Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

TÄTIGKEITSBERICHT ZUM DATENSCHUTZ 2021

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 8920 - 0
Telefax +49 (0) 6131 8920 - 299
poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

August 2022

INHALT

VORWORT


Prof. Dr. Dieter Kugelmann

Leider hat sich bewahrheitet, was zu befürchten war: Auch dieser Jahresbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit steht unter dem Zeichen der Pandemie. Das Jahr 2021 war erneut von der Pandemie geprägt. Dies wiederum hatte Auswirkungen auf die Arbeit der Behörde des LfDI. Erneut stellten sich hohe Anforderungen an die Einsatzbereitschaft und Flexibilität der Mitarbeitenden. Diese wurden vorbildlich bewältigt. Die Behörde war und ist arbeitsfähig und in der Lage, den erheblichen rechtlichen und praktischen Herausforderungen der Pandemie im Hinblick auf den Datenschutz gerecht zu werden. Die einzelnen Fragen werden in den Sachkapiteln des Tätigkeitsberichts näher erläutert. Das Verhältnis von Arbeitnehmerinnen und Arbeitnehmern zur Arbeitgeberseite war eines der vordringlichsten Probleme, die sich im Zusammenhang mit Testpflicht, Nachweispflichten und Beschäftigungsrahmenbedingungen gestellt haben. Der Beschäftigtendatenschutz rückte so einmal mehr in den Blickpunkt. Umso erfreulicher ist es, dass in der Koalitionsvereinbarung auf Bundesebene ein Beschäftigtendatenschutzgesetz vorgesehen ist. Die vielen Einzelheiten der unterschiedlichen Corona-Verordnungen haben meine Behörde in vielfältigen Zusammenhängen beschäftigt. Hervorzuheben ist dabei, dass auch auf der Ebene der Zusammenarbeit mit der Landesregierung eine Reihe von schwierigen Fragen ausgeräumt werden konnten, bevor konkrete Regelungen in Kraft traten. Die Mitarbeitenden des LfDI haben einmal mehr in konstruktiver und zügiger Kooperation einen Beitrag zu einer modernen Digitalisierung gerade auch in Krisenzeiten leisten können.

Der Alltagsbetrieb der Behörde war von der einmal mehr hohen Zahl an Eingängen geprägt. Das Aufkommen an Beschwerden hat sich auf sehr hohem Niveau eingependelt. Erneut erheblich zugenommen hat die Anzahl der Meldungen von Datenschutzverletzungen. Derartige Datenpannen können sehr unterschiedliche Intensität haben. Manche Fälle sind veranlasst durch umfangreiche Angriffe auf informationstechnische Systeme die vielerorts zu ungewollten und unrechtmäßigen Ausleitungen personenbezogener Daten an Unberechtigte führen. Manche Einzelfälle lassen sehr schnell erahnen, dass hinter der einzelnen Datenpanne ein systemisches Problem des Verantwortlichen steht, das angegangen wer-

den muss. Andere Datenpannen beruhen schlicht auf kleinen Versehen. Ungeachtet ihrer Intensität sind alle Meldungen von Datenschutzverletzungen auf ihre Gehalte zu prüfen. Bei schweren Verletzungen ist die Benachrichtigung der betroffenen Personen erforderlich. Dies alles zu kontrollieren und zu überblicken ist eine zunehmend intensive Aufgabe, der sich der LfDI stellen muss.

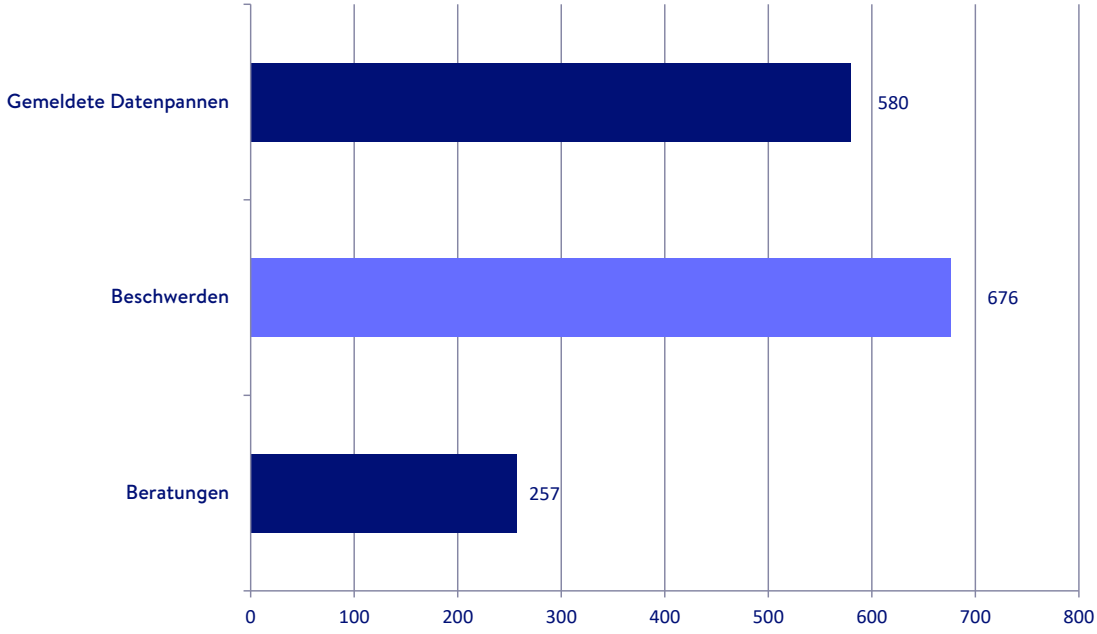
Im Koalitionsvertrag der neuen Bundesregierung nehmen der Datenschutz und die Vorkehrungen für eine sinnvolle Digitalisierung erheblichen Raum ein. Dies gilt genauso für die Ebene des Landes, indem etwa im Zusammenhang mit der Digitalisierung von Verwaltungsleistungen große Anstrengungen erforderlich sind, um modernen Gegebenheiten einer Informationsgesellschaft Rechnung zu tragen. Ich unterstütze dabei mit meinem Team die Bemühungen, diese Regelungen in einer Art und Weise zu gestalten und umzusetzen, die den Grundrechtsschutz der Bürgerinnen und Bürger sicherstellt.

Neuere Erhebungen und Untersuchungen machen deutlich, dass der Datenschutz zunehmend in Wirtschaft und Gesellschaft akzeptiert wird. Dabei ist klar, dass vielerorts Datenschutz einen gewissen Aufwand erfordert. Dieser Aufwand trägt aber Früchte für das Vertrauen der Bevölkerung in die Unternehmen und die Verwaltungen, die Daten verarbeiten. In einer digitalen Gesellschaft gehört das Vertrauen in rechtmäßige und angemessene Datenverarbeitungen dazu. Für mich und meine Behörde ist es eine zentrale Aufgabe, zu den Rahmenbedingungen für die dauerhafte Erhaltung von Vertrauen einen Beitrag zu leisten.

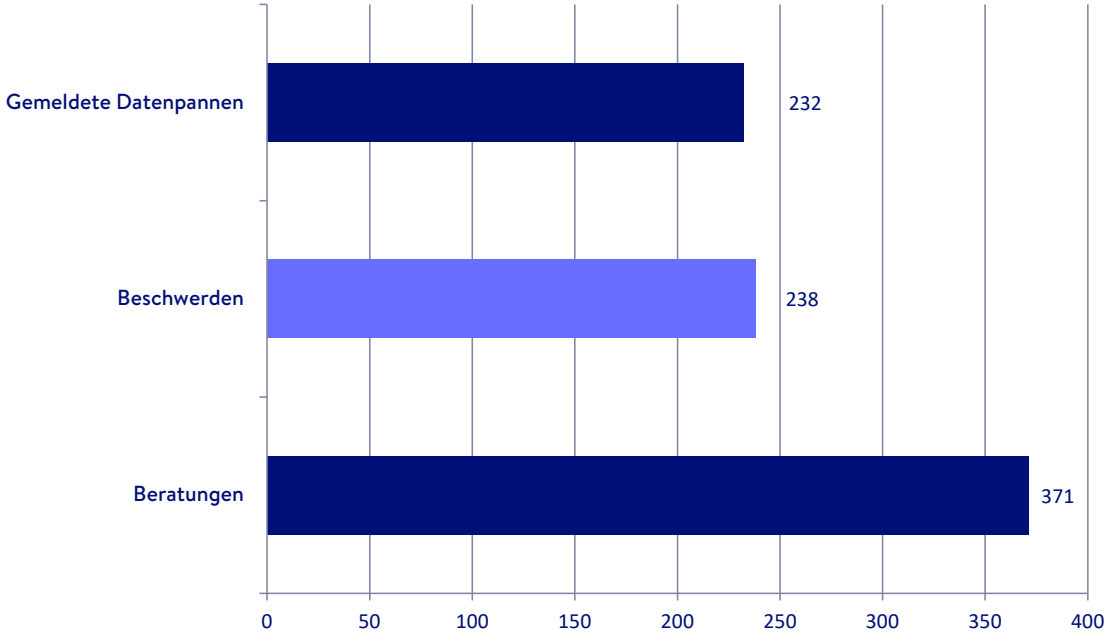
Prof. Dr. Dieter Kugelmann

I.
ZAHLEN UND FAKTEN

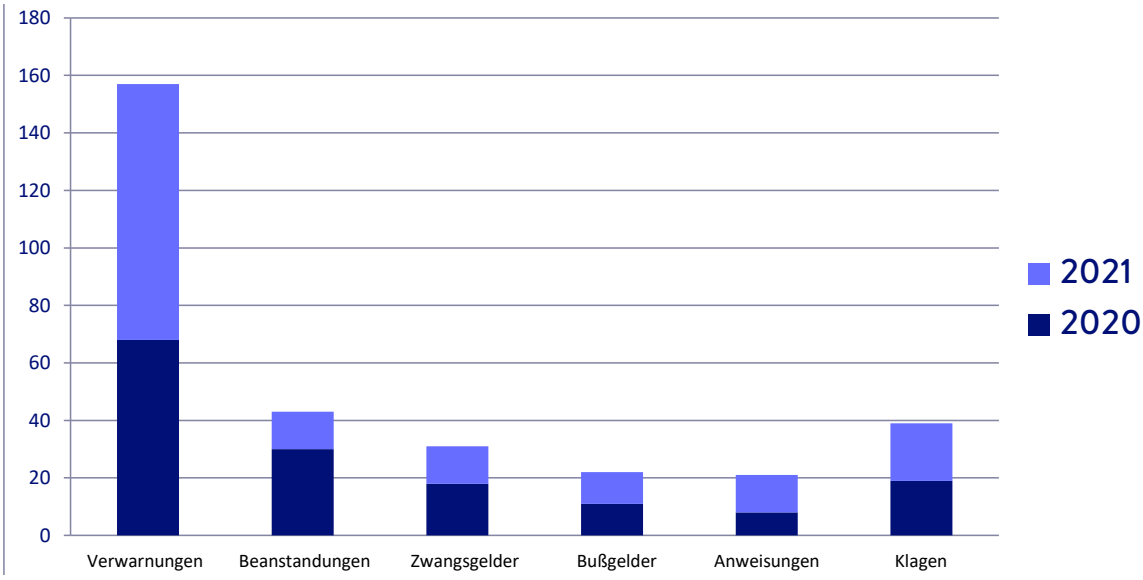
1. Geschäftsstatistik 2021: Privater Bereich



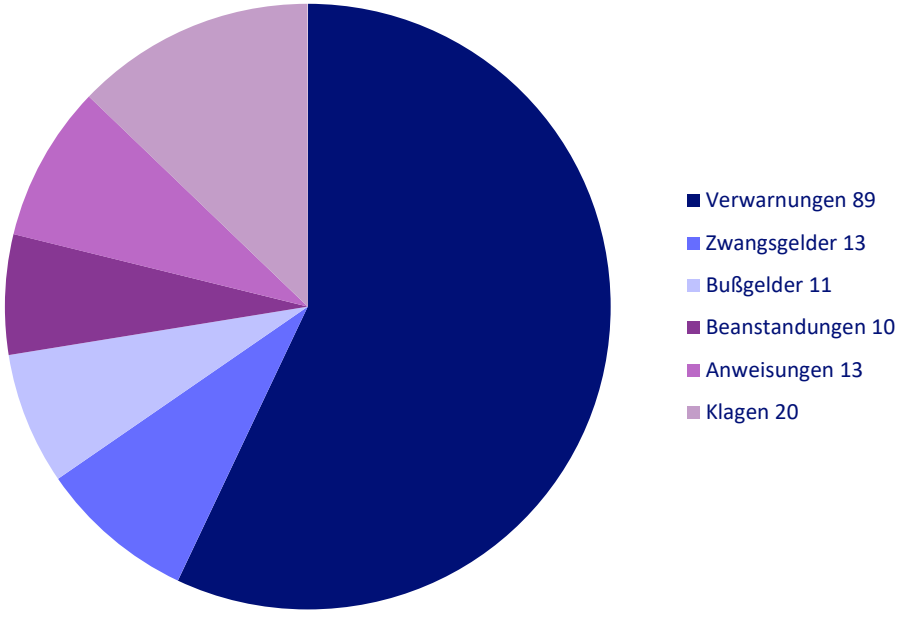
2. Geschäftsstatistik 2021: Öffentlicher Bereich



3. Ausgeübte Befugnisse 2020 und 2021



4. Ausgeübte Befugnisse 2021



II.
SACHGEBIETE

II. SACHGEBIETE

1. SICHERHEIT

1.1 Unberechtigte Datenbankabfragen von Polizeibeamt:innen

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit ist im Anwendungsbereich des Landesdatenschutzgesetzes befugt, Geldbußen im Rahmen von § 24 Landesdatenschutzgesetz zu verhängen. Adressat der Vorschrift ist neben der Behörde selbst auch jede/r Mitarbeiter:in als natürliche Person. Dies gilt über die Verweisung von § 72 LDSG auch und gerade für Tätigkeiten der Polizeibeamt:innen. Diese haben ein breites Spektrum an Abfragemöglichkeiten in unterschiedlichsten polizeilichen Informationssystemen, die jedoch nur zur Aufgabenerfüllung und im Rahmen der Befugnisse nach dem Polizei- und Ordnungsbehördengesetz und der Strafprozessordnung genutzt werden dürfen.

Da Gelegenheit bekanntlich Diebe macht, kommt es immer wieder einmal vor, dass Polizist:innen aus persönlichen Gründen ihre Abfragebefugnisse überschreiten. Da die Abfragen ausnahmslos protokolliert werden, werden jedoch viele dieser Fälle aufgedeckt.

Seit Inkrafttreten des neuen Landesdatenschutzgesetzes wurden dem LfDI von Seiten der Polizeipräsidien etliche Fälle als Datenpannen gemeldet, bei denen der Verdacht einer unberechtigten Abfrage von polizeilichen Informationssystemen im Raum stand. Auch durch die jeweiligen Disziplinarstellen erfolgten entsprechende Meldungen.

Hieraus resultierten in den letzten drei Jahren 13 Bußgeldverfahren, welche mit Geldbußen zwischen 200 € und 2000 € abgeschlossen wurden.

Bisher wurde ein Bußgeldbescheid im Wege des Einspruchs vor dem Amtsgericht Mainz angefochten. Das Gericht hat in der mündlichen Verhandlung im Juli 2021 ganz klar dargelegt, dass die Abfragen von Datenbanken und Informationssystemen durch einen Polizeibeamten zu privaten Zwecken einen Datenschutzverstoß darstellt. Dem kann weder entgegengehalten werden, dass der Arbeitgeber die Möglichkeit des Datenzugriffs uneingeschränkt zur Verfügung stellt, noch, dass eine Abfrage vielleicht für dienstliche Zwecke relevant werden könnte.

1.2 Datenverarbeitung zur Prävention bei Fußballspielen? Neuausrichtung der Datei „Gewalttäter Sport“ und Vorzüge der Datei PrävPol in Rheinland-Pfalz

Bei der Datei „Gewalttäter Sport“ handelt es sich um eine bundesweite Verbunddatei, in der Daten von Personen gespeichert sind, die Polizeibehörden im Zusammenhang mit Sportveranstaltungen (vor allem Fußballspielen) aufgefallen sind. Zugriff haben die Polizeibeamtinnen und Beamten der Länder und des Bundes. Die Behörden, in denen Vorfälle registriert werden, speichern die Daten und sind für Auskünfte verantwortlich.

