriffe in sein elementares Recht auf informationelle Selbstbestimmung zu dulden, als dies allein aufgrund innerstaatlicher Vorschriften zulässig wäre. In diesem Fall kommt zwar grundsätzlich der Weg über eine Einwilligungserklärung des Beschäftigten in Betracht. § 26 Abs. 2 BDSG gestattet aber die Verarbeitung personenbezogener Daten von Beschäftigten aufgrund einer Einwilligung nur, wenn diese freiwillig erteilt wurde. Von Freiwilligkeit ist wiederum nur auszugehen, wenn der Beschäftigte eine echte Wahlmöglichkeit hat. Für die Beurteilung der Freiwilligkeit der Einwilligung sind insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Von einer echten Wahlmöglichkeit ist nicht mehr auszugehen, wenn der betroffene Beschäftigte ohne die Einwilligung seine berufliche Tätigkeit faktisch nicht mehr ausüben könnte. Sollte ein Beschäftigter seine Einwilligung verweigern, muss also sichergestellt werden, dass er in anderen Bereichen des Unternehmens eingesetzt werden kann.

Ein weiteres Problem ergibt sich, wenn im Visumsantrag sensible Daten, wie beispielsweise das Vorhandensein psychischer Erkrankungen abgefragt werden. Dabei handelt es sich um besondere Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO (DS-GVO). Solche dürfen gemäß § 26 Abs. 3 BDSG zu Zwecken des Beschäftigungsverhältnisses nur verarbeitet werden, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und dem Sozialschutz erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen (zu der Bedeutung siehe 7.3.).

Weiterhin bedenklich ist die Verpflichtung zur Angabe personenbezogener Daten von am Beschäftigungsverhältnis nicht Beteiligten, z. B. Kindern, Ehegatten oder Eltern. Diese Datenverarbeitung bemisst sich nicht nach § 26 BDSG, da diese Vorschrift nur im Verhältnis zwischen Arbeitgeber und Arbeitnehmer zum Tragen kommt. Ein anderer Tatbestand der DS-GVO, der diese Art der Datenverarbeitung rechtfertigten würde, ist nicht ersichtlich.

Zwar ist auch im deutschen Recht die Verarbeitung von personenbezogenen Daten, die nicht im unmittelbaren Zusammenhang mit dem Beschäftigungsverhältnis stehen, im Rahmen von Sicherheitsüberprüfungen unter den Voraussetzungen des Sicherheitsüberprüfungsgesetzes (SÜG) zulässig. Solche werden immer dann vorgenommen, wenn Personen im Rahmen ihrer beruflichen Tätigkeit mit sicherheitsempfindlichen Tätigkeiten im Sinne des SÜG betraut werden sollen. Je nachdem, für welche Geheimhaltungsstufe eine Freigabe erfolgt, ist auch die Überprüfung von Lebenspartner oder anderen einzubeziehenden Personen vorgesehen und damit auch die Übermittlung deren personenbezogener Daten an die überprüfende Stelle. Zu diesem Personenkreis gehören jedoch weder die Eltern noch die Kinder der zu überprüfenden Person. Außerdem ist auch in diesem Fall die Einwilligung des Beschäftigten und der einzubeziehenden Person für die Durchführung der Sicherheitsüberprüfung unumgänglich.

Mit Blick auf die wirtschaftliche Bedeutung international agierender Unternehmen ist es wichtig, die unternehmerischen Interessen mit den geltenden Datenschutzregeln, vor allem derer zugunsten von Beschäftigten, in Einklang zu bringen. Transparenz und Einwilligung kommen daher eine maßgebliche Bedeutung zu.

Steht bereits vor Aufnahme der Tätigkeit fest, dass Geschäftsreisen in Drittländer mit geringem Datenschutzniveau notwendig werden, ist daher spätestens im Bewerbungsgespräch auf diesen Umstand hinzuweisen und die Voraussetzungen für die Visumsbeantragung transparent zu machen. Der Bewerber kann dann im Vorfeld darüber entscheiden, ober er eine solche Stelle annehmen möchte oder nicht. Dabei muss auch darauf hingewiesen werden, dass das Einholen der Einwilligung der von der Visumsbeantragung betroffenen sonstigen Personen zwingend erforderlich ist.

8. MEDIEN

Wie in allen Bereichen waren auch im Medienbereich mit Geltungsbeginn der DS-GVO ein erhöhtes Beschwerdeaufkommen und eine erhöhte Nachfrage nach Informationen durch Verantwortliche zu verzeichnen.

8.1. Veröffentlichung von Bildern

Eine regelmäßige Tätigkeit war die Bearbeitung von Beschwerden gegen die Veröffentlichung von Fotografien der Beschwerdeführer auf Webseiten oder in sozialen Netzwerken durch andere Personen. Diese Veröffentlichungen erfolgen regelmäßig durch verschiedenste Akteure, z.B. durch Vereine, durch Arbeitgeber, durch Kommunen oder durch Privatpersonen. Der LfDI hat bei Beschwerden gegen solche Verarbeitungen regelmäßig zu prüfen, ob eine Rechtsgrundlage für die Veröffentlichung der personenbezogenen Daten vorliegt und falls nicht, auf die Löschung der Fotografien hinzuwirken.

Als Rechtsgrundlage für die Veröffentlichung von Personenfotografien durch privatrechtliche Verantwortliche kann in bestimmten Konstellationen die Verarbeitung aufgrund berechtigter Interessen 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. Sprechen aber im konkreten Fall die Interessen der abgebildeten Person gegen eine Verarbeitung nach Art. 6 Abs. 1 lit. f DS-GVO, kann die Verarbeitung in der Regel nur aufgrund einer informierten, freiwilligen und ausdrücklichen Einwilligung nach Art. 6 Abs. 1 lit. a, Art. 7 DS-GVO erfolgen. In beiden Fällen können die betroffenen Personen auch im Nachhinein die Löschung der

Fotografien verlangen. Während für die Verarbeitung nach Art. 6 Abs. 1 lit. f DS-GVO ein Widerspruchsrecht besteht, kann eine Einwilligung mit Wirkung für die Zukunft zurückgenommen werden.

8.2. DSGVO-Konformität von Webseiten

Der in datenschutzrechtlicher Hinsicht rechtmäßige Betrieb von Webseiten hat den LfDI ebenfalls besonders beschäftigt.

Zum einen gingen viele Anfragen von Verantwortlichen ein, die Hinweise darauf erhalten wollten, welche Anforderungen der DS-GVO sie umzusetzen haben. Allerdings liegt der datenschutzkonforme Betrieb von Webseiten in der Verantwortung der Betreiber. Eine Einzelfallberatung ist nicht leistbar und gehört auch nicht zu den Aufgaben des LfDI. Allerdings enthält das Webangebot des LfDI die wichtigsten Informationen und Arbeitsmaterialien zu diesem Themenbereich.

Zum anderen erreichten den LfDI zahlreiche Hinweise auf möglicherweise datenschutzwidrige Webseiten. Diesen Hinweisen geht der LfDI im Rahmen seiner Ressourcen nach. Eine zeitnahe Bearbeitung aller Hinweise ist aber aufgrund ihrer Vielzahl nicht immer möglich gewesen. Regelmäßig ergab die Überprüfung der Webseiten, dass Datenschutzerklärungen nicht den Anforderungen der DS-GVO entsprachen. In der Regel reagierten die Webseitenbetreiber schon auf ein Informationsersuchen des LfDI mit der Überarbeitung ihrer Datenschutzerklärung.

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

8.3. Facebook Fanpages und gemeinsame Verantwortung

Am 5.6.2018 entschied der EuGH (Az: C-210/16), dass zwischen Facebook-Fanpage-Betreibern und Facebook eine gemeinsame Verantwortlichkeit besteht. Die DSK hat am 5.9.2018 einen Beschluss zu den hieraus entstehenden Pflichten der Fanpage-Betreiber gefasst. Diese können die Verantwortung für die Verarbeitung der Nutzungsdaten der Besucher ihrer Fanpages nicht einseitig auf Facebook schieben, sondern sind für die Einhaltung der Regelungen der DS-GVO mitverantwortlich und müssen gegenüber Facebook darauf hinwirken, die Voraussetzungen für einen datenschutzkonformen Betrieb der Fanpages zu schaffen. Gemäß Art. 26 DS-GVO ist außerdem 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.

