Der Landesbeauftragte für
den **DATENSCHUTZ** und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

TÄTIGKEITSBERICHT ZUM DATENSCHUTZ 2024

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

Mai 2025

INHALT

VORWORT

Prof. Dr. Dieter Kugelmann

Datenschutz ist Grundrechtsschutz. Das Recht auf informationelle Selbstbestimmung sichert die individuellen Freiheiten der Bürgerinnen und Bürger in Rheinland-Pfalz, Deutschland und Europa. Es verpflichtet globale Konzerne zur Achtung europäischer Standards und ist ein Grundpfeiler unseres Wertesystems als freie demokratische Gesellschaft. Die Rechte und Freiheiten der Einzelnen zu achten und zu verteidigen: Das macht uns als Europäerinnen und Europäer aus.

In fordernden Zeiten ist es wichtig, den Grundgedanken und das leitende Ziel des Datenschutzes unermüdlich in Erinnerung zu rufen. Als Landesbeauftragter für den Datenschutz und die Informationsfreiheit war ich im Jahr 2024 mit der Tendenz konfrontiert, dass Abwägungen zwischen der informationellen Selbstbestimmung der Bürgerinnen und Bürger und wirtschaftlichen Interessen zunehmend einseitig vorgenommen werden. Diese Tendenz scheint sich im Jahr 2025 fortzusetzen. Die Bedeutung wirtschaftlicher Entwicklung ist selbstverständlich anzuerkennen, Innovation und Wirtschaftsförderung können aber auch mit funktionierendem Datenschutz gelingen.

Mein Bestreben ist es, mit meinem kompetenten Team täglich zu demonstrieren, wie das geht: mit transparenter Kommunikation, persönlichen Ansprechpartnerinnen und Ansprechpartnern in meiner Behörde und mit Beratung vor Ort, selbstverständlich bei genauer Kenntnis der unternehmensspezifischen Bedürfnisse und von regionalen Besonderheiten. Ich teile das politische Ziel, Datenschutz effizient und mit Augenmaß anzuwenden und bürokratische Lasten zu verringern, gerade für kleine und mittlere Unternehmen. Meine Behörde verfolgt schon immer den Ansatz, das jeweilige Risiko einer konkreten Datenverarbeitung zu berücksichtigen und unsere Maßnahmen am mehr oder weniger hohen Risikograd differenziert auszurichten. Als Vorsitz des Arbeitskreises DSK 2.0 der Datenschutzkonferenz setze ich mich gemeinsam mit den Datenschutzaufsichtsbehörden des Bundes und der Länder für eine

effizientere und einheitlichere Datenschutzaufsicht ein. Das Jahr 2024 stand unter dem Vorzeichen, eine Reihe europäischer Rechtsakte in eine angemessene Anwendung zu bringen. Zudem war bis zum vorzeitigen Ende der Legislaturperiode eine Reform des Bundesdatenschutzgesetzes vorgesehen, die auch Zuständigkeiten und Arbeitsweise der Datenschutzaufsichtsbehörden betroffen hätte. Angesichts von Tendenzen zu einer Zentralisierung der Aufsichtsstrukturen gerade im Hinblick auf die innerstaatliche Verwirklichung des europäischen Rechts haben die Landesdatenschutzaufsichtsbehörden jüngst in einem gemeinsamen Papier konkrete Reformvorschläge veröffentlicht (**www.s.rlp.de/reform**).

Pionierarbeit möchte ich mit der Einrichtung einer „Datenschutz-Sandbox“ leisten, die es Unternehmen und Behörden ermöglicht, neue digitale Anwendungen rechtssicher und risikofrei auf Datenschutzkonformität zu testen. Zu diesem Zweck habe ich im Jahr 2024 gemeinsam mit der Universität Bayreuth ein Forschungsprojekt konzipiert und erfolgreich beim Bundesministerium für Bildung und Forschung zur Förderung vorgeschlagen. Über einen Zeitraum von drei Jahren werden wir die Bedingungen für die Realisierung eines regulatorischen Experimentierraums ausloten und testweise eine Sandbox bei meiner Behörde einrichten. Die Erkenntnisse werden wir in einer Handreichung für andere Behörden aufbereiten und als Grundlage für Vorschläge zur Fortentwicklung des regulatorischen Rahmens nutzen. So sieht gelebte Innovation Hand in Hand mit dem Datenschutz aus.

Stichwort Innovation: Künstliche Intelligenz, ihre Potenziale und ihre Anziehungskraft, aber auch die zahlreichen noch unzureichend geklärten Rechtsfragen hinsichtlich ihrer Anwendung in Behörden und Unternehmen sind nach wie vor ein Schwerpunkt meiner Arbeit. Mit der Gründung eines eigenen Arbeitskreises Künstliche Intelligenz, dessen Leitung ich gemeinsam mit meinem baden-württembergischen Amtskollegen übernommen habe, wurde dieser Schwerpunkt Ende 2024 auch innerhalb der Datenschutzkonferenz auf Dauer institutionalisiert. Rechtliche und technische Aspekte, die uns im Arbeitskreis stark beschäftigen, umfassen die Erhebung und Vorbereitung von Trainingsdaten, das Training mit personenbezogenen Daten, Art und Umfang von risikomindernden Maßnahmen sowie die Auswirkungen eines möglicherweise rechtswidrigen Trainings auf die Rechtmäßigkeit des Einsatzes eines KI-Modells sowie die Umsetzung von Betroffenenrechten.

\In sicherheitspolitischen Belangen erleben wir, dass die Prinzipien des Datenschutzes unter Druck geraten. In Zeiten objektiv und subjektiv erlebter Krisen ist das oft der Fall. Aktuell konnten und können wir diese Tendenz in der Migrationsdebatte und bei Diskussionen um erweiterte Befugnisse der Sicherheitsbehörden verfolgen, auf nationaler Ebene und in Rheinland-Pfalz. Die Einführung eingriffsintensiver Befugnisse, die zunehmend automatisiert und KI-gestützt erfolgen sollen, erfordert jedoch eine grundrechtssensible und verfassungskonforme Gesetzgebung. Das rheinland-pfälzische Polizei- und Ordnungsbehördengesetz, dessen Änderung 2024 diskutiert wurde und 2025 erfolgte, verfolgt hier eine zu begrüßende zurückhaltende Linie, indem etwa keine biometrische Gesichtserkennung eingeführt wurde. Eine ausgewogene Balance zwischen Freiheit und Sicherheit ist eine grundlegende Bedingung des demokratischen und resilienten Rechtsstaats.

In Gesetzgebungsprozesse haben wir uns im Jahr 2024 in besonders intensiver Weise eingebracht: Die Änderung des Polizei- und Ordnungsbehördengesetzes in Rheinland-Pfalz haben wir konstruktiv und kritisch begleitet. Wir haben die Fristen im Blick, die aus den großen europäischen Verordnungen zum Digitalisierungs- und Datenrecht resultieren und Gesetzgebung auf nationaler Ebene verlangen. Einige der Fristen wurden im Jahr 2024 bereits wirksam, andere stehen in den kommenden Monaten bevor. Hier versuchen wir in Kooperation mit anderen deutschen Datenschutzaufsichtsbehörden Einfluss auf Bundesebene zu nehmen. Prägend war die Debatte um die Ausgestaltung des Bundesdatenschutzgesetzes, zu der wir im Rahmen der Datenschutzkonferenz beigetragen haben. Die Novellierung des Bundesdatenschutzgesetzes wurde mit dem Ende der Ampel-Koalition zurückgestellt. Die Novellierung muss in der kommenden Legislaturperiode aufgegriffen und mit gutem Ergebnis abgeschlossen werden. Zugunsten einer effizienten Datenschutzaufsicht setzen wir uns gemeinsam mit den deutschen Datenschutzaufsichtsbehörden dabei unter anderem für eine effektive Regelung der Zuständigkeit bei bundesweiten Sachverhalten und für die Institutionalisierung der Datenschutzkonferenz mit einer Geschäftsstelle ein.

2024 war ein besonders politisches Jahr für den Datenschutz, 2025 wird aller Voraussicht nach noch politischer werden. Angekündigte Reformvorhaben der neuen Bundesregierung werden wir aufmerksam begleiten und, soweit erforderlich, nachdrücklich für aus unserer Sicht nötige Anpassungen der Pläne eintreten. Ich werde die Belange des Datenschutzes in Rheinland-Pfalz und für Rheinland-Pfalz weiter nach Kräften voranbringen – im Dienst der Bürgerinnen und Bürger, deren Rechte wir schützen.

Prof. Dr. Dieter Kugelmann

I.
DER LFDI RHEINLAND-PFALZ IN DEUTSCHLAND UND EUROPA

I. DER LFDI RHEINLAND-PFALZ IN DEUTSCHLAND UND EUROPA

1. EFFEKTIVE ZUSAMMENARBEIT UND EFFIZIENTER GRUNDRECHTSSCHUTZ IM FÖDERALEN STAAT: ARBEIT DES AK DSK 2.0

Die Datenschutzaufsichtsbehörden des Bundes und der Länder rücken immer enger zusammen, um einen kohärenten Datenschutz in Deutschland gemeinsam und effektiv zu gewährleisten. Der Arbeitskreis DSK 2.0 setzt sich dazu unter meinem Vorsitz kontinuierlich für die Fortentwicklung der Datenschutzkonferenz als Abstimmungs-, Kooperations-, Entscheidungs- und Expertengremium ein. Wichtige Eckpunkte konnten wir dazu im Jahr 2024 in einer Stellungnahme zur Novellierung des Bundesdatenschutzgesetzes formulieren. Parallel wurden die Rahmenbedingungen für die von uns geforderte Ständige Geschäftsstelle als wichtiger Teilaspekt für die avisierte Institutionalisierung der Datenschutzkonferenz weiter ausgearbeitet. Einigkeit, Schlagkraft und Weitsicht wurden insbesondere in unserem Positionspapier zur künftigen Marktüberwachung über KI-Verfahren in Deutschland gezeigt. In einer Strategieklausur in Speyer haben wir neben fachlichen Diskussionen etwa zum Personenbezug von KI-Modellen insbesondere neue Formen kooperativer Arbeitsweisen und neue Verfahren zur einheitlichen Entscheidungsfindung diskutiert, um diese Themen im AK DSK 2.0 weiter anzugehen.

Die unabhängigen Datenschutzaufsichtsbehörden nehmen gegenüber Bürgerinnen und Bürgern und Verantwortlichen vielfältige Aufgaben war. Daneben ist es uns ein überaus wichtiges Anliegen, die breite Expertise, die dank des Föderalismus in allen Bundesländern und beim Bund angesiedelt ist, stark zu machen für einen effektiven, schlagkräftigen, möglichst einheitlichen, zugänglichen und nachhaltigen Datenschutz in Deutschland und Europa. Dazu im Einzelnen:

1.1 Institutionalisierung der Datenschutzkonferenz durch Novellierung des BDSG

Die Bundesregierung der 20. Legislaturperiode legte im Februar 2024 einen Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG-E) vor (BT-Drs. 20/10859) und bat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) über ihren Vorsitz (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) um Stellungnahme. Diese wurde im AK DSK 2.0 federführend erarbeitet und koordiniert. Ein wichtiges Anliegen war dabei die Institutionalisierung der Datenschutzkonferenz. In einem neuen § 16a BDSG-E sollte die bereits bestehende DSK verankert und klarstellend geregelt werden, dass sich diese eine Geschäftsordnung geben kann. Über das Mittel der Geschäftsordnung verfügt die DSK bereits seit vielen Jahren mit dem Ziel, Abstimmungsprozesse und Verfahrensfragen zu regeln. In der Geschäftsordnung sind auch Anwendungsbereich und Verfahren von Mehrheitsentscheidungen definiert. Diese Festlegung erzeugt eine Selbstbindung der DSK-Mitglieder und hat sich als tragfähig erwiesen. Einen Mehrwert würde die Regelung im BDSG dann bringen, wenn sie die Zielsetzung enthalten würde, dass die Datenschutzkonferenz ein Gremium

zur Koordinierung und Zusammenarbeit von eigenständigen und unabhängigen Aufsichtsbehörden zur Förderung der einheitlichen Anwendung des Datenschutzrechts handelt. Des Weiteren hat die Datenschutzkonferenz gefordert, die Einrichtung einer Ständigen Geschäftsstelle zu regeln. Die Geschäftsstelle soll das administrative Gegenstück der Datenschutzkonferenz darstellen und die Harmonisierungsmaßnahmen der DSK organisatorisch unterstützen.

Neben diesen Anliegen hat die Datenschutzkonferenz außerdem u.a. folgende Regelungen kritisch gewürdigt:

- Schutz von Betriebs- und Geschäftsgeheimnissen bei Auskunftsansprüchen: Die DSK hat Zweifel, ob die geplanten Regelungen (§ 34 Abs. 1 S. 2 BDSG-E und § 83 Abs. 1 S. 2 SGB-X-E) mit Art. 23 DS-GVO vereinbar sind, da die europarechtlichen Einschränkungen der Betroffenenrechte eng auszulegen sind.

- Scoring: Die DSK hält es für erforderlich, im weiteren Gesetzgebungsverfahren zu prüfen, ob die Neuregelung in § 37a BDSG-E mit den Anforderungen des Art. 23 DS- GVO zur Einschränkung von Betroffenenrechten in Einklang steht. Um eine rechtssichere Regelung von Kreditwürdigkeitsprüfungen durch Scoringverfahren zu erreichen, empfiehlt die DSK eine Erörterung im Rahmen einer Sachverständigenanhörung. Zudem weist sie auf zahlreiche Unklarheiten in den Regeln hin und regt Nachbesserungen an.

- Länderübergreifende Datenverarbeitungsvorhaben: Bei gemeinsamer Verantwortlichkeit (§ 40a, § 27 Abs. 5 BDSG-E) im nichtöffentlichen Bereich soll es den beteiligten Unternehmen ermöglicht werden, eine einzige Aufsichtsbehörde festzulegen. Die DSK hält es in solchen Fällen für notwendig, zumindest eine vorgeschaltete Prüfung durch die beteiligten Aufsichtsbehörden zu den Fragen vorzusehen, ob überhaupt eine gemeinsame Verantwortlichkeit vorliegt und wie sich eine gemeinsam verantwortete Verarbeitung abgrenzen lässt.

Die umfangreiche Stellungnahme finden Sie unter **www.s.rlp.de/dsk-bdsge**. Ich hoffe, dass die Anliegen von der neuen Bundesregierung konstruktiv aufgenommen werden.

1.2 Ständige Geschäftsstelle der Datenschutzkonferenz: Der Bedarf wächst

Die von uns geforderte Ständige Geschäftsstelle der Datenschutzkonferenz hat das Ziel, die Entscheidungsprozesse und praktischen Bedingungen fortlaufender und effektiver Zusammenarbeit sicherzustellen und die Einheitlichkeit der Bewertung von Datenschutzfragen und ihrer Vermittlung zu verbessern. Zum Aufgabenportfolio soll die Unterstützung des Vorsitzes der Datenschutzkonferenz bei der Organisation und Durchführung der Konferenzen sowie bei der Durchführung der Umlaufbeschlüsse und Abstimmung anderer internen Entscheidungen der Datenschutzkonferenz zählen. Dies würde einen Gewinn an Effizienz und eine Steigerung der Kontinuität im Handeln der DSK bedeuten. Die Wahrung dieser Kontinuität bei gleichzeitiger effektiver Aufgabenwahrnehmung wird auch vor dem Hintergrund der fortschreitenden Technologien auf Dauer eine Herausforderung bleiben, die einen überschaubaren, aber angemessenen Verwaltungsunterbau erfordert. Zur Effizienzsteigerung und Vereinfachung der Meldeprozesse soll bei der Geschäftsstelle zudem ein Meldeportal angesiedelt werden, das zentrali-

siert Meldungen von Datenschutzbeauftragten oder von Datenpannen, die möglicherweise mehrere Bundesländer betreffen, empfangen und an die zuständigen Datenschutzaufsichtsbehörden verteilen kann.