Der LfDI vertritt dazu, dass eine Neuausrichtung der Datei „Gewalttäter Sport“ sinnvoll wäre und dazu führen könnte, dass die Datensammlung transparenter und nachvollziehbarer ausgestaltet wird. Zudem müssen die Betroffenenrechte gestärkt werden: Personen, deren Daten in die Datei eingespeist wurden, sollten proaktiv von den Behörden benachrichtigt werden. So sieht Rheinland-Pfalz bereits seit 2015

vor, dass betroffene Personen, die aufgrund von präventiv-polizeilichen Maßnahmen eingetragen werden, benachrichtigt werden. Betroffene müssen überdies verbindlich wissen, an wen sie sich bei Nachfragen und Beschwerden wenden können – etwa wenn Informationen aus ihrer Sicht falsch gespeichert wurden oder Verfahren mittlerweile eingestellt sind. Aufgrund des Verbundcharakters der Datei ist dies nicht immer transparent.

Des Weiteren hat sich der LfDI dafür stark gemacht, dass die Schwellenwerte erhöht werden in Bezug auf die Anlassstraftaten, die zu einer Speicherung führen können. Dies würde den Datenumfang auf die relevanten „Gewalttaten" beschränken, von denen man zur effektiven Sicherheitsgewährleistung bei Fußballspielen Kenntnis haben muss.

Diese Kritikpunkte greift dagegen die in Rheinland-Pfalz eingerichtete Datei „Präventivpolizeiliche Maßnahmen bei Sportveranstaltungen" auf. Diese Datei zur Reduzierung gewalttätiger Auseinandersetzung im Zusammenhang mit Sportveranstaltungen für die Polizeidienststellen des Landes Rheinland-Pfalz läuft seit Juli 2021 im Wirkbetrieb. Zweck der Datei ist die Abwehr von im Zusammenhang mit Sportveranstaltungen stehenden Gefahren für die öffentliche Sicherheit und Ordnung, insbesondere zur Reduzierung von Gefahren für friedliche Teilnehmer an Sportveranstaltungen als auch Unbeteiligte und die Verhütung von Straftaten, insbesondere von gewalttätigen Auseinandersetzungen, sowie der Vorsorge für die Verfolgung von Straftaten und bedeutenden Ordnungswidrigkeiten.

Da in der Datei auf die Speicherung von Kontakt- und Begleitpersonen verzichtet wird, ist der Umfang der betroffenen Personen geringer. Des Weiteren bestehen für die Erstspeicherung im Vergleich zur Datei Gewalttäter Sport höhere Hürden, niedrigschwellige Delikte, wie etwa Beleidigungen reichen nicht aus, sondern es müsste der Tatbestand z.B. eines Gewaltdeliktes oder eines Landesfriedenbruchs erfüllt sein. Des Weiteren ermöglicht die Datei eine Rehabilitation dadurch, dass die Speicherungsdauer grundsätzlich nur ein Jahr beträgt. Danach wird erneut geprüft, ob entsprechender Datensatz zu löschen ist oder im Falle weiterer Delikte im Zusammenhang mit Sportveranstaltungen für ein weiteres Jahr zu speichern ist.

Aus Gründen der Transparenz, aber auch der Generalprävention wurde zudem eine proaktive Benachrichtigungspflicht eingeführt. Diese Benachrichtigung orientiert sich an die bestehenden Rechte der betroffenen Person auf Informationen nach §§ 43, 44 Landesdatenschutzgesetz. In der Folge werden die gespeicherten Personen z.B. über den Zweck der Verarbeitung, ihre Betroffenenrechte, über die Rechtsgrundlage der Verarbeitung, die Kategorien der Empfänger benachrichtigt.

2. JUSTIZ

2.1 Datenschutz in der Justiz - Schulung der Datenschutzbeauftragten der Gerichte und Staatsanwaltschaften im OLG Bezirk Zweibrücken

Datenschutz im Bereich der Justiz hat eine ganz besondere Ausprägung. Zum einen prallen verschiedene Datenschutzregime aufeinander: Während in der Zivil- und Verwaltungsgerichtsbarkeit die Datenschutz-Grundverordnung gilt, finden im Rahmen der Arbeit der Strafgerichte und Staatsanwaltschaften zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung die Gesetze zur Umsetzung der Richtlinie (EU) 2016/680 Anwendung. Zum anderen bestehen (Teil-) Bereichsausnahmen, was die Datenschutzaufsicht betrifft: Von der Zuständigkeit der Datenschutzaufsichtsbehörden sind zudem die justiziellen Tätigkeiten der Gerichte gem. Art. 55 Abs. 3 DS-GVO bzw. § 41 Abs. 2 LDSG ausgeschlossen.

Am 10.12.2021 hat der LfDI im Rahmen einer Online- Fachtagung für behördliche Datenschutzbeauftragte der Amts- und Landgerichte sowie Staatsanwaltschaften im Bezirk des Pfälzischen Oberlandesgerichts Zweibrücken diese Abgrenzungsfragen und weitere datenschutzrechtliche Themen wie z.B. die Gewährleistung von Betroffenenrechte, Aufgaben und Stellung der Datenschutzbeauftragten sowie die Maßnahmen zum Datenschutzmanagement in der Justiz behandelt. Im Anschluss konnten die Teilnehmerinnen und Teilnehmer aufgetretene problematische Praxisfälle vorstellen und gemeinsam mit den Referentinnen besprechen. Da der Austausch mit der Praxis auch aus Sicht des LfDI immer mit einen immensen Erkenntnisgewinn für dessen aufsichtsbehördliche Arbeit einhergeht und es zudem wichtig ist, dass der Datenschutz als Teil der Aufgabenerfüllung der Verantwortlichen aufgefasst wird, war die Fachtagung mit den interessierten und sachkundigen Teilnehmer:innen für alle Beteiligten sehr ertragreich.

2.2 Aufsichtszuständigkeit im Bereich Justiz- Justizielle Tätigkeit

Die Auslegung des Begriffs der justiziellen Tätigkeit im Sinne des Art. 55 Abs. 3 DS-GVO, § 41 Abs. 2 LDSG und die in diesem Zusammenhang auftretende Freistellung von der Datenschutzaufsicht durch den LfDI ist immer wieder Gegenstand von Zuständigkeitsfragen.

Der Begriff der justiziellen Tätigkeit wurde im Berichtsjahr wiederholt zwischen dem Ministerium der Justiz und dem LfDI aufgrund anhängiger Beschwerdeverfahren, die u.a. Tätigkeiten von Rechtspflegern betrafen, erörtert. Im Hinblick auf die Aufsichtszuständigkeit des LfDI wurde ein klarer Dissens festgestellt.

Nach der Einschätzung des Ministeriums der Justiz stellen auch Rechtspfleger „unabhängige Organe“ der Justiz dar, die von der Datenschutzaufsicht durch den LfDI ausgenommen seien.

Nach der Rechtsauffassung des LfDI bezieht sich dagegen der Begriff der justiziellen Tätigkeit allein auf solche, die im Bereich der „richterlichen Unabhängigkeit“ liegen, also mit der gerichtlichen Entscheidungsfindung in Zusammenhang stehen. Dazu gehören insbesondere alle vorbereitenden und der Durchführung dienenden Tätigkeiten. Die Tätigkeiten der Rechtspflege sind indes im deutschen Recht dem Bereich der Exekutive zuzuordnen und daher nach der Begriffsauslegung des LfDI nicht von der Bereichsausnahme des Art. 55 Abs. 3 DS-GVO erfasst. Unabhängig von der Frage der Aufsichts-

zuständigkeit finden die europa- und verfassungsrechtlichen Grundsätze des Datenschutzes, sowie das diese ausgestaltende nationale Recht in allen Bereichen der Justiz Anwendung, sodass das beidseitige Ziel übereinstimmend in der materiell-rechtlichen Umsetzung des Datenschutzrechts besteht und man sich dahingehend verständigte, dass der aufgezeigte Dissens durch eine konstruktive Kooperation unter Einbeziehung des Ministeriums der Justiz zu lösen ist.

Im Berichtszeitraum befasste sich der LfDI auch im Zusammenhang mit notariellen Tätigkeiten mit der Reichweite seiner Aufsichtszuständigkeit. Im konkreten Beschwerdefall weigerte sich ein Notar unter Hinweis auf eine mangelnde Zuständigkeit des LfDI, das an ihn gerichtete Informationsersuchen zu beantworten. Die eingebundene Notarkammer vertrat im weiteren Verfahren die Auffassung, dass die Bereichsaufnahme des Art. 55 Abs. 3 DS-GVO nicht wörtlich, sondern vielmehr autonom auszulegen sei. Maßgeblich sei, ob die Verarbeitung der Daten im Rahmen justizieller Unabhängigkeit erfolge. Notare und Notarinnen seien in Ihrer Stellung aufgrund der in § 1 BNotO garantierten Unabhängigkeit der eines Richter bzw. einer Richterin angenähert.

Der LfDI teilt auch diese Rechtsauffassung nicht. Art. 55 Abs. 3 DS-GVO enthält nach seinem eindeutigen Wortlaut lediglich eine Bereichsausnahme für die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen. Notare sind damit bereits rein funktional nicht von der Regelung erfasst. Aber auch eine interpretative Gleichstellung der Notare mit Gerichten kommt nicht in Betracht. Denn der europäische Normgeber hat die Gerichte gerade deshalb von einer externen Datenschutzaufsicht ausgenommen, weil sie aufgrund ihrer spezifischen Eigenorganisation eine hinreichende Sicherheit dafür bieten, dass das Recht auf informationelle Selbstbestimmung der Betroffenen gewahrt bleibt. Dies ist bei Notaren nicht der Fall.

2.3 Angaben im Stempel zum Nachweis einer in der JVA durchgeführten Corona-Impfung

Auch Justizvollzugsanstalten haben den Herausforderungen der Corona-Pandemie zu begegnen und dabei sowohl den infektionsschutzrechtlichen als auch den datenschutzrechtlichen Belangen in angemessener Weise zu entsprechen. Dass dies nicht immer einfach ist, zeigten die in JVAs angebotenen Corona-Schutzimpfungen.

Eine an den LfDI herangetragene Beschwerde stellte die datenschutzrechtliche Vereinbarkeit eines in einer JVA bei den Impfungen gegen COVID 19 verwendeten Stempels in Frage, mit dem Validität der Impfungen bestätigt werden sollte. Hintergrund hierfür war die Tatsache, dass der auf den Impfnachweisen aufgebrachte Stempel die Angabe „JVA“ enthielt. Damit war für diejenigen, denen ein derartiger Nachweis vorgelegt wurde, erkennbar, wo die Impfung durchgeführt wurde. Damit bestand aus Sicht des Beschwerdeführers die Gefahr, dass mit der Vorlage des Impfweises Dritte auf den Umstand einer Inhaftierung schließen konnten, was zumindest potentiell zu einer Stigmatisierung der geimpften Personen führen könnte.

Grundsätzlich dient der Impfnachweis und die damit einhergehende Pflicht zur Verarbeitung personenbezogener Daten der Klarstellung der medizinischen Verantwortlichkeit für die vorgenommene Impfung, weshalb gemäß § 22 Abs. 2 Nr. 4 Infektionsschutzgesetz eine Impfdokumentation „Name und Anschrift der für die Durchführung der Schutzimpfung verantwortlichen Person“ enthalten muss. Diese infektionsrechtliche Rechtsgrundlage ist in-

des nach dem LfDI nicht geeignet, eine datenschutzrechtliche Befugnis für die Nennung der „JVA“ als Einrichtung, in der die Impfung vorgenommen worden ist, zu liefern. Vielmehr wird eine etwaige Rückverfolgbarkeit der Impfung und der damit zusammenhängenden Verantwortung allein durch Nennung der medizinisch verantwortlichen Personen erreicht. Die Angabe der „JVA“ als Einrichtung, in der eine Impfung stattgefunden hat, ist somit infektionsschutzrechtlich nicht erforderlich um der Zielsetzung eines Nachweises der Integrität und der Authentizität der attestierten Impfung Genüge zu tun. Der datenschutzrechtliche Grundsatz der Datenminimierung ist dabei bei jeder Art von Datenverarbeitung zu beachten, weshalb es irrelevant ist, dass die Impfung freiwillig erfolgte. Aus datenschutzrechtlicher Perspektive kommt hinzu, dass die Erwähnung der JVA im Stempel durchaus geeignet ist, die hiervon betroffenen Personen zu stigmatisieren. Denn ohne einen persönlichen Bezug der geimpften Personen zu einer JVA - entweder als Mitarbeiter:in oder als inhaftierte Person - wäre es für Bürger nicht möglich, sich dort impfen zu lassen.

Aufgrund der dargestellten datenschutzrechtlichen Vorgaben wurde in allen Justizvollzugseinrichtungen im Lande auf die Verwendung der ursprünglich eingesetzten Stempel mit der Angabe „JVA“ verzichtet. Den betroffenen Personen wird zudem angeboten, bereits ausgestellte Impfnachweise noch zu korrigieren.

3. VIDEOÜBERWACHUNG

Im Jahr 2021 hat sich der Trend zu verstärkten Beschwerden aus dem nachbarschaftlichen Bereich fortgesetzt. Der LfDI leitete hierzu 256 Verfahren ein. Dabei lässt sich feststellen, dass in vielen Fällen nur der Verweis auf den Zivilrechtsweg verbleibt, da der LfDI nicht sicherstellen kann, dass Kameras nach Beantwortung der Informationsersuchen nicht umgestellt und damit rechtswidrig eingesetzt werden. Dieser Bereich bindet weiterhin einen Großteil der für die Videoüberwachung vorhandenen personellen Ressourcen.

Videoüberwachung im gewerblichen Bereich war in 40 Fällen Grund für die Einleitung eines Verfahrens, wobei es hier teils um den Schutz der Beschäftigten ging, teils Betriebe aus dem Freizeitsektor betroffen waren. Die Kooperation der Verantwortlichen konnte hier durchweg als gut bis sehr gut festgestellt werden. Insgesamt scheint sich ein Verständnis für die Belange des Datenschutzes abzuzeichnen und eine Bereitschaft, zumindest im Rahmen eines Verfahrens, notwendige Anpassungen vorzunehmen.

Der LfDI konnte im Jahr 2021 die Prüfung der Videoüberwachungsanlagen in Impfzentren in Rheinland-Pfalz abschließen (https://s.rlp.de/vwu4q). Hier zeigt sich ein sparsamer Einsatz von Videoanlagen, welche der notwendigen Abwägung zwischen Datenschutz und Sicherheitsinteressen Rechnung trug. Auch fand eine umfangreiche Prüfung eines neuen Videosystems zur Überwachung von Autobahnraststätten statt.

Ein im abgelaufenen Jahr verstärkt auftretendes Thema war die Nutzung von Wildkameras in Forstbereichen, sowohl durch private Jagdpächter als auch durch öffentliche Stellen. Besondere Probleme stellten sich dabei bei der Ermittlung der Verantwortlichen. Auch lässt sich feststellen, dass vielen Verantwortlichen in diesem Bereich noch die Sensibilität dafür fehlt, dass Waldgebiete insgesamt der Erholung der Bevölkerung dienen und daher auch hier der Datenschutz beachtet werden muss.

Schließlich hat das OVG Koblenz am 25.06.2021 (10 A 10302/21.OVG) entschieden, dass eine Aufsichtsbehörde im Rahmen von Art. 58 Abs. 2 DS-GVO nicht über die Möglichkeiten verfügt, die Deinstallation von Videokameras anzuweisen. Allein mit der nachgewiesenen Deaktivierung sei ein datenschutzkonformer Zustand hergestellt, aufgrund fehlender Datenverarbeitung bestehe keine Zuständigkeit der Aufsichtsbehörde mehr.