Die Thematik betrifft neben den privatrechtlichen Fanpage-Betreibern auch öffentliche Stellen in Rheinland-Pfalz[1]. Für diese hat der LfDI schon im Jahr 2016 einen Handlungsrahmen zur Nutzung sozialer Medien veröffentlicht. Dieser Handlungsrahmen wird nach endgültiger gerichtlicher Klärung (erwartet im Herbst 2019) entsprechend aktualisiert werden.

8.4. Webseiten-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. 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. mit Cookies oder Analyse-Diensten wie Google Analytics, sei im Regelfall gemäß Art. 6 Abs. 1 lit. f DS-GVO als Verarbeitung für berechtigte Interessen zulässig und sahen darin teilweise eine Fortführung der bisherigen Erlaubnis zur Profilbildung aus § 15 Abs. 3 TMG. Diese Rechtsauffassung ist auch als „opt-out" 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.

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 Orientierungshilfe 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 des Tracking die Verarbeitung gerade nicht aufgrund berechtigter Interessen durchgeführt werden kann, sondern einer ausdrücklichen Einwilligung bedarf. Die Verarbeitung darf also nur dann stattfinden, wenn die Nutzer eingewilligt haben „opt-in".

Die Positionsbestimmung wurde am 29.3.2019 durch eine Orientierungshilfe konkretisiert und ausdifferenziert. Diese Positionen der DSK werden die Aufsichtstätigkeit hinsichtlich des Trackings im Internet in Zukunft in relevanter Weise betreffen, denn viele Webseiten entsprechen dieser Rechtslage nicht.

[1] Siehe bereits 26. Tätigkeitsbericht, S. 38 f.

9. GESUNDHEIT

9.1. Informationskampagne für Ärzte und Psychotherapeuten zur DS-GVO

Im April 2018 starteten der LfDI und die Kassenärztliche Vereinigung Rheinland-Pfalz zusammen mit der Landesärztekammer und der Landespsychotherapeutenkammer im Rahmen der Initiative „Mit Sicherheit gut behandelt" eine Informationskampagne für Ärzte und Psychotherapeuten zur EU DS-GVO (DS-GVO). Ziel war es einerseits, den Heilberuflern die mit dem Wirksamwerden der DS-GVO verbundene verbreitete Verunsicherung über die datenschutzrechtlichen Vorgaben zu nehmen, andererseits sollten die auf der Website der Initiative veröffentlichten zahlreichen Handlungsempfehlungen zur Umsetzung der DS-GVO (**https://www.mit-sicherheit-gut-behandelt.de/eu-datenschutz-grundverordnung.htm**l) der Fachöffentlichkeit präsentiert werden. Mit dem Informationsangebot versicherten die Kooperationspartner den Teilnehmern ihre Unterstützung bei der Sicherstellung des Datenschutzes im Praxisbetrieb.

In den insgesamt vier Veranstaltungen, die in Trier, Neustadt an der Weinstraße, Koblenz und Mainz stattfanden, konnten über 650 Ärzte und Psychotherapeuten und deren Mitarbeiter erreicht werden. Bei allen Terminen nutzten die Teilnehmer die Gelegenheit, mit den anwesenden Vertretern des LfDI, der KV und den Kammern praktische Fragen zur Umsetzung der datenschutzrechtlichen Vorgaben konstruktiv zu erörtern.

Inhaltliche Schwerpunkte der Veranstaltungen waren einerseits ein Überblick über die mit dem Wirksamwerden der DS-GVO verbundenen Neuerungen des Datenschutzrechts und den sich daraus ergebenden Auswirkungen auf den Praxisbetrieb, andererseits die Bereitstellung eines Maßnahmenplans zur Sicherstellung des Datenschutzes im ärztlichen Alltag. Aus der Beratungspraxis von LfDI und KV wiederkehrende Fragestellungen (FAQ) wurden in einer offenen Diskussionsrunde beantwortet. Schließlich präsentierte der LfDI seine künftige Strategie als Aufsichtsbehörde zur Sicherstellung eines nachhaltigen Datenschutzmanagements in den seiner Aufsicht unterliegenden Heilberufspraxen. Die in der Abschlussveranstaltung der Informationskampagne am 24.10.2018 in Mainz gehaltenen Präsentationen stehen auf der Website der Initiative (**https://www.mit-sicherheit-gut-behandelt.de/eu-datenschutz-grundverordnung/veranstaltungen.html**) zum Abruf bereit.

Die Informationskampagne wurde durch die Darstellung ausgewählter Themenfelder zum Datenschutz in der Arztpraxis in mehreren Ausgaben des rheinland-pfälzischen Ärzteblatts flankiert. Die Landespsychotherapeutenkammer richtete zudem eigens für ihre Mitglieder einen eigenen Newsletter zum Datenschutz ein.

Für das Jahr 2019 haben die Kooperationspartner vereinbart, am Beispiel zweier Pilotpraxen die Umsetzung des Datenschutzrechts direkt zu begleiten und die dabei gemeinsam mit den Praxen erarbeiteten Dokumente als Best-Practice-Beispiele zu veröffentlichen. Das Projekt soll zum Jahresende 2019 abgeschlossen sein.

9.2. Nachlässigkeit im Gesundheitsamt und seine Folgen

Welche gravierenden Folgen sich aus einer Vernachlässigung technisch-organisatorischer Vorkehrungen im Geschäftsbetrieb eines Gesundheitsamtes ergeben können zeigte sich in

einer an den LfDI gerichteten Beschwerde. Gegenstand der Eingabe war das Schreiben eines rheinland-pfälzischen Gesundheitsamtes an eine Bürgerin. Diese wurde um Ausfüllen eines detaillierten Fragebogens gebeten, nachdem bei ihr von einem Labor bestimmte, nach dem Infektionsschutzgesetz meldepflichtige Krankheitserreger nachgewiesen worden waren. In der Betreffzeile des an die Bürgerin gerichteten Anschreibens waren u.a. Informationen zu den nachgewiesenen Krankheitserregern bzw. der sich daraus ergebenden Verdachtsdiagnose enthalten. Trotz der Verwendung eines verschlossenen Briefumschlags war der Inhalt der Betreffzeile durch das Sichtfenster für Dritte wie z.B. den Mitarbeitern des beauftragten Postdienstleisters jederzeit lesbar. Aufgrund dessen bat die Betroffene den LfDI um datenschutzrechtliche Prüfung der Angelegenheit.

Im Rahmen der Sachverhaltsermittlung stellte sich heraus, dass bei dem Verfassen des Schreibens 3 der ursprünglich 5 in der verwendeten Dokumentenvorlage vorgesehenen Leerzeilen zwischen dem Adressfeld und der Betreffzeile gelöscht worden waren. Anders als im Adressfeld waren diese Leerzeilen nicht technisch gegen Veränderungen wie z.B. einer Löschung geschützt. Durch die Löschung und der damit verbundenen Veränderung der räumlichen Anordnung der Betreffzeile war es Dritten möglich, durch das Sichtfenster des verwendeten Briefumschlags den Inhalt des Betreffs zur Kenntnis zu nehmen.

Der LfDI sprach gegenüber der betroffenen Kreisverwaltung eine Beanstandung nach § 17 Abs. 1 Satz 3 LDSG aus. Hauptvorwurf waren die unzureichenden technischen Schutzvorkehrungen gegen Veränderungen der von dem Gesundheitsamt verwendeten Dokumentenvorlagen. Das sich daraus ergebende latente Risiko einer individuellen Verletzung besonders sensibler personenbezogener Daten hatte sich im konkreten Fall bedauerlicherweise realisiert. Aufgrund der besonderen Schutzbedürftigkeit der Gesundheitsdaten und der sich daraus für die Betroffene ergebenden beachtlichen Risiken für ihre Rechte und Freiheiten war aus Sicht des LfDI eine Sanktionierung des Vorfalls geboten.

10. SOZIALES

10.1. Übersendung medizinischer Unterlagen zur Durchführung von Sozialleistungsverfahren

Im Berichtszeitraum war der LfDI wiederholt mit der Frage der datenschutzrechtlichen Zulässigkeit einer Übersendung von Patientenakten oder Bestandteilen daraus durch rheinland-pfälzische Ärzte an das Landesamt für Soziales, Jugend und Versorgung (LSJV) befasst. Die Unterlagen wurden in den zugrunde liegenden Sachverhalten regelmäßig für die Durchführung von Sozialverwaltungsverfahren nach dem SGB IX benötigt. Die anfragenden Arztpraxen waren aufgrund der mit dem Wirksamwerden der DS-GVO seit Mai 2018 geltenden verschärften Sanktionsmöglichkeiten verunsichert, ob ihre bisherige Praxis einer weitgehend standardmäßigen Bereitstellung der von dem LSJV angeforderten Unterlagen ohne unmittelbare Kenntnis der im Einzelfall erforderlichen Schweigepflichtentbindung überhaupt zulässig war.