Auch in Bezug auf die unterschiedlichen Akteure und Aufsichtsstrukturen der EU-Digitalisierungsrechtsakte (Digital Market Act, Digital Service Act, AI Act, Data Governance Act, Data Act) sowie der NIS-2-Richtlinie bietet die Geschäftsstelle einen echten Mehrwert. Sie könnte als Kooperationsschnittstelle für Informationsaustausch und Abstimmungsprozesse zwischen den für die EU- Digitalrechtsakten zuständigen Fachbehörden und den Datenschutzbehörden von Bund und Ländern fungieren und damit einer ggf. fragmentierten Aufsicht gegensteuern.

Die Einrichtung der Ständigen Geschäftsstelle soll durch eine Verwaltungsvereinbarung zwischen Bund und Ländern erfolgen, die zugleich auch ihre Finanzierung regelt. Zu diesem Zweck hat der AK DSK 2.0 den Entwurf einer Verwaltungsvereinbarung erarbeitet, der jederzeit operationalisiert werden kann.

1.3 Strategieklausur der Datenschutzkonferenz in Speyer

Als Vorsitz des AK DSK 2.0 lud ich meine Amtskolleginnen und -kollegen der Datenschutzaufsichtsbehörden des Bundes und der Länder vom 30. August bis 1. September 2024 zur Erörterung strategischer Fragen nach Speyer ein. Die Klausurtagung findet seit 2023 außerhalb des Sitzungsrhythmus der Datenschutzkonferenz statt. Sie hat sich erneut als probates Instrument zur Verbesserung der Vollzugskoordinierung erwiesen und den angemessenen, vertraulichen und konstruktiven Rahmen geboten, gemeinsame Grundsatzfragen sowie notwendige Impulse für die Fortentwicklung des Datenschutzes und der Datenschutzkonferenz zu analysieren.

Einen fachlichen Schwerpunkt bildete dabei die Diskussion datenschutzrechtlicher Fragestellungen zur Nutzung von Künstlicher Intelligenz. Wir vertraten einhellig die Auffassung, dass es unsere Aufgabe ist, Behörden und Unternehmen beim Einsatz von die KI mit unserer Expertise für den Schutz personenbezogener Daten eng und praxisorientiert zu begleiten. Dies beginnt bereits mit dem Training generativer KI- Modelle, die künftig das Kernelement der meisten in der Praxis eingesetzten KI-Systeme bilden werden.

Einigkeit bestand außerdem in der Sorge, dass die bisherigen Ankündigungen digitalpolitischer Schwerpunkte den Datenschutz für die im Jahr 2024 begonnene europäische Legislaturperiode vernachlässigen. Tatsächlich ergeben sich aus der Nutzung von Künstlicher Intelligenz grundlegende Veränderungen der Durchsetzungsbedingungen für die Rechte und Freiheiten der Bürgerinnen und Bürger. Für ein kohärentes europäisches Daten-, Digital- und KI-Recht bedarf es einer sorgfältigen Analyse und Diskussion über spezifische datenschutzrechtliche Anforderungen, die beim Ringen um die KI-Verordnung ausgeblendet wurden.

Nicht zuletzt wurde die Bestrebung nach einheitlichen Mehrheitsentscheidungen und arbeitsteiligem Vorgehen der Aufsichtsbehörden der Datenschutzkonferenz vertieft. Der Spagat zwischen einer föderalen Aufsichtsstruktur mit unabhängigen Behörden und dem Bedürfnis nach effektiver und kohärenter Aufsichtspraxis ist leistbar durch Verfahrensabsprachen, gegenseitiges Vertrauen und Verständnis für verbleibende ländertypische Besonderheiten, die keiner Vereinheitlichung zugänglich sind. Unsere Überlegungen sind in konkrete Reformvorschläge zugunsten einer einheitlicheren und effizienteren Datenschutzaufsicht gemündet, die unter **www.s.rlp.de/reform** öffentlich bereitstehen.

2. SCHWERPUNKT: KÜNSTLICHE INTELLIGENZ

2.1 Die europäische KI-Verordnung: Der Regulierungsrahmen steht

Im März 2024 nahm das Europäische Parlament die Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz an, am 1. August trat die KI-Verordnung, auch AI Act genannt, in Kraft. Damit fand ein umfangreiches und langwieriges Gesetzgebungsvorhaben seinen Abschluss. Hersteller, Anbieter, Betreiber und Händler von KI-Systemen haben seither einen Orientierungsrahmen, der die Anforderungen an KI-Systeme in den einzelnen Phasen der Wertschöpfungskette grundsätzlich klarstellt.

Das Verhältnis von Künstlicher Intelligenz zum Datenschutz ist ein Schwerpunkt meiner Behörde. Schon 2019 haben wir in unserer Hambacher Erklärung als deutsche Datenschutzaufsichtsbehörden eine humanistische und damit grundrechtsschützende Ausrichtung von KI als Standard gefordert. Ich freue mich, dass dieser Anspruch sich im europäischen Regulierungsrahmen wiederfindet. Die KI-Verordnung stellt sicher, dass die Entwicklung und Verwendung von KI-Systemen einen menschenzentrierten, vertrauenswürdigen und damit wertebasierten Ansatz verfolgt. In der EU soll die KI den Menschen dienen und nicht umgekehrt.

In den zahlreichen Fällen, in denen KI-Systeme personenbezogene Daten verarbeiten, bleiben das Datenschutzrecht und der damit gesicherte Grundrechtsschutz von der KI-Verordnung unberührt. Dabei sind die Synergien offenkundig: Viele Mechanismen, die zu einer transparenten und vertrauenswürdigen KI beitragen, sind bereits aus der Datenschutz-Grundverordnung und der Richtlinie für Polizei und Justiz bekannt. Wer über ein gutes Datenschutzmanagement verfügt, kann dieses für die Umsetzung der Anforderungen der KI-Verordnung nutzbar machen. Durch Transparenz- und Dokumentationsvorgaben wird Vertrauen in die Systeme geschaffen, zudem haben die betroffenen Personen ein Recht auf Erläuterung der Entscheidungsfindung, das zu den Betroffenenrechten der DS-GVO hinzutritt. Auch wenn die Risiko-Klassifizierung der KI-Verordnung einem strikteren Konzept folgt als in der Datenschutz-Grundverordnung, können die Instrumente, mit denen Risiken gemanagt werden, sinnvoll ineinandergreifen: Risikomanagementsysteme nach Art. 9 KI-VO könnten etwa mit dem Datenschutzmanagement kombiniert werden, die Grundrechte-Folgenabschätzung für Hochrisiko-Systeme öffentlicher Stellen nach Art. 27 KI-VO lässt sich gegebenenfalls mit der Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO verbinden.

Synergien zwischen den Anforderungen der KI-Verordnung und der Datenschutz-Grundverordnung hat der Verordnungsgeber auch erkannt, als er den Datenschutzaufsichtsbehörden die Funktion der Marküberwachung über die Hochrisiko-Systeme im Bereich der Strafverfolgung, Justiz, Migration und Wahlen zuwies. Erklärtes Ziel des Verordnungsgebers ist dabei die Sicherstellung einer einheitlichen Aufsicht.

Mit dem Inkrafttreten der KI-Verordnung liefen verschiedene mit ihr verbundene Umsetzungsfristen an. Zum 2. Februar 2025 werden bestimmte hochriskante Praktiken der künstlichen Intelligenz verboten. Hierzu zählt das Verbot biometrischer Echtzeit-Fernüberwachung sowie das Verbot von Social Scoring. Zum 2. August 2025 müssen die nationalen Aufsichtsbehörden für die KI-Verordnung benannt sein. Weitere Regelungen treten gestaffelt in Kraft, spätestens zum 2. August 2026 entfaltet die KI-Verordnung vollumfänglich Wirksamkeit.

2.2 Nationale Zuständigkeiten für die KI-Verordnung

Nach Inkrafttreten der KI-Verordnung (KI-VO) am 1. August 2024 muss in Deutschland innerhalb von zwölf Monaten eine behördliche Aufsichtsstruktur eingerichtet werden. Damit besteht dringender Handlungsbedarf für die Gesetzgeber in Bund und Ländern zur Klärung der Frage, wer die Aufsicht in Deutschland wahrnehmen soll.

Die DSK wies angesichts dieser Situation schon im Mai 2024 darauf hin, dass die KI-VO in vielen Fällen bereits eine sektorspezifische Zuständigkeit der Datenschutzbehörden als Marktüberwachungsbehörden vorsieht. Im Sinne einer einheitlichen Anwendung der KI-VO empfahl die DSK, als Marktüberwachungsbehörden nach der KI-VO den bzw. die Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) sowie die Landesdatenschutzbehörden zu benennen. Die BfDI sollte nach Vorstellungen der Datenschutzkonferenz Deutschland im Europäischen Ausschuss für KI vertreten.

Die DSK argumentierte, dass mit dieser Konzeption Doppelstrukturen und zusätzlicher Bürokratieaufwand vermieden werden können. Die Datenschutzaufsichtsbehörden haben ohnehin in allen Fällen, in denen KI-Systeme personenbezogene Daten verarbeiten, die Aufsicht nach der Datenschutz-Grundverordnung. Nur durch die Zuweisung von Zuständigkeiten für die KI-VO an die Datenschutzaufsichtsbehörden wird eine Beratung und Aufsicht aus einer Hand möglich.

Das Positionspapier „Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO)“ entstand innerhalb des Arbeitskreises DSK 2.0, der unter meiner Leitung die Stärkung der Zusammenarbeit zwischen den deutschen Datenschutzaufsichtsbehörden zum Ziel hat. Es ist unter **www.s.rlp.de/dsk-posKIVO** abrufbar.

2.3 Orientierungshilfe der DSK zu Künstlicher Intelligenz

Im Mai 2024 legte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) eine Orientierungshilfe mit datenschutzrechtlichen Kriterien für die Auswahl und den datenschutzkonformen Einsatz von KI-Anwendungen vor. Erarbeitet wurde die Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ von der Taskforce KI unter meinem Vorsitz. Sie richtet sich an Unternehmen, Behörden und andere Organisationen. Das Papier dient als Leitfaden insbesondere für datenschutzrechtlich Verantwortliche, um KI-Anwendungen auszuwählen, zu implementieren und zu nutzen. Die Orientierungshilfe wird künftig weiterentwickelt und an aktuelle Entwicklungen angepasst.

Erstellt wurde die Orientierungshilfe vor dem Hintergrund, dass viele öffentliche und private Stellen sich derzeit fragen, unter welchen Voraussetzungen sie KI-Anwendungen datenschutzkonform einsetzen können. Besonderes Interesse gilt dabei den sogenannten Large Language Models (LLM), die häufig als Chatbots angeboten werden, aber auch als Grundlage für andere Anwendungen dienen können. Der Schwerpunkt der Orientierungshilfe „KI und Datenschutz“ liegt daher auf diesen KI-Anwendungen. Über die LLM hinaus gibt es zahlreiche weitere KI-Modelle und KI-Anwendungen, deren Einsatz infrage kommen kann und für die viele der Erwägungen in dem Papier bedeutsam sind.

Praxisnah adressiert die Orientierungshilfe Fragen, die datenschutzrechtlich Verantwortliche bei der Konzeption des Einsatzes, der Auswahl, der Implementierung und der Nutzung von KI-Anwendungen stellen und beantworten müssen. Ob Zweckbestimmung, Transparenzpflichten, Betroffenenrechte oder Richtigkeit von Ergebnissen: Die Orientierungshilfe erörtert – auch anhand von Beispielen – wichtige Kri-

terien entlang der Vorgaben der Datenschutz-Grundverordnung und zeigt Leitlinien für entsprechende Entscheidungen auf.

Die Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ richtet sich mittelbar auch an Entwickler, Hersteller und Anbieter von KI-Systemen. Denn sie enthält Hinweise zur Auswahl datenschutzkonformer KI-Anwendungen, die auf die Gestaltung der Produkte zurückwirken. Die Entwicklung von KI-Anwendungen und das Training von KI-Modellen sind allerdings nicht Schwerpunkt dieser Orientierungshilfe.

Die Orientierungshilfe ist unter **www.s.rlp.de/OH-KI** auf meiner Webseite abrufbar.

2.4 Vorsitz im Arbeitskreis „Künstliche Intelligenz“ der Datenschutzkonferenz

Die DSK richtete auf ihrer 108. Konferenz am 14. November 2024 in Wiesbaden mit einstimmigem Beschluss einen eigenen Arbeitskreis Künstliche Intelligenz ein. Den Vorsitz übernehme ich gemeinsam mit meinem baden-württembergischen Amtskollegen. Ziel des Arbeitskreises ist es, Anforderungen und Handlungsempfehlungen zu entwickeln, um KI datenschutzkonform zu realisieren und einzusetzen.

Basierend auf der produktiven Arbeit der Taskforce KI in den vergangenen Jahren ist die Institutionalisierung als regulärer Arbeitskreis innerhalb der DSK ein logischer Schritt. Ich freue mich, die Erfahrungen aus der von mir geleiteten Taskforce in den Arbeitskreis einzubringen. Wir unterstützen in der DSK den fortschrittsorientierten und rechtskonformen Einsatz von Künstlicher Intelligenz. Gerade hier wird der Arbeitskreis dazu beitragen, Innovation und Datenschutz gemeinsam zu denken.

Der Arbeitskreis KI vereinigt technische und rechtliche Expertise aller in der DSK verbundenen Aufsichtsbehörden. Er soll die Entwicklungen und Wirkungen sowohl der KI-Technologien als auch der KI-Regulierung beobachten, konstruktiv-kritische Beiträge zu aktuellen Diskussionen um KI leisten, Handreichungen und Orientierungshilfen herausgeben und dazu beitragen, dass sich die Aufsichtstätigkeit innovationsfreundlich und risikospezifisch fortentwickeln kann.

2.5 EDSA-Stellungnahme zu Künstlicher Intelligenz

Im Dezember 2024 veröffentlichte der Europäische Datenschutzausschuss (EDSA) eine Stellungnahme, die wesentliche Grundfragen der Anwendung des Datenschutzrechts auf Künstliche Intelligenz behandelt. Anlass für die Befassung mit dem Thema war ein Stellungnahmeersuchen der irischen Datenschutzbehörde an den EDSA.

Die Stellungnahme trifft keine Aussagen zur Zulässigkeit konkreter KI-Modelle, die bereits auf dem Markt sind, sondern errichtet Leitplanken für eine datenschutzrechtliche Prüfung von KI-Systemen im Einzelfall und für deren Gestaltung. Die Stellungnahme bringt damit die datenschutzrechtliche Diskussion um KI in der EU/EWR deutlich voran. Ich begrüße die Stellungnahme des EDSA grundsätzlich als wichtigen Schritt in Richtung Rechtssicherheit sowohl für Entwickler und Anwender von KI-Systemen als auch für Personen, deren Daten in diesem Zusammenhang verarbeitet werden. Ich betrachte die Stellungnahme außerdem als hilfreiche Orientierungspunkte für die Ausübung der aufsichtsrechtlichen Befugnisse der Datenschutzbehörden in Deutschland.

Der weitere Weg zu zukunftsträchtiger und zugleich datenschutzgerechter KI ist damit offen. Für Europa ist es eine große Chance, anwendungsorientierte KI-Systeme zu entwickeln, bei denen vielleicht nicht immer die grundlegenden Modelle den Standards des EU-Daten-

schutzrechts entsprechen, aber die darauf aufbauenden Anwendungen sehr wohl.

Einzelheiten zur EDSA-Stellungnahme:

Die irische Datenschutzbehörde ersuchte den EDSA gemäß Artikel 64 Abs. 2 DSGVO um eine Stellungnahme zu Fragen von allgemeiner Geltung bzw. mit Auswirkungen in mehr als einem Mitgliedstaat:

- Können KI-Modelle, die mit personenbezogenen Daten trainiert wurden, auch als personenbezogen einzustufen sein? Oder sind sie in jedem Fall als anonym zu behandeln?