Im öffentlichen Bereich ist das Beratungsaufkommen nach wie vor hoch. Öffentliche Plätze oder Parkanlagen, aber auch Schulgebäude und Wertstoffsammelstellen sind weiterhin Orte, an denen es oft zu Vandalismus und Müllablagerungen kommt. Öffentliche Stellen erhoffen sich dort durch Videoüberwachungsanlagen Abschreckung aber auch Aufklärung. Viele Stellen sind inzwischen durch die behördlichen Datenschutzbeauftragten schon umfangreich informiert und wenden sich dann zur letzten Abklärung an den LfDI. Beschwerden über diesen Bereich gab es 2021 nur sehr wenige, was darauf schließen lässt, dass der Einsatz von Videoüberwachung im Vergleich zu Vorjahren restriktiver und mit mehr Augenmaß erfolgt.

Pandemiebedingt war die Anzahl der Veranstaltungen, die durch Behörden, Polizei oder sonstige öffentlichen Stellen mit Videoüberwachung begleitet wurden, auch im Jahr 2021 gering.

4. WIRTSCHAFT

4.1 Datenverarbeitung durch Private in Zeiten von Corona auch im Jahr 2021

Die weiterhin bestehenden und sich stets verändernden Einschränkungen aufgrund der Corona-Pandemie stellten die Verantwortlichen in der Privatwirtschaft neben vielen anderen auch weiterhin vor datenschutzrechtliche Herausforderungen. Neben den nach wie vor aktuellen Fragen zur Kontakterfassung standen im Jahr 2021 Fragen nach der Kontrolle des Geimpft-, Genesenen- oder Testnachweises im Vordergrund.

Nach der Corona-Bekämpfungsverordnung Rheinland-Pfalz gilt für den Besuch von Einrichtungen, die Teilnahme an Veranstaltungen und die Inanspruchnahme von Dienstleistungen die sog. 2G- oder 3G-Regel. Entweder dürfen nur noch Geimpfte oder Genesene eingelassen werden oder auch Personen, die einen negativen Testnachweis vorlegen.

Geimpfte und Genesene sowie Personen mit negativem Testergebnis müssen ihren entsprechenden Nachweis vor Betreten der Einrichtung oder der Inanspruchnahme der Dienstleistung vorlegen und dies bei über 16-Jährigen zusammen mit einem amtlichen Lichtbildausweis. Der Verantwortliche muss sich also davon überzeugen, dass der Gast oder die Besucherin bzw. der Besucher auch tatsächlich Inhaber des Nachweises ist.

Geimpften und genesenen Personen gleichgestellt sind Kinder im Alter bis zwölf Jahre und drei Monaten sowie Personen, die sich aus medizinischen Gründen nicht impfen lassen können. Diese Personen müssen eine ärztliche Bescheinigung vorlegen, aus der sich mindestens nachvollziehbar die Grundlage für die ärztliche Diagnose ergeben muss. Zudem muss ein Testnachweis (Schnelltest durch geschultes Personal oder PCR-Test, bei Minderjährigen auch ein Selbsttest unter Aufsicht) erbracht werden.

Die Besucher bzw. Gäste sind verpflichtet, diese Zugangsvoraussetzungen einzuhalten, die Verantwortlichen verpflichtet, dies zu kontrollieren.

Durch die Kenntnisnahme des 2G- bzw. 3G-Nachweises werden personenbezogene Gesundheitsdaten durch die Verantwortlichen der genannten Einrichtungen verarbeitet. Diese Datenverarbeitung findet ihre Rechtgrundlage in Art. 9 Abs. 2 lit. i, Art. 6 Abs. 1 lit. b oder c DS-GVO i.V.m. § 32 Satz 1, § 28 Abs. 1 Satz 1 und 2 IfSG und den Vorschriften der jeweils aktuellen Corona-Bekämpfungsverordnung. Dabei ist datenschutzrechtlich Folgendes zu beachten:

Auf Grundlage des 2G- oder 3G-Nachweises ist lediglich darüber zu entscheiden, ob die betroffene Person die Einrichtung betreten darf oder nicht. Eine Dokumentation der Prüfung oder auch eine Kopie des Nachweises durch den Betreiber der Einrichtung sind weder nach der Verordnung noch nach dem Infektionsschutzgesetz erforderlich und können damit auch nicht darauf als Rechtsgrundlage gestützt werden. Auch ersetzt eine Kopie des Nachweises nicht die ggf. erforderliche Kontakterfassung, da z. B. in der Testbescheinigung mehr Daten enthalten sind als für die Kontakterfassung erforderlich sind. Die Erfassung der Kontaktdaten hat also unabhängig hiervon in datenschutzgerechter Weise zu erfolgen.

Es dürfen nur so viele Daten erhoben werden, wie für die gesetzlich vorgesehene Kontrolle erforderlich sind. Dies spielt insbesondere bei der Prüfung der elektronischen Zertifikate eine Rolle. Für die Kontrolle der elektronischen Impf- oder auch Genesenenzertifikate stehen entsprechende Kontroll-Apps zur Verfügung. Die Kontrolle mit der zugehörigen Kontroll-

App (QR-Code-Scan) ist gegenüber der Inaugenscheinnahme der digitalen Zertifikate datensparsamer, da sie nur bestätigt, dass ein gültiger 2G-Schutz besteht, ohne dem kontrollierenden Personal z.B. das Datum der Impfung oder den Impfstoff anzuzeigen. Die Kontrolle mit der Kontroll-App prüft außerdem, ob möglicherweise ein unrechtmäßig ausgestelltes digitales Zertifikat vorliegt, welches als ungültig gekennzeichnet wurde. Die Kontrolle elektronischer 2G-Zertifikate ist daher mit einer entsprechenden Kontroll-App durchzuführen. Die so verarbeiteten Daten werden auch nicht gespeichert.

Konkret bedeutet dies, dass z.B. der Gastronom, Händler oder Dienstleister bzw. das von ihm beauftragte Personal die Gültigkeit eines elektronischen Zertifikats mittels der o.g. Möglichkeiten überprüfen und dazu zusätzlich den Personalausweis einsehen muss.

Hier zweifeln einige Bürgerinnen und Bürger an, dass Privatpersonen berechtigt sind, den Ausweis einzusehen. Nach dem Personalausweisgesetz kann der Inhaber den Ausweis bei öffentlichen und nichtöffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden. Da eine entsprechende Legitimation verpflichtend in der Corona-Bekämpfungsverordnung vorgesehen ist und sowohl Verantwortlicher als auch betroffene Person dieser Verpflichtung nachkommen müssen, bestehen keine datenschutzrechtlichen Bedenken gegen das Vorzeigen des Ausweises auch gegenüber nichtöffentlichen Stellen.

Ein Einscannen oder ein Foto des analogen Zertifikats, also z.B. des Impfausweises, oder auch des Ausweisdokuments und eine damit einhergehende, auch nur kurzfristige Speicherung zu Dokumentationszwecken sind nicht erforderlich und damit auch ohne Einwilligung der betroffenen Person datenschutzrechtlich nicht zulässig. Ein Einscannen des analogen Impfausweises ermöglicht auch keine Prüfung der Echtheit oder Gültigkeit.

Auch ergibt sich aus der Corona-Bekämpfungsverordnung keine Rechtsgrundlage dafür, die Daten im Falle eines positiven Ergebnisses bei zulässigen Schnelltests vor Ort an Dritte, z.B. das Gesundheitsamt, zu übermitteln. Bei einem positiven Ergebnis ist lediglich der Zutritt zu verweigern. Nach § 2 Abs. 2 der Landesverordnung zur Absonderung bei Verdacht einer SARS-CoV-2-Infektion Rheinland-Pfalz (CoronaVAbsondV) muss sich die positiv getestete Person unverzüglich absondern. Derzeit sind weder eine Melde- noch eine Hinweispflicht des Betreibers der Einrichtung gegenüber der positiv getesteten Person ersichtlich.

Die betroffenen Personen müssen zum Zeitpunkt der Datenerhebung durch den Betreiber der Einrichtung entsprechend den Anforderungen der Datenschutz-Grundverordnung (Art. 13 DS-GVO) informiert werden.

4.2 Datenweitergabe an Rechtsbeistände

Im Rahmen von Rechtsstreitigkeiten kommt es häufig zur Frage, ob eine Partei die Daten der anderen Partei ihrem Rechtsbeistand zur Verfügung stellen darf.

Grundsätzlich dürfen sich Personen der Hilfe eines Dritten bedienen, um ihre rechtlichen Interessen durchzusetzen. Dies kann z.B. die Einschaltung einer Rechtsanwältin oder eines Rechtsanwaltes sein. Dann ist es aber auch erforderlich, dass der Rechtsbeistand im Rahmen dieser berechtigten Beauftragung die Kontaktdaten des Gegners in einer Rechtsstreitigkeit erhält. Damit dient die entsprechende Weitergabe der Daten und damit die Verarbeitung der Wahrung des berechtigten Interesses des Ver-

antwortlichen und ist damit gem. Art. 6 Abs. 1 lit. f DS-GVO grundsätzlich gerechtfertigt.

4.3 Löschung von Kundendaten

Der LfDI unterstützt Bürgerinnen und Bürger bei der Durchsetzung ihrer Auskunfts- und Löschansprüche im Rahmen der Datenschutz-Grundverordnung. Hierbei kommt es gerade im Bereich der Löschungen immer wieder zu Unklarheiten.

Nach Art. 17 DS-GVO haben betroffene Personen unter bestimmten Voraussetzungen ein Recht auf Löschung ihrer Daten, es sei denn, der Verantwortliche unterliegt einer rechtlichen Verpflichtung zur weiteren Speicherung der Daten. Eine solche rechtliche Verpflichtung stellen in der Regel die gesetzlichen Aufbewahrungspflichten insbesondere nach der Abgabenordnung und dem Handelsgesetzbuch dar. Entsprechend wird bei Löschbegehren von den Verantwortlichen argumentiert.

In der Praxis stellt sich die Frage, welche personenbezogenen Daten im Rahmen der steuerlichen und handelsrechtlichen Aufbewahrungspflichten aufbewahrt werden müssen und damit auch nur dürfen. Nach dem Umsatzsteuergesetz muss z. B. eine Rechnung den vollständigen Namen und die vollständige Anschrift des Leistungsempfängers enthalten, eine Ausnahme gilt für Kleinbeträge unter 250 Euro. Bei Geschäftsabschlüssen fallen aber oft mehr personenbezogene Daten an, wie E-Mail-Adresse, Telefonnummer, Geburtsdatum, (abweichende) Lieferanschrift etc. Fraglich ist hier, ob auch diese Daten im Rahmen der gesetzlichen Aufbewahrungsfristen zu speichern sind.

Für die steuerlichen Aufbewahrungsregeln können die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) herangezogen werden: Danach sind Aufzeichnungen über Geschäftsvorfälle aufzubewahren (vgl. Ziffer 1.7 GoBD). Geschäftsvorfälle sind alle rechtlichen und wirtschaftlichen Vorgänge, die innerhalb eines bestimmten Zeitabschnitts den Gewinn bzw. Verlust oder die Vermögenszusammensetzung in einem Unternehmen dokumentieren, beeinflussen oder verändern (vgl. Ziff. 1.9 GoBD).

Außerdem sind auch Handels- und Geschäftsbriefe sowie Handelsbriefe nach Handelsrecht aufzubewahren. Dabei versteht man unter Handelsbriefen sämtliche Schriftstücke – unabhängig von ihrer postalischen Versendungsform –, die ein Handelsgeschäft betreffen. Sie betreffen ein Handelsgeschäft, wenn sie dessen Vorbereitung, Abschluss, Durchführung oder Rückgängigmachung zum Gegenstand haben.

Bei der Aufbewahrung ist für den Zeitraum der Aufbewahrungspflicht insofern u.a. der Grundsatz der Unveränderbarkeit zu beachten, welcher während der Dauer der Aufbewahrungsfrist nachweisbar erfüllt werden und erhalten bleiben muss (vgl. Ziff. 3, Rn. 27 GoBD). Sind aufzeichnungs- und aufbewahrungspflichtige Daten, Datensätze, elektronische Dokumente und elektronische Unterlagen im Unternehmen entstanden oder dort eingegangen, sind sie auch in dieser Form aufzubewahren und dürfen vor Ablauf der Aufbewahrungsfrist nicht gelöscht werden. Sie dürfen daher nicht mehr ausschließlich in ausgedruckter Form aufbewahrt werden und müssen für die Dauer der Aufbewahrungsfrist unveränderbar erhalten bleiben (z. B. per E-Mail eingegangene Rechnung im PDF-Format oder bildlich erfasste Papierbelege) (vgl. GoBD Ziff. 9, Rn. 119).

Eine nachträgliche Löschung einzelner Datensätze aus den bereits entstandenen Geschäftsvorgängen würde damit einen Verstoß gegen

die gesetzlichen Aufbewahrungspflichten bedeuten.

Diesem Grundsatz der Unveränderlichkeit der Geschäftsunterlagen steht aber der Grundsatz der Erforderlichkeit gegenüber: So sind in den meisten Fällen z.B. E-Mail-Adressen, Telefonnummern oder Lieferanschriften für steuerrechtliche Nachweise nicht erforderlich. Wenn sie sich aber in den Geschäftsunterlagen befinden, dürften sie gem. den oben dargestellten Anforderungen der GoBD nicht herausgelöst und gelöscht werden.

Der LfDI hat hier eine Weigerung der Löschung der „personenbezogenen Daten“ insgesamt nicht beanstandet, wenn sich die Verantwortlichen auf die gesetzlichen Aufbewahrungspflichten gestützt haben. Es wurde jedoch aufgegeben, diese Daten nicht mehr anderweitig zu nutzen, sie also zu sperren.Während der Sachverhalt im Berichtszeitraum abschließend ermittelt werden konnte, sind die aufsichtsrechtlichen Maßnahmen und Sanktionen im Berichtszeitraum noch zu keinem Abschluss gekommen und werden den LfDI im Jahr 2021 weiter begleiten.

5. LEBEN DIGITAL

5.1 Anforderungen an die Einwilligung bei der Aufzeichnung von Telefonaten (Hotlines)

Unternehmen haben häufig ein Interesse daran, Anrufe von Kund:innen in ihren Servicecentern bzw. bei ihren Service-Hotlines aufzuzeichnen.

Aufgrund einer Beschwerde gegen ein Unternehmen wurde der LfDI darauf aufmerksam gemacht, dass ein Unternehmen Anrufe ohne Einwilligung der Anrufer:innen aufzeichnen würde. Das Unternehmen teilte hingegen mit, es würden keine Anrufe ohne Einwilligung der Anrufer :innen aufgezeichnet. Stattdessen würden diese zu Beginn des Telefonats darauf hingewiesen, dass die Anrufe zur Qualitätssicherung aufgezeichnet würden. Sollte man damit nicht einverstanden sein, sei darum gebeten worden, das Anliegen schriftlich vorzubringen. Eine ausdrückliche Antwort in Bezug auf das Einverständnis oder etwa die Bestätigung durch einen Tastendruck sei nicht abgefragt worden.

Im Hinblick auf den Beschluss der DSK vom 23.03.2018 zur Aufzeichnung von Telefongesprächen vertritt der LfDI die Auffassung, dass dieses Vorgehen nicht den Anforderungen an eine wirksame Einwilligung genügt und diese auch nicht auf Art. 6 Abs. 1 lit. f DS-GVO gestützt werden kann.

Soweit es um die vorliegende Aufzeichnung von Telefongesprächen geht, stellt insbesondere Art. 6 Abs. 1 lit f. DS-GVO (berechtigte Interessen) keine einschlägige Rechtsgrundlage dar, da zu dem verfolgten Zweck der Qualitätssicherung eine Aufzeichnung der Gespräche nicht erforderlich ist und insbesondere die Interessen der betroffenen Personen die Interessen an der Aufzeichnung überwiegen.

Ebenso ist vorliegend Art. 6 Abs. 1 lit. a DS-GVO (Einwilligung) keine einschlägige Rechtsgrundlage, da das Gespräch ohne eine wirksame Einwilligung aufgezeichnet wurde.