Der LfDI vertrat in diesem Zusammenhang folgende Rechtsauffassung:

Die Weitergabe patientenbezogener Befundangaben durch Ärzte an Sozialleistungsträger stellt datenschutzrechtlich eine Übermittlung personenbezogener Daten dar, die nur dann zulässig ist, wenn entweder eine Rechtsgrundlage die Berufsangehörigen zur Herausgabe der Daten befugt oder die Patienten darin eingewilligt haben (§ 100 Abs. 1 SGB X). Liegt eine dieser Befugnisse vor, verletzt die Datenübermittlung auch nicht die berufsrechtlichen Vorgaben der ärztlichen Schweigepflicht.

Aus den im Zusammenhang mit der Gewährung von Leistungen nach dem Sozialgesetzbuch IX heranzuziehenden sozialrechtlichen Regelungen kann regelmäßig keine gesetzliche Übermittlungsbefugnis für die beteiligten Ärzte im Sinne von § 100 SGB X entnommen werden, so dass es für die Zulässigkeit der Befundübermittlung auf das Vorliegen einer Einwilligungserklärung der Patienten ankommt. Klärungsbedürftig ist, ob die Ärzte nur dann zur Datenübermittlung befugt sind, wenn ihnen die hierzu erforderliche Einwilligungs- und Schweigepflichtentbindungserklärung des betroffenen Patienten vorliegt, oder ob es ausreicht, dass ihnen der Sozialleistungsträger dessen Existenz versichert.

Die zur Gewährung von Leistungen nach dem SGB IX maßgeblichen Bestimmungen enthalten auch insoweit leider keine Aussage. So fehlt es z.B. – sofern Leistungen zur Teilhabe schwerbehinderter Menschen gewährt werden sollen - in § 152 SGB IX und § 12 Abs. 2 des Gesetzes über das Verwaltungsverfahren der Kriegsopferversorgung (KOVVfG) an einer gesetzgeberischen Klarstellung. Auch in der Berufsordnung für Ärztinnen und Ärzte in Rheinland-Pfalz ist keine entsprechende Festlegung zu erkennen. Letztendlich sind zur Klärung der aufgeworfenen Frage die in den folgenden Regelungen enthaltenen Rechtsgedanken zu berücksichtigen:

- § 67d Abs. 1 Satz 2 SGB X
  Hiernach trägt im Falle der Übermittlung von Sozialdaten auf Ersuchen eines Dritten dieser die Verantwortung für die Richtigkeit der Angaben in seinem Ersuchen. Dies bedeutet, dass die Stelle, die von einem Sozialleistungsträger um Übermittlung von Sozialdaten gebeten wird, darauf vertrauen darf, dass die in dem Übermittlungsersuchen enthaltenen Angaben – hier die Mitteilung, es liege eine wirksame Einwilligungserklärung vor – richtig ist.

› § 19 Abs. 1 Satz 2 LDSG
Aus dieser Regelung geht sinngemäß hervor, dass im Falle der auf eine Einwilligung gestützten Übermittlung von Gesundheitsdaten an öffentliche Stellen des Landes wie z.B. dem LSJV die beteiligten Stellen Kenntnis von Inhalt und Reichweite der Einwilligung haben sollten. Danach wäre es zumindest anzustreben, dass auch die übermittelnden Stellen, also im konkreten Fall die Ärzte, nähere Angaben zu der von ihren Patienten erteilten Einwilligungen erhalten.

Auch wenn die Regelung des § 67d Abs. 1 Satz 2 SGB X nicht vollständig auf den zugrunde liegenden Sachverhalt angewendet werden kann, da die Regelung keine Aussage über die berufsrechtlichen Anforderungen an die Zulässigkeit einer Weitergabe schweigepflichtiger Patientendaten an Sozialleistungsträger trifft, ist der darin enthaltene Ansatz durchaus zielführend. Zumindest aus datenschutzrechtlicher Sicht wäre es deshalb vertretbar, wenn das LSJV als anfordernde Stelle den Ärzten glaubhaft das Vorliegen einer wirksamen Einwilligungserklärung versichert und sie dabei über Inhalt und Reichweite der Erklärung unterrichtet.

Angesichts der Relevanz der Angelegenheit in Bezug auf die ärztliche Schweigepflicht hat der LfDI den anfragenden Arztpraxen empfohlen, sich bei weiterem Klärungsbedarf direkt an die für berufsrechtliche Fragen für sie zuständige Heilberufskammer zu wenden. Denn unabhängig von der datenschutzrechtlichen Zulässigkeit der Übermittlung von Patientendaten bedarf es angesichts der strafrechtlichen Relevanz des Informationsaustauschs einer rechtssicheren Klärung, ob für ein befugtes Offenbaren der Patientendaten im Sinne des ärztlichen Berufsrechts die unmittelbare Kenntnis der Schweigepflichtentbindungserklärung durch die Ärzte erforderlich ist.

11. KOMMUNALES

11.1. Zeitkontingent für Datenschutzbeauftragte von Kommunen

Im Datenschutzbericht 2016/2017 wurde über das gemeinsam mit vier ausgewählten Kommunalverwaltungen aus unterschiedlichen Bereichen (Landkreis, kreisfreie Stadt, große kreisangehörige Stadt, Verbandsgemeinde) durchgeführte Projekt “Datenschutz update in der Kommunalverwaltung“ berichtet.

Im Rahmen dieses Projekts wurde nach Möglichkeiten gesucht, strukturelle Verbesserungen bei der Sicherstellung von Datenschutz und Datensicherheit in den Kommunen herauszuarbeiten. Als (Teil-) Ergebnis wurde der maßgebliche Anteil einer bzw. eines kommunalen Datenschutzbeauftragten daran festgestellt, dass Kommunen dazu in der Lage sind, die ihnen übertragenen Aufgaben effektiv und zugleich datenschutzgerecht erfüllen zu können.

Mit einer Fachveranstaltung im Juni 2017 und der Vorlage von Best-Practice-Empfehlungen zur Stärkung des Datenschutzes in der Kommunalverwaltung incl. eines Papiers zur Stellenbemessung und Stellenbewertung der Funktion des kommunalen Datenschutzbeauftragten fand das Projekt seinen Abschluss.

Als einer der zentralen Punkte wurde dabei vom LfDI empfohlen, für die Wahrnehmung der Funktion der bzw. des Datenschutzbeauftragten

› in Landkreisen, kreisfreien und großen kreisangehörigen Städten mindestens einen Personalbedarf in Höhe von 50% einer Vollzeitstelle des 3. Einstiegsamtes vorzusehen,

› in Verbandsgemeinde- und verbandsfreien Gemeindeverwaltungen ein festes Zeitkontingent einzuführen, wobei der Personalbedarf von dem in den Verwaltungen der oben genannten Gebietskörperschaften abweichen kann.

Diese Empfehlung konnte durch eine Im Herbst 2017 begonnene Abstimmung mit dem Rechnungshof RP konkretisiert und mit einer gemeinsamen Position abgesichert werden. Im Einzelnen soll Folgendes gelten:

1. Die Bewertung der Stelle einer bzw. eines Datenschutzbeauftragten ist bis zur Besoldungsgruppe A 11 möglich.

2. Als Personalbedarf für die Wahrnehmung der Funktion der bzw. des Datenschutz-beauftragten kann in Kreisverwaltungen sowie in Verwaltungen kreisfreier und großer kreisangehöriger Städte grundsätzlich bis zu 50 % einer Vollzeitarbeitskraft angesetzt werden.

3. Vorübergehend kann in einer Phase der Implementierung und Umsetzung des Datenschutzrechts in diesen Verwaltungen befristet bis 25.05.2020 nach einer Einzelfallbetrachtung der Personalbedarf auch mehr als 50 % betragen.

Als Personalbedarf für die Wahrnehmung der Funktion der bzw. des Datenschutzbeauftragten kann in Verwaltungen von Verbandsgemeinden und verbandsfreien Gemeinden mit über 30.000 Einwohnern grundsätzlich bis zu 50 % einer Vollzeitarbeitskraft angesetzt werden.

Als Personalbedarf kann in Verwaltungen von Verbandsgemeinden und verbandsfreien Gemeinden mit 12.000 bis 30.000 Einwohnern grundsätzlich bis zu 30 % einer Vollzeitarbeitskraft angesetzt werden.