  Praxisrelevant ist diese Frage, weil von der Antwort abhängt, ob die KI-Modelle dem Datenschutzrecht unterliegen.

- Unter welchen Umständen können sich Entwickler und Anbieter von KI-Modellen auf Art. 6 Abs. 1 lit. f DS-GVO (Verarbeitung aufgrund berechtigter Interessen) als datenschutzrechtliche Rechtsgrundlage für das Training und die Anwendung von KI-Modellen beziehen, soweit hierbei personenbezogene Daten verarbeitet werden?

  Dies spielt vor allem dann eine Rolle, wenn personenbezogene Daten als Trainingsdaten für KI-Modelle aus dem freien Internet gesammelt werden oder wenn die Betreiber von Social-Media-Plattformen die Daten ihrer Nutzer und Nutzerinnen für das Training von KI-Modellen weiterverwenden möchten. Soweit die Datenverarbeitung sich tatsächlich auf ein berechtigtes Interesse stützen ließe, wäre dies ohne die Einwilligung der betroffenen Personen möglich.

- Welche Auswirkungen auf den Einsatz eines KI-Modells als Teil eines KI-Systems hat es, falls festgestellt wird, dass ein KI-Modell datenschutzwidrig trainiert wurde? Kann zum Beispiel ein Unternehmen oder eine Behörde ein KI-Modell einsetzen, obwohl dieses unrechtmäßig trainiert wurde, wenn der spätere Einsatz selbst nicht gegen datenschutzrechtliche Vorschriften verstößt?

  Die Frage trägt dem Umstand Rechnung, dass KI-Technologie entlang einer komplexen Wertschöpfungskette verlaufen kann, auf der in unterschiedlichen Verarbeitungsphasen verschiedene Akteure wirken können.

Der EDSA hält fest, dass **KI-Modelle regelmäßig personenbezogene Daten enthalten**. Vollständig anonyme KI-Modelle sind denkbar. Sofern sie jedoch mit personenbezogenen Daten trainiert wurden, lässt sich der notwendige Nachweis der Anonymität nur schwer führen. Damit ist das Datenschutzrecht regelmäßig auf KI-Modelle anwendbar, die mit personenbezogenen Daten trainiert wurden.

Im Hinblick auf das **berechtigte Interesse als Rechtsgrundlage** betont die Stellungnahme, dass unterschiedliche Szenarien zu unterschiedlichen Bewertungen führen können. Allerdings können die Rechte und Freiheiten der betroffenen Personen einer Verarbeitung zu Zwecken des Trainings von KI-Modellen oder der Verarbeitung bei der späteren Anwendung der Modelle im Rahmen von KI-Systemen durchaus entgegenstehen. Dies ist insbesondere dann der Fall, wenn die Verwendung der personenbezogenen Daten zu KI-Zwecken für die betroffenen Personen nicht vorhersehbar war oder wenn die Verarbeitung nicht als angemessen erscheint. Bürgerinnen und Bürger müssen nicht grundsätzlich damit rechnen und es auch nicht generell akzeptieren, dass alle über sie im Internet verfügbaren Daten frei zum Training von KI eingesetzt werden.

Der Einsatz eines KI-Modells, das unter Verstoß gegen Datenschutzrecht trainiert wurde, in einem KI-System durch Dritte wird von der

Stellungnahme des EDSA nicht in jedem Fall kategorisch ausgeschlossen. Jedoch treffen die Endanwender im Rahmen der Auswahl der von ihnen verwendeten KI-Modelle in einem solchen Fall erhöhte Sorgfaltspflichten. Rechtswidrig trainierte KI-Modelle können nicht bedenkenlos verwendet werden.

Zusammenfassend lässt sich festhalten, dass nicht alle datenschutzbezogenen Rechtsfragen im Hinblick auf KI von der EDSA-Stellungnahme abschließend beantwortet werden. Angesichts der Komplexität und Dynamik der Debatte war eine abschließende Befassung in der Kürze der im Verfahren vorgesehenen Zeit aber auch nicht zu erwarten. Auf der Grundlage der gesetzlichen Regelungen und der durch die EDSA-Stellungnahme vorliegenden Weichenstellungen ist es künftig die Aufgabe der Datenschutzaufsichtsbehörden, die verbleibenden Fragen weiter zu bearbeiten und auf eine koordinierte Rechtsanwendung in Deutschland und Europa hinzuwirken.

3. SCHWERPUNKT: INNERE SICHERHEIT

Das Jahr 2024 war in besonderer Weise geprägt durch sicherheitspolitische Debatten, die allzu oft in der Forderung mündeten: Mehr Befugnisse für Polizei und Sicherheitsbehörden, weniger Einschränkungen durch den Datenschutz. Wer so verkürzt argumentiert, verkennt die grundlegende Funktion des Datenschutzrechts als Garant für individuelle Grund- und Freiheitsrechte. Angesichts vorschnell und hitzig vorgebrachter Rufe nach Maßnahmen wie automatisierter Datenanalyse, KI-gestützter biometrischer Gesichtserkennung oder – wieder einmal – der Vorratsdatenspeicherung habe ich mit meinem Team zentrale Thesen zur Vereinbarkeit von Datenschutz und Sicherheit formuliert, die ich im Folgenden ausführe.

3.1 Datenschutz als Unterstützung für eine freiheitswahrende Sicherheit

Die Daueraufgabe des Ausgleichs von Freiheit und Sicherheit erfordert eine effektive Sicherstellung des Grundrechtsschutzes einschließlich des Rechts auf informationelle Selbstbestimmung. Datenschutz ist dabei ein Erfolgsfaktor für eine effektive und gleichsam verhältnismäßige Sicherheitsgewährleistung. Die Informationsgewinnung, der Informationsaustausch und der Vorhalt von Informationen in polizeilichen Dateien und Informationssystemen bilden das Fundament einer effektiven polizeilichen Arbeit. Datenschutz gewährleistet die Qualität dieser Daten und die Vertraulichkeit und Integrität der Informationen der Sicherheitsbehörden. Datenschutz stellt sicher, dass die besonders eingreifenden Befugnisse und Maßnahmen lediglich Beschuldigte und Verursacher von Gefahren treffen und nicht oder nur in einem zumutbaren Maß unbeteiligte Dritte. Datenschutz und seine Prinzipien, wie die Zweckbindung, bewahren die Sicherheitsbehörden davor, in einem Gemenge von unstrukturierten, veralteten und unterschiedlich relevanten Daten agieren zu müssen. Die Interessen des Datenschutzes und der Strafverfolgung treffen sich in der Sicherstellung einer hohen Datenqualität.

3.2 Datenschutzaufsicht als Freiheitsgarant der Sicherheitsarchitektur

Insbesondere das Bundesverfassungsgericht hat die Funktion der Datenschutzaufsichtsbehörden als integralen Bestandteil der Sicherheitsarchitektur etabliert, um den betroffenen Personen einen nachträglichen und / oder kompensierten Rechtsschutz zu gewähren. Durch Kontrollen, Anhörungen, aber auch Konsultationen und Beratungen gewährleisten die Datenschutzaufsichtsbehörden, dass die

Datenschutzanforderungen des Verfassungsrechts und der einschlägigen Richtlinie (EU) 2016/680 in die polizeiliche Datenverarbeitung und Informationslandschaft integriert werden. Diese elementaren Aufgaben erfordern Expertise und Ressourcen. Damit die Datenschutzaufsichtsbehörden ausreichend handlungsfähig sind, ist es daher zwingend erforderlich, diese mit ausreichenden Mitteln auszustatten.

3.3 Datenschutz als Korridor für eine moderne und effektive Polizeiarbeit

Mit dem Projekt Polizei 2020 soll die Informationsarchitektur der Sicherheitsbehörden modernisiert und effektiviert werden. Damit werden derzeit wichtige Leitplanken der Polizeien des Bundes und der Länder erarbeitet, um nachhaltig Sicherheit und gleichsam Daten- und Grundrechtsschutz gewährleisten zu können. Datenschutz wurde als ein Ziel des Projekts festgelegt und sollte auch ein Bestandteil bleiben. Die Datenschutzaufsichtsbehörden stehen ihren Aufgaben entsprechend für eine konstruktive Beratung und Sensibilisierung (weiterhin) zur Verfügung.

3.4 Datenschutz für moderne und nachhaltige Sicherheitsgesetzgebung

Durch das sogenannte Sicherheitspaket sollte im Jahr 2024 das Instrumentarium der Sicherheits- und Strafverfolgungsbehörden erheblich erweitert werden. Insbesondere wurde die Forderung formuliert, sowohl ein Verfahren der automatisierten Datenanalyse als auch Systeme zur Identifizierung im virtuellen Raum zu ermöglichen.

Verfahren zur automatisierten Datenanalyse können einen Mehrwert für die polizeiliche Informationsverarbeitung bieten, sie unterliegen dabei jedoch verfassungsrechtlichen Grenzen und die Anforderungen an Eingriffsschwellen, Rechtsgüterschutz und Verfahrensvorkehrungen sind aufgrund der erheblichen Eingriffsintensität ausdifferenziert und hoch. Der Einsatz von komplexen Algorithmen und Komponenten Künstlicher Intelligenz wird zudem die Beachtung der gesteigerten Anforderungen der KI-Verordnung erfordern.

Das sogenannte Sicherheitspaket, das sowohl die Sicherheitsbehörden des Bundes als auch die Strafverfolgungsbehörden der Länder betrifft, sah Befugnisse zur automatisierten Datenanalyse vor, die diese Maßgaben unzureichend umsetzen und damit die Grundrechte zahlreicher Unbeteiligter gefährden würden, anstatt ein sinn- und maßvolles Instrumentarium gegen schwere Verbrechen und Terrorismus zu bieten. Die je nach Eingriffsgewicht variierenden Vorgaben des Bundesverfassungsgerichts bieten die Handhabe, für Legislative und Exekutive eine der Zielerreichung dienende und gleichzeitig möglichst grundrechtsschonende Bestimmung des sinnvollen Regelungsgehalts der Eingriffsbefugnis vorzunehmen. Nicht zuletzt sollte die automatisierte Datenanalyse auch dem Datenschutz dienen und die Gewährleistung von Transparenz und die Inanspruchnahme der Betroffenenrechte der Bürgerinnen und Bürger unterstützen.

Vorsicht sollte grundsätzlich beim Einsatz von Gesichtserkennungssystemen durch Sicherheitsbehörden geübt werden. Im sogenannten Sicherheitspakt sollten Befugnisse zur biometrischen Gesichtserkennung im Internet geschaffen werden. Diese liefen konträr zum expliziten Verbot der KI-Verordnung, Datenbanken zur Gesichtserkennung durch das ungezielte KI-basierte Auslesen von Gesichtsbildern aus dem Internet zu erstellen. Wenn Regelungen zur Gesichtserkennung und biometrischen Fernidentifizierung retrograd, in Echtzeit, im Internet oder im öffentlichen Raum geschaffen werden sollen, sind die hohen Grenzen des Verfassungs- und europäischen Rechts zu wahren,

um die grundrechtlichen Risiken insbesondere für unbeteiligte Bürgerinnen und Bürger einzudämmen.

4. EUROPA

4.1 Die Arbeit des Europäischen Datenschutzausschusses

Der Europäische Datenschutzausschuss (EDSA) hat zur Aufgabe, die einheitliche Anwendung der Datenschutz-Grundverordnung sicherzustellen. Dazu stehen ihm unterschiedliche Instrumente zur Verfügung, etwa das Erarbeiten von Leitlinien oder gemeinsamer Stellungnahmen. Zudem wurden Initiativen etabliert, die die einheitliche Anwendung der Datenschutz-Grundverordnung in den europäischen Mitgliedsstaaten fördern sollen. Auf ausgewählte Ergebnisse und Veröffentlichungen des EDSA aus dem Jahr 2024 möchte ich im Folgenden hinweisen.

Im Januar hat der EDSA seinen Bericht zur CEF-Aktion „Coordinated Enforcement Action, Designation and Position of Data Protection Officers“ veröffentlicht. Das Coordinated Enforcement Framework trägt seit seiner Gründung im Jahr 2020 zu einer intensiveren Kooperation der europäischen Datenschutzaufsichtsbehörden bei. Der Bericht zur CEF-Aktion 2023, die die Benennung und Rolle von Datenschutzbeauftragten zum Gegenstand hatte, problematisiert insbesondere die mangelnden Ressourcen, die teils fehlende Unabhängigkeit und die unzureichende Einbindung der Datenschutzbeauftragten. Zugleich schlägt er Maßnahmen zur Verbesserung vor. Der Bericht steht unter **www.s.rlp.de/cef2023** zum Download zur Verfügung.

Der EDSA führte im Jahr 2024 zahlreiche Opinion-Verfahren durch und erarbeitete infolgedessen Stellungnahmen zu Angelegenheiten und Rechtsfragen von allgemeiner Geltung. Besondere Bedeutung für den wirtschaftlichen Bereich hat die Stellungnahme 04/2024 zum Begriff der Hauptniederlassung eines Verantwortlichen in der Union gemäß Artikel 4 Absatz 16 Buchstabe a der DSGVO. Der EDSA kommt in dieser Stellungnahme zu dem Schluss, dass der „Ort der Hauptverwaltung“ eines Verantwortlichen in der Union nur dann als Hauptniederlassung angesehen werden kann, wenn dort die Entscheidungen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten getroffen werden und wenn sie befugt ist, diese Entscheidungen umsetzen zu lassen.

Die für die Praxis äußerst wichtige Stellungnahme 08/2024 zur „Wirksamkeit von Einwilligungen im Kontext von ‚Consent or Pay‘-Modellen großer Online-Plattformen“ beleuchtet die Vorgaben der Datenschutz-Grundverordnung, die bei diesem Geschäftsmodell zu beachten sind. Herausforderungen und Anforderungen stellen sich dabei insbesondere in Bezug auf die Freiwilligkeit der Einwilligung.

Mit Hochdruck wurde Ende des Jahres an der EDSA-Stellungnahme „Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models“ vom 17. Dezember 2024 gearbeitet. Die Stellungnahme behandelt wesentliche Grundfragen der Anwendung des Datenschutzrechts auf Künstliche Intelligenz und war für mich als Vorsitz des AK KI von besonderer Bedeutung. Näheres zu dieser Stellungnahme findet sich unter Punkt 2.5 dieser Einleitung.

Seine künftige strategische Ausrichtung hat der EDSA in seinem Strategiepapier für die Jahre 2024-2027 formuliert, das sich in vier Säulen aufstellt:

- Säule 1 – Verbesserung der Harmonisierung und Förderung der Einhaltung der Vorschriften,
- Säule 2 – Stärkung einer gemeinsamen Durchsetzungskultur und effektiven Zusammenarbeit,

- Säule 3 – Datenschutz bei der Entwicklung der digitalen und regulierungsübergreifenden Landschaft,
- Säule 4 – Beitrag zum globalen Dialog über Datenschutz.

Untermauert hat der EDSA diese Strategie mit einem Arbeitsprogramm, das die Ziele für die Jahre 2024 und 2025 festhält. Ein besonderes Augenmerk will der EDSA auf das Verhältnis der Datenschutz-Grundverordnung zu den weiteren Digital-Rechtsakten der EU legen. Spannend ist dabei vor allem das Verhältnis der KI-Verordnung zum Datenschutzrecht sowie die dort vorgesehenen Aufsichtsstrukturen zur Datenschutzaufsicht. Mit seiner Erklärung 3/2024 zur Rolle der Datenschutzbehörden im Rahmen der Verordnung über Künstliche Intelligenz führt der EDSA an, dass die Datenschutzaufsichtsbehörden geeignete Kandidaten für die Rolle der Marktüberwachungsbehörden unter der KI-VO seien. Ohnehin ist dies für Hochrisiko-KI-Verfahren im Bereich Sicherheit, Justiz, Migration und Wahlen schon durch Art. 74 Abs. 8 KI-VO vorgesehen.