Eine datenschutzrechtlich wirksame Einwilligung im Sinne von Art. 4 Nr. 11 DS-GVO setzt voraus, dass der externe Gesprächspartner vor Beginn der beabsichtigten Aufzeichnung gefragt wird, ob er mit der Aufzeichnung einverstanden ist, und falls er einverstanden ist, gebeten wird, sein Einverständnis beispielsweise durch Aussprechen eines „Ja“ oder durch eine aktive bestätigende Handlung (etwa durch das Betätigen einer Telefontaste) eindeutig zum Ausdruck zu bringen. Diese Einwilligung umfasst nicht eine biometrische Auswertung. Die bloße Einräumung einer Widerspruchsmöglichkeit und das anschließende Fortsetzen des Telefonats stellen keine datenschutzrechtlich wirksame Einwilligung im Sinne der DS-GVO dar. Da der datenschutzrechtlich Verantwortliche nachweisen können muss, dass die betroffene Person eine wirksame Einwilligung erteilt hat (Art. 7 Abs. 1 DS-GVO), muss er auch nachweisen können, dass die betroffene Person die Einwilligung „in informierter Weise“ abgegeben hat (vgl. Art. 4 Nr. 11 DS-GVO).

Das bloße „Weitersprechen“ ist nicht als konkludente Einwilligung zu werten, weder durch das Aufrechterhalten der Telefonverbindung noch durch Fortführung des Gespräches. Ein konkludentes Verhalten liegt nur dann vor, wenn diesem ein eindeutiges Erklärungsverhalten zukommt, dass auf den konkreten Willen des Erklärenden schließen lässt.

5.2 Energieversorger – Verarbeitung von Positivdaten

Auch im Jahr 2021 beschäftigte sich der LfDI erneut mit dem Thema der Positivdaten im Rahmen von Verträgen mit Energieversorgern.

Bei Auskunfteien und Energieversorgern gibt es Überlegungen oder hat es solche gegeben, einen zentralen Datenpool („Energieversorgerpool“) unter anderem zu Strom- und Gasverträgen zu schaffen. Darin sollen auch Daten von Kund:innen gespeichert werden, die sich stets vertragskonform verhalten haben – sogenannte Positivdaten.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat nun mit Beschluss vom 15. März 2021 festgehalten, dass entsprechende Pläne nach Maßgabe von Art. 6 Abs. 1 S. 1 lit. f DS-GVO rechtswidrig wären. Es bestehe die Gefahr der „gläsernen Verbraucher:innen“.

In dem Beschluss heißt es unter anderem: „Jede Bürgerin und jeder Bürger hat […] das Recht, den Wettbewerb zwischen den Energieversorgern zu nutzen und am Markt nach günstigen Angeboten zu suchen. Der Wunsch, vermeintliche „Schnäppchenjäger“ in einem zentralen Datenpool zu erfassen, um sie bei Vertragsanbahnung als solche identifizieren und ggf. von Angeboten ausschließen zu können, stellt kein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 Satz 1 lit. f DS-GVO dar. Es war gerade das Ziel des Gesetzgebers, durch die Liberalisierung des Energiemarktes einen wirksamen und unverfälschten Wettbewerb bei der Versorgung mit Elektrizität und Gas zu ermöglichen. Der Versuch, preisbewusste und wechselfreudige Verbraucher*innen zu identifizieren und sie ggf. von bestimmten Angeboten auszuschließen, liefe dieser Zielsetzung zuwider.“

Vergangenes Jahr sind die Pläne von Auskunfteien und Energieversorgern publik geworden. Ein Arbeitskreis der DSK hat daraufhin einen diesbezüglichen Beschluss vorbereitet. Nach Auffassung des LfDI dürfen Personen, die einen neuen Strom- oder Gasvertrag abschließen möchten, keine Restriktionen drohen, sofern diese sich zuvor immer vertragsgemäß verhalten haben. Nicht zulässig wäre es daher, wenn Kund:innen in einem Datenpool etwa wegen eines Anbieterwechsels als „problematisch“ eingestuft werden könnten. Die Vertragsfreiheit ist weiterhin zu gewährleisten.

Dem DSK-Beschluss zufolge können die Informationen, die offenbar gesammelt werden sollen oder sollten (etwa über die Anzahl abgeschlossener Verträge und die jeweilige Vertragsdauer), Hinweise darauf geben, ob Verbraucherinnen und Verbraucher eine längere Vertragsbeziehung zu einem Stromversorger beabsichtigen oder regelmäßig Neukunden-Angebote nutzen. Die Folge wäre, dass Verbraucherinnen und Verbraucher, die regelmäßig das für sie kostengünstigste Angebot am Markt wählen, später von Versorgungsunternehmen bei preislich attraktiven Angeboten ausgeschlossen werden könnten. Mit Blick auf die rechtliche Bewertung formuliert die DSK daher: „Selbst wenn die Interessen der Unternehmen als berechtigt angesehen würden, überwiegen in derartigen Fällen die schutzwürdigen Interessen und Grundrechte der Kund*innen. Vertragstreue Verbraucher*innen dürfen zu Recht erwarten, dass keine über den Vertragszweck hinausgehende Verarbeitung ihrer Daten erfolgt, die ggf. ihre Möglichkeiten einschränkt, frei am Markt agieren zu können.“

Der Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder „Energieversorgerpool darf nicht zu gläsernen Verbraucher*innen führen“ ist hier zu finden: https://s.rlp.de/Fk3tq

5.3 Online-Seminar „Datenschutz im Verein“

Der LfDI beteiligte sich im Dezember am Projekt „Digital in die Zukunft“ der Landesregierung, welches von der Leitstelle Ehrenamt und Bürgerbeteiligung in der Staatskanzlei zusammen mit medien+bildung.com, einer Tochter der Medienanstalt Rheinland-Pfalz, umgesetzt wird. In Rahmen einer neuen Reihe von Online-Fortbildungen zu aktuellen Vereinsthemen erläuterte ein Referent des LfDI am 09. Dezember 2021 die Grundlagen des Datenschutzrechts und gab spezifische Praxishinweise, Hilfestellungen sowie Tipps für Vereine. Die Fragen der Teilnehmenden zeigten, dass die Vereine sowohl die Lösung typischer Sachverhalte aus dem Vereinsalltag wie auch der Umgang mit der derzeitigen Pandemiesituation beschäftigt. Insbesondere die Veröffentlichung von Fotografien, die Verwaltung von Mitgliederdaten sowie Fragen im Zusammenhang mit der Verarbeitung des Impf- und Genesenenstatus waren von Interesse.

5.4 Verarbeitung von Positivdaten von Privatpersonen aus Verträgen über Mobilfunkdienste und Dauerhandelskonten durch Auskunfteien

Standen Anfang des Jahres vornehmlich die Energieverträge im Fokus, entzündeten sich gegen Ende des Jahres vermehrt Diskussionen insbesondere um Mobilfunkverträge. Gegenstand war die mutmaßlich seit mehreren Jahren praktizierte Verarbeitung von Positivdaten über Verträge von Mobilfunkdiensten und Dauerhandelskonten durch bestimmte Auskunfteien.

Wie schon im Falle der Energieversorger sieht der LfDI ebenso die Verarbeitung von Positivdaten von Kund:innen mit Mobilfunkverträgen und/oder Dauerhandelskonten kritisch. Im Gegensatz zu Negativdaten, welche einen unmittelbaren Rückschluss auf vertragswidriges Verhalten der Kund:innen zulassen, sind Positivdaten solche Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben

Datenschutzrechtlich zulässig ist etwa die Speicherung und Beauskunftung solcher Daten nur dann, soweit hierfür eine entsprechende Rechtsgrundlage gemäß Art. 5 Abs. 1 lit. a i.V.m. Art. 6 Abs. 1 DS-GVO vorliegt. Neben einer ausdrücklichen Einwilligung durch den Kunden (Art. 6 Abs. 1 lit. a DS-GVO) ist hier insbesondere die Datenverarbeitung aufgrund eines berechtigten Interesses (Art. 6 Abs. 1 lit. f DS-GVO) relevant. Eine solche setzt allerdings voraus, dass im Rahmen einer Abwägung die Interessen insbesondere der Anbieter an der Datenverarbeitung höher zu bewerten sind, als die Interessen der betroffenen Kundinnen und Kunden an deren Schutz ihrer personenbezogenen Daten. Dass hier der Datenschutz der Kundinnen und Kunden hinter den Interessen der Unternehmen zurückstehen muss, ist aus Sicht des LfDI jedoch zweifelhaft. Typischerweise erfolgt die Tätigkeit von Wirtschaftsauskunfteien zur Absicherung von Zahlungsausfällen, also vertragswidrigem Verhalten.

Diese Voraussetzungen dürften hier jedoch in der Regel nicht vorliegen.

Auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat daher mit Beschluss vom 22. September 2022 entschieden, dass der Beschluss der DSK vom 11.06.2018 aufrechterhalten wird, so dass weiterhin die Übermittlung und Verarbeitung von sog. Positivdaten an bzw. durch Handels- und Wirtschaftsauskunfteien grundsätzlich nicht auf Art. 6 Abs. 1 lit. f DS-GVO gestützt werden kann und es für eine Übermittlung und Verarbeitung dieser regelmäßig einer wirksamen Einwilligung der be-

troffenen Person unter Beachtung der hohen Anforderungen an die Freiwilligkeit bedarf.

Der Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder „ Verarbeitung von Positivdaten von Privatpersonen aus Verträgen über Mobilfunkdienste und Dauerhandelskonten durch Auskunfteien“ ist hier zu finden: https://s.rlp.de/positivdaten

5.5 Verarbeitung des Immunisierungsstatus im Rahmen der Planung von Vereinstätigkeiten

Aufgrund vermehrter Anfragen von Vereinen im Zusammenhang mit der Corona-Pandemie hat der LfDI im Rahmen des Internetangebots konkrete Hinweise zur Verarbeitung des Impf- bzw. Immunisierungsstatus auf Basis der Einwilligung erarbeitet. Der Hintergrund ist, dass aufgrund der zahlenmäßigen Beschränkung von nicht-immunisierten Personen z.B. bei Vereinsveranstaltungen bei Vereinen das Bedürfnis besteht, schon vorab Kenntnis über den Immunisierungsstatus der Gäste zu erhalten und eine Sichtkontrolle hier in vielen Fällen nicht ausreichend praktikabel ist

Bei zahlenmäßigen Beschränkungen von Teilnehmer:innen stehen Vereine vor dem Problem, dass Planung und Durchführung hygienekonformer Trainings und Spiele, Proben und Auftritte praktisch nur dann realisierbar sind, wenn bereits im Vorfeld der Planung eine Abfrage der Teilnehmenden bezüglich des Immunisierungsstatus erfolgen kann. Möchten Vereine Veranstaltungen planen, ist dies im Vorfeld nur praktikabel möglich, wenn der Verein bzw. der Veranstalter einen Überblick darüber haben, welche Teilnehmenden welchen Immunisierungsstatus haben. Hierbei ist zu beachten, dass es sich bei der Information, ob eine Person bereits immunisiert ist oder nicht, um ein besonders geschütztes gesundheitsbezogenes Datum im Sinne des Art. 9 Abs. 1 DS-GVO handelt. Im Rahmen der Planung von Veranstaltungen, Trainings oder Proben ist die Verarbeitung dieser Information daher nur zulässig, wenn die betroffene Person bzw. bei Kindern und Jugendlichen die sorgeberechtigte Person hierin freiwillig und informiert eingewilligt hat. Es spricht nicht gegen die Freiwilligkeit der Einwilligung, wenn eine Teilnahme an einem Training, Wettkampf oder an einer sonstigen Veranstaltung von der Angabe des Immunisierungsstatus abhängig gemacht wird. Die Kenntnis des Immunisierungsstatus kann aufgrund der Regelungen der jeweils geltenden Corona-Bekämpfungsverordnung zur Planung und Durchführung der Veranstaltung erforderlich sein.

Ebenso ist es denkbar, dass nach dem Verkauf der Tickets bzw. nach Vergabe der Teilnahmeplätze kurz vor der Veranstaltung eine andere Regelung und damit eine andere Zahl zugelassener nicht-immunisierter Personen gilt. In diesem Fall ist es für die Durchführung der Veranstaltung erforderlich, dass der Veranstalter die Möglichkeit hat, die Planung anzupassen. Dies ist wiederum nur möglich, wenn er bis zum Veranstaltungsbeginn die Möglichkeit hat, die Zahl der nicht-immunisierten Personen einzuschätzen.

Sollen im Rahmen der Planung einer Veranstaltung, der Trainings- oder Wettkampforganisation oder beim Proben- und Auftrittsbetrieb der Breiten- und Laienkultur im Vorfeld von Teilnehmenden der Immunisierungsstatus abgefragt werden, ist dies mittels ausdrücklicher, freiwilliger und ausreichend informierter Einwilligung durch die Teilnehmenden grundsätzlich möglich.

Weitere Informationen hierzu finden Sie unter: https://www.datenschutz.rlp.de/de/themenfelder-themen/vereine/

6. BESCHÄFTIGTENDATENSCHUTZ

6.1 Datenschutz bei 3G am Arbeitsplatz

Durch eine Änderung des Infektionsschutzgesetzes zum 24.11.2021 hat sich die Rechtslage hinsichtlich der Zulässigkeit einer Abfrage nach dem Impfstatus im Beschäftigungsverhältnis grundlegend geändert. Während zuvor eine Abfrage des Impfstatus nur in wenigen besonders gefährdeten Einrichtungen zulässig war, galt ab diesem Zeitpunkt flächendeckend die sog. 3G-Regelung an Arbeitsstätten. Das bedeutete, dass nur noch geimpfte, genesene oder getestete Personen die Arbeitsstätte betreten dürfen (§ 28b Abs. 1 IfSG). Korrespondierend hierzu wurden Kontrollpflichten des Arbeitgebers hinsichtlich der 3G-Regelung und das Recht zur Verarbeitung der Gesundheitsdaten eingeführt (§ 28b Abs. 3 IfSG).

Arbeitgeber durften daher ab dem genannten Stichtag folgende Daten ihrer Mitarbeiterinnen und Mitarbeiter erfragen und sich entsprechende Nachweise vorlegen lassen: Die Tatsache, dass ein 3G-Nachweis in Form eines gültigen Zertifikates vorliegt sowie die Gültigkeitsdauer des Zertifikates, sofern das Ablaufdatum vor dem Außerkrafttreten des Gesetzes am 19.3.2022 liegt. Nicht erforderlich und daher unzulässig war die Abfrage und Speicherung des Impfdatums (Erst-, Zweit-, und Booster-Impfung) oder des verabreichten Impfstoffs.

Mit Einwilligung des Beschäftigten konnten die Nachweise über den Status „geimpft“ oder „genesen“ beim Arbeitgeber hinterlegt werden, weil dann die tägliche Kontrolle entbehrlich war. Der LfDI wies in Pressemitteilungen aber darauf hin, dass diese Informationen getrennt von der Personalakte gespeichert werden müssen und empfahl die Nutzung der vom Robert-Koch-Institut herausgegebenen CovPassCheck-App (https://www.digitaler-impfnachweis-app.de/covpasscheck-app/), da durch das Einscannen des QR-Codes die Gültigkeit des Zertifikates datensparsam überprüft werden konnte (geimpft oder genesen).

Wesentliche datenschutzrechtliche Fragestellungen, die mit der „3G-Regelung“ am Arbeitsplatz einhergehen, wurden von der DSK in einer Orientierungshilfe zusammengefasst: https://s.rlp.de/i7V3N

6.2 Krankmeldungen über WhatsApp

Im Berichtszeitraum wurde in mehreren Beschwerden die Weiterleitung von Krankmeldungen über WhatsApp im Arbeitsverhältnis thematisiert. In diesem Zusammenhang spielte auch die Bildung von betriebsinternen WhatsApp-Gruppen eine Rolle.

Mitteilungen innerhalb einer betrieblichen WhatsApp-Gruppe sind bereits aufgrund der Wahl eines amerikanischen Messengerdienstes, bei dem mit Blick auf die nicht zu unterbindenden Datenübertragungen in die USA eine datenschutzkonforme Nutzung in aller Regel nicht sichergestellt werden kann, unzulässig. Erst recht eignet sich der Messenger nicht, um besonders schützenswerte Gesundheitsdaten, wie beispielsweise die Kopie einer Arbeitsunfähigkeitsbescheinigung, zu kommunizieren. Der LfDI sprach in diesen Fällen stets eine Verwarnung aus. Die Unternehmen hatten zuvor von sich aus beschlossen, die betriebliche Nutzung von WhatsApp einzustellen.