In Verwaltungen von solchen Gemeinden mit weniger als 12.000 Einwohnern kann der Personalbedarf diesen Wert von 30 % auch unterschreiten.

Vorübergehend kann in einer Phase der Implementierung und Umsetzung des Datenschutzrechts in den Verwaltungen von Verbandsgemeinden und verbandsfreien Gemeinden bis 30.000 Einwohnern befristet bis 25.05.2020 nach einer Einzelfallbetrachtung der Personalbedarf auch mehr als 30 % bis 50 % betragen.

Bei einer solchen Einzelfallbetrachtung kann berücksichtigt werden, dass auch die Wahrnehmung der Funktion der bzw. des Datenschutzbeauftragten von Ortsgemeinden, Kindertagesstätten in kommunaler Trägerschaft oder Jagdgenossenschaften erfolgt (Art. 37 Abs. 3 DS-GVO), die als öffentliche Stellen gemäß Art. 37 Abs. 1 lit. a DS-GVO auf jeden Fall eine Datenschutzbeauftragte bzw. einen Datenschutzbeauftragten zu benennen haben.

4. Nach dem Abschluss dieser Phase der Implementierung und Umsetzung des Datenschutzrechts soll die Höhe des für die Erledigung der Aufgaben einer bzw. eines Datenschutzbeauftragten notwendigen Zeitkontingents auf der Basis einer Evaluation neu bewertet werden.

Eine Pflicht für eine entsprechende Ausweisung im Stellenplan einer Kommune ist damit nicht verbunden. Die Entscheidung darüber obliegt im Rahmen der Reichweite der Selbstverwaltungsgarantie letztlich der Organisations- und Personalhoheit des Dienstherrn.

Festzustellen ist aus der Sicht der Datenschutzaufsichtsbehörde aber jedenfalls, dass sich mit dem Wirksamwerden der DS-GVO

und der Umsetzung der Richtlinie für Polizei und Justiz auch die Aufgaben der behördlichen Datenschutzbeauftragten in den rheinland-pfälzischen Kommunalverwaltungen verändert haben. Anders als bislang werden künftig zeitaufwändige risikoorientierte Management- und Compliance-Aufgaben den Alltag der bzw. des Daten-schutzbeauftragten wesentlich prägen. Dem vielfältigen Aufgabenkatalog der bzw. des internen Datenschutzbeauftragten auf der einen Seite stehen umfassende Unterstützungspflichten des Verantwortlichen auf der anderen Seite gegenüber.

12. MEDIENBILDUNG UND SCHULE

12.1. Medienkompetenzförderung durch den LfDI

12.1.1. Schüler-Workshops

Zentrales Element der Medienkompetenzförderung durch den LfDI sind weiterhin die seit 2010 existierenden kostenlosen Schülerworkshops. In 2018 fanden insgesamt 538 Workshops statt. Hierfür wurden im Berichtszeitraum neue Konzepte und Materialien entwickelt, erprobt und veröffentlicht:

Auf Grundlage neuer sozialwissenschaftlicher Forschungsergebnisse (KIM-Studie 2016) zum Medienhandeln von Kindern und den Rückmeldungen der Workshop-Referentinnen und Referenten entwickelte der LfDI ein grundlegend neues Konzept für Workshops in der Grundschule. Hierbei wurde der Nutzung von Smartphones und Apps durch Kinder im Grundschulalter Rechnung durch eine Themenerweiterung getragen. Aufbauend darauf wurde der zeitliche Rahmen des Workshop-Konzepts von zwei auf vier Schulstunden erhöht.

Grundsätzlich verfolgt das Angebot einen sensibilisierenden Ansatz. Ausgehend von dem Medienbesitz und der Mediennutzung der Grundschülerinnen und Schüler werden konkrete Regeln und Hilfestellungen zum sicheren Umgang mit datenschutzrelevanten Aspekten erarbeitet und vermittelt. Hierbei kommen multimedial aufbereitete Schulungsunterlagen und auf die Bedürfnisse von Grundschülern abgestimmte Arbeitsblätter zum Einsatz. Die im Konzept enthaltenen Methoden, Arbeitsblätter und Powerpoints wurden zunächst in Workshops evaluiert. Die Rückmeldungen aus den

Workshops haben den LfDI dazu veranlasst, auch die Inhalte anzupassen. So wurde die von jüngeren Kindern oft benutzte App „Tik-Tok", ein Soziales Netzwerk für Kurzvideos, in die Materialien mit aufgenommen. Gleiches gilt für Sprachassistenten und weitere Elemente des vernetzten Haushalts.

Sämtliche pädagogischen Konzepte stehen jedem Interessierten als lizenzfreies Bildungsmaterial über die Datenschutzseite für Jugendseite www.youngdata.de zur freien Verfügung: **www.youngdata.de/was-gibts-in-deiner-naehe/rheinland-pfalz/materialien-grundschulworkshops**.

12.1.2. Elternabende in Kitas

Die Beratungs- und Schulungsangebote des LfDI wurden im Berichtszeitraum auch in Bezug auf Zielgruppen erweitert. Bislang konzentrierten sich die Sensibilisierungsmaßnahmen vorwiegend auf junge Onliner.

Im 26. Datenschutzbericht wurde darüber berichtet, dass in Kooperation mit dem Verbraucherschutzministerium und der Verbraucherzentrale Rheinland-Pfalz das Schüler-Workshop-Projekt auch auf Fortbildungsangebote speziell für Familieneinrichtungen erweitert wurde. Im Berichtszeitraum wurde dieses Angebot – was die Zielgruppe angeht - nochmals erweitert: In Zusammenarbeit mit dem Verbraucherschutzministerium, der Verbraucherzentrale Rheinland-Pfalz und dem Ministerium für Bildung wurde ein pädagogische Konzept zu den Themen Datenschutz und Verbraucherschutz für Elternabende in Kitas erarbeitet. Dabei werden die Eltern für medienpädagogische und datenschutzrelevante Fragestellungen sowie Verbraucherschutzthemen sensibilisiert. Hierzu gehören u. A. Kostenfallen bei der Smartphone- und App-Nutzung (Ortungsfunktion, App-Berechtigungen, In-App-Käufe), Sensibilisierung für Problematiken bei der Weitergabe von personenbezogenen Daten, Bildern und Videos über Messenger-Dienste und in Sozialen Netzwerken sowie bei der Nutzung von Digitalen Sprachsteuerungen (Alexa, Siri und Co.) und Smart Toys (vernetztes Spielzeug). Zudem erhalten die Eltern Einblicke in rechtliche Rahmenbedingungen sowie konkrete Hilfestellungen und Tipps zum sicheren Umgang mit personenbezogenen Daten sowohl im Rahmen der Mediennutzung im familiären Kontext als auch für die Schnittstelle Kindergarten und Elternhaus. Die Veranstaltungen können über das Internetangebot des LfDI – ähnlich wie dies bei den Schüler-Workshops der Fall ist – online angefragt werden.

12.1.3. YoungData

Angesichts der jüngsten Entwicklungen im Bereich Sprachassistenten musste die gemeinsame Jugendseite der Datenschutzaufsichtsbehörden und des Kantons Zürich www.Youngdata.de überarbeitet werden.

Der Menüpunkt „WhatsApp, Skype & Co" wurde um das Untermenü „Alexa, Siri & Co" erweitert. Es wird dargestellt, inwiefern die Haushaltshelfer Daten über die Bewohner sammeln oder ob Dritte sich unbemerkt Zugriff auf Smart-Home-Geräte verschaffen können. Ein Leitfaden, wie der Nutzer am besten mit den Sprachassistenten umgeht, ist ebenfalls auf der Webseite zu finden. Aber auch sonstige Menüpunkte wurden redaktionell aktualisiert und überarbeitet.

Um Schülerinnen und Schülern eine leicht zugängliche Informationsquelle zu bieten, veröffentlicht der LfDI auf Youngdata regelmäßig

in kurzen Abständen Newsartikel. Im Jahr 2018 wurden 55 Artikel auf der Webseite veröffentlicht. Die News eignen sich zudem als themenbezogener Einstieg im Rahmen eines Datenschutz-Workshops.

12.1.4. Nutzung eigener Endgeräte durch Lehrkräfte ("Bring your own device")

Im Berichtszeitraum erreichten den LfDI zahlreiche Anfragen von Lehrerpersonalräten, die Datenschutzfragen bei der Nutzung eigener privater Endgeräte zum Gegenstand hatten. Insbesondere ging es dabei um die Zulässigkeit und den Umfang von Kontrollmaßnahmen. Teilweise wurde die Auffassung vertreten, eine solche Kontrolle sei nur auf der Basis eines richterlichen Beschlusses zulässig.