Zum EU-U.S. Data Privacy Framework hat der EDSA sowohl für die betroffenen Personen als auch für europäische Unternehmen FAQs erstellt.

Mit Verabschiedung der „Leitlinie 1/2024 zum berechtigten Interesse gem. Art. 6 Abs. 1 lit. f DS-GVO“ haben komplexe Arbeiten insbesondere der Key-Provision-Expert-Subgroup ihren vorläufigen Abschluss gefunden. Die Leitlinien sind wichtig, um die Anwendung der praxisrelevanten und gleichwohl sehr unbestimmten Rechtsgrundlage rechtssicher zu gewährleisten. Dabei bietet insbesondere der 3-stufige Ansatz eine Orientierung für die Verantwortlichen. Aufgrund der Praxisrelevanz wurde die Leitlinie einer öffentlichen Konsultation unterzogen. Diese wird im kommenden Jahr ausgewertet und die Leitlinien ggf. angepasst.

4.2 Ergebnisse der Coordinated-Enforcement-Aktion 2024 zum Auskunftsrecht

Das Coordinated Enforcement Framework (CEF) wurde im Jahr 2020 durch den Europäischen Datenschutzausschuss (EDSA) gegründet, um die Kooperation der Aufsichtsbehörden in Europa, die einheitliche Durchsetzung der Datenschutz-Grundverordnung und die Arbeiten des EDSA zu fördern.

Im Jahr 2024 hat der EDSA die Umsetzung des Auskunftsrechts als Thema seiner dritten koordinierten Aktion ausgewählt. Das Auskunftsrecht ermöglicht es Einzelpersonen zu überprüfen, ob ihre personenbezogenen Daten von Organisationen gesetzeskonform verarbeitet werden. Es ist eines der wichtigsten und am häufigsten ausgeübten Rechte der Bürgerinnen und Bürger und fungiert regelmäßig als Türöffner für die Ausübung anderer Betroffenenrechte, etwa des Rechts auf Berichtigung und Löschung. Oft münden die entsprechenden Vorgänge in Beschwerden bei den Datenschutzaufsichtsbehörden.

In Deutschland beteiligten sich neben meiner Behörde die Landesdatenschutzaufsichtsbehörden aus Bayern (BayLDA), Brandenburg, Mecklenburg-Vorpommern, Niedersachsen, Saarland und Schleswig-Holstein sowie die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und prüften insgesamt 116 Verantwortliche. Insgesamt werteten die beteiligten 30 Aufsichtsbehörden auf EU-Ebene Angaben von 1.185 Verantwortlichen aus.

Der Gesamtbericht des EDSA beleuchtet positive Erkenntnisse und Best Practices, identifiziert aber auch Nachbesserungsbedarf und weiterhin bestehende Herausforderungen.

Positive Erkenntnisse

- Die Leitlinien 01/2022 zum Auskunftsrecht haben sich insbesondere bei nicht-

öffentlichen Verantwortlichen als wertvolles Instrument erwiesen. Bei vielen Verantwortlichen wurden Geschäftsprozesse und Praktiken etabliert, die in den Leitlinien empfohlen wurden: z.B. die Einführung von Antrags-Formularen oder die interne Schulung der Mitarbeitenden, um ein reibungsloses Auskunftsverfahren sicherzustellen.

- Verantwortliche haben ihre Prozesse zur Gewährleistung des Auskunftsrechts durch technische Lösungen optimiert, z.B. durch Nutzung von spezieller Software oder Anwendungen, um die Auskunftsanträge und die Prozesse zur Gewährleistung der Auskünfte zu managen und nicht zuletzt auch zu dokumentieren.

- Als Best Practices wurde identifiziert, dass zum Zwecke der Gewährleistung einer umfassenden und zeitnahen Auskunft in den einzelnen Abteilungen zuständige Personen festgelegt wurden, die mit den Anträgen umgehen sollen. Bei anderen Verantwortlichen wurde ein Team etabliert, das für die Zusammenstellung der Informationen und Gewährleistung des Auskunftsrechts zuständig ist bis hin zur Eskalation in die Rechtsabteilung oder zum Datenschutzbeauftragten hin.

- Eine besonders betroffenenfreundliche Umsetzung des Auskunftsrechts erfolgt bei vielen Verantwortlichen durch die Zurverfügungstellung von Formularen, um die Geltendmachung des Auskunftsrechts für die betroffenen Personen zu erleichtern und gleichzeitig sicherzustellen, dass alle relevanten Informationen der betroffenen Person mitgeteilt werden. Außerdem wurde bei einigen Verantwortlichen die Möglichkeit der Nutzung von Self-Service-Portalen etabliert, in denen die Daten heruntergeladen werden können, um dem Recht auf Auskunft effektiv und fristgerecht zu nachzukommen (mit Verifizierungstool).

- Einige Verantwortliche stellen den betroffenen Personen ergänzende Informationen zur Verfügung, um die beauskunfteten Daten zu erläutern.

- Durch Veröffentlichung der in Bezug auf das Auskunftsrecht etablierten Geschäftsprozesse auf der Webseite schaffen Verantwortliche eine stärkere Transparenz für die betroffenen Personen.

Nachbesserungsbedarf und Empfehlungen

- Die Reichweite des Auskunftsrechts wurde in den vergangenen Jahren durch Rechtsprechung des EuGH und durch die Leitlinien des EDSA stärker konkretisiert. Trotzdem sind sich viele Verantwortliche der Reichweite und Bedeutung des Betroffenenrechts nicht bewusst. Dies hat vielerorts zur Folge, dass das Recht in unzulässiger Weise beschnitten wird, etwa wenn nicht alle Datenkategorien beauskunftet oder keine vollständigen Kopien zur Verfügung gestellt werden, obwohl dies zur Kontextualisierung der Daten erforderlich wäre.

- Auskunftsanträge und begleitende Kommunikation sollten nicht mit den sonstigen Geschäfts- oder Verwaltungsvorgängen aufbewahrt werden, die die betroffene Person betreffen. Viele Verantwortliche handhabten dies anders mit der Konsequenz, dass Informationen zu langen Speicherfristen unterlagen und der Zugriff nicht dem Zweck entsprechend begrenzt wurde.

- Insbesondere bei kleinen Unternehmen und Behörden wurde festgestellt, dass keine internen Geschäftsprozesse zur Gewährleistung des Auskunftsrechts etabliert wurden. Dies kann dazu führen, dass Auskünfte falsch eingeordnet und verspätet erteilt werden.

- Einige Verantwortliche stellten zum Teil unzulässige Hürden für die Geltendmachung des Auskunftsrechts auf, etwa indem pauschal Zusatzinformationen oder im Einzelfall nicht erforderliche Identifikationsdokumente bei der betroffenen Person angefordert wurden.

- Die gesetzlichen Einschränkungen des Auskunftsrechts werden von vielen Verantwortlichen zu extensiv ausgelegt. So wurden Auskunftsanträge bereits dann als offenkundig unbegründet abgelehnt, wenn die Anträge zu unpräzise waren, hohe Kosten verursachten oder damit andere Ziele verfolgt wurden als die des Datenschutzes. Dies steht nicht im Einklang mit der betreffenden Rechtsprechung des EuGH.

- Viele Datenschutzaufsichtsbehörden stellten fest, dass im Fall eines unspezifischen Auskunftsantrags um Präzisierung gebeten wurde, ohne zuvor die Informationssysteme und Dateien des Verantwortlichen nach Daten zu überprüfen. Damit lagen die die Präzisierung flankierenden Anforderungen in Erwägungsgrund 63 Satz 7 DS-GVO nicht vor. Die Möglichkeit zur Präzisierung sollte nicht dazu genutzt werden, das Auskunftsrecht einzuschränken oder Informationen vor der betroffenen Person zu verbergen. Daher wird empfohlen, der betroffenen Person zeitgleich mit der Bitte um Präzisierung Informationen zur Verfügung zu stellen über die Datenverarbeitungstätigkeiten, die die betroffene Person betreffen könnten.

- Außerdem wurde in vielen Fällen festgestellt, dass die Informationen nach Art. 15 Abs. 1 und Abs. 2 DS-GVO nur unzureichend auf die betroffenen Personen zugeschnitten sind. Teilweise wurden schlichtweg die allgemeinen Informationen nach Art. 13, 14 DS-GVO zur Verfügung gestellt. Dies betraf insbesondere Informationen über die Empfänger der personenbezogenen Daten oder die Angabe der Speicherdauer ohne Unterscheidung zwischen Verarbeitungstätigkeiten oder Datenkategorien und steht nicht im Einklang mit der Rechtsprechung des EuGH vom 12.01.2023 (Rs. C-154/21, Österreichische Post).

Den identifizierten Herausforderungen stellt der CEF-Bericht spezifische Empfehlungen gegenüber. Verantwortliche sollten schon im Rahmen des Datenschutzmanagements sicherstellen, dass ausreichende Vorkehrungen für eine umfassende und zeitgerechte Auskunft getroffen werden. Dazu zählt die Kenntnis über die grundlegenden Datenbanken und Datenverarbeitungen und die Festlegung von Geschäftsprozessen zur Gewährleistung des Auskunftsrechts.

Die Aufsichtsbehörden werden aufgefordert, die praxisrelevanten Leitlinien 01/2022 und die einschlägige Rechtsprechung des EuGHs weiter zu verbreiten und die Verantwortlichen zu sensibilisieren. Insbesondere zu dem Feld der Einschränkungen des Auskunftsrechts sollen die Leitlinien zudem noch um Best Practices und Fallbeispiele ergänzt werden, um den Verantwortlichen eine stärkere Orientierung zu bieten.

Die gewonnenen Erkenntnisse und europaweit abgestimmten Handlungsempfehlungen geben den Aufsichtsbehörden die Gelegenheit, auf breiterer Grundlage zu handeln. Das Spannungsverhältnis zwischen effektiver Verwirklichung des Rechts und Begrenzung des Aufwands für die Verantwortlichen kann mit gezielten Maßnahmen zu großen Teilen aufgelöst werden. Damit kommt die europaweite Kooperation der Aufsichtsbehörden und die gebündelte Expertise, die in den Bericht der CEF-Aktion geflossen ist, den Verantwortlichen und damit wiederum den betroffenen Personen zugute.

5. ÖFFENTLICHKEITSARBEIT

5.1 Festakt „50 Jahre Landesdatenschutzgesetz“

Das Landesdatenschutzgesetz feierte im Jahr 2024 ein großes Jubiläum: Seit 50 Jahren verankert es den Datenschutz in Rheinland-Pfalz. Als das rheinland-pfälzische Landesdatenschutzgesetz am 25. Januar 1974 in Kraft trat, war der Landtag Rheinland-Pfalz der erst dritte Gesetzgeber weltweit, der mutig und vorausschauend eines der zentralen Themen des 20. und 21. Jahrhunderts anging. Das 50. Jubiläum des Landesdatenschutzgesetzes habe ich am 7. Februar 2024 mit einem Festakt im rheinland-pfälzischen Landtag in Mainz mit rund 100 geladenen Gästen gefeiert. Zu den Gästen aus Politik, Gesellschaft, Wirtschaft und Verwaltung zählte auch der frühere rheinland-pfälzische Ministerpräsident Rudolf Scharping, der in den 1970er Jahren als junger Landtagsabgeordneter in der Datenschutzkommission mitgewirkt hatte.

Die anhaltende Relevanz des richtungsweisenden Gesetzes würdigte die Vizepräsidentin des Landtags Kathrin Anklam-Trapp in ihrem Grußwort. Sie hob die Bedeutung der Arbeit der Datenschutzkommission hervor, in der sich von den Fraktionen entsandte Landtagsabgeordnete sowie eine Vertretung der Landesregierung für den Datenschutz engagieren.

Die rheinland-pfälzische Ministerpräsidentin Malu Dreyer betonte die Bedeutung des Datenschutzes im Kontext der Bürgerrechte. Sie legte dar, dass das Landesdatenschutzgesetz seit einem halben Jahrhundert ein Eckpfeiler des gemeinsamen Bemühens um den Schutz der Privatsphäre und der informationellen Selbstbestimmung sei. Insbesondere in einer Zeit der Digitalisierung seien die Datenschutzvorgaben von zentraler Bedeutung. Sie schafften klare Regeln und Standards für den Umgang mit personenbezogenen Daten in digitalen Prozessen.

Anu Talus, Vorsitzende des Europäischen Datenschutzausschusses, stellte in einer Videobotschaft die Bedeutung des Datenschutzes als europäisches Projekt heraus. Sie betonte, wie wichtig die jahrzehntelange Erfahrung der rheinland-pfälzischen und weiteren deutschen Datenschutzaufsichtsbehörden für die Zusammenarbeit auf europäischer Ebene sei.

Die Festrede hielt der Politikwissenschaftler und Autor Adrian Lobe. Er machte deutlich, wie zentral ein wacher und kritischer Umgang mit Daten und dem Recht auf informationelle Selbstbestimmung in unserer digitalisierten Gesellschaft ist. Und er skizzierte, wie die europäische Idee des Datenschutzes sich zum Standortvorteil entwickeln könne.

5.2 Veranstaltungen

Das Thema Künstliche Intelligenz dominierte mit weitem Abstand die zahlreichen Vorträge, Tagungen, Diskussionsrunden und weiteren Veranstaltungen, die ich mit meinem Team im Jahr 2024 organisierte oder zu denen ich als Vortragender eingeladen war. Eine Auswahl der von meiner Behörde angebotenen Veranstaltungen aus dem Jahr 2024 sind im Folgenden näher vorgestellt.

KI-Veranstaltungsreihe mit den Industrie- und Handelskammern

In Kooperation mit den vier rheinland-pfälzischen Industrie- und Handelskammern (IHK) veranstalteten wir über das Jahr hinweg Vortrags- und Diskussionsformate in Trier, Koblenz, Mainz und – im ersten Quartal 2025 – Kaiserslautern. Die vier Veranstaltungen richteten sich an Mitglieder der Kammern. Im Zentrum der Formate stand die Frage des Einsatzes von Systemen künstlicher Intelligenz in der Wirtschaft, insbesondere in kleinen und mittleren Unternehmen (KMU). Im interdisziplinären Austausch mit Wissenschaftler:innen und Praktiker:innen aus der Unternehmenswelt war

es mir wichtig, die Chancen des datenschutzkonformen Einsatzes von KI-Tools zu betonen, ohne die Risiken außer Acht zu lassen. Aus der Veranstaltung bei der IHK für Rheinhessen im November 2024 ging ein dreiteiliger Podcast „KI im Mittelstand" hervor, der unter **www.s.rlp.de/podcast-KI-mittelstand** zum Nachhören bereitsteht.

Runder Tisch der rheinland-pfälzischen Wirtschaft

Am 7. Oktober 2024 lud ich zum 4. Runden Tisch der rheinland-pfälzischen Wirtschaft ein. Im Zentrum des Austauschs standen sowohl Dauerbrenner des Datenschutzes als auch Themen, die durch aktuelle Rechtsprechung oder Gesetzgebung in Bewegung waren. Gastgeberin war die Debeka in Koblenz.

Auf der Tagesordnung des Treffens standen Themen mit hoher Aktualität und konkretem Praxisbezug für größere ebenso wir für kleinere und mittlere Unternehmen. Dazu zählte ein Beitrag aus der unternehmerischen Praxis zur Prüfung von KI im Rahmen der Datenschutz-Folgenabschätzung sowie Beiträge aus behördlicher Sicht zu automatisierten Entscheidungen im Einzelfall im Lichte des Schufa-Urteils und zu aktuellen Entwicklungen im Auskunftsrecht sowie im Umgang mit sogenannten Datenpannen.