7. MEDIEN

7.1 Webseiten, Cookies und Tracking

Auch im Jahr 2021 stellte die Überprüfung von Webseiten hinsichtlich der Verarbeitung von Nutzungsdaten einen deutlichen Schwerpunkt im Bereich Medien dar. Weiterhin erreichten den LfDI eine Vielzahl von Beschwerden über und Hinweisen auf Webseiten, die die datenschutzrechtlichen Anforderungen an die Verarbeitung von Nutzungsdaten der Webseitenbesucher:innen nicht erfüllten oder aus Sicht der Beschwerdeführer:innen und Hinweisgeber:innen nicht zu erfüllen scheinen. Hierbei ging es inhaltlich regelmäßig um den Einsatz von Cookies und Tracking-Tools zu unterschiedlichen Zwecken, insbesondere für Werbung und Datenhandel. Eine flächendeckende Überprüfung aller in Rheinland-Pfalz ansässigen Webseiten von Amts wegen war personell für den LfDI nicht leistbar, auf Beschwerden und Hinweise wurde aber durch die Einleitung von Prüfverfahren reagiert.

Die Überprüfung der Webseiten erfordert in der Regel ein Zusammenarbeiten des Medienbereiches mit dem Bereich Technik. Überprüft werden das Vorhandensein und die grafische sowie technische Gestaltung von sogenannten Einwilligungsbannern, der Inhalt von Datenschutzerklärungen und die tatsächlichen Datenverarbeitungen auf den Webseiten, also etwa welche Cookies gesetzt werden und welche weiteren Dienste in die Webseite eingebunden sind, z.B. Social Plugins, Webfonts, etc.

Zum Ende des Jahres am 1.12.2021 trat das neue „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien“ (TTDSG) in Kraft. Dieses setzte insbesondere im Hinblick auf den Einsatz von Cookies die Rechtsprechung des Bundesgerichtshofs zum früheren § 15 Abs. 3 Telemediengesetz (TMG) im Urteil vom 1.10.2019 zur Rechtssache C-673/17 (Planet49) gesetzlich um und führte damit nach vielen Jahren schließlich zu einer europarechtskonformen Umsetzung der ePrivacy-Richtlinie in Deutschland. Obwohl das Gesetz erst im Dezember in Kraft trat, prägte es schon viele Monate zuvor die Arbeit der Aufsichtsbehörden des Bundes und der Länder im Bereich Webseiten, Cookies und Tracking. Aufgrund der Neuregelung wurde es nötig, die Orientierungshilfe der Aufsichtsbehörden für Telemedienanbieter aus dem März 2019 zu aktualisieren und sie an den neuen Rechtsrahmen anzupassen. Aufgrund der frühzeitigen und intensiven Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder gelang die Veröffentlichung der neuen Orientierungshilfe bereits zum 20. Dezember 2022.

Etwa zeitgleich mit dem Inkrafttreten des TTDSG stieg die Zahl von Beschwerden und Hinweisen auf nicht datenschutzkonforme Webseiten sprunghaft an. Die Anzahl überstieg die personellen Ressourcen des LfDI zum Jahresende 2021 deutlich. Die Bearbeitung konnte nur durch eine Priorisierung nach der Schwere der Verstöße und der Reichweite der Webseiten geleistet werden.

Obwohl hinsichtlich der Durchsetzung der Rechtslage noch große aufsichtsrechtliche Anstrengungen bevorstehen, waren aber bereits deutliche Verbesserungen wahrnehmbar. Viele Webseitenbetreiber bemühten sich bereits, ihre Angebote der Rechtslage anzupassen. Zum Beispiel waren im Lauf des Jahres 2021 immer mehr Einwilligungsbanner auf Webseiten zu finden, die neben der Möglichkeit zum „Akzeptieren“ von Cookies und Werbetracking auch eine leicht auffindbare und leicht bedienbare Möglichkeit zum „Ablehnen“ bereithalten. Dennoch ist davon auszugehen, dass zum Ende des Jahres 2021 der überwiegende Teil aller Webseiten in Rheinland-Pfalz noch nicht datenschutzkonform betrieben wird.

7.2 Zuständigkeit für Webmail-Dienste

Zum 1.12.2021wurde das Telekommunikationsgesetz aktualisiert. Ab diesem Zeitpunkt gelten Webmail-Dienste (wieder) als Telekommunikationsdienste. Telekommunikationsdienste unterliegen der datenschutzrechtlichen Aufsicht durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die seit 2019 beim LfDI Rheinland-Pfalz liegende datenschutzrechtliche Aufsicht über die E-Mail-Marken Web.de und GMX, die von der 1&1 Mail Media GmbH angeboten werden, liegt daher seit dem 1.12.2021 in der Zuständigkeit des BfDI.

Zuvor waren Webmail-Dienste seit einem entsprechenden Urteil des Europäischen Gerichtshofs vom 13.6.2019 (GMail) nicht als Telekommunikationsdienste eingeordnet worden und fielen damit nicht in die Sonderzuständigkeit des BfDI für Telekommunikationsdienste. Die Webmail-Dienste der 1&1 Mail & Media GmbH waren seitdem aufgrund des Hauptsitzes des Mutterkonzerns „United Internet“ in Montabaur für eine Zeitraum von knapp zweieinhalb Jahren in die örtliche Zuständigkeit des LfDI gefallen.

7.3 Unerwünschte Werbezusendungen

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

Im Gegensatz zu Werbezusendungen per Briefpost, die ohne vorherige Einwilligung im Rahmen einer Abwägung grundsätzlich nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO erlaubt sind, richtet sich die Zulässigkeit der Werbung per E-Mail danach, ob die betroffenen Person Bestandskund:in ist oder nicht. Werbe-E-Mails an Bestandskund:innen sind aus datenschutzrechtlicher Sicht in der Regel zulässig, wenn die betroffene Person der Zusendung von Werbung nicht nach Art. 21 DS-GVO widersprochen hat. Die werbliche Ansprache per E-Mail in allen anderen Fällen ist lediglich mit einer expliziten Einwilligung durch die betroffene Person möglich. Jede Verarbeitung von personenbezogenen Daten muss sich nämlich auf mindestens eine der im Art. 6 Abs. 1 DS-GVO genannten Voraussetzung stützen. Für den Versand von Werbe-E-Mails bzw. Newslettern kommt lediglich die Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO als Rechtsgrundlage in Frage.

In den meisten Fällen können die Betroffenen selbst gegen unerwünschte Werbe-E-Mails und Newsletter vorgehen und ihre ggf. erteilte Einwilligung widerrufen. Bei zulässiger Bestandskund:innenwerbung haben betroffene Personen nach Art. 21 Abs. 2 DS-GVO das Recht, Werbung per E-Mail gegenüber dem werbenden Unternehmen mit Wirkung für die Zukunft zu widersprechen. Oftmals lässt sich dieser Widerruf mit Anklicken des Abmeldelinks in der entsprechenden E-Mail tätigen. Sollte ein solcher nicht vorhanden sein, kann der Widerspruch an den Absender der E-Mail oder an das werbende Unternehmen per E-Mail gesendet werden. Sollte der Werbe-Widerspruch keinen Erfolg haben, können die Betroffenen gegen Unternehmen mit Sitz in Rheinland-Pfalz beim LfDI eine Beschwerde einlegen.

Viele Beschwerdeführer:innen wenden sich daher an den LfDI und rügen die Zusendung von Werbe-E-Mails bzw. Newslettern durch Unternehmen, die sie nicht kennen und denen sie wissentlich keine Einwilligung erteilt haben. In diesen Fällen obliegt es dem Verantwortlichen die Einwilligung zum Newsletter-Versand an die betroffenen Personen zu beweisen. Dafür muss der Verantwortliche u.a. die Dokumentation zur Eingabe der E-Mail-Adresse durch die betrof-

fene Person vorlegen sowie die Dokumentation der Verifizierungs-Mail und deren Versand an die angegebene E-Mail-Adresse und die Dokumentation des Klicks auf den in der Verifizierungs-Mail enthaltenen Bestätigungslink. Kann der Verantwortliche die Einwilligung nicht vorlegen, geht der LfDI davon aus, dass keine Rechtsgrundlage für die Zusendung der Werbe-E-Mails vorgelegen hat.

Der LfDI hat im Jahr 2021 nicht nur Verwarnungen gegenüber Verantwortlichen aufgrund fehlender Rechtsgrundlagen beim Versenden von Werbe-E-Mails ausgesprochen, sondern musste auch in einigen Fällen die Vorlage der Beweise für die Einwilligung anordnen. In einem Verfahren war der LfDI gezwungen, ein Bußgeldverfahren gegen ein werbendes Unternehmen zu eröffnen, da dieser Verantwortliche auch nach Widerruf der Einwilligung und nach erhaltener Verwarnung weiterhin Werbe-E-Mails an die selbe betroffene Person verschickt hat.

8. GESUNDHEIT

8.1 Meldepflicht nach Art. 33 DS-GVO bei Verletzung von Gesundheitsdaten

Der Umfang der Meldepflicht nach Art. 33 Abs. 1 DS-GVO war im Berichtszeitraum Gegenstand von Abstimmungen mit einem rheinland-pfälzischen Unternehmen. Konkret ging es um die Frage, ob im Falle von Postfehlversänden ein meldepflichtiges Risiko im Sinne von Art. 33 Abs. 1 DS-GVO in der Regel anzunehmen ist, wenn Gesundheitsdaten betroffen sind. Das Unternehmen stellte die regelmäßige Meldepflicht insbesondere dann in Frage, wenn Empfänger der irrtümlich übersandten Gesundheitsdaten Berufsgeheimnisträger sind.

Im Ergebnis geht der LfDI bei der unzulässigen Verarbeitung von Gesundheitsdaten regelmäßig von dem Vorliegen eines daraus resultierenden Risikos für die Rechte und Freiheiten der betroffenen Personen und damit dem Bestehen einer Meldepflicht nach Art. 33 Abs. 1 DS-GVO aus. Dies gilt in besonderem Maße dann, wenn die Gesundheitsdaten durch professionelle Datenverarbeiter wie z.B. Ärzte oder Krankenversicherungen, die selbst einer berufs- oder strafrechtlichen Geheimhaltungspflicht unterliegen, unrechtmäßig verarbeitet werden. Denn Gesundheitsdaten unterliegen als besondere Kategorein personenbezogener Daten im Sinne von Art. 9 Abs. 1 DS-GVO per se einem erhöhten Schutzbedarf. Werden sie unrechtmäßig verarbeitet, müssen die betroffenen Personen im Regelfall gravierende Nachteile wie z.B. den Verlust der Vertraulichkeit von Informationen über den eigenen Gesundheitszustand aushalten. Dies wiegt umso schwerer, je eher die Betroffenen aufgrund der berufs- oder strafrechtlichen Geheimhaltungspflichten von einem hohen Schutzniveau bei der verantwortlichen Stelle ausgehen durften. Der Eintritt eines aus der Datenschutzverletzung folgenden nicht unerheblichen Schadens für die Persönlichkeit der Betroffenen ist deshalb naheliegend. Daran ändert sich auch nichts, wenn die Datenschutzverletzung auf einem unbeabsichtigten Postfehlversand beruht und der Empfänger als Berufsgeheimnisträger wiederum einer beruflichen Schweigepflicht unterliegt. Denn bereits mit dem Postfehlversand ist der Vertraulichkeitsverlust eingetreten, gleichgültig, ob der unbefugte Empfänger die Daten noch an Dritte weitergeben würde oder nicht. Lediglich wenn im Einzelfall konkrete Anhaltspunkte für den vollständigen Ausschluss des mit der unrechtmäßigen Datenverarbeitung normalerweise einhergehenden Vertraulichkeitsverlusts berufsrechtlich geschützter Gesundheitsdaten vorliegen, kann die Meldepflicht ausnahmsweise entfallen. Dies wäre z.B. der Fall, wenn Gesundheitsdaten irrtümlich an einen unbefugten Empfänger versendet wurden, dieser die Daten zwar erhalten, aber noch nicht – z.B. aufgrund einer bestehenden Verschlüsselung - zur Kenntnis genommen hat.

Zudem ist in diesem Zusammenhang ein weiterer wichtiger Zweck der Meldepflicht nach Art. 33 DS-GVO zu berücksichtigen. Neben der Aufklärung des Einzelfalls dient die Verpflichtung zur Meldung von Datenschutzverletzungen auch der externen Datenschutzkontrolle von Verantwortlichen, die in einem hohen Maße mit besonders schutzbedürftigen personenbezogenen Daten umgehen. Die Datenschutzaufsicht erhält über die Zahl eingehender Meldungen einen validen Überblick über das bestehende Schutzniveau und einen ggf. bei der Datensicherheit vorhandenen Optimierungsbedarf bei diesen Stellen, unabhängig von den Umständen des Einzelfalls oder möglicherweise bei ihr eingehenden Beschwerden der Betroffenen.

Schließlich besteht auch aufgrund der am 14. Dezember 2021 beschlossenen Guidelines

01/2021 on Examples regarding Personal Data Breach Notification des EDSA kein Anlass, von dieser Rechtsauffassung abzuweichen. Vielmehr stellen die Leitlinien auch weiterhin den durch Datenschutzverletzungen möglichen Verlust von Vertraulichkeit bei Berufsgeheimnissen als einen wichtigen Grund für die datenschutzrechtlichen Melde- und Unterrichtungspflichten heraus. So führt hiernach bereits der Diebstahl von analog gespeicherten Gesundheitsdaten, die im Zusammenhang mit einer Heilbehandlung stehen, zu einem hohen Risiko im Sinne von Art. 34 DS-GVO. Eine Rolle spielen dabei neben den potentiellen Risiken für die betroffene Person auch der Umstand, dass ein medizinisch relevantes Geheimnis gebrochen wurde. Im Ergebnis betonen somit die überarbeiteten Leitlinien auch weiterhin die besondere Sensibilität von Gesundheitsdaten und die hohe Bedeutung von beruflichen Schweigepflichten, die im medizinischen Kontext stehen, für die Beurteilung der Meldepflicht nach Art. 33 DS-GVO.

8.2 Untersuchungsbefugnisse der Datenschutzaufsicht bei Berufsgeheimnisträgern wie z.B. Ärzten

Die Reichweite der Untersuchungsbefugnisse der Datenschutz-Aufsichtsbehörden bei Ärzten oder sonstigen Berufsgeheimnisträgern steht immer wieder im Fokus an den LfDI herangetragener Diskussionen. Hintergrund dafür ist die Regelung des Art. 90 Abs. 1 DS-GVO. Danach können die Mitgliedstaaten die Befugnisse der Aufsichtsbehörden im Sinne des Art. 58 Abs. 1 lit. e und lit. f DS-GVO gegenüber den Verantwortlichen oder den Auftragsverarbeitern, die einem Berufsgeheimnis unterliegen, regeln, sofern dies notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Geheimhaltungspflicht in Einklang zu bringen. Mit anderen Worten: Die den Aufsichtsbehörden durch die Verordnung eingeräumten Rechte auf Zugang zu allen personenbezogenen Daten und Informationen, die für ihre Aufgabenerfüllung erforderlich sind, sowie auf Zugang zu den Geschäftsräumen und Datenverarbeitungsanlagen von Verantwortlichen können bei Bedarf durch nationale Regelungen so ausgestaltet werden, dass sie die berechtigten Anliegen derjenigen, die durch die Berufsgeheimnisse geschützt werden, nicht aushebeln. Konkret geht es also z.B. um den Schutz der Patienten einer Arztpraxis, deren von der ärztlichen Schweigepflicht umfassten Behandlungsdaten von der Praxis gespeichert werden. Nach der Vorstellung des Verordnungsgebers soll zumindest gesetzgeberisch verhindert werden können, dass durch Prüfungen z.B. im Rahmen von datenschutzrechtlichen Beschwerden über Ärzte die Daten nicht der Beschwerdeführer, sondern aller dort behandelter Patienten der Aufsichtsbehörde aufgrund der ihr zustehenden Untersuchungsbefugnisse ohne weitere Abwägungen offenbart werden müssen.