Die Bedenken waren für den LfDI durchaus nachvollziehbar. Sicherlich wäre es der einfachste Weg, wenn den Lehrkräften dienstliche Geräte zur Verfügung gestellt werden könnten. Angesichts von annähernd 40.000 Lehrkräften im Land erscheint dies jedoch haushaltsrechtlich problematisch. Alternativ könnte die Verarbeitung von Schüler- und Elterndaten lediglich in den Räumlichkeiten der Schule stattfinden, sofern entsprechende Rechner dort vorhanden sind. Dies würde jedoch dazu führen, dass mehrere Lehrkräfte die in der Schule vorhandenen Geräte nutzen müssten, was mit einem zusätzlichen organisatorischen und administrativen Aufwand einhergehen würde.

Die Schulordnungen enthalten daher Regelungen zur Zulässigkeit der Verarbeitung personenbezogener Daten auf privateigenen Datenverarbeitungsgeräten von Lehrkräften. Voraussetzung ist, dass die Schulleitung dies im Einzelfall genehmigt hat, das Einverständnis dafür vorliegt, dass das Datenverarbeitungsgerät unter den gleichen Bedingungen wie dienstliche Geräte kontrolliert werden kann und den Belangen des Datenschutzes Rechnung getragen ist (vgl. § 49 Abs. 4 Grundschulordnung; § 89 Abs. 4 Übergreifende Schulordnung).

Den „Belangen des Datenschutzes" ist aber nicht nur in Bezug auf schulische Daten, sondern auch in Bezug auf die Lehrkräfte Rechnung zu tragen: Dies bedeutet, dass namentlich bei Kontrollmaßnahmen die Privatsphäre der Lehrkräfte zu beachten ist. Um dies sicherzustellen, wurde die hier zum Einsatz kommende „Datenschutzerklärung" in Abstimmung mit dem Ministerium für Bildung etwas abgemildert: Während sich die Lehrkraft in einer früheren Fassung mit dem Betreten des häuslichen Arbeitszimmers für Kontrollzwecke einverstanden erklären sollte, wurde diese Passage gestrichen und als mildere Maßnahme die Kontrolle in den Räumlichkeiten der Schule aufgenommen **https://s.rlp.de/datenschutzerklrunglehrer**.

Selbstverständlich darf sich eine Kontrolle der Datenverarbeitungsgeräte lediglich auf schulische Daten erstrecken. Der Trennung zwischen „dienstlich" und „privat" kommt insoweit eine maßgebliche Bedeutung zu. In technischer Hinsicht könnte dies beispielsweise über sog. Container-Lösungen oder unter Nutzung eines Fernzugriffs mittels VPN-Tunnel bewerkstelligt werden. Denkbar wäre es auch, sofern dies vom Betriebssystem unterstützt wird, auf dem Endgerät mehrere Benutzerkonten einzurichten. Die Nutzung eines Sticks, auf dem die Daten verschlüsselt werden, wäre insoweit auch ein gangbarer Weg.

Die Datenschutzaufsichtsbehörden sind derzeit bestrebt, gemeinsam mit der KMK eine Handreichung zur Thematik „Bring your own device" zu erstellen. Zwischenzeitlich sind die Schulen aber nicht gehindert, in Zusammenarbeit mit ihren schulischen Datenschutzbeauftragten, ggf.

auch unter Beteiligung der Schulträger oder der Schulaufsichtsbehörden, eigene datenschutzfreundliche Lösungen zu erarbeiten.

12.2. Umsetzung der DS-GVO im Schulbereich

Auch Schulen in Rheinland-Pfalz müssen die europarechtlichen Vorgaben der DS-GVO beachten. Die Zulässigkeit der Datenverarbeitung durch Schulen ist über sogenannte Öffnungsklauseln der Grundverordnung weiterhin im Schulgesetz und in den Schulordnungen geregelt. Dennoch bestand für Schulen ab Wirksamwerden der Grundverordnung am 25. Mai 2018 ein gewisser Handlungsbedarf in Bezug auf formelle Verpflichtungen:

- So muss beispielsweise jede Schule unabhängig von ihrer Größe einen Datenschutzbeauftragten bestellen. Bisher war das nur bei Schulen mit mehr als zehn Beschäftigten der Fall. Um dies sicherzustellen, wurde auf Vorschlag des LfDI ein zentraler schulischer Datenschutzbeauftragter für die kleineren Grundschulen bestellt. Die Stelle ist bei der ADD angesiedelt und wurde mit einem Juristen besetzt. Die Zusammenarbeit funktioniert seitdem reibungslos. So wurden z.B. die Grundschulen in Abstimmung mit dem LfDI z.B. über darüber informiert, wie das Verzeichnis der Verarbeitungstätigkeiten geführt werden sollte und welche Datenschutzanforderungen beim schulischen Internetauftritt zu beachten sind. Die Grundschulen werden vom schulischen Datenschutzbeauftragten regelmäßig über datenschutzrechtliche und -technische Themen informiert und umfassend beraten.

- Zur Stärkung der Betroffenenrechte ist es nach der DS-GVO erforderlich, dass die Eltern der Schülerinnen und Schüler bei der Schulanmeldung darüber informiert werden, welche ihrer Daten zu welchem Zweck erhoben und verarbeitet werden. In Kooperation mit dem Ministerium für Bildung hat der LfDI Handreichungen erstellt, die den Schulen einen Überblick über die neue Rechtslage geben und die Umsetzung der DS-GVO erleichtern sollen.

  Diese und weitere Datenschutz-Hinweise können auf der Homepage des Pädagogischen Landesinstituts zusammengefasst unter **https://s.rlp.de/DSSchule** abgerufen werden.

Zusätzlich wurden für Lehrkräfte und schulische Datenschutzbeauftragte Schulungen und Informationsveranstaltungen angeboten, um Schulleitungen und Lehrkräfte mit der neuen Rechtsmaterie vertraut zu machen.

Trotz der umfangreichen Informationsangebote kam es nach Wirksamwerden der Grundverordnung zu einem massiven Anstieg von Beratungsgesuchen aus dem schulischen Kontext. Auch wenn der LfDI keine Beratungsaufgabe mehr gegenüber öffentlichen Stellen gesetzlich zugewiesen bekommen hat, ist er bemüht, auch allgemeine Anfragen zum schulischen Datenschutz im Rahmen seiner Möglichkeiten zu beantworten.

13. MELDEWESEN

13.1. Anforderungen an die Eintragung einer Auskunftssperre

Aufgrund einer Beschwerde hatte sich der LfDI mit den Anforderungen an die Eintragung einer Auskunftssperre wegen einer Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interesse, zu befassen (§ 51 Abs. 1 BMG).

Im konkreten Fall hatte die Exfrau des jetzigen Lebenspartners der Beschwerdeführerin beim Meldeamt deren derzeitige Anschrift erhalten. In einem gewissen zeitlichen Zusam¬menhang hierzu kam es zu einer Sachbeschädigung des Autos der Beschwerdeführerin, die bei Polizei und Staatsanwaltschaft zur Anzeige gebracht wurde. Einige Zeit später war auf Videoaufnahmen zu sehen, dass sich Familienangehörige der Exfrau unbefugt auf dem Grundstück der Beschwerdeführerin aufgehalten und dort Fotos gemacht hatten.

Die Beschwerdeführerin beantragte daher die Eintragung einer Auskunftssperre beim Meldeamt einer Stadtverwaltung. Dieser Antrag wurde jedoch abgelehnt. Telefonisch teilte man der Beschwerdeführerin mit, dass man auch im Falle ihres Umzugs ihre neue Anschrift mitteilen würde. Erst wenn ihr „etwas Schlimmes passieren würde“, könnte sie eine Auskunftssperre erhalten.

Der LfDI wies die Stadtverwaltung auf Folgendes hin: § 51 Abs. 1 BMG normiert, dass die Meldebehörde auf Antrag oder von Amts wegen eine Auskunftssperre im Melderegister einzutragen hat, wenn Tatsachen vorliegen, die die Annahme rechtfertigen, dass der betroffenen Person durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann. Hinzuweisen war im Übrigen auch auf § 8 BMG, welcher normiert, dass schutzwürdige Interessen der betroffenen Person durch die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nicht beeinträchtigt werden dürfen. Schutzwürdige Interessen werden insbesondere beeinträchtigt, wenn die Erhebung, Verarbeitung oder Nutzung gemessen an ihrer Eignung und ihrer Erforderlichkeit zu dem vorgesehenen Zweck, die betroffene Person unverhältnismäßig belasten. Diese Interessenabwägung hat vor jeder Erteilung einer Melderegisterauskunft zu erfolgen.