Eröffnet wurde die Veranstaltung durch ein Grußwort von Annabritta Biederbick, Vorständin der Debeka, sowie von Regierungsrätin Dr. Marlene Gottwald vom Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau des Landes Rheinland-Pfalz.

Freiheit vs. Sicherheit: „Nicht jedes technische Mittel darf reflexartig für die Polizeiarbeit gefordert und genutzt werden"

Das Spannungsverhältnis zwischen Freiheit und Sicherheit stand im Zentrum des Film- und Diskussionsabends „Watching You", den ich am 17. Oktober im Kino CinéMayence in Mainz veranstaltete. Anlässlich des 40. Jahrestags der fiktiven Gegenwart von George Orwells Roman „1984" sprach ich mit dem Präsidenten des Landeskriminalamts Mario Germano sowie dem Autor Adrian Lobe über die Überwachungswirklichkeit in Deutschland.

Der Dokumentarfilm WATCHING YOU – DIE WELT VON PALANTIR UND ALEX KARP (Deutschland 2024) vertiefte schließlich die kritische Auseinandersetzung mit globalen Überwachungsinteressen. Der Dokumentarfilm forscht anhand der US-Firma Palantir und deren Gründer Alex Karp dem Zusammenhang von Überwachung, Politik und Wirtschaft nach. Das öffentlich zurückhaltend auftretende Unternehmen entwickelt und vermarktet Datenanalyse-Software, die weltweit von Militärs und Polizeibehörden eingesetzt wird oder werden soll – auch in Deutschland.

Das große Interesse der Bürgerinnen und Bürger an der Veranstaltung belegte die Relevanz des Themas. So waren alle Tickets für den Film- und Diskussionsabend innerhalb weniger Tage vergriffen. Wir möchten das Spannungsverhältnis von Freiheit und Sicherheit weiterhin engagiert im Blick halten und zum öffentlichen Diskurs mit Publikationen und Veranstaltungen beitragen.

3. Datenschutztag Hessen & Rheinland-Pfalz: KI und kommende Herausforderungen

„Datenschutzbeauftragte auf Zukunftskurs" – so lautete das Motto des 3. Datenschutztags Hessen & Rheinland-Pfalz, zu dem am 25. Juni 2024 mehr als 200 behördliche, kommunale und betriebliche Datenschutzbeauftragte in Frankfurt am Main zusammenkamen. Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. hatte gemeinsam mit uns und dem Hessischen Beauftragte für Datenschutz und Informationsfreiheit (HBDI) zu der Konferenz eingeladen.

Einen inhaltlichen Schwerpunkt der Keynotes und Fachvorträge bildete der Einfluss neuer technischer und gesetzgeberischer Entwicklungen auf die Arbeit der Datenschutzbeauftragten – allen voran Künstliche Intelligenz und die KI-Verordnung, die sie reguliert.

Der Datenschutztag Hessen & Rheinland-Pfalz lud zu insgesamt 17 zum Teil parallel stattfindenden Keynotes, Fachvorträgen und Podiumsdiskussionen ein. Ein besonderes Merkmal der Tagung ist seit der Premiere vor drei Jahren die Gelegenheit für die Teilnehmenden, sich nicht nur untereinander auszutauschen, sondern mit ihren Fragen auch direkt an die Fachleute aus den Aufsichtsbehörden heranzutreten. Das gilt sowohl für die Tagungspausen als auch für das interaktive Abschlusspanel „Die Aufsichtsbehörden beantworten Ihre Fragen“. Die vierte Ausgabe des Datenschutztages Hessen & Rheinland-Pfalz wird am 2. Juli 2025 in Frankfurt am Main stattfinden.

13. Speyerer Forum zur digitalen Lebenswelt: Interdisziplinärer Austausch mit Rekordteilnehmerzahl

Mit der Rekordteilnahmezahl von rund 200 Teilnehmerinnen und Teilnehmern ging am 19. April 2024 das 13. Speyerer Forum zur digitalen Lebenswelt zu Ende. Zwei Tage lang hatten Expertinnen und Experten beleuchtet, wie Künstliche Intelligenz die Digitalisierung der Verwaltung beeinflussen kann – aktuell und zukünftig. Juristische Überlegungen, insbesondere zur KI-Verordnung, spielten dabei ebenso eine Rolle wie technische und gesellschaftliche Aspekte. Die etablierte Fachtagung wurde erneut von der Deutschen Universität für Verwaltungswissenschaften gemeinsam mit meiner Behörde sowie dem LfDI Baden-Württemberg und dem rheinland-pfälzischen Ministerium für Arbeit, Soziales, Digitalisierung und Transformation veranstaltet.

5.3 Kommunikation

Seit März 2024 präsentiert sich die Webseite meiner Behörde in neuem Design. Ziel der Überarbeitung war es, den Bürgerinnen und Bürgern einen leichteren, aktuellen und transparenten Zugang zu unseren Informationen zu bieten. Ein großes Plus der neuen Seite ist ihre Flexibilität. Sie erlaubt es uns, schnell auf wichtige Themen einzugehen und relevante Informationen für unsere Nutzerinnen und Nutzer hervorzuheben.

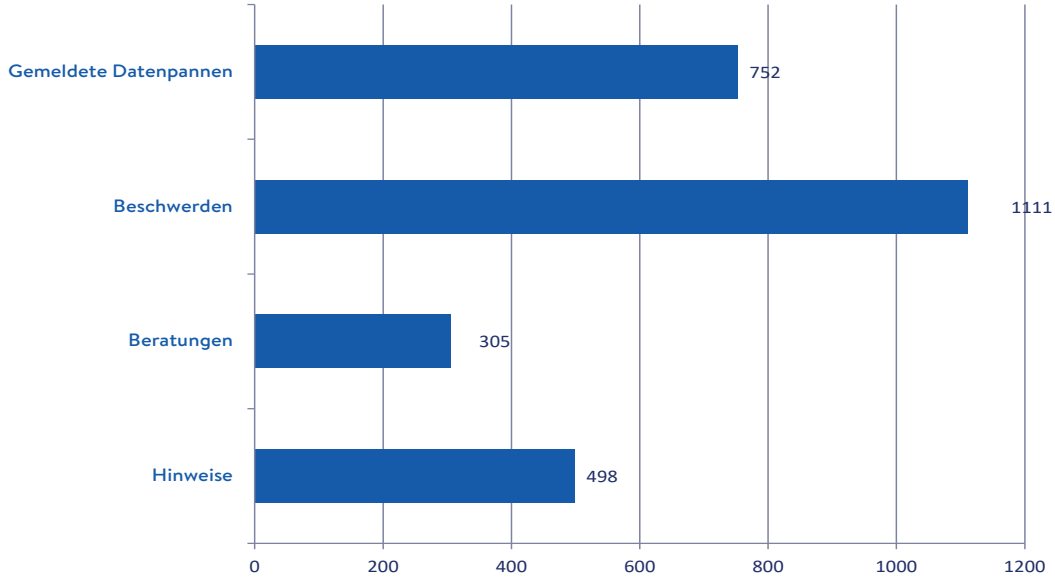
Auf **www.datenschutz.rlp.de** können Bürgerinnen und Bürger mit wenigen Klicks Beschwerden einreichen. Öffentliche und private Stellen können die Webseite nutzen, um schnell und nachvollziehbar Datenpannen zu melden. Die entsprechenden Online-Formulare sind ab sofort schon von der Startseite des neuen Webauftritts aus zugänglich.

Die neue Webseite ergänzt die Werkzeuge meiner Behörde für die Kommunikation mit den Bürgerinnen und Bürgern. Seit Oktober 2023 gehört ein eigener Account auf Mastodon, der datenschutzfreundlichen Alternative zum Kurznachrichtendienst X, dazu. Bereits seit 2020 vermittelt ein eigener Podcast namens „Datenfunk“ aktuelle datenschutzrechtliche Hintergründe im Audio-Format. Mit dem Relaunch der Webseite wurde auch der Newsletter meiner Behörde wiederaufgenommen.

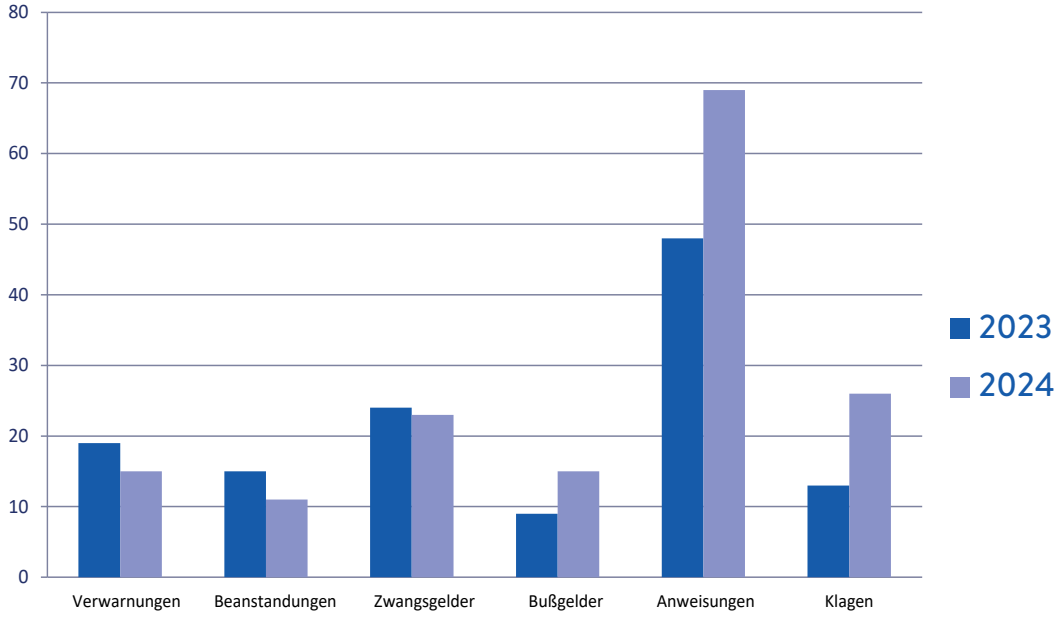
Anlass des Relaunches war der technisch notwendige Umzug auf eine neue Version des Redaktionssystems TYPO-3. Der LfDI konnte bei der Überarbeitung der Webseite auf die vom Landesbetrieb Daten und Information (LDI) entwickelte TYPO3-Zentralinstanz zurückgreifen. Das Hosting und der technische Betrieb der Webseite liegen weiterhin beim LDI.

II.
ZAHLEN UND FAKTEN

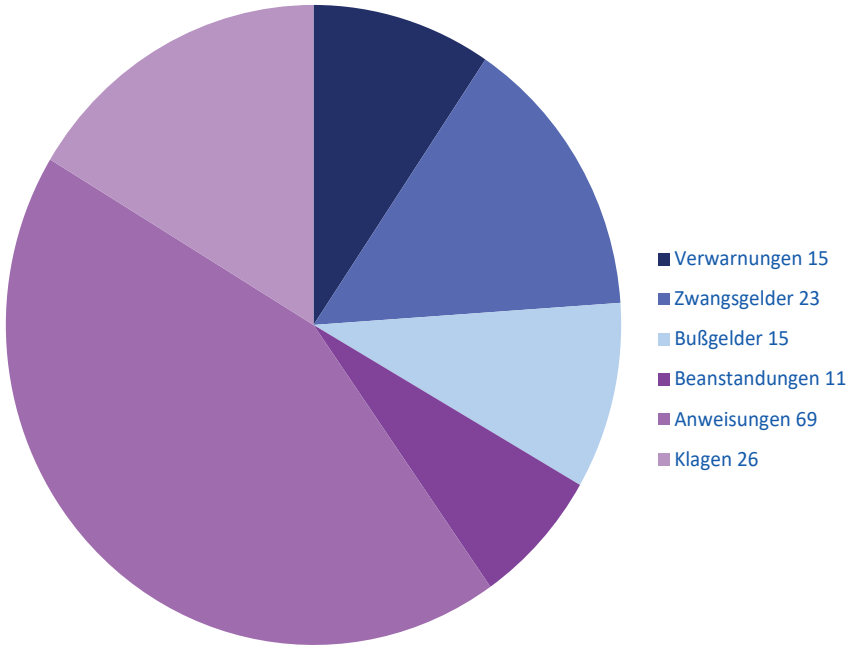
1. Geschäftsstatistik 2024



2. Ausgeübte Befugnisse 2023 und 2024



3. Ausgeübte Befugnisse 2024



III.
SACHGEBIETE

II. SACHGEBIETE

1. SICHERHEIT

1.1 Beratungen zu polizeilichen Verfahren und Gesetzgebung im Sicherheitsbereich

1.1.1 Polizeiliche Datenverarbeitungspraxis

Im Berichtszeitraum war die Beratung und Konsultation zu verschiedenen datenschutzrechtlichen Themen und Projekten erneut ein zentraler Bestandteil der Tätigkeit des LfDI Rheinland-Pfalz.

Besonders hervorzuheben ist die fortlaufende Begleitung des Projekts @rtus, einem Interims-Vorgangsbearbeitungssystem (iVBS) im Rahmen der Optimierung des Datenaustauschs und der Datenlandschaft der Polizeien des Bundes und der Länder im Projekt P 20. Auch hier steht der LfDI weiterhin in engem Austausch mit den Projektverantwortlichen, um die datenschutzrechtliche Konformität des Projekts sicherzustellen.

Darüber hinaus hat der LfDI in enger Abstimmung mit dem Arbeitskreis Sicherheit (AK Sicherheit) einen Leitfaden zum Auskunftsrecht betroffener Personen nach der Richtlinie 2016/680 (sog. JI-Richtlinie) entwickelt. Dieser wurde dem Ministerium des Innern und für Sport Rheinland-Pfalz zur Weitergabe an die nachgeordneten Stellen sowie die behördlichen Datenschutzbeauftragten zur Verfügung gestellt.

Im Tätigkeitsbericht 2023, Seite 22, Ziffer 1.1.2, hat der LfDI bereits die Ergebnisse seiner Prüfung zu besonders eingriffsintensiven Maßnahmen dargelegt. Dabei hatte der LfDI insbesondere die Überarbeitung der Benachrichtigungspraxis und des Benachrichtigungsformulars gefordert, um die Anforderungen klarer und rechtssicher zu gestalten. Die Pflicht zur Benachrichtigung bei besonders eingriffsintensiven Maßnahmen ergibt sich aus § 48 Abs. 2 POG und § 1a S. 3 POG i.V.m. § 44 Abs. 1 LDSG. Die Formularkommission des Landeskriminalamtes hat die Formulare entsprechend meiner Forderung überarbeitet. Die Einführung der überarbeiteten Formulare ist im ersten Quartal 2025 geplant.

1.1.2 Novellierung des Polizei- und Ordnungsbehördengesetzes – Freiheit soll auch im modernen Rechtsstaat erhalten bleiben!

Im Rahmen der Ressortanhörung wurde der LfDI Rheinland-Pfalz zu der jüngsten Novellierung des Polizei- und Ordnungsbehördengesetzes um Stellungnahme gebeten. Das Polizei- und Ordnungsbehördengesetz bestimmt in Rheinland-Pfalz den Rahmen, in dem die Polizeien und Ordnungsbehörden effektiv Sicherheit gewährleisten können unter gleichzeitiger Achtung der Freiheitsgrundrechte der Bürgerinnen und Bürger. Durch die kritische und gleichsam konstruktive Begleitung von Gesetzgebungsverfahren kann der LfDI frühzeitig prüfen, ob die Balance zwischen Freiheit und Sicherheit auch bei der Einführung neuer Befugnisse oder der Verschärfung bestehender Befugnisse gewahrt bleibt. Dies entspricht der Funktion der Behörde gem. § 41 Abs. 3 Nr. 3 LDSG, den Landtag und die Landesregierung über legislative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen auf die Verarbeitung personenbezogener Daten zu beraten.