In Deutschland wurde von der Öffnungsklausel in § 29 Abs. 3 BDSG Gebrauch gemacht. Danach bestehen gegenüber den in § 203 Abs. 1, 2a und 3 StGB genannten Personen und deren Auftragsverarbeitern die Untersuchungsbefugnisse der Aufsichtsbehörden nach Art. 58 Abs. 1 lit. e und lit. f DS-GVO nicht, soweit deren Inanspruchnahme zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. Zugleich verlängert sich der Geheimnisschutz auch auf die Aufsichtsbehörden, falls sie gleichwohl im Rahmen ihrer Tätigkeit hiervon erfasste Informationen zur Kenntnis bekommen.

Durch die Regelung ist es den Aufsichtsbehörden erschwert, von den Berufsgeheimnisträgern unmittelbaren Zugang zu personenbezogenen Daten bzw. ihren Geschäftsräumen und ihrer IT zu verlangen. Sofern es beispielsweise durch einen Besuch in der Arztpraxis zu einer

Verletzung der ärztlichen Schweigepflicht kommen würde, weil die Aufsichtsbehörde im Falle einer Prüfung vor Ort die Daten aller dort anwesenden Patienten zur Kenntnis nehmen könnte, ohne dass hierzu eine Offenbarungsbefugnis bestand, könnte die Arztpraxis den Zutritt während der Öffnungszeiten verweigern. Dies wäre aus der Perspektive der Aufsichtsbehörde sachgerecht und würde ihren Kontrollauftrag mit den berechtigten Anliegen der von der Geheimhaltungspflicht geschützten Personen in Einklang bringen.

Umstritten ist allerdings, ob den Aufsichtsbehörden mit der Regelung des § 29 Abs. 3 BDSG sämtliche Zugangsmöglichkeiten im Rahmen ihrer Tätigkeit per se entzogen sind. Darüber hinaus steht die Frage im Raum, ob den Aufsichtsbehörden auch noch die Befugnis nach Art. 58 Abs. 1 lit. a DS-GVO genommen oder deutlich beschränkt werden soll, von den Verantwortlichen die Bereitstellung personenbezogenen Informationen, die für ihre Aufsichtstätigkeit erforderlich sind, anzuweisen.

Beides ist im Ergebnis zu verneinen. Der LfDI vertritt in diesem Zusammenhang folgende Rechtsauffassung:

1. Die Aufsichtsbehörden haben bei der Ausübung ihrer Untersuchungsbefugnisse nach Art. 58 Abs. 1 lit. e und lit. f DS-GVO bei Berufsgeheimnisträgern u.ä. gemäß Art. 90 Abs. 1 DS-GVO den Verhältnismäßigkeitsgrundsatz zu beachten. Dies bedeutet, dass sie im Falle eines von ihnen beabsichtigten Zugangs zu personenbezogenen Daten oder Geschäftsräumen bzw. IT der Berufsgeheimnisträger im Einzelfall zwischen dem Recht auf Schutz personenbezogener Daten und der Geheimhaltungspflicht der Verantwortlichen abwägen und diese angemessen in Einklang bringen müssen. Insbesondere ist zu berücksichtigen, welche Auswirkungen mit einem eingeschränkten oder gänzlich unterbliebenen Tätigwerden der Aufsichtsbehörde im Vergleich zu einer Offenlegung geheimhaltungsbedürftiger personenbezogener Daten durch die Verantwortlichen verbunden wären. Maßstab sind dabei u.a. die jeweils mit einem möglichen Datenschutzverstoß bzw. einer Kenntnisnahme der geheimhaltungsbedürftigen Inhalte durch die Aufsichtsbehörde verbundenen Risiken für die Rechte und Freiheiten der betroffenen Personen, die Zahl der hiervon betroffenen Personen, die Art der personenbezogenen Daten sowie die ggf. zur Verfügung stehenden technisch-organisatorischen Maßnahmen, die zu einem angemessenen Ausgleich zwischen der Kontrollaufgabe und dem Geheimnisschutz beitragen können. Nur beim Überwiegen der Geheimhaltungsinteressen der Berufsgeheimnisträger haben die Aufsichtsbehörden von der Ausübung ihrer Befugnisse abzusehen. § 29 Abs. 3 Satz 1 BDSG hat angesichts des ohnehin geltenden und von den Aufsichtsbehörden immer zu beachtenden Verhältnismäßigkeitsgrundsatzes somit lediglich deklaratorischen Charakter.

2. § 29 Abs. 3 Satz 2 BDSG lässt eine Kenntnisnahme geheimhaltungsbedürftiger personenbezogener Daten durch die Aufsichtsbehörde im Rahmen einer Unter¬suchung ausdrücklich zu. Damit geht der Gesetzgeber selbst davon aus, dass trotz der in § 29 Abs. 3 Satz 1 BDSG geregelten Einschränkung der Untersuchungs¬befugnisse die Aufsichtsbehörden unter dem Vorbehalt der in Art. 90 Abs. 1 Satz 1 DS-GVO ausdrücklich genannten Bedingungen der Notwendigkeit und Verhältnismäßigkeit auch bei Berufsgeheimnisträgern personenbezogene Daten, die einem besonderen Geheimnisschutz unterliegen, im Rahmen ihrer Aufgabenerfüllung verarbeiten dürfen. § 29 Abs. 3 Satz 1 BDSG ist damit europarechtskonform auslegbar.

3. Unabhängig von den mit § 29 Abs. 3 BDSG verbundenen Beschränkungen sind

die Aufsichtsbehörden jederzeit befugt, im Rahmen ihrer Untersuchungsbefugnis nach Art. 58 Abs. 1 lit. a DS-GVO Berufsgeheimnisträger zur Bereitstellung von personenbezogenen Daten anzuweisen, die für ihre Aufgabenerfüllung erforderlich sind. Die Auffassung, dass den Aufsichtsbehörden ein derartiges Tätigwerden gegenüber Berufsgeheimnisträgern aufgrund der Regelung des § 29 Abs. 3 BDSG grundsätzlich versagt sein soll, ist unzutreffend.

9. SOZIALES

9.1 Kein Einsatz von Vordrucken zur Bankauskunftsermächtigung mehr!

In rheinland-pfälzischen Sozialverwaltungen werden immer noch Vordrucke zur sog. Bankauskunftsermächtigung eingesetzt, die bereits seit Jahren regelmäßig Gegenstand datenschutzrechtlicher Beschwerden sind. Ziel der Vordrucke ist es, dass die Antragsteller die von ihnen benannten Geldinstitute zur Auskunftserteilung gegenüber dem Sozialhilfeträger ermächtigen. Teilweise werden die Antragsteller von den Sozialverwaltungen unter Hinweis auf die Mitwirkungspflichten nach § 60 SGB I, teilweise rein freiwillig zur Abgabe derartiger Erklärungen aufgefordert.

Angesichts der in § 117 Abs. 3 SGB XII enthaltenen Ermittlungsmöglichkeiten der Sozialhilfeträger bestehen grundlegende Bedenken gegen den Einsatz der Vordrucke zur Bankauskunftsermächtigung. Nach § 117 Abs. 3 SGB XII sind u.a. diejenigen, die für einen Antragsteller von Sozialhilfe Guthaben führen, verpflichtet, dem Sozialhilfeträger auf Verlangen hierüber sowie über damit in Zusammenhang stehendes Einkommen und Vermögen Auskunft zu erteilen, soweit es zur Durchführung von Leistungen nach dem SGB XII im Einzelfall erforderlich ist. Vor diesem Hintergrund ist kein Raum für den Einsatz dieser Vordrucke. Dies gilt auch dann, wenn eine solche Erklärung lediglich auf freiwilliger Basis erbeten wird. Denn mit dem Vordruck wird den Betroffenen suggeriert, dass sie selbst die Ermittlungsmöglichkeiten des Sozialhilfeträgers beeinflussen könnten. Dies ist aber rechtlich nicht der Fall. Allerdings sollten die Sozialhilfeträger die Antragsteller frühzeitig über ihre Befugnisse nach § 117 Abs. 3 SGB XII informieren.

Die von einzelnen Beschwerdeverfahren betroffenen Sozialverwaltungen haben sich mittlerweile alle unter Anerkennung der vom LfDI vertretenen Rechtsauffassung bereit erklärt, auf den Einsatz der Vordrucke zur Bankauskunftsermächtigung zu verzichten. Der LfDI legt dies auch den übrigen Sozialhilfeträgern im Lande nahe.

9.2 Öffentliche Zustellung von Bescheiden

Im Rahmen einer an den LfDI RP gerichteten Beschwerde wurde die präzise Behördenbezeichnung bei der öffentlichen Zustellung eines Sozialleistungsbescheides thematisiert. Dabei hatte die Kreisverwaltung einen Bescheid des kommunalen Jobcenters öffentlich zugestellt. In der öffentlichen Bekanntmachung, die im konkreten Fall in der lokalen Zeitung erfolgte, war neben der Adressangabe auch das Jobcenter ausdrücklich als die Stelle benannt worden, bei der das Dokument eingesehen werden konnte. Hiergegen hatte sich die betroffene Person gewandt, da damit ihr Bezug von Sozialleistungen öffentlich bekannt gegeben worden sei.

Rechtsgrundlage für die öffentliche Zustellung von Bescheiden ist § 10 VwZG in Verbindung mit den hierzu erlassenen landesrechtlichen Regelungen. Hiernach kann die öffentliche Zustellung durch Bekanntmachung einer Benachrichtigung an der Stelle, die von der Behörde hierfür allgemein bestimmt ist, erfolgen. Dies kann z.B. die lokale Presse sein. Die Benachrichtigung muss gesetzlich benannten Angaben enthalten. Hierzu gehören neben der Behördenbezeichnung u.a. auch die Angabe der Stelle, bei der das zuzustellende Dokument eingesehen werden kann. Diesbezüglich ist es aus Sicht des LfDI zumindest im Bereich der Sozialverwaltung fraglich, ob damit regelmäßig auch die fachlich präzise Bezeichnung dieser Stelle zulässig ist. Denn vor dem Hintergrund der Reichweite des Sozialgeheimnisses

und des Grundsatzes der Datenminimierung ist eine Auslegung der gesetzlichen Zustellungsvorschriften in der Weise geboten, dass mit der Angabe der Stelle, in der das zuzustellende Dokument eingesehen werden kann, Dritten nicht potentiell ein möglicher Sozialleistungsbezug offengelegt wird. Lediglich dann, wenn die Einsichtnahme in das Dokument zwingend die fachliche Bezeichnung der Stelle erfordert, wäre eine derartige Angabe datenschutzrechtlich hinnehmbar

In dem der Beschwerde zugrunde liegenden Sachverhalt war die Angabe des „Jobcenters“ als Stelle, bei der das zuzustellende Dokument eingesehen werden konnte, entbehrlich. Denn mit der Angabe der Kreisverwaltung, des Zusatzes „Außenstelle“ sowie der dazu gehörenden Adressangabe und ggf. des Raums der Einsichtnahme wäre für die betroffene Person ausreichend erkennbar gewesen, wo sie das zuzustellende Dokument einsehen konnte. Damit wäre den gesetzlichen Vorgaben zur öffentlichen Zustellung ausreichend entsprochen gewesen. Die Kreisverwaltung kündigte an, künftig entsprechend zu verfahren.

Der LfDI empfiehlt aufgrund der dargelegten Erwägungen, bei der öffentlichen Zustellung von Bescheiden im Bereich der Sozialverwaltung jeweils im Einzelfall zu prüfen, ob die fachlich präzise Bezeichnung der Stelle, bei der das zuzustellende Dokument eingesehen werden kann, erforderlich ist.

10. KOMMUNALES

10.1 Datenverarbeitung zur Erstellung von Mietspiegeln

Mietspiegel sind von Gewicht für die Ermittlung der ortsüblichen Vergleichsmiete. Ihre Bedeutung hat in der Vergangenheit stetig zugenommen. Sie dienen u.a. als Begrün-dungsmittel für Mieterhöhungsverlangen (siehe Internetangebot des Bundesministeriums für Justiz).

Auch der LfDI hat sich mehrfach mit entsprechenden Beratungsanfragen befasst und im Tätigkeitsbericht über das Ergebnis informiert (DSB 2018, III-13.2, S. 62; DSB 2019, III-11.1, S. 63).

Die Aufstellung eines Mietspiegels ist entsprechend § 558 c Abs. 4 S. 1 BGB eine im öffentlichen Interesse liegende Aufgabe bzw. eine Aufgabe der Daseinsvorsorge, die den Kommunen obliegt. Nach § 22c Sozialgesetzbuch – Zweites Buch sollen die Kreise und kreisfreien Städte zur Bestimmung der angemessenen Aufwendungen für Unterkunft und Heizung insbesondere auch Mietspiegel berücksichtigen.

Dabei stellte sich für den LfDI u.a. die Frage, ob es zulässig ist, wenn Kreisverwaltungen zur Erfüllung dieser Aufgabe insbesondere auf den Adressbestand von Vermieterinnen und Vermietern des Abfallwirtschaftsbetriebes des Landkreises zurückgreifen.

Als Prüfungsergebnis (DSB 2019, III-11.1, S. 63) war festzustellen, dass einem solchen Anliegen § 41 BMG entgegensteht. Stattdessen können die erforderlichen Daten bei den Grundsteuerstellen kreisangehöriger Gemeinden und über eine Gruppenauskunft im Einwohnermelderegister erhoben werden.

Ab 01. Juli 2022 gelten dann das Mietspiegelreformgesetz (MsRG) vom 10.08.2021 und die Mietspiegelverordnung (MsV) vom 28.10.2021. Mit dem MsRG als Artikelgesetz werden zivilrechtliche Regelungen und Vorschriften des Sozialgesetzbuches geändert und spezialgesetzliche Grundlagen für Datenerhebung und -verarbeitung – auch durch Auftragsverarbeiter – geschaffen. Die MsV regelt Methodik, Verfahren, Dokumentation und Veröffentlichung von Mietspiegeln.

10.2 Netzwerktreffen mit den behördlichen Datenschutzbeauftragten

Im Jahr 2021 fanden nach einer einjährigen coronabedingten Pause wieder zwei Netzwerktreffen mit den behördlichen Datenschutzbeauftragen rheinland-pfälzischer Kommunalverwaltungen statt. Jeweils über 80 Teilnehmer:innen standen mit Mitarbeitern des Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) RP in einem konstruktiven Austausch und informierten sich über aktuelle Entwicklungen des Datenschutzrechts. Aufgrund der bestehenden Pandemie wurden beide Veranstaltungen in rein digitaler Form durchgeführt und auf Präsenzveranstaltungen verzichtet.

Beispielhaft wurden folgende Themen kurz angesprochen:

Zum Thema einer sicheren elektronischen Kommunikation wurden die unterschiedlichen Verschlüsselungsarten bei der Übermittlung von E-Mails erläutert und dargelegt, welche Schutzmaßnahmen zwingend zu beachten und zu ergreifen sind. Auch auf die Verarbeitung personenbezogener Daten bei der Übersendung eines Telefaxes wurde eingegangen und die neueste Rechtsprechung erläutert. Gerade hier gab es in der jüngeren Vergangenheit eine zunehmend kritische Betrachtung, was den Schutz der Daten anbelangt. Insbesondere bei

der Verarbeitung von personenbezogenen Daten mit hohem Risiko und bei Berufsgeheimnisträgern, wie z.B. den Sozialarbeiter:innen, sollte deshalb auf sicherere Kommunikationsmittel gesetzt werden.

Ein weiteres, immer wiederkehrendes Thema, behandelte die Veröffentlichung von Alters- und Ehejubiläen sowie die Weitergabe von Meldedaten an Ortsbürgermeister:innen. Die Ermächtigungsgrundlagen hierzu ergeben sich aus dem Bundesmeldegesetz und sind relativ klar gefasst. Gleichwohl kommt es in der praktischen Anwendung immer wieder zu Unsicherheiten, die letztendlich zu datenschutzrechtlichen Verstößen und entsprechenden Beschwerden führen. Darüber hinaus wurde auf Datenpannen bei der Übermittlung von Meldedaten für Wahlwerbung eingegangen (Näheres siehe unter ....1).