Die Kumulation der o.g. durch Tatsachen belegten Umstände lässt aus Sicht des LfDI durchaus die Annahme zu, dass bedeutende Rechtsgüter der Beschwerdeführerin gefährdet sein könnten. Da die Beschwerdeführerin bereit war, zum Schutz ihrer Privatsphäre einen Umzug in Kauf zu nehmen, war es umso mehr befremdlicher, als das Meldeamt ihr gegenüber mitteilte, dass auch künftig eine Auskunftserteilung erfolgen würde und die Eintragung einer Auskunftssperre daher nicht zielführend sei. Das Meldeamt hat sich im konkreten Fall gleich mehrfach rechtlich unzutreffend gegenüber der Beschwerdeführerin geäußert. Nach entsprechenden Hinweisen des LfDI wurde schließlich zugestanden, dass bei einem Umzug der Beschwerdeführerin eine Auskunftssperre unter der neuen Anschrift eingetragen wird.

13.2. Die Rolle der Abfallbehörden bei der Erstellung eines Mietspiegels

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

hatte für die Erstellung eines Mietspiegels Meldedaten an ein Dienstleistungsunternehmen weitergegeben; durch eine falsche Verknüpfung dort wurden Eigentümerangaben und Mieterangaben miteinander verwechselt und an unberechtigte Personen übermittelt. Bei der Befassung mit dieser Datenpanne prüfte der LfDI auch die Frage, ob es überhaupt zulässig ist, wenn Kreisverwaltungen zur Erfüllung dieser Aufgabe auf den Datenbestand des Abfallwirtschaftsbetriebes zurückgreifen und diese Daten an einen Dienstleister weitergeben.

Da diese Daten dem Abfallwirtschaftsbetrieb von den Meldebehörden lediglich „zur Veranlagung von Abfallentsorgungsgebühren" regelmäßig zur Verfügung gestellt werden (§ 7 der Meldedatenlandesverordnung), 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.

Die DS-GVO eröffnet im öffentlichen Bereich die Möglichkeit, spezifischere Regelungen – auch zur Zulässigkeit einer zweckändernden Datennutzung – in nationalem Recht zu treffen. Der Gesetzgeber hat hiervon mit dem Bundesmeldegesetz (BMG) und dem LDSG Gebrauch gemacht (Art. 6 Abs. 1 lit. e in Verbindung mit Art. 6 Abs. 2 und Abs. 3 DS-GVO).

Die bereichsspezifische Regelung in § 41 BMG steht einer Zweckänderung im vorliegenden Fall entgegen: Hiernach 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.

Als andere gesetzliche Bestimmung in diesem Sinne kommt jedenfalls § 7 LDSG nicht in Frage, da hier Zweckänderungen nur unter ganz engen Voraussetzungen, die hier nicht einschlägig sind, zugelassen sind.

Art. 6 Abs. 4 DS-GVO, der eine Zweckänderungen unter bestimmten Voraussetzungen zulässt, steht dieser Sichtweise nicht entgegen: Diese Regelung greift nur dann, wenn weder eine Einwilligung der betroffenen Personen vorliegt, noch der nationale Gesetzgeber Regelungen zur Zweckänderung getroffen hat. Dies ist jedoch hier gerade nicht der Fall. Sowohl § 41 BMG als auch § 7 LDSG enthalten diesbezügliche nationale Zweckbestimmungsregelungen.

Selbst wenn man Art. 6 Abs. 4 DS-GVO für anwendbar hielte, sprechen sowohl die Erwartungshaltung der Betroffenen (lit. a), als auch die Umstände der Datenerhebung durch das Meldeamt (lit. b) vorliegend gegen die Zulässigkeit einer Zweckänderung:

Denn die betroffenen Personen teilen aufgrund gesetzlicher Mitwirkungspflichten ihre Daten dem Meldeamt mit und rechnen nicht damit, dass diese Daten sodann zunächst an die Abfallbehörde und von dort an die Kreisverwaltung und von dort weiter an einen externen privaten Dienstleister weitergegeben werden, wobei gleich zweimal eine Zweckänderung vorgenommen wird.

Im Ergebnis bedeutet dies, dass eine Übermittlung von Meldedaten durch Abfallwirtschaftsbetriebe an die Kreisverwaltung für die Erstellung eines Mietspiegels grundsätzlich nicht möglich ist. Die Kreisverwaltungen sind daher gehalten, die für die Mietwerterhebung benötigten Daten unmittelbar bei den Meldebehörden zu erfragen."

13.3. Melderecht und die DS-GVO

Im letzten Datenschutzbericht wurde bereits dargestellt, dass die melderechtlichen Bestimmungen vor dem Hintergrund der DS-GVO neu bewertet werden müssen. Im Berichtszeitraum sind weitere Fragen zum Verhältnis des BMG zur DS-GVO zu Tage getreten:

Mit dem Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz (Drs. 19/4674 vom 1.10.2018) steht auf Bundesebene eine weitere Anpassung des BMG an die DS-GVO bevor. Vorge¬sehen sind erhebliche Einschränkungen der Betroffenenrechte, was Auskunfts-, Berichtigungs- und Löschungsansprüche betrifft. Die hiergegen erhobenen datenschutzrechtlichen Bedenken (vgl. Drs. 430/1/18 vom 05.10.2018) wurden jedoch im Verlauf der Beratungen größtenteils nicht berücksichtigt.

Nach Wirksamwerden der DS-GVO sind auch öffentliche Stellen, wie die Meldeämter verpflichtet, die betroffenen Personen bei der Datenerhebung (also beispielsweise bei der Anmeldung einer neuen Wohnanschrift) über bestimmte Datenverarbeitungsvorgänge zu informieren (Art. 13 DS-GVO). Hierzu hat die „länderoffene Arbeitsgemeinschaft zum BMG einen Mustertext erarbeitet, der über die Innenministerien an die Meldeämter weitergegeben wurde. Aus Sicht des LfDI stellt dieses Papier lediglich einen kursorischen und völlig unzureichenden Überblick über die tatsächlich stattfindenden Datenverarbeitungsprozesse für die betroffenen Personen dar. Welche öffentlichen Stellen landesweit Meldedaten online abfragen können oder im Wege regelmäßiger Datenübermittlungen informiert werden, wird nicht mit der gebotenen Transparenz dargestellt. Auch die Tatsache, dass mit dem BMG auch bundeslandübergreifende Datenabfragen durch Sicherheitsbehörden „rund um die Uhr“ ermöglicht wurden, bleibt unerwähnt. Aus Sicht des LfDI sollten sämtliche Datenempfänger explizit benannt werden: Dass insbesondere Sicherheits-, Steuer- , Schul-, Sozial- und Abfallbehörden, Kreisverwaltung, Ortsgemeinden, Religionsgesellschaften, Südwestrundfunk sowie die Zentrale Stelle des Programms zur Früherkennung von Brustkrebs Meldedaten auch ohne Einwilligung der Betroffenen erhalten, ist kaum bekannt. Für die betroffenen Personen wäre es sicher auch interessant zu erfahren, dass im Melderegister solch sachfremde Informationen, wie z.B. die Steuer-ID oder das Bestehen einer waffenrechtlichen Erlaubnis gespeichert werden. Hier müsste aus Sicht des LfDI mehr Transparenz geschaffen werden.

Auch schon vor Wirksamwerden der DS-GVO beschwerten sich viele Bürger über die Weitergabe ihrer Meldedaten für Jubiläumszwecke oder an Parteien im Vorfeld von Wahlen, ohne zuvor eingewilligt zu haben. Die Zahl der Beschwerden hat nach der öffentlichen Diskussion über die DS-GVO noch weiter zugenommen.