Mit dem Gesetzentwurf zur Änderung des Polizei- und Ordnungsbehördengesetzes sollten die ordnungsbehördlichen und polizeilichen

Befugnisse – orientiert an den technischen Entwicklungen und aktuellen Gefahrenlagen – fortentwickelt und gezielt gestärkt werden, um auch künftig eine effektive Aufgabenerfüllung der Polizei- und Ordnungsbehörden zu gewährleisten. Im Rahmen des Ziels sah der Gesetzentwurf die Schaffung einer Reihe neuer Befugnissen sowie die Erweiterung bereits bestehender Befugnisse vor. Dies führt zu einer Ausweitung der Grundrechtseingriffe durch das Gesetz, insbesondere im Hinblick auf Befugnisse mit teils erheblicher Streubreite. Drei Änderungen sollen hier besonders herausgestellt werden.

Im Rahmen der Novellierung wurde in § 30 Abs. 8 des Entwurfs des POG eine Rechtsgrundlage zur Einführung der sogenannten Monocam geschaffen. Die Monocam ist ein intelligentes Kameraüberwachungssystem, das zur Überwachung des Handyverbots im Straßenverkehr eingesetzt wird. Dabei werden anlasslos Bilder von Fahrzeugführer:innen sowie deren Kennzeichen erfasst. Aufgrund der damit verbundenen Eingriffe in die Persönlichkeitsrechte der betroffenen Personen war es notwendig, für den Einsatz der Monocam eine klare und bereichsspezifische gesetzliche Grundlage zu schaffen. Auf diese Notwendigkeit hat der LfDI bereits während der Begleitung des Pilotverfahrens hingewiesen und ein solche gefordert. Vor diesem Hintergrund hat der LfDI die Einführung des § 30 Abs. 8 POG begrüßt, gleichwohl darauf hingewirkt, dass diese präventive Befugnis sich rechtstechnisch in das präventiv-polizeiliche Gesetz einfügt, indem es auf die Verhütung des Verstoßes der Handynutzung abzielt und nicht auf den Anfangsverdacht als Ausgangspunkt für die bildliche Erfassung der oder des Fahrzeugführenden.

Die Einführung körpernah getragener Videokameras (Bodycams) wurde durch den LfDI Rheinland-Pfalz seit der Pilotierung in den Jahren 2015 bis 2017 begleitet. Dabei ist der Gesetzgeber bedacht vorgegangen, indem zunächst der praktische Nutzen unter wissenschaftlicher Begleitung pilotiert und evaluiert wurde (siehe LT-Drs. 17/820). Dieses Vorgehen hatte zur Folge, dass empirisch belegt werden konnte, in welchen Einsatzszenarien und in welcher Funktionsweise der präventive Zweck der Bodycam erfüllt wird. Anhand dieser Einhegung hatte sich der rheinland-pfälzische Gesetzgeber bislang entschlossen, den verfassungsrechtlich bedenklichen Einsatz der Bodycams in Wohnungen sowie die Funktion des Pre-Recordings nicht zuzulassen. Mit der Novellierung 2024/2025 wurde diesbezüglich eine Richtungsänderung eingeschlagen: Der Einsatz der Bodycam sollte auch für die kommunalen Vollzugsbeamten möglich werden, zudem wurde die Funktion des Pre-Recordings eingeführt und der Einsatz in Wohnungen erlaubt. Insbesondere zur letzten Neuerung hat der LfDI erhebliche Bedenken geäußert. Zum einen sind zu vergleichbaren Regelungen derzeit noch Verfassungsbeschwerden anhängig, womit die Nachhaltigkeit dieser invasiven Einsatzmodalität fraglich ist, zum anderen bestehen erhebliche verfassungsrechtliche Bedenken, die die Geeignetheit der Maßnahme zur Erreichung des Eigensicherungs-Zwecks betreffen sowie die Einhaltung der grundrechtlichen Schranken des Art. 13 Abs. 5 GG.

Aufgrund der verfassungsrechtlichen Vorgaben des Art. 13 Abs. 1 GG wurde § 31 Abs. 2 POG so konzipiert, dass er im Spielraum der Schranken-Regelungen der Art. 13 Abs. 4 und 5 GG dem Zweck der Eigensicherung der beim Einsatz tätigen Personen dienen soll. In diesem Zusammenhang hat der LfDI positiv bewertet, dass sich dies im Wortlaut widerspiegelt und in der Folge der Einsatz ausschließlich zum Schutz der bei einem Einsatz in Wohnungen tätigen Personen zur Abwehr einer dringenden Gefahr für Leib und Leben erlaubt ist. Damit ist der Zweck enger gefasst als in vergleichbaren Regelungen in Bayern, im Saarland oder in Nordrhein-Westfalen. Jedoch ist der Einsatz von Bodycams in Wohnungen nicht auf die Eigensicherung zu beschränken. Angesichts der Ein-

satzszenarien in Wohnung fällt der Zweck der Eigensicherung unweigerlich mit der Verhütung der Straftaten an Opfern, z.B. im Fall von häuslicher Gewalt, zusammen. Vor diesem Hintergrund ist fraglich, ob in Bezug auf Bodycams überhaupt ein Anwendungsbereich von Art. 13 Abs. 5 GG verbleibt. Geschützt werden in der Wohnung tätige Personen, damit kann der Personenkreis über Polizeibedienstete hinaus erweitert werden, denn tätig werden können etwa auch ein Notarzt oder eine Psychologin. Dabei ist hervorzuheben, dass der Regelungszweck des Art. 13 Abs. 5 GG die Eigensicherungserfordernisse der verdeckt ermittelnden Personen in Wohnungen war. Dieses Schutzbedürfnis greift bei uniformierten und in der Regel in Begleitung agierenden Bediensteten der Polizei nicht. Die Regelung ist von Art. 13 Abs. 5 GG nicht gedeckt und damit nach Ansicht des LfDI verfassungswidrig.

Mit der Novellierung wurde zudem die Befugnis der automatisierten Datenanalyse (§ 65 a POG) eingeführt. In seiner Entscheidung zu HessenData hat das Bundesverfassungsgericht mit Urteil vom 16.02.2023 Anforderungen aufgestellt, um diese eingriffsintensive Befugnis verhältnismäßig zu regeln. Der LfDI Rheinland-Pfalz teilt zwar die Auffassung des Gerichts, dass durch eine automatisierte Datenanalyse oder -auswertung für die Verhütung von Straftaten relevante Erkenntnisse erschlossen werden können, die auf andere, grundrechtsschonendere Weise nicht gleichermaßen zu gewinnen wären, sowie die Folgerung, dass das Instrument damit nicht nur als ein geeignetes, sondern auch als ein erforderliches Mittel der polizeilichen Datenverarbeitung angesehen werden kann (BVerfG, Urteil vom 16.02.2023, 1 BvR 1547/19 und 1 BvR 2634/20, NJW 2023, 1196 (1199 Rn. 53)). Dabei sollte die automatisierte Datenanalyse jedoch einen angemessenen Grundrechtsschutz und Rechtssicherheit bieten, auf gesetzlicher Ebene und auf Ebene der Verwaltung. Dazu ist in der gesetzlichen Befugnis dem Grunde nach das Eingriffsgewicht insbesondere durch die Bestimmung von Art und Umfang der verarbeitbaren Daten und die Umschreibung der zugelassenen Methode der Datenanalyse festzulegen. Die Verwaltungsebene kann demgegenüber ermächtigt werden, nähere Regelungen organisatorischer und technischer Art zu treffen.

Diese durchaus variablen Leitplanken des Bundesverfassungsgerichts wurden im ersten Entwurf der Regelung nicht durchgehend eingehalten. Fundierte Kritik hat der LfDI in seiner Stellungnahme insbesondere im Hinblick auf die Ausgestaltung der Befugnis und die Eingriffsschwellen sowie die Reduzierung des Eingriffsgewichts bzgl. des Datenumfangs geübt. Dem Grunde nach überzeugend hat der LfDI dagegen die Regelungen der grundrechtssichernden Einschränkungen der Verfahren sowie die Vorgaben im Hinblick auf die Rollen und Berechtigungskonzepte bewertet, wobei dazu noch offene Fragen und Konkretisierungsbedarf bestehen. Im Jahr 2025 wird der LfDI die Operationalisierung und Einführung des Verfahrens der automatisierten Datenanalyse beratend und im Rahmen der eingeführten Anhörungsverpflichtung der Behörde weiter konstruktiv begleiten.

1.2 Beschwerden und Hinweise

1.2.1 Fehlerhafte Öffentlichkeitsfahndung: Unbeabsichtigte Veröffentlichung sensibler Daten durch IT-Panne

Unter einem Fahndungslink betrieb die Polizei eine Öffentlichkeitsfahndung zu einem Tankstellenräuber. Wohl aufgrund einer IT-Panne bei einem technischen Relaunch der Webseite waren dort zeitweise jedoch nicht bloß Fotos des Täters zu sehen, sondern – beim Aufruf der Vergrößerungsfunktion für die Bilder – auch Zeugnisfotokopien von gänzlich unbeteiligten Praktikant:innen, ein Lichtbild eines Polizeibe-

amten sowie ein Video zu einem mutmaßlichen Wohnungseinbruchsdiebstahl.

Auf den Hinweis eines Bürgers hin forderte der LfDI das zuständige Polizeipräsidium zur unverzüglichen Entfernung der fälschlich hinterlegten Dateien auf, was auch umgehend geschah. Die IT-Panne kam im Zusammenhang mit einer parallel zum Relaunch der Webseite stattfindenden Bewerbungsaktion der Polizei zustande. Zeugniskopien interessierter Praktikant:innen wurden zwischengespeichert, ohne dass dies erforderlich war, und wurden im Zuge des Relaunches unbeabsichtigt verlinkt. Die entsprechenden Einstellungen wurden seitens des Landesbetriebs Daten und Information (LDI) deaktiviert und alle zwischengespeicherten Zeugniskopien wurden sofort und unwiderruflich gelöscht.

1.2.2 Die Zulässigkeit von Lichtbildanforderungen im Bußgeldverfahren: Ein Fallbeispiel mit Besonderheiten

Immer wieder sieht sich der LfDI mit der Frage konfrontiert, ob bzw. unter welchen Voraussetzungen die Anforderungen von Lichtbildern bei den Meldebehörden durch die Verfolgungs- bzw. Ermittlungsbehörden zum Zwecke des Abgleichs mit „Blitzerfotos“ in einem straßenverkehrsrechtlichen Bußgeldverfahren datenschutzrechtlich zulässig sind. So war dies auch im vorliegenden Fall, der mehrere bemerkenswerte Besonderheiten aufwies. Zum einen wurden, nach Angaben des Beschwerdeführers, über soziale Netzwerke Freundschaftsanfragen von Mitgliedern der ermittelnden Dienstgruppe gestellt, um an sein Lichtbild zu gelangen. Zum anderen erfolgten Kontaktaufnahmen zu seinen Vorgesetzten, die über den üblichen Ermittlungsrahmen hinausgingen.

Der Fall begann mit dem Auftrag der Verfolgungsbehörde eines anderen Bundeslands an die rheinland-pfälzische Polizei, den verantwortlichen Fahrzeugführer zu ermitteln, nachdem sich die in Rheinland-Pfalz wohnhafte Halterin im Anhörungsverfahren nicht äußerte. Der Auftrag umfasste sowohl die Identifizierung des Fahrers als auch dessen Anhörung vor Ort.

Ein besonders heikler Aspekt des Falls ergab sich aus der Tatsache, dass der Beschwerdeführer selbst Angehöriger der rheinland-pfälzischen Polizei war.

Ermittlungen und Lichtbildanforderungen

Aufgrund seiner persönlichen Bekanntschaft einer Polizeibeamtin kam der Beschwerdeführer frühzeitig als Tatverdächtiger in Betracht. Obwohl die Polizei die Halteranschrift wiederholt ohne Erfolg aufgesucht hatte, ergab eine Recherche im Einwohnermelderegister, dass der Beschwerdeführer dort gemeldet war. Vor der Anhörung wurde sein Lichtbild bei der Einwohnermeldebehörde angefordert. Der Abgleich mit der Überwachungsaufnahme erhärtete den Verdacht.

Die Ermittlungen der Polizei stützten sich auf §§ 161, 163 StPO i.V.m. § 53 Abs. 1 OWiG. Im Rahmen dieser Befugnisse war es zur Aufgabenerfüllung erforderlich, eine Meldedatenabfrage gem. §§ 34 a Abs. 1, 38 Abs. 2 Bundesmeldegesetz zu der Halterin vorzunehmen, wobei festgestellt wurde, dass der Beschwerdeführer an derselben Meldeadresse wohnhaft ist. Diese Maßnahme war verhältnismäßig, da der Beschwerdeführer trotz mehrfachen Aufsuchens persönlich nicht angetroffen wurde.

Allerdings war die Lichtbildanforderung weder Bestandteil des Ermittlungsauftrags noch stand sie im Einklang mit den Anforderungen gemäß § 24 Abs. 2 Personalausweisgesetz i.V.m. dem Rundschreiben des Ministeriums des Innern und für Sport Rheinland-Pfalz zur „Vorlage und Übermittlung von Lichtbildern aus dem Pass- und Personalausweisregister im

Rahmen der Verfolgung von Straßenverkehrsordnungswidrigkeiten“, zuletzt geändert durch das Rundschreiben im Jahr 2002. Diese verlangen vor der Passbildanforderung eine schriftliche Anhörung des Betroffenen. Dies gebieten der sogenannte Direkterhebungsgrundsatz und das Gebot der Verhältnismäßigkeit.

Ungewöhnliche Ermittlungsmethoden und deren datenschutzrechtliche Bewertung

Nach Darstellung des Beschwerdeführers sollen Mitglieder der mit den Ermittlungen zum verantwortlichen Fahrer betrauten Dienstgruppe auch versucht haben, über Freundschaftsanfragen in sozialen Netzwerken Kontakt zum Beschwerdeführer aufzunehmen, um auf diesem Weg an dessen Lichtbild für einen Abgleich zu gelangen.

Darüber hinaus erfolgten im zeitlichen Zusammenhang mit den polizeilichen Ermittlungen Kontaktaufnahmen zu einem ehemaligen sowie dem aktuellen Vorgesetzten des Beschwerdeführers. Ziel dieser Erkundigungen soll nach dessen Darstellung gewesen sein, im Rahmen des Bußgeldverfahrens weitere Informationen über den Beschwerdeführer zu erhalten.

Unter Einhaltung bestimmter Anforderungen sind Recherchen im öffentlichen Teil sozialer Netzwerke durch die Polizeibehörden durchaus zulässig, allerdings nur unter einem Alias und in einer sicheren Umgebung. Das Verfahren gab dem LfDI die Gelegenheit, dies noch einmal in Erinnerung zu rufen. Die datenschutzrechtliche Untersuchung der Freundschaftsanfragen ergaben hingegen keine Hinweise darauf, dass diese zu dienstlichen Zwecken erfolgten. Es wurde daher von einer privaten Veranlassung ausgegangen. Der Algorithmus der sozialen Netzwerke könnte dabei eine Rolle gespielt haben. Da der Beschwerdeführer ebenfalls Polizeibeamter ist und möglicherweise aufgrund der Nähe der Wohnorte ein gemeinsamer Bekannten- bzw. Kollegenkreis wahrscheinlich war, konnte nicht ausgeschlossen werden, dass der Beschwerdeführer den Polizeibeamten durch das soziale Netzwerk vorgeschlagen wurde. Eine solche Datenverarbeitung zu privaten oder familiären Zwecken unterliegt jedoch aufgrund der Bereichsausnahme des Art. 2 Abs. 2 lit. c DS-GVO nicht dem Anwendungsbereich der Datenschutz-Grundverordnung und damit auch nicht der Aufsichtszuständigkeit des LfDI.