Um ähnliche Fehler in Zukunft weitestgehend zu verhindern, wird die Plattform des Netzwerktreffens dafür genutzt, um die Vertreter:innen der Kommunalverwaltungen für die bestehenden Problematiken zu sensibilisieren.

Die vollständigen Schulungsdokumente der Netzwerktreffen vom Mai und Dezember 2021 sind erhältlich auf der Internetseite des LfDI unter

https://s.rlp.de/2QEIu
(Netzwerktreffen vom 6. Mai 2021)

https://s.rlp.de/1In0k
(Netzwerktreffen vom 16. Dezember 2021)

10.3 Verfahrensänderung als Erfolg aufsichtsrechtlicher Prüfung – ausgewählte Fälle

Ausstellung von Sonderparkausweisen

Der Beschwerdeführer, ein Betreiber eines ambulanten Pflegedienstes mit mehreren Angestellten und zahlreichen Fahrzeugen zur Versorgung pflegebedürftiger Menschen in der häuslichen Umgebung, problematisierte die Vergabe von Sonderparkausweisen durch die zuständige Stadtverwaltung.

War es bislang ausreichend, eine Kopie der Zulassungsbescheinigung Teil I (Fahrzeugschein) zu übermitteln, wurde nach einer Verfahrensänderung plötzlich verlangt, bei der Beantragung oder Verlängerung eines Antrages weitreichende personenbezogene Dokumente vorzulegen. Dazu gehörten u.a. die Namen sämtlicher Mitarbeiter:innen des Gewerbebetriebs, welche die betreffenden Fahrzeuge nutzen, inklusive der jeweiligen persönlichen beruflichen Qualifikation unter Vorlage von Examenszeugnissen und Tätigkeitsnachweisen.

In diesem Zusammenhang ist datenschutzrechtlich seitens der zuständigen Straßenverkehrsbehörde der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) sowie der Grundsatz der Erforderlichkeit (§ 3 LDSG) zu beachten. Erforderlichkeit heißt, dass die im Rahmen des Antragsverfahrens verarbeiteten personenbezogenen Daten unabdingbar sein müssen, damit die Stadtverwaltung als Verantwortliche die ihr übertragenen Aufgaben erfüllen kann.

Der LfDI vertrat dabei den Standpunkt, dass das Interesse an der Vertraulichkeit von Name und Qualifikation von Mitarbeiter:innen das Interesse der Straßenverkehrsbehörde an

der Kenntnisnahme dieser Datenkategorien zum Zweck der Prüfung der Voraussetzungen der oben genannten Vorschriften überwiegt und sah sich durch die Vorgehensweise anderer Straßenverkehrsbehörden in seiner Auffassung bestätigt.

Gemeinsam mit dem fachlich zuständigen Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau konnte erreicht werden, dass die Antragsprozesse in der betroffenen Stadtverwaltung umgehend geändert wurden. Qualifikationsnachweise werden zukünftig nicht mehr verlangt und bereits erhobene Nachweise nicht länger vorgehalten.

Protokollierung von Zugangsdaten mittels einer elektronischen Schließanlage

Eine Kommune hatte in mehreren Liegenschaften, darunter ein Rathaus und ein Feuerwehrhaus, eine neue Schließanlage installiert, sodass sich die Türen mittels eines RFID-Chips öffnen lassen und nicht mehr in herkömmlicher Art und Weise durch einen Schlüssel.

Hierbei werden in jedem Fall personenbezogene Daten insoweit verarbeitet, dass festgehalten wird, welcher Zugangschip welcher Person zugeordnet ist und welche Schlösser damit geöffnet werden.

Alleine dieses Szenario begegnet jedoch noch keinen datenschutzrechtlichen Bedenken. Unter Beachtung des Grundsatzes der Datenminimierung (Art 5 Abs. 1 lit. c DS-GVO) sind diese Daten ausreichend, um den eigentlichen Zweck – eine ordnungsgemäße Zutrittskontrolle zu gewährleisten – zu erfüllen. Ein elektronisches Schließsystem verarbeitet in dieser Hinsicht keine zusätzlichen Daten im Vergleich zu einer konventionellen, herkömmlichen Schließanlage.

Allerdings legte der Beschwerdeführer gegenüber dem LfDI dar, dass zusätzlich protokolliert werde, welche Personen zu welchem Zeitpunkt das jeweilige Türschloss geöffnet oder verschlossen haben. Dadurch war individuell nachvollziehbar, wer das jeweilige Gebäude wann betreten oder verlassen hatte.

Auf Nachfragen des LfDI, auf welche Erlaubnisgrundlage die Datenverarbeitung gestützt werde, machte die Verantwortliche in Bezug auf das Feuerwehrgerätehaus insbesondere geltend, man habe entsprechende Einwilligungen der betreffenden Feuerwehrleute eingeholt (Art. 6 Abs. 1 S. 1 lit. a DS-GVO).

Die Einwilligung als Verarbeitungsgrundlage kann in diesem Fall aber nicht herangezogen werden, weil Einwilligungen im Rahmen eines Über- / Unterordnungsverhältnisses i.d.R. keine gültige Rechtsgrundlage liefern (vgl. hierzu Erwägungsgrund 43 zur DS-GVO). Aufgrund des bestehenden Verhältnisses zwischen der Verbandsgemeinde als Träger der Feuerwehr auf der einen Seite und den ehrenamtlichen Feuerwehrleuten bzw. den Beschäftigten auf der anderen, ist ein deutliches Ungleichgewicht im Sinne des Erwägungsgrundes 43 gegeben.

Eine Protokollierung von Schließvorgängen mit entsprechender personenbezogener Zuordnung steht somit nicht im Einklang mit den zu berücksichtigenden datenschutzrecht-lichen Vorgaben.

Angesichts einer Anhörung vor Erlass der Anweisung einer Maßnahme nach Art. 58 Abs. 2 lit. d DS-GVO durch den LfDI lenkte die Verantwortliche ein und teilte letztendlich mit, dass die bislang rechtswidrig durchgeführte Protokollierungspraxis geändert werde und keine Protokollierung mehr stattfinde. Eine bestehende Dienstanweisung, welche Regelungen zur Protokollierung enthielt, wurde in diesem Zusammenhang entsprechend geändert.

Bereitstellung eines kommunalen „Online-Archives“

Im Rahmen einer Beschwerde wurde offenkundig, dass eine Verbandsgemeinde ein „Online-Archiv“ dergestalt pflegt, dass über die Homepage der Kommune zum Teil mehrere jahrzehntealte Rats- und Ausschussprotokolle aufrufbar bereitgehalten werden, die mitunter personenbezogene Daten von Bürger:innen enthalten. Die jahrelange Veröffentlichung erfolgt laut Aussage der Verantwortlichen zur Förderung der Transparenz im kommunalen Verwaltungshandeln.

Auch wenn die Begründung aus diesem Blickwinkel sinnvoll erscheinen mag, so dürfen gleichwohl datenschutzrechtliche Belange nicht außer Acht gelassen werden, zumal es keine einschlägige Rechtsgrundlage zur Veröffentlichung von Niederschriften kommunaler Gremien im Internet gibt, die auch personenbezogene Daten enthalten.

Die Regelungen zur Niederschrift ergeben sich unmittelbar aus § 41 GemO. Danach ist über jede Sitzung des Gemeinderats eine Niederschrift anzufertigen. Über deren Ergebnisse soll die Gemeindeverwaltung die Einwohner nach § 41 Abs. 5 GemO in geeigneter Form unterrichten. Zur Erfüllung dieser Aufgabe durch die Kommune ist es jedenfalls nicht erforderlich, personenbezogene Daten zu verarbeiten. Eine Fassung der Niederschrift, mit der die Pflicht zur Veröffentlichung aus § 41 Abs. 5 GemO erfüllt werden soll, muss daher grundsätzlich so formuliert sein, dass keine personenbezogenen Daten aufgeführt werden.

Hierzu hat sich der LfDI bereits mehrfach, u.a. unter https://s.rlp.de/6tvzd, positioniert.

Denn im Gegensatz zu der Möglichkeit für die Bürger:innen, die Niederschrift über eine öffentliche Sitzung in den Räumlichkeiten der Gemeindeverwaltung einsehen zu können (§ 41 Abs. 4 GemO), stellt die Veröffentlichung im Internet eine größere, weltweite Verbreitung und dauerhaft einfachere Zugänglichkeit bzw. Wiederauffindbarkeit dar. Für die Rechte und Freiheiten betroffener Personen besteht somit ein höheres Gefährdungspotential. Die Speicherung dieser Daten im privaten Bereich ist nicht beherrschbar.

U.a. deswegen sieht § 14 Abs. 2 Satz 5 des Landesgesetzes zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz (eGovGRP) vor, dass die in einer über öffentlich zugängliche Netze verbreiteten elektronischen Fassung einer Veröffentlichung – rechtmäßig enthaltenen - personenbezogene Daten unkenntlich zu machen sind, wenn der Zweck ihrer Veröffentlichung erledigt ist und eine fortdauernde Veröffentlichung das Recht der betroffenen Person auf informationelle Selbstbestimmung unangemessen beeinträchtigen würde.

In der Abwägung zwischen dem Informationsinteresse der Allgemeinheit und dem Datenschutzinteresse des Einzelnen überwiegt dann erst recht der Datenschutz, wenn in Niederschriften enthaltene personenbezogene Daten ohne Rechtsgrundlage veröffentlicht wurden.

Nach Intervention durch den LfDI wurde gemeinsam mit der betroffenen Verbandsgemeinde eine datenschutzfreundliche Vorgehensweise vereinbart, die sowohl den Belangen des Datenschutzes als auch einem berechtigten Transparenzinteresse Rechnung trägt.

11. BILDUNG

11.1 Überarbeitung Handbuch „Schule.Medien.Recht“

Der LfDI beteiligte sich intensiv an der Überarbeitung des umfangreichen datenschutz- und medienrechtlichen Handbuchs für Schulen mit dem Titel „Schule.Medien.Recht“, welches vom Ministerium für Bildung herausgegeben wird. Diese Sammlung wurde erstmals 2009 in Zusammenarbeit mit dem Pädagogischen Landesinstitut für alle Schulen im Land erstellt, sowohl als Loseblatt-Ordner, als auch digital abrufbar. Den datenschutzrechtlichen Part des Handbuchs steuerte der LfDI bei.

Die konzeptionellen Arbeiten im Jahr 2021 sahen vor, das Handbuch auf ein rein digitales Angebot umzustellen. Inhaltlich waren umfangreiche Aktualisierungen und Ergänzungen vonnöten. So lag der letzte Überarbeitungsstand des Handbuchs noch vor Inkrafttreten der DS-GVO. Neue Bereiche, wie das für Schulen immer wichtiger werdende Thema „Recht am eigenen Bild“, wurden aufgenommen.

Im Zuge der Überarbeitung wirkte der LfDI ebenfalls bei der Erstellung von Mustertexten und Vorlagen für die Schulen mit, um eine landesweit einheitliche Handhabung sicherzustellen. Das Handbuch ist unter folgender Adresse zu finden: https://schulemedienrecht.rlp.de

11.2 Kopie von Impfpässen oder ärztlichen Attesten

Auch im Jahr 2021 erreichten des LfDI zahlreiche Anfragen nach der Zulässigkeit des Fertigens von Kopien des Impfpasses oder von ärztlichen Attesten im Zusammenhang mit der Befreiung von der Maskenpflicht. Unabhängig davon, ob es sich um Impfnachweise gegen Masern oder Corona handelt und ob die Nachweise bei der Kita oder der Schule vorzulegen sind, gilt die Regel, dass Kopien grundsätzlich nur mit Einwilligung des Betroffenen gemacht werden dürfen. Zulässig ist aber die Dokumentation der Tatsache, dass ein Nachweis vorgelegt wurde, Name der Arztes bzw. der Ärztin sowie ein etwaiger Gültigkeitszeitraum der Bescheinigung.

Sofern in Beschwerden die Bekanntgabe von medizinischen Daten gegenüber der Schule problematisiert wurde, sah der LfDI keine Möglichkeit, gegenüber Schulen tätig zu werden. Denn im weiteren Verlauf der Pandemie wurde die Corona-Bekämpfungsverordnung um eine entsprechende Formulierung ergänzt , wonach die Unmöglichkeit oder Unzumutbarkeit der Einhaltung der Maskenpflicht durch eine ärztliche Bescheinigung glaubhaft zu machen ist, aus der sich mindestens nachvollziehbar ergeben muss, auf welcher Grundlage die ärztliche Diagnose gestellt wurde und aus welchen Gründen das Tragen einer Maske im konkreten Fall eine unzumutbare Belastung darstellt. Die Zulässigkeit der Anforderung diesbezüglicher Nachweise hatten gerichtliche Entscheidungen zuvor bestätigt.

11.3 Schülerworkshop-Programm

Die Datenschutz-Schülerworkshops, die in 2020 aufgrund pandemiebedingter Schulschließungen nur in eingeschränktem Umfang stattfinden konnte, wurden in 2021 wieder stärker von den Schulen nachgefragt. Insgesamt konnten 331 Veranstaltungen durchgeführt werden, wovon rund 20 als Online-Workshops umgesetzt wurden. Inhaltlich stellten auch die beiden Wahlen – Landtagswahl im März und Bundestagswahl im September für die Referentinnen und Referenten vielfältige Anknüpfungspunkte an die Themen Manipula-

tion durch Daten und Fake News. Durch eine Kooperation mit dem Fußball Bundesligisten Mainz 05 werden die Workshops seit Beginn des Schuljahrs 2021/22 auch in dessen Schulprojekte „05er Klassenzimmer“ unter dem Modul „Digitale Selbstverteidigung“ eingebunden. Zusätzliche Mittel zur Durchführung des Programms in größerem Umfang wurden weiterhin durch das Ministerium für Frauen, Familie, Kultur und Integration bereitgestellt.

11.4 Webinare und Online-Veranstaltungen für Lehrkräfte

Einem gestiegenen Nachfrageaufkommen seitens Schulen und Lehrkräften begegnete der LfDI in 2021 mit mehreren Online-Fortbildungen und Info-Webinaren. Eine Veranstaltung mit dem Titel „Datenschutz meets Schule“ am Zentrum für Lehrerbildung der Johannes Gutenberg-Universität Mainz vermittelte angehenden Lehrkräften die Grundlagen der datenschutzrelevanten Vorgänge an Schulen. In einer weiteren Online-Fortbildung gezielt für schulische Datenschutzbeauftragte wurden den Teilnehmer: innen zum Schuljahresbeginn vertiefende Kenntnisse und Qualifikationen für ihre Arbeit und zur Einhaltung der datenschutzrechtlichen Vorgaben für Schulen vermittelt. Gemeinsam mit dem BM widmete sich Prof. Dr. Dieter Kugelmann in einem Info-Webinar den speziellen Belangen der berufsbildenden Schulen (BBS) hinsichtlich deren Anforderungen an cloudbasierte außereuropäische Softwareanwendungen. Insbesondere Fragestellungen rum um Microsoft 365 in der schulischen und betrieblichen Ausbildung standen hier im Fokus. Der LfDI erläuterte mit dem Teilnehmer:innen der BBSen die mögliches Einsatzszenarien und empfahl angesichts der derzeitigen Rechtslage und der diesbezüglichen EuGH-Rechtsprechung („Schrems II“) erneut die Nutzung landeseigner Softwareprodukte, wie z.B. BigBlueButton als Videokonferenzsystem und den Schulcampus als digitale Kommunikations- und Austauschplattform.

12. MELDEWESEN | WAHLEN

Zahlreiche Beschwerden über politische Parteien erreichten den Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) im Vorfeld der Bundestagswahl 2021 aus verschiedenen Landesteilen von Rheinland-Pfalz. Etliche Erziehungsberechtigte von Minderjährigen beklagten sich darüber, dass ihre noch nicht wahlberechtigten Kinder persönlich adressierte Wahlwerbung erhalten hatten.