Viele Beschwerdeführer gehen nämlich davon aus, dass für die Weitergabe ihrer Meldedaten eine ausdrückliche Einwilligungserklärung vorliegen müsse. Tatsächlich sieht die DS-GVO als Einwilligung eine „eindeutige bestätigende Handlung“ vor (Erwägungsgrund 32). Bloße Untätigkeit, wie die Nichtausübung eines Widerspruchs, reicht als Erklärung nicht aus. Das BMG sieht aber - nach wie vor - nur eine so genannte Widerspruchslösung vor: Die genannten Auskünfte dürfen von den Meldebehörden erteilt werden, sofern die betroffenen Personen der Übermittlung ihrer Daten nicht widersprochen haben (§ 50 BMG). Zwar ist auf diese Widerspruchsmöglichkeit bei der Anmeldung sowie einmal jährlich durch ortsübliche Bekanntmachung hinzuweisen, diese Information wird aber häufig von den Betroffenen nicht wahrgenommen.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder hatten sich in den letzten Jahren gegenüber dem Gesetzgeber leider vergeblich darum gemüht, die derzeitigen Widerspruchslösungen durch das Erfordernis einer ausdrücklichen Einwilligungserklärung abzulösen, Entschließung vom 22.8.2012: **https://s.rlp.de/entschliessungdsk2012**.

Es bleibt zu hoffen, dass durch gerichtliche Entscheidungen geklärt wird, ob die derzeitigen melderechtlichen Widerspruchsmöglichkeiten mit der DS-GVO zu vereinbaren sind. Einige Kommunen im Rheinland-Pfalz sind bereits jetzt dazu übergegangen, die bestehenden Widerspruchsmöglichkeiten durch Einwilligungserklärungen der Betroffenen zu ersetzen. Dies ist aus Sicht des LfDI zu unterstützen.

14. VERWALTUNG DIGITAL, EINSCHLIESSLICH FINANZEN

14.1. Neue datenschutzrechtliche Aufsicht für die Finanzverwaltung

Mit Wirksamwerden der DS-GVO haben sich Änderungen bei der Datenschutzaufsicht im Bereich der Finanzverwaltung ergeben. So ist nun für die Verarbeitung personenbezogener Daten im Anwendungsbereich der novellierten Abgabenordnung der BfDI die zuständige datenschutzrechtliche Aufsichtsbehörde über die Finanzbehörden (§ 32 Abs. 1 AO). Kommunale Steuerämter werden auch zukünftig vom LfDI datenschutzrechtlich beaufsichtigt. Nur für den Bereich der Realsteuern (Grund- und Gewerbesteuern) ist der BfDI die zuständige Datenschutzaufsichtsbehörde für die kommunalen Steuerämter, soweit das Besteuerungsverfahren auf der Grundlage der novellierten Abgabenordnung erfolgt.

14.2. Tourismus- und Gästebeiträge

War es bisher problematisch für Städte und Gemeinden, Tourismus- oder Gästebeiträge zu erheben, wenn sie nicht Kurorte waren, hat sich dies mit Wirkung zum 1. Januar 2016 geändert: Im Kommunalabgabengesetz wurde eine Rechtsgrundlage aufgenommen, die es den Kommunen erlaubt, auf Grundlage einer entsprechenden Satzung Tourismus- oder Gästebeiträge zu erheben.

Viele Kommunen haben von dieser Möglichkeit Gebrauch gemacht und entsprechende Satzungen erlassen. Danach sind in der Regel Übernachtungsgäste zur Abgabe eines bestimmten Tagesbeitrages im einstelligen Bereich verpflichtet. Die Erhebung der erforderlichen Daten erfolgt durch die Beherbergungsbetriebe

im Rahmen der nach Melderecht auszufüllenden Meldebescheinigung. Auch der entsprechende Betrag wird regelmäßig von den Beherbergungsbetrieben vereinnahmt und an die Stadt oder Gemeinde abgeführt.

Insbesondere nach Wirksamwerden der DS-GVO führt das Verfahren sowohl bei Kommunen als auch bei Beherbergungsbetrieben zu datenschutzrechtlichen Fragen.

Im Ergebnis lässt sich feststellen, dass das Verfahren auch unter Geltung der DS-GVO nicht grundsätzlich auf datenschutzrechtliche Bedenken stößt.

Die Datenverarbeitung ist für die Kommune auf Grundlage des Art. 6 Abs. 1 lit. e i.V.m. Abs. 2 und 3 DS-GVO zulässig, denn sie dient der gesetzlichen bzw. satzungsmäßigen Aufgabenerfüllung. Für die Datenverarbeitung durch die Beherbergungsbetriebe gilt Art. 6 Abs. 1 lit. c DS-GVO: Diese müssen die Daten erheben und an die Kommune weitergeben, um eine rechtliche Verpflichtung, die sich aus der Satzung ergibt, zu erfüllen.

Die Gemeinden dürfen durch Satzung zusätzlich zu den im BMG genannten Daten weitere, für die Erhebung von Tourismus- und Gästebeiträgen nach § 12 Abs. 1 und 2 KAG (Kommunalabgabengesetz) erforderliche Daten auf dem Meldeschein erheben und verarbeiten. Auf dem Meldeschein ist die Satzung zu benennen, durch die die Erhebung und Verarbeitung angeordnet wird. Dies ist in § 26 Abs. 2 MDLVO (Meldedatenlandesverordnung) geregelt. In den meisten Beitragssatzungen ist vorgegeben, dass der Inhaber des Beherbergungsbetriebes für jeden Kalendermonat die Meldevordrucke an die Kommune übermittelt. Zudem ist ebenso regelmäßig vorgesehen, dass die Stadt oder Gemeinde die zur Ermittlung der Beitragspflichtigen, zur Beitragsfestsetzung und die zur Durchführung aller weiteren Bestimmungen nach der Satzung erforderlichen Daten z.B. aus den Mitteilungen der Beherbergungsbetriebe erheben darf. Da regelmäßig die Gäste beitragspflichtig sind, darf die Kommune auch die Namen und Adressdaten dieser Beitragspflichtigen erheben. Die so erhobenen Daten unterliegen natürlich dem Steuergeheimnis und dürfen nur zweckgebunden verarbeitet werden.

15. ZERTIFIZIERUNG

15.1. Entwicklung eines Akkreditierungsverfahrens

Die DS-GVO schafft in den Artikeln 42 und 43 DS-GVO die Rechtsgrundlagen für ein Akkreditierungs- und Zertifizierungsverfahren: Zertifizierungen, Siegel und Prüfzeichen sollen als Nachweis dienen, dass eine Verarbeitung von personenbezogenen Daten gesetzeskonform durchgeführt wird. Neben den Zertifizierungen nach Art. 42 DS-GVO werden keine weiteren Zertifizierungen nach der DS-GVO zulässig sein.

Bei der datenschutzrechtlichen Akkreditierung und Zertifizierung handelt es sich um eine Neuerung durch die Datenschutzreform: Der Bundesgesetzgeber sah zwar schon vor Inkrafttreten der DS-GVO in § 9a BDSG a.F. die Möglichkeit von Datenschutzaudits vor. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter sollten durch besonderes Gesetz geregelt werden. Entsprechende Regelungsversuche eines Bundesgesetzes kamen jedoch über parlamentarische Beratungen nicht hinaus.

Da ein datenschutzrechtliches Akkreditierungsverfahren vor der Geltung der DS-GVO nicht vorgesehen war, arbeiteten die Datenschutz-Aufsichtsbehörden gemeinsam mit der Deutschen Akkreditierungsstellen GmbH (DAkkS) im Berichtszeitraum an der Ausgestaltung eines solchen Verfahrens. Die Akkreditierung erfolgt nach der neuen Rechtslage durch die Datenschutz-Aufsichtsbehörden des Bundes und der Länder in Zusammenarbeit mit der DAkkS. Gemäß § 39 BDSG erfolgt die Erteilung der Befugnis, als Zertifizierungsstelle gemäß Art. 43 Abs. 1 S. 1 DS-GVO tätig zu werden, durch die für die Zertifizierungsstelle zuständige Aufsichtsbehörde auf der Grundlage einer Akkreditierung, die durch die DAkkS im Einvernehmen mit der Aufsichtsbehörde durchgeführt wird. Um die Grundlagen für diese Zusammenarbeit zu schaffen, entwarfen die genannten Stellen den Entwurf einer Kooperationsvereinbarung zu den Akkreditierungsaufgaben sowie den Entwurf eines gemeinsamen Papiers zu den Anforderungen zur Akkreditierung.

In dem zukünftigen Akkreditierungsverfahren legt zu akkreditierende Stelle der zuständigen Aufsichtsbehörde die Zertifizierungskriterien (das sogenannte Prüfprogramm) vor. In diesem stellt sie dar, nach welchen Kriterien sie beabsichtigt nach erfolgter Akkreditierung zu zertifizieren. Die nähere Ausgestaltung des Akkreditierungsverfahrens steht zum gegenwärtigen Zeitpunkt noch nicht fest.