Anders fiel jedoch die datenschutzrechtliche Bewertung der Erkundigungen bei dem ehemaligen und aktuellen Vorgesetzten des Beschwerdeführers aus. Ermittlungen bei einem früheren Arbeitgeber oder Dienstherrn zu den persönlichen Verhältnissen im Zusammenhang mit einer Verkehrsordnungswidrigkeit sind in der Regel unüblich und im vorliegenden Fall auch nicht erforderlich. Die Weitergabe der dienstlich erlangten Kenntnisse über das Ordnungswidrigkeitenverfahren an die Vorgesetzten konnte nicht auf eine geeignete Rechtsgrundlage gestützt werden.

Dies wurde förmlich gegenüber dem betreffenden Polizeipräsidium festgestellt. Der Verantwortliche nahm das Verfahren zum Anlass, alle Beteiligten über die Bandbreite an unterschiedlichen datenschutzrechtrechtlichen Fragestellungen umfassend zu informieren.

1.2.3 Unzulässige Speicherung von Altverfahren im polizeilichen Vorgangsbearbeitungssystem POLADIS

Ein Rechtsanwalt wandte sich mit einer Beschwerde an den LfDI wegen der Datenverarbeitungspraxis der Polizei im Rahmen eines gegen ihn geführten Ermittlungsverfahrens.

In dem Verfahren wurde im Abschlussvermerk ein Vermerk zu früheren Ermittlungsverfahren dokumentiert, die seiner Behauptung nach von unzufriedenen ehemaligen Mandant:innen oder Prozessgegner:innen im Zusammenhang mit seiner anwaltlichen Tätigkeit angestoßen worden waren. Die Verfahren seien mangels

Anfangsverdachts eingestellt worden. Zudem waren die Vorwürfe, die im aktuell gegen den Rechtsanwalt geführten Strafverfahren erhoben wurden, nicht nur im polizeilichen Vorgangsbearbeitungssystem POLADIS, sondern auch im Informationssystem POLIS zur vorbeugenden Bekämpfung gespeichert worden. Die Verfahrensbeteiligten erhielten Akteneinsicht.

Der Rechtsanwalt richtete seine Beschwerde gegen die Dokumentation im Abschlussvermerk, die Speicherung in POLIS sowie gegen die Akteneinsicht. Aus seiner Sicht waren weder Dokumentation noch Speicherung der Daten erforderlich. Zudem sah er durch die Offenbarung der im Abschlussvermerk enthaltenen Altverfahren an Verfahrensbeteiligte einen Datenschutzverstoß, da dies anderen Verfahrensbeteiligten Zugang zu diesen Daten ermöglichte.

Bei der datenschutzrechtlichen Überprüfung war zunächst zwischen der Datenverarbeitung im polizeilichen Vorgangsbearbeitungssystem POLADIS, dem polizeilichen Informationssystem POLIS und dem Akteneinsichtsrecht zu unterscheiden.

Datenschutzrechtliche Prüfung der Speicherung im System POLADIS

Im polizeilichen Vorgangsbearbeitungssystem POLADIS erfolgt die Bearbeitung und Vorgangsverwaltung sämtlicher Ermittlungsverfahren und polizeilich relevanter Sachverhalte.

Die Dokumentation der Altverfahren im Abschlussvermerk des Vorgangs in POLADIS war unzulässig. Die Bearbeitung von Daten in POLADIS zu Zwecken der Vorgangsverwaltung und Dokumentation muss strikt von Daten zur Aufgabenerfüllung getrennt werden, um insbesondere die Regelungen zur Vorsorgespeicherung nach den § 52 Abs. 2-5 POG nicht zu umgehen. POLADIS unterscheidet insoweit zwischen Vorgangsverwaltungsdaten und Vorgangssachbearbeitungsdaten. Bei den dokumentierten Altverfahren handelte es sich um Vorgangsverwaltungsdaten.

Vorgangsverwaltungsdaten, die gegenüber den Vorgangssachbearbeitungsdaten einen erheblich geringeren Umfang an Einzelinformationen aufweisen, sind als solche zu verstehen, die ausschließlich zu Zwecken der Behördendokumentation gemäß § 485 S. 4 StPO i.V.m. § 52 Abs. 1 Alt 3 POG gespeichert werden. Die Bearbeitung von Daten zu Zwecken der Vorgangsverwaltung und Dokumentation ist strikt von Daten zur Aufgabenerfüllung zu trennen. Eine Verarbeitung dieser Daten zum Zwecke der Aufgabenerfüllung – wie das im vorliegenden Fall geschehen war – war daher unzulässig.

Speicherung im System POLIS

Die Datenspeicherung der Vorwürfe in POLIS war hingegen rechtmäßig.

Das Polizeiliche Informationssystem Rheinland-Pfalz (POLIS) ist ein Bestandteil des „Rheinland-pfälzischen Informations-, Vorgangsbearbeitungs-, Auswerte- und Recherchesystems“ (RIVAR). Funktional ist es Teil des gemäß § 2 Abs. 3 BKA-Gesetz als Zentralstelle zu unterhaltenden gemeinsamen elektronischen Datenverbunds zwischen Bund und Ländern (INPOL).

Die Speicherung beruhte auf § 52 Abs. 2 S. 1 POG, der es der Polizei ermöglicht, personenbezogene Daten von Personen, die einer Straftat verdächtig sind, zu speichern und anderweitig zu verarbeiten, soweit dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Diese Voraussetzungen lagen vor, da der Rechtsanwalt Straftaten von einigem Gewicht verdächtigt wurde und eine Wiederholungsprognose vorlag. Aufgrund der der Polizei zum gegenständlichen Strafverfahren vorliegenden Erkenntnisse konnte sie annehmen, dass der Rechtsanwalt mit hinreichender Wahrscheinlichkeit zukünftig weitere Straftaten begehen werde. Der Prognose stand auch nicht ent-

gegen, dass die Staatsanwaltschaft eine Tat nach § 170 Abs. 2 StPO eingestellt hatte, da ein Restverdacht fortbestand. Aus der Gesamtschau ergab sich somit eine Wiederholungsgefahr, die Voraussetzung für die Speicherung in POLIS ist.

Akteneinsicht und Datenschutz

Schließlich war auch die Gewährung der Akteneinsicht selbst durch die Staatsanwaltschaft an Verfahrensbeteiligte nicht zu beanstanden. Die beanstandete Datenverarbeitung beruhte nicht auf der gewährten Akteneinsicht selbst, sondern auf Daten, die von der Polizei in einem Aktenvermerk unzulässig verarbeitet wurden. Für die Rechtmäßigkeit der Dokumentation im Abschlussvermerk war die Polizei datenschutzrechtlich verantwortlich. Aus dem Aktenvermerk selbst ergab sich aus Sicht der Staatsanwaltschaft nicht, dass die Polizei die verwendeten Vorgangsverwaltungsdaten in unzulässiger Weise verarbeitet hatte. Dies stand erst nach Gewährung der Akteneinsicht fest, als die Polizei die Staatsanwaltschaft nach § 54 Abs. 2 S. 5 POG hierüber informierte.

Anhand des konkreten Verfahrens konnte die Bedeutsamkeit einer klaren Zwecktrennung bei der polizeilichen Datenverarbeitung noch einmal gegenüber dem betreffenden Polizeipräsidium, aber auch dem Ministerium des Innern und für Sport anschaulich gemacht werden. Dabei wurden auch wichtige Erkenntnisse für die Umstellung von POLADIS auf @rtus transportiert.

1.3. Kontrollpraxis des LfDI im Sicherheitsbereich

1.3.1 Prüfung der Rechtsextremismus- und Antiterrordatei bei der Polizei Rheinland-Pfalz

Im 32. Tätigkeitsbericht wurde die beabsichtigte datenschutzrechtliche Kontrolle der Rechtsextremismus-Datei (RED) und der Antiterrordatei (ATD) angekündigt (III. 1.1.1, S. 22).

Zweck der RED und der ATD ist es, die Sicherheitsbehörden bei der Aufklärung und Bekämpfung des gewaltbezogenen Rechtsextremismus und des internationalen Terrorismus sowie der Verfolgung der selbigen zu unterstützen (§ 1 Rechtsextremismus-Datei-Gesetz – RED-G und § 1 Antiterrordateigesetz – ATDG).

Gemäß § 11 Abs. 1 S. 2 und Abs. 2 RED-G, § 10 Abs. 1 S. 2 und Abs. 2 ATDG werden die Datenschutzaufsichtsbehörden dazu angehalten, im Abstand von zwei Jahren die Dateien zu überprüfen.

Im September und Oktober führte der LfDI Rheinland-Pfalz eine Kontrolle der RED und der ATD beim LKA Rheinland-Pfalz sowie den beiden Polizeipräsidien Koblenz und Rheinpfalz durch. Dem ging im Dezember 2023 ein Informationsbesuch beim LKA voraus. Ziel der Kontrolle war es, anhand durch das LKA vorab übermittelter Protokolldaten stichprobenartig Einzelfälle auf ihre Datenschutzkonformität hin zu überprüfen.

Diese Kontrollen dienen dem Zweck, die Einhaltung der Datenschutzbestimmungen sicherzustellen und damit die informationelle Selbstbestimmung und die Privatsphäre der Bürger:innen im Wege des sogenannten quasikompensatorischen Grundrechtsschutzes aufgrund des erschwerten Individualrechtsschutzes zu schützen. Datenschutzkontrollen gewährleisten nicht nur die Rechtmäßigkeit und Transparenz der Datenverarbeitung, sondern auch das Vertrauen der Bürger:innen in staatliche Institutionen, die mit ihren Daten umgehen.

Bei den Kontrollen wurden zahlreiche Defizite festgestellt, die zu einer erheblichen Anzahl von Empfehlungen führten. Nachstellbedarf bestand insbesondere im Hinblick auf die Dokumentation des Anlasses und der Erforder-

lichkeit der Erstspeicherungen und fortgesetzten Speicherungen. Auch bei den geprüften Abfragen konnte in vielen Fällen nur durch eine ergänzende Recherche die Plausibilität der Abfragen geklärt werden, die Anlässe der Abfragen waren dagegen nur unzureichend protokolliert. Des Weiteren wurde in zwei Fällen die Verlängerung von Speicherungen in der ATD mit Speicherungen in POLIS begründet, die selbst kein Anlassdelikt nach dem ATDG darstellten. Dabei wurde dem Rechtsgedanken der Mitziehklausel des § 52 Abs. 5 S. 2 POG gefolgt, obwohl die – ohnehin datenschutzrechtlich kritische – Vorschrift selbst auf die Dateien nicht anwendbar ist.

Erforderliche Maßnahmen und korrespondierende Empfehlungen

Angesichts der festgestellten Defizite hat der LfDI die folgenden Empfehlungen ausgesprochen, um die ordnungsgemäße Speicherung, Dokumentation und Transparenz der Abfragen sowie die Einhaltung der datenschutzrechtlichen Vorgaben zu gewährleisten:

- **Einführung eines Datenblatts** zu jeder Einspeicherung in der RED und ATD, in dem Datum und Anlass der Erstspeicherung, Dokumentation der Negativprognose und Gründe für eine etwaige weitere Speicherung dokumentiert werden.
- **Schulungs- und Sensibilisierungsmaßnahmen** für die Mitarbeiter:innen
- **Dokumentation von Abfragen:** Jede Abfrage sollte detailliert und nachvollziehbar unter Verwendung des Freitextfeldes begründet werden. Das Freitextfeld ist zu nutzen, um den Abfragegrund und den zugehörigen Sachverhalt darzulegen.
- **Leitfaden für Abfragen:** Entwicklung eines Leitfadens für Abfragen, der den Gebrauch des Freitextfeldes vorschreibt und auf die Notwendigkeit hinweist, den Abfragegrund konkret zu dokumentieren.
- **Speicherung in Gruppenlaufwerken:** Die Speicherung von Daten in Gruppenlaufwerken als „Aktenersatz“ stellte eine Verletzung der Grundsätze ordnungsgemäßer Aktenführung dar. Es wurde empfohlen, alle relevanten Informationen ordnungsgemäß zu verakten und in dafür vorgesehenen Systemen zu speichern.
- **Einhaltung der Speicherfristen:** Festgelegte Speicherfristen sind einzuhalten. Insbesondere muss verhindert werden, dass Speicherungen durch die Anwendung der Mitziehklausel bei Taten, die keine Anlassdelikte nach dem ATDG und dem RED-G darstellen, unzulässig verlängert werden.
- **Verantwortlichkeit für die Speicherung:** Zur Vermeidung von Unsicherheiten bezüglich der Verantwortlichkeit für die Speicherung von Personendaten in der RED sollte eine klare Zuweisung der Zuständigkeiten zwischen den verschiedenen Behörden erfolgen.

Die defizitären Speicherungen wurden bereits ohne Anordnungen des LfDI gelöscht. Durch seine Empfehlungen will der LfDI sicherstellen, dass die zukünftige Praxis verbessert wird. Der Umstand, dass die Praxisrelevanz der beiden Extremismusdateien von den geprüften Behörden zum Teil infrage gestellt wurde, kann nicht dazu führen, dass die Speicherungen entgegen der klaren gesetzlichen Vorgaben erfolgen.

1.3.2 Einsatz von Bodycams bei der rheinland-pfälzischen Polizei

Der LfDI Rheinland-Pfalz hat die Pilotierung und Einführung des Einsatzes der körpernahen Kameras (Bodycams) durch die rheinland-pfälzische Polizei seit 2017 eng begleitet (siehe TB 2014/2015, S. 59 Ziffer 4.3, TB 2016/2017 S. 67 Ziffer 4.5). Auch der praktische Einsatz der Bodycams wurde nun im Wege einer Kontrolle

überprüft. Besonderes Augenmerk lag darauf, dass die Aufzeichnungen unter den gesetzlich vorgesehenen Voraussetzungen erfolgen. Dazu wurde die Nutzung der Bodycams stichprobenweise in einer Reihe von Einzelfällen überprüft. Die Kontrolle hat in Bezug auf den präventiven Einsatz der Bodycam keine wesentlichen datenschutzrechtlichen Defizite ergeben. Gleichwohl waren folgende Empfehlungen im Nachgang der Kontrolle angezeigt:

- **Zweckänderung**

  Grundsätzlich ist der präventive Einsatz der Bodycam zum Zwecke der Eigen- und Fremdsicherung vorgesehen. Eine zweckändernde Nutzung der Aufnahmen ist jedoch unter bestimmten Voraussetzungen möglich. Auch wenn dazu ein landeseinheitliches Zweckänderungsformular eingeführt wurde, konnte der Grund der zweckändernden Nutzung in vielen Fällen nur durch Recherche nachvollzogen werden. Deswegen sollte das landeseinheitliche Zweckänderungsformular künftig um eine nachvollziehbare und detaillierte Begründung der Zweckänderung ergänzt sowie – wenn möglich – das Aktenzeichen des Korrespondenzvorgangs angegeben werden. Dies würde nicht nur die nachträgliche datenschutzrechtliche Kontrolle seitens der betroffenen Person oder meiner Behörde erleichtern, sondern auch die Transparenz und Nachvollziehbarkeit der Zweckänderung im Einklang mit der Rechenschaftspflicht gemäß § 32 LDSG gewährleisten.

- **Besondere Kategorien personenbezogener Daten / Berufsgeheimnisträger**

  Auch für die Datenerhebungen nach § 31 POG müssen geeignete Garantien für besondere personenbezogene Daten gemäß § 27 Abs. 2 POG getroffen werden. Gewonnene Erkenntnisse müssen im weiteren Verfahren nach Vorgaben der §§ 59 f. LDSG voneinander unterschieden werden. Im Falle einer Zweckänderung, bei der besondere Kategorien personenbezogener Daten betroffen sind, sollte die betreffende Tonspur entweder entfernt oder gelöscht werden. In besonderem Maße gilt dies für Fälle, in denen die Inhalte dem Berufsgeheimnis unterliegen.