Doch das Versehen lag nicht bei den Parteien, sondern bei den Auskunft gebenden Einwohnermeldeämtern. Diese hatten fehlerhafte Abfragen im Meldesystem durchgeführt und Datensätze unter Anwendung von nicht ausreichend konkreten Parametern erstellt, wodurch auch Daten von nicht wahlberechtigten Personenkreisen übermittelt wurden.

Grundsätzlich sieht das im Bundesmeldegesetz verankerte Meldewesen ein Auskunftsprivileg für Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen vor, wenn die begehrte Auskunft im Zusammenhang mit Wahlen und Abstimmungen steht. Ab sechs Monaten vor der Wahl dürfen die Parteien gewisse personenbezogene Daten aus dem Melderegister erhalten. Voraussetzung dafür ist, dass es sich um eine vorher festgelegte Altersgruppe handelt. Dies ergibt sich aus § 50 Bundesmeldegesetz - Melderegisterauskünfte in besonderen Fällen. Dadurch können die Parteien gezielt z.B. die Gruppe der Erstwähler:innen oder der Senior:innen ansprechen. Die Parteien dürfen die Meldedaten aber nur für diesen Zweck verwenden und müssen die Daten spätestens einen Monat nach der Wahl vernichten.

Da den anfragenden Gruppierungen zwar Name und Anschrift mitgeteilt wird, nicht aber das Geburtsdatum oder das Alter der Adressaten, hatten die Parteien in den aktuellen Fällen keine Kenntnis darüber, wie alt die Empfänger:innen der Wahlwerbung tatsächlich waren. Vielmehr mussten sie davon ausgehen, dass die erhaltenen Meldesätze ausschließlich die Daten von Erstwähler:innen enthielten und alle anderen Personen ausgeschlossen waren – was aber nicht der Fall war. Und so kam es, dass teilweise Kleinkinder an sie gerichtete Wahlwerbung erhielten.

Der LfDI sprach in allen Fällen eine förmliche Beanstandung aus und nahm die aktuellen Vorfälle zum Anlass, erneut für das Thema zu sensibilisieren, damit ähnliche Vorkommnisse bei zukünftigen Wahlen weitestgehend vermieden werden.

13. VERWALTUNG DIGITAL

13.1 Sammlung und Erschließung sog. Amtsdruckschriften als Aufgabe des Landesbibliothekszentrums

Bei diesem Thema ging es um die Frage, inwiefern die Sammlung und Erschließung sog. Amtsdruckschriften (§ 4 LBibG) als Aufgabe des LBZ zu verstehen ist und inwieweit dafür die Verarbeitung personenbezogener Daten bzw. deren Veröffentlichung im Internet bzw. in öffentlichen Netzen erforderlich und damit zulässig ist.

Amtsdruckschriften (oder Amtsdrucksachen, amtliche Veröffentlichungen, amtliche Publikationen) sind Dokumente, die von einem öffentlich-rechtlichen Herausgeber veranlasst oder verlegt werden oder in dessen Auftrag erscheinen. Zu diesen Herausgebern zählen auch die Kommunen. Amtsdruckschriften können ausschließlich amtlichen Inhalts sein, aber auch nicht-amtlichen Inhalt besitzen, z.B. Kultur-, Vereinsinformationen o.ä.

Die ursprüngliche Fassung der datenschutzrechtlich problematischen Vorschrift in einem Entwurf für eine Verordnung zur Durchführung des LBibG lautete:

„Die ablieferungspflichtigen Stellen haben ihre amtlichen Veröffentlichungen in unkörperlicher Form unmittelbar nach der Veröffentlichung dem LBZ zu übermitteln. Die amtlichen Veröffentlichungen werden durch das LBZ gespeichert, erschlossen und dauerhaft der Öffentlichkeit online zur Verfügung gestellt. Ebenso wird dem LBZ das Recht zur Zugänglich-machung in öffentlichen Datennetzen eingeräumt, sofern die Herausgeber dies unaufgefordert aus rechtlichen Gründen nicht ausdrücklich einschränken oder untersagen."

In der Ressortabstimmung wurde vom LfDI angemerkt, dass im amtlichen Teil von Amtsdruckschriften personenbezogene Daten enthalten sein können, deren Veröffentlichung aufgrund von Löschverpflichtungen zeitlich begrenzt ist.

So enthält das Wahlrecht Regelungen, die einen konkreten Zeitpunkt für die Löschung von Internetveröffentlichungen vorgeben. Beispielsweise erlaubt § 88 Abs. 1 S. 2 Landeswahlordnung, dass öffentliche Bekanntmachungen zusätzlich im Internet erfolgen können, aber Bekanntmachungen von Wahlkreisvorschlägen und Landes- und Bezirkslisten einen Monat nach dem Tag der Wahl zu löschen sind.

Zu berücksichtigen sind auch öffentliche Zustellungen gem. § 10 VwZG. So war beispielsweise ein Bußgeldbescheid über 3 Jahre in einer Online-Ausgabe des Amtsblattes einer Kommune verfügbar, obwohl die Begleichung des Bußgeldes längst erfolgt, die Zustellung somit bewirkt und die damit einhergehende namentliche Nennung des Bürgers wegen der ein¬getretenen Zweckerfüllung nicht mehr erforderlich und somit unzulässig waren.

Das LBZ hätte nach Ansicht des LfDI die amtlichen Veröffentlichungen ebenso wie die ablieferungspflichtigen Stellen dementsprechend bereinigen müssen. Demgegenüber hat das LBZ als Ziel formuliert, die auf einem zentralen Server gespeicherten Inhalte solcher Publikationen ohne zeitliche Begrenzung oder räumliche Einschränkung im Sinn einer barrierefreien Zugänglichmachung von staatlichen Informationen zur Verfügung stellen zu wollen.

Begründet hat das LBZ dieses Vorhaben damit, dass mit der Sammlung von Pflichtexemplaren und Amtsdruckschriften das schriftliche kulturelle Erbe von RP gesichert werde. Die Schrif-

ten im Original seien als Teil der kulturellen Überlieferung eine wichtige Grundlage für jede Form historischer Forschung.

Darauf hat der LfDI im weiteren Verfahren ergänzend erwidert, dass der oben wiedergegebene Text des VO-E den in § 8 LBibG im Zusammenhang mit dieser Aufgabenstellung beschriebenen rechtlichen Rahmen zur Verarbeitung personenbezogener Daten – Erschließung und Verzeichnung von Beständen – überschreitet. Denn Erschließung bedeutet die Nutzbarmachung der in Archivgut enthaltenen Informationen durch Ordnung und Verzeichnung, als deren Ergebnis die sog. Findmittel entstehen.

Als abschließenden Standpunkt zu § 8 S. 1 LBibG hat der LfDI vertreten, dass nicht jede einzelne Amtsdruckschrift aus dem Bestand vollständig im Original über öffentliche Netze zur Verfügung gestellt werden darf, sondern der Gesamtbestand an Amtsdruckschriften indirekt über ein (Online-) Findmittel digital im Internet zugänglich gemacht wird.

Die problematisierten Regelungen der oben wiedergegebenen Sätze 2 und 3 sind nicht in den Verordnungstext übernommen worden, der letztendlich in Kraft getreten ist.

13.2 eGovG RP und Umsetzung des OZG - datenschutzrechtliche Begleitung durch den LfDI

Durch das Onlinezugangsgesetz werden die öffentlichen Verwaltungen verpflichtet, ihre Leistungen bis Ende 2022 auch digital über entsprechende Verwaltungsportale anzubieten. Der Gang beispielsweise zum Rathaus, zur Zulassungsstelle oder zur Arbeitsagentur soll entfallen können und im Idealfall vollständig online abgebildet werden. Bis dahin wartet auf die Beteiligten noch viel Arbeit, denn schließlich müssen über 6.000 Verwaltungsleistungen, die zu 575 OZG-Leistungsbündeln in 14 Themenfeldern zusammengefasst wurden, digitalisiert werden.

Damit dies gelingen kann, sollen Leistungen auch von einem Bundesland so digitalisiert werden, dass andere Bundesländer sie nachnutzen können und den Online-Prozess nicht nochmal selbst entwickeln müssen. Deshalb ist das arbeitsteilige, zeitsparende Vorgehen nach dem Prinzip „EfA – Einer für Alle“ - besonders relevant. Ein Land oder eine Allianz aus mehreren Ländern entwickelt eine Leistung zentral und betreibt diese. Anschließend kann die Leistung anderen Ländern und Kommunen zur Verfügung gestellt werden, die den Dienst dann mitnutzen können. Hierfür müssen sie sich mittels standardisierter Schnittstellen anbinden. Ein Dienstleister betreibt die IT für das digitalisierte Angebot zentral.

EfA führt insbesondere zu der Frage, wem die Verantwortlichkeit für bestimmte Datenverarbeitungsschritte in einem OZG-Umsetzungsprojekt zufällt und auf welcher Erlaubnisgrundlage der bzw. die Verantwortliche personenbezogene Daten verarbeiten darf.

So wird vertreten eine grundsätzliche Trennung zwischen vorgelagertem bzw. Assistenz-Verfahren (Registrierung) bei der Antragseingabe und dem Fachverfahren, das der Durchführung des eigentlichen Verwaltungsverfahrens und der Entscheidungsfindung durch die sachlich zuständige Behörde dient.

Da sich im Rahmen der OZG-Umsetzung noch weitere datenschutzrechtliche Fragen stellen, wird der LfDI aufgrund seiner Expertise als beratende und unterstützende Behörde hinzugezogen.

Eingebunden war der LfDI bislang

- in einen Austausch zur Frage der erforderlichen Einwilligung sog. „Altkunden“ für die bundesweit interoperable Nutzung des Nutzerkontos;

- bei dem Projekt „Digitale Schulzeugnisse“, wodurch beispielsweise digitale Bewerbungsprozesse erleichtert werden sollen;

- in die Bewertung eines Datenschutzkonzeptes für die Antrags- und Prozessplattform (APP) RP. Die APP bietet den Antragsteller:innen eine Antragsplattform (Frontend-Lösung), über die Verwaltungsleistungen online beantragt werden können. Die hierdurch ausgelösten Fachprozesse werden in einer Prozessplattform (Backend-Lösung) standardisiert fachlich abgebildet, visuell dargestellt und technisch verarbeitet.

Darüber hinaus ist der LfDI über den Arbeitskreis Verwaltung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in einem bundesweiten Gremium vertreten.

Ziel ist es, bei der Digitalisierung der Verwaltungsleistungen ein hohes Datenschutzniveau zu gewährleisten, welches bei digitalen Behördengängen den gleichen Schutzstandard bietet wie ein Vor-Ort-Besuch.

14. RECHTSDURCHSETZUNG

Wie schon das Jahr 2020 war auch das Jahr 2021 durch Corona-Einschränkungen geprägt. Im Gegensatz zu dem Vorjahr fanden allerdings mündliche Verhandlungen in Gerichtsverfahren – unter Einhaltung besonderer Hygieneregelungen – statt. Der Landesbeauftragte machte auch in diesem Jahr von seinen Ermittlungs- und Abhilfebefugnissen Gebrauch.

Hierbei ist zunächst darauf hinzuweisen, dass der Landesbeauftragte zwecks Sachverhaltsermittlung auf Informationsersuchen angewiesen ist. Vor diesem Hintergrund sind Verantwortliche und Autragsverarbeiter verpflichtet, auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen zu arbeiten. In 37 Fällen war dies nicht der Fall, so dass die Behörde in 18 Fällen die Anwendung von Zwangsgeldern androhen musste und in 19 Fällen aufgrund der Nichtbeantwortung von Informationsersuchen Zwangsgelder gegenüber den Adressaten festgesetzt hat.

Im Jahr 2021 wurden 10 Bußgelder verhängt. Die Bußgeldhöhen waren 2 x 200 Euro, 250 Euro, 400 Euro, 2 x 500 Euro, 700 Euro, 1.500 Euro, 2.000 Euro und 60.000 Euro. Das höchste Bußgeld i.H.v. 60.000 Euro wurde gegen ein Unternehmen aufgrund der Nichterfüllung eines Auskunftsersuchens nach Art. 15 DS-GVO verhängt.

Gegen den Landesbeauftragten wurden in diesem Jahr 19 Gerichtsverfahren geführt. Streitgegenstand dieser Verfahren waren sowohl durch den Landesbeauftragten erlassene Abhilfebefugnisse (u.a. Verwarnungen und Bußgelder) als auch Beendigungen von Beschwerdeverfahren aufgrund des Nichtvorliegens eines Datenschutzverstoßes.

15. ZERTIFIZIERUNG UND AKKREDITIERUNG

Auch im Jahr 2022 arbeitete der Arbeitskreis Zertifizierung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder an der Fortentwicklung der Akkreditierung und Zertifizierung in Deutschland. Dabei arbeitete der Arbeitskreis wie schon in den vergangenen Jahren mit der Deutschen Akkreditierungsstelle GmbH (DAkkS) zusammen. Dies hat den Hintergrund, dass das Akkreditierungsverfahren von den Datenschutzaufsichtsbehörden in Kooperation mit der DAkkS betrieben wird.

Der Unterarbeitskreis Prüfkriterien des AK Zertifizierung hat das Papier „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme – Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6)“ entworfen. Das Papier wurde im April 2021 von der DSK verabschiedet. Das Dokument beschreibt die Mindestanforderungen an die Zertifizierungskriterien, die ergänzend zu den Vorgaben der DIN EN ISO/IEC 17067 von allen Zertifizierungsprogrammen erfüllt sein müssen. Es soll den deutschen Aufsichtsbehörden bei der Bewertung von Zertifizierungsprogrammen als einheitliche Bewertungsgrundlage dienen und Programmeignern sowie Zertifizierungsstellen bei der Erstellung ihrer Dokumente als Orientierung helfen.

Zur Vorbereitung einer Akkreditierung muss die Zertifizierungsstelle oder der Programmeigner ein Zertifizierungsprogramm erstellen und durch die DAkkS gem. DIN EN ISO/IEC 17011 auf Eignung prüfen lassen (vgl. DAkkS-Regel 71 SD 0016). Wesentlicher Teil dieses Zertifizierungsprogramms sind die Zertifizierungskriterien zur Umsetzung der datenschutzrechtlichen Anforderungen. Diese werden gem. Art. 57 Abs. 1 lit. n DSGVO i. V. m. Art. 42 Abs. 5 DSGVO entweder von der zuständigen Datenschutzaufsichtsbehörde genehmigt oder (i. d. R. über die zuständige Aufsichtsbehörde) dem Europäischen Datenschutzausschuss zur Genehmigung bzw. Billigung gem. Art. 63, 64 Abs. 1 lit. c übermittelt.

Das Papier ist abrufbar unter
https://s.rlp.de/O1W4F

ABKÜRZUNGSVERZEICHNIS

Berufsbildende Schule	BBS
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	BFDI
Bürgerliches Gesetzbuch	BGB
Ministerium für Bildung des Landes Rheinland-Pfalz	BM
Bundesmeldegesetz	BMG
Bundesnotarordnung	BNotO
Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff	BoBD
Datenschutz-Grundverordnung	DS-GVO
Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder	DSK
Der Europäische Datenschutzausschuss	EDSA
Landesgesetz zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz	eGovG
Europäische Union	EU
Gemeindeordnung	GemO
Infektionsschutzgesetz	InfSG
Justizvollzugsanstalt	JVA
Landesbibliotheksgesetz Rheinland-Pfalz	LBibG
Landesdatenschutzgesetz Rheinland-Pfalz	LDSG
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz	LfDI
Landeswahlordnung Rheinland-Pfalz	LWO

Mietspiegelreformgesetz	MsRG
Mietspiegelverordnung	MsV
Oberlandesgericht Rheinland-Pfalz	OLG
Onlinezugangsgesetz	OZG
Sozialgesetzbuch	SGB
Strafgesetzbuch	StGB
Telekommunikation-Telemedien-Datenschutz-Gesetz	TTDSG
Verwaltungszustellungsgesetz	VwZG

Hintere Bleiche 34 | 55116 Mainz
Postfach 3040 | 55020 Mainz

Telefon +49 (0) 6131 8920 - 0
Telefax +49 (0) 6131 8920 - 299

poststelle@datenschutz.rlp.de