16. RECHTSDURCHSETZUNG UND PROAKTIVER DATENSCHUTZ

16.1. LfDI veröffentlicht Muss-Listen zur Durchführung der DSFA

Art. 35 DS-GVO verpflichtet Verantwortliche zur Durchführung einer DSFA, wenn dessen Verarbeitungsvorgänge voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen hervorruft. Ist dieser Schwellwert überschritten, muss ein Verantwortlicher eine umfangreiche Risikoprognose erstellen. Er muss zunächst die Verarbeitungsvorgänge und die hiermit verfolgten Zwecke systematisch beschreiben sowie die Risiken für die Rechte und Freiheiten der betroffenen Personen und die zu ihrer Verringerung getroffenen Abhilfemaßnahmen bewerten.

Daher stellt sich für die Verantwortlichen zunächst die Frage, ob die eigenen Verarbeitungsvorgänge den Schwellwert zu dem hohen Risiko überschreiten und daher die Durchführung einer DSFA obligatorisch ist. Die DS-GVO konkretisiert das hohe Risiko durch drei Regelbeispiele in Art. 35 Abs. 3. Zudem hat die Artikel-29-Datenschutzgruppe in ihrem Working Paper 248 zur Ermittlung des Risikos neun Kriterien herausgearbeitet. Trotz der vorgenannten Prüfungsschritte bestand bei zahlreichen Verantwortlichen Rechtsunsicherheit dahingehend, ob eine konkrete Verarbeitungstätigkeit ein hohes Risiko verwirklicht oder nicht.

Um dieser Rechtsunsicherheit entgegenzuwirken, hat der LfDI zwei sog. „Muss-Listen" nach Art. 35 Abs. 4 DS-GVO veröffentlicht. Die Muss-Liste wird auch als „Blacklist" bezeichnet. Das Ziel dieser Listen ist die Erzeugung von Transparenz, die sowohl der betroffenen Person als auch dem Verantwortlichen zu Gute kommt. Letztendlich soll die Muss-Liste zur Entscheidungsfindung beitragen, in dem eine Hilfestellung zur Eingruppierung eigener Verarbeitungsvoränge (DSFA erforderlich: ja oder nein?) bereitgestellt wird. Die Muss-Liste hat nicht den Anspruch der Vollständigkeit, wenngleich versucht wird, möglichst viele der DSFA-pflichtigen Verarbeitungsvorgänge zu berücksichtigen. Wird eine Verarbeitungstätigkeit in dieser Liste nicht aufgeführt, so ist hieraus nicht der Schluss zu ziehen, dass für diese keine DSFA durchgeführt werden müsse.

Der LfDI hat zwei unterschiedliche Listen veröffentlicht, getrennt nach öffentlichem und nicht-öffentlichem Bereich. Die Listen zählen hochriskante Verarbeitungsvorgänge auf und beschreiben typische Einsatzfelder und Beispiele dieser Vorgänge mit dem Ziel, dass ein Verantwortlicher das Risiko seiner eigenen Verarbeitungsvorgänge leichter bewerten kann.

Auf Grund der Schnelllebigkeit im digitalen Umfeld kann die Muss-Liste nur als „lebendiges" Papier angesehen werden, das ständigen Änderungskontrollen hinsichtlich der Aufnahme neuer Verarbeitungsvorgänge unterliegt.

Die Muss-Listen sind abrufbar unter **https://s.rlp.de/dsfa.**

16.2. Zahlreiche Meldungen von Datenpannen an den LfDI

Verantwortliche sind nach der DS-GVO verpflichtet, die Verletzungen des Schutzes personenbezogener Daten der Aufsichtsbehörde zu melden. Dieser Verpflichtung kamen seit dem Geltungsbeginn der DS-GVO zahlreiche Verantwortliche nach: Seit dem 25. Mai 2018 gingen bei dem LfDI im Berichtszeitraum insgesamt 105 Meldungen von Datenpannen ein,

wobei 80 Meldungen dem öffentlichen und 25 Meldungen dem nicht-öffentlichen Bereich zuzuordnen sind. In allen Fällen prüfte der LfDI die Sachverhalte zeitnah mit dem Ziel festzustellen, ob noch Maßnahmen zu veranlassen sind, um ein bestehendes Risiko für die Rechte und Freiheiten natürlicher Personen zu reduzieren. Solche Maßnahmen waren unter anderem die Benachrichtigung der betroffenen Personen sowie die Umsetzung von technischen und organisatorischen Maßnahmen, um das Risiko von zukünftigen Datenpannen zu verringern.

Die gemeldeten Lebenssachverhalte unterschieden sich grundlegend: So meldeten Verantwortliche beispielsweise die versehentlich falsche Adressierung von E-Mails, den Datenverlust durch Hacker-Angriffe oder die rechtswidrige Entsorgung von Akten. Die Häufigkeit der Meldungen liegt sowohl daran, dass diese in einem Strafverfahren sowie in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder den Benachrichtigenden nur mit dessen Zustimmung verwendet werden darf (§ 42 Abs. 4, § 43 Abs. 4 BDSG) als auch an der Tatsache, dass eine rechtswidrig unterbliebene Meldung mit einem Bußgeld geahndet werden kann.

Um eine unkomplizierte, strukturierte und zeitnahe Meldung zu ermöglichen, integrierte der LfDI ein Formular zur Meldung von Datenpannen in sein Internetangebot. Im Rahmen dieses Formulars wird die meldende Person strukturiert alle Angaben abgefragt, welche notwendig sind, um den Vorfall zu erfassen und datenschutzrechtlich zu bewerten. Das Meldeformular ist jedoch nur eine Möglichkeit, eine Meldung zu tätigen. Den meldenden Personen steht es weiterhin frei, den Vorfall beispielsweise per E-Mail zu melden. Vereinzelt meldeten Verantwortliche ihre Datenpannen auch über den herkömmlichen Postweg. Mit Blick auf die 72-Stunden-Frist (welche auch nicht durch Sonn- oder Feiertage unterbrochen wird) empfiehlt der LfDI diesen Weg der Meldung jedoch nicht. Mehrere Verantwortliche meldeten Sachverhalte (vorab) per Telefon. Diese Vorgehensweise ist häufig bei besonderer Dringlichkeit geboten, insbesondere um bereits vorab eine vorläufige Risikoeinschätzung des LfDI zu erhalten.

16.3. LfDI macht von neuen Abhilfebefugnissen Gebrauch

Die DS-GVO stattet die Aufsichtsbehörden mit neuen Befugnissen aus, um Datenschutzverstößen abzuhelfen: Die Befugnisse haben jeweils eine unterschiedliche Eingriffsintensität und eine unterschiedliche Zielrichtung. So kann der LfDI seit dem Geltungsbeginn der Verordnung je nach Vorfall und Verantwortlichkeit einen Verantwortlichen vor einem Verstoß warnen, ihn bei dem Vorliegen eines Verstoßes verwarnen oder ihn beanstanden, ihn anweisen, eine Anordnung treffen oder ein Bußgeld verhängen.

Um zu einer einheitlichen und angemessenen Handhabung der Befugnisse zu gelangen, erarbeitete der LfDI zusammen mit den anderen Aufsichtsbehörden des Bundes und der Länder ein Bußgeldkonzept, um nachvollziehbar angemessene Geldbußen ermitteln und diese auch nach deren Verhängung noch überprüfen zu können. Das Bußgeldkonzept wurde im Berichtszeitraum noch nicht verabschiedet und wird aller Voraussicht nach ein „lebendiges Papier“ bleiben, um Änderungen der Sach- und Rechtslage berücksichtigen zu können.

Der LfDI machte seit dem Geltungsbeginn der DS-GVO vermehrt von den neuen Abhilfebefugnissen Gebrauch: Er beanstandete 9 Verantwortliche, verwarnte in 16 Fällen und verhängte 2 Anordnungen bzw. Anweisungen.

Aufgrund des zeitlichen Vorlaufs eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten verhängte er im Berichtszeitraum noch kein Bußgeld aufgrund von Verstößen nach dem Geltungsbeginn der DS-GVO, allerdings vier Geldbußen nach der alten Rechtslage. In der Mehrheit der der Befugnis zugrundeliegenden Fälle verarbeiteten Verantwortliche personenbezogene Daten ohne das Vorliegen einer Rechtsgrundlage, in einigen Fällen hatten Verantwortliche in unzureichendem Maße technische und organisatorische Maßnahme umgesetzt oder verstießen gegen die Betroffenenrechte nach den Artikeln 12 ff. DS-GVO.

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