- **Hinweispflicht**

  In Fällen, in denen Dritte nachträglich in die Einsatzmaßnahme involviert werden, sollte auch diesen gegenüber der Einsatz der Bodycam in geeigneter Form angezeigt wird, sofern dies die Umstände des Einzelfalls gestatten. Hierdurch kann eine frühzeitige Kenntnisnahme und Wahrung der datenschutz- und berufsrechtlichen Vorgaben sichergestellt werden.

- **Dauer des Einsatzes im Einzelfall**

  In einigen Fällen wurde die Aufnahme fortgeführt, obwohl keine entsprechende Gefahrenlage mehr bestand. Die Polizeikräfte sind deswegen dahingehend zu sensibilisieren, dass die Rechtmäßigkeit des Bodycam-Einsatzes während des Einsatzgeschehens kontinuierlich überprüft wird, insbesondere hinsichtlich der fortlaufenden Erforderlichkeit der Aufzeichnung.

Ein Aspekt, der noch zwischen dem LfDI und dem betreffenden Polizeipräsidium erörtert wird, betrifft Aufnahmen, die klar zeigten, dass diese von Anfang an zum Zwecke der Strafverfolgung erfolgten. Dazu wird der LfDI im kommenden Tätigkeitsbericht weiter berichten.

2. JUSTIZ

Der Austausch mit der Praxis ist aufgrund des damit verbundenen immensen Erkenntnisgewinns von großer Bedeutung für die aufsichtsbehördliche Arbeit des LfDI. Deshalb wirkte der LfDI auch im Jahr 2024 an verschiedenen Fortbildungsveranstaltungen im Bereich Justiz mit.

2.1 Fortbildungsveranstaltung bei der Generalstaatsanwaltschaft Koblenz

Der LfDI besuchte am 25. Januar 2024 die Generalstaatsanwaltschaft Koblenz zu der Fortbildungsveranstaltung „Datenschutz und Strafverfolgung".

Das Zusammentreffen wurde zunächst dazu genutzt, sich mit dem Generalstaatsanwalt des Bezirks Koblenz, dessen Vertreter und dessen behördlichen Datenschutzbeauftragten zu aktuellen Herausforderungen der Digitalisierung und des Datenschutzes in der Strafverfolgung auszutauschen, insbesondere zum bevorstehenden Start der elektronischen Akte.

Die eigentliche Fortbildungsveranstaltung für die Assessorinnen und Assessoren sowie die Datenschutzbeauftragten der Behörden im Bezirk der Generalstaatsanwaltschaft Koblenz eröffnete der Landesbeauftragte Prof. Dr. Dieter Kugelmann mit einem Vortrag zum Spannungsfeld zwischen dem Grundrecht auf informationelle Selbstbestimmung einerseits und der Gefahrenabwehr und Strafverfolgung andererseits. In Ansehung der verfassungs- und europarechtlichen Vorgaben legte Prof. Dr. Kugelmann dar, dass Datenschutz und Strafverfolgung vereinbar sind. Wesentliche Stellschrauben sind die Zwecke der Datenverarbeitung im Rahmen der Ermittlungen und die Verhältnismäßigkeit der Maßnahmen. Rechtsstaatliche Sicherung erfolgt durch Verfahrensvorkehrungen wie Richtervorbehalte und einen rechtmäßigen Vollzug durch die Staatsanwaltschaften.

Einen spezifischeren Überblick erhielten die Teilnehmer:innen durch einen Vortrag der zuständigen Bereichsleiterin und Referentin des LfDI über die datenschutzrechtlichen Pflichten der Staatsanwaltschaft in ihrem Arbeitsalltag, insbesondere der Benachrichtigungs- und Löschungspflichten sowie dem Umgang mit dem Recht auf Auskunft im Lichte der aktuellen EuGH-Rechtsprechung.

Den Abschluss der Veranstaltung bildete eine Besichtigung der Landeszentralstelle Cybercrime Rheinland-Pfalz, der zentralen Koordinierungs- und Ansprechstelle für die Bekämpfung von Straftaten, die im Internet oder mithilfe des Internets begangen werden. Diese Kombination aus Austausch, Vorträgen und praktischen Einblicken machte die Fortbildung zu einer gewinnbringenden Veranstaltung für alle Beteiligten.

2.2 Fortbildungsveranstaltung „Datenschutz im Justizvollzug" in Kooperation mit dem Ministerium für Justiz

Am 15. Oktober 2024 veranstaltete der LfDI in Kooperation mit dem Ministerium für Justiz des Landes Rheinland-Pfalz eine ganztägige Fortbildungsveranstaltung für die Mitarbeitenden der rheinland-pfälzischen Justizvollzugsbehörden.

Den Teilnehmer:innen wurde dabei zunächst ein Grundlagenwissen im Datenschutzrecht, insbesondere ein Überblick über das für den Justizvollzug geltende Landesjustizvollzugsdatenschutzgesetz (LJVollzDSG) vermittelt.

Im Anschluss wurden die behandelten Themen anhand von Praxisfällen gemeinsam mit den Referierenden besprochen. Nach der Fortbildungsveranstaltung bestand für die Datenschutzbeauftragten der rheinland-pfälzischen Justizvollzugsanstalten die Möglichkeit zum Austausch.

Die Konzeption der Veranstaltung ermöglichte es den Teilnehmenden, ihre eigenen Erfahrungen und Herausforderungen aus dem Justizvollzugsalltag zu teilen und zusammen mit den Referierenden des Ministeriums für Justiz und des LfDI konkrete Lösungsansätze zu entwickeln, die in der täglichen Praxis umgesetzt werden können.

2.3 Geburtstagswünsche per E-Mail durch die Notarkammer

Im Rahmen einer an den LfDI herangetragenen Beschwerde wurde der Versand von Geburtstagswünschen durch eine rheinland-pfälzische Notarkammer an deren Mitglieder per dienstlicher E-Mail infrage gestellt, da eine ausdrückliche Einwilligung der Mitglieder zur Versendung des Gratulationsschreibens nicht vorlag.

Nach Art. 5 Abs. 1 lit. b DS-GVO müssen personenbezogene Daten grundsätzlich für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. § 7 LDSG normiert dagegen die Ausnahmen, in denen die Verarbeitung personenbezogener Daten durch rheinland-pfälzische öffentliche Stellen zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, zulässig ist.

Die Notarkammern erheben die personenbezogenen Daten ihrer Mitglieder, insbesondere die Geburtsdaten, zur Erfüllung ihrer standesorganisatorischen Aufgaben u.a. im Sinne des § 67 BNotO. Die Weiterverarbeitung dieser Daten mit der Intention der kollegialen Beziehungspflege ist aus datenschutzrechtlicher Sicht nicht mit diesen Erhebungszwecken zu vereinbaren. Die Weiterverarbeitung stellt daher eine rechtfertigungsbedürftige Zweckänderung dar, für die keine Rechtsgrundlage ersichtlich war, insbesondere lag keine Einwilligung der Mitglieder vor.

Im Ergebnis konnte der LfDI deswegen darauf hinwirken, dass die Praxis der betreffenden Notarkammer dahingehend geändert wurde, dass zukünftig bereits bei Eintritt der Mitglieder erfragt wird, ob zukünftig Geburtstagsglückwünsche erwünscht sind und zu diesem Zweck die Mitgliedsdaten verwendet werden dürfen.

3. VIDEOÜBERWACHUNG

3.1 Neue Vorgehensweise zur Videoüberwachung durch Privatpersonen

Im Bereich der Videoüberwachung ist die Anzahl der Verfahren im privaten bzw. nachbarschaftlichen Bereich im Vergleich zum Vorjahr erneut angestiegen. Der LfDI hat im Jahr 2024 mehr als 440 Verfahren eingeleitet und 80 schriftliche Beratungen geführt. Daraus ergibt sich, dass das Bedürfnis, zur Stärkung des Sicherheitsgefühls eine Videoüberwachung durchzuführen, steigt. Zudem steigt allerdings auch die Anzahl der Personen, die sich durch den Überwachungsdruck in ihrem Persönlichkeitsrecht beeinträchtigt fühlen. Auch im gewerblichen Bereich ist ein Anstieg der Verfahrenszahl zu verzeichnen. Hier erreichten den LfDI 43 Beschwerden und 61 Hinweise.

Da insbesondere im nachbarschaftlichen Bereich die Zahl der Verfahren erneut gestiegen ist, wurde im Hinblick auf die vorhandenen personellen Ressourcen die Bearbeitungspraxis dieser Verfahren angepasst.

In der Regel handelt es sich hier um Eingaben, die letztlich von einem angespannten Nachbarschaftsverhältnis begleitet bzw. geprägt sind. In der Überprüfungspraxis stellt sich regelmäßig heraus, dass die Videoüberwachung größtenteils zulässig ist und das eigene Grundstück umfasst und lediglich geringfügige Änderungen erforderlich sind (z.B. die Verpixelung nicht notwendiger Bildausschnitte oder die Nachbesserung der Hinweisschilder).

Im Hinblick darauf ergeht nunmehr beim Eingang einer Eingabe bzgl. einer möglichen Videoüberwachung von Nachbargrundstücken und der öffentlichen Straße durch eine Privatperson ein verfahrensabschließender Hinweis gem. Art. 58 Abs. 1 lit. d DS-GVO an den Verantwortlichen. In diesem Schreiben wird er über die Zulässigkeitsvoraussetzungen einer Videoüberwachung, insbesondere des eigenen Grundstücks, informiert bzw. belehrt.

Bei der Festlegung der Vorgehensweise hat der LfDI die eingeschränkten Kontrollmöglichkeiten und die Tatsache berücksichtigt, dass eine Befugnis zur Entfernung von Kameras durch die Datenschutzaufsichtsbehörde nicht gegeben ist (OVG Koblenz, Urteil vom 25.06.2021 – 10 A 10302/21). Letztlich können die Beschwerdeführer:innen oft nur auf den Zivilrechtsweg verwiesen werden, zumal die Überprüfung der Videoüberwachung größtenteils von der Mitwirkung der Verantwortlichen abhängt. Im Hinblick darauf bietet der Hinweis gem. Art. 58 Abs. 1 lit. d DS-GVO im Vergleich zu den anderen in Art. 58 Abs. 1 DS-GVO aufgeführten Befugnissen vorliegend die effektivste Möglichkeit, trotz der eingeschränkten Handlungsmöglichkeiten die Verantwortlichen über die datenschutzrechtlichen Zulässigkeitsvoraussetzungen zu informieren und dadurch auf eine rechtmäßige Videoüberwachung hinzuwirken.

3.2 Pilotprojekt zur mobilen Videoüberwachung gegen illegale Müllablagerungen in Ludwigshafen

Am 15. August 2024 startete die Stadt Ludwigshafen nach Beratung durch den LfDI ein Pilotprojekt zur mobilen Videoüberwachung gegen illegale Müllablagerungen im Stadtgebiet.

Aus datenschutzrechtlicher Sicht ist der Einsatz von Kameras in solchen Fällen grundsätzlich nicht zulässig, da Videoüberwachung im öffentlichen Raum immer auch eine Überwachung unbeteiligter Bürger:innen bedeutet.

Das Ludwigshafener Vorhaben weist aber Besonderheiten auf, sodass zumindest für ein sechsmonatiges Pilotprojekt keine datenschutzrechtlichen Bedenken bestanden und die Durchführung vom LfDI gebilligt wurde.

Dabei wurde auch berücksichtigt, dass die Belastung durch illegale Müllverschmutzung in Ludwigshafen ungewöhnlich hoch ist. Sie betrifft nicht allein Müllsammelplätze, sondern auch städtische Wohnbereiche, was konkrete Gefahren für Gesundheit und Umwelt nach sich zieht. Die Stadtverwaltung hat in der Vergangenheit zahlreiche mildere Maßnahmen im Kampf gegen Verschmutzung eingesetzt und ausgereizt. Hierzu zählen Kontrollgänge durch sogenannte Müllsheriffs, Beratungsangebote und kreative Öffentlichkeitsarbeit.

Bei der Umsetzung der mobilen Videoüberwachung ergreift die Stadt Ludwigshafen zudem umfangreiche technisch-organisatorische Maßnahmen, die den datenschutzrechtlichen Eingriff für die einzelnen Bürger:innen reduzieren. Das vom LfDI gebilligte Konzept des Pilotprojektes sieht mobile Videoüberwachungen nur an ausgewählten Orten im Ludwigshafener Stadtgebiet vor. Der Einsatz der punktuellen Videoüberwachung muss innerhalb der engen rechtlichen Grenzen erfolgen für den klar definierten Zweck, Gefahren abzuwehren, illegale Abfallablagerungen zu unterbinden und deren Urheber:innen zu ermitteln. Am Standort der Videokameras, die in einem für diesen Zweck umgebauten Fahrzeug installiert sind, wird öffentlich und sichtbar auf die Überwachung der betroffenen Örtlichkeit hingewiesen. Die Kameras dürfen keine Eingangsbereiche von Häusern und Gebäuden oder Spielplätze erfassen.

Das Projekt muss seine Wirksamkeit noch unter Beweis stellen. Die abschließende datenschutzrechtliche Beurteilung erfolgt daher nach dem Ende des Projekts. Die Ergebnisse der sechsmonatigen Pilotphase werden Grundlage einer weiteren datenschutzrechtlichen Beurteilung sein.

Das Gesamtkonzept zum Pilotprojekt ist auf der Internetseite der Stadt Ludwigshafen sowie über die Transparenzplattform des Landes Rheinland-Pfalz öffentlich zugänglich (**www.s.rlp.de/tpp-vumuell**).

3.3 Konkrete Verfahren bzgl. Videoüberwachung aufgrund von illegaler Müllablagerung

Nicht nur die Stadt Ludwigshafen, sondern auch andere Kommunen in Rheinland-Pfalz beklagen die Belastung durch illegale Müllablagerungen. Es ist festzuhalten, dass Überwachungsmaßnahmen nur unter strengen Voraussetzungen und nach sorgfältiger Prüfung der Rechtsgrundlage zulässig sind. Insbesondere müssen die Erforderlichkeit und die Angemessenheit solcher Maßnahmen von den Kommunen belegt werden. Zwei Ortsgemeinden hatten Videoüberwachungen von Müllcontainerplätzen durchgeführt. Nach einer Klärung des Sachverhalts stellte sich jedoch als Ergebnis der Prüfung heraus, dass die Videoüberwachung in beiden Fällen auf keine ausreichende Rechtsgrundlage gestützt werden konnte.

Im ersten Fall wurde die Videoüberwachung mit dem Zweck betrieben, Ordnungswidrigkeiten und Straftaten zu verhindern sowie die Verursacher:innen zu identifizieren und entsprechende Verfahren gegen sie betreiben zu können. Die Ortsgemeinde hatte vorgetragen, dass die Videoüberwachung insbesondere umweltgefährdende Straftaten sowie Gefahren durch körperverletzende Müllablagerungen abwehren sollte, die vor allem für Kinder eine Gefahr darstellen könnten. Auch sollte die Videoüberwachung helfen, die Müllablagerung als Ordnungswidrigkeit zu verfolgen, um die Verursacher:innen im Rahmen des Ordnungswidrigkeitenverfahrens zu identifizieren.

Die datenschutzrechtliche Bewertung erfolgte anhand der Vorgaben von § 21 LDSG. Als Voraussetzung der Verarbeitung personenbezogener Daten zum Schutz des Eigentums ist das Vorliegen einer konkreten Gefahrensituation erforderlich. Die Ortsgemeinde konnte jedoch keine ausreichende Dokumentation vorlegen, die die Häufigkeit, Art und Höhe möglicher Schäden belegte. Eine Videoüberwachung we-

gen Bagatellschäden wäre dabei unverhältnismäßig und somit unzulässig.

Soweit die Ortsgemeinde die Videoüberwachung zur vorbeugenden Bekämpfung von Straftaten durchführen wollte, war sie hierfür nicht zuständig. Die vorbeugende Bekämpfung von Straftaten ist eine Aufgabe, die gemäß § 1 Abs. 1 S. 3, § 30 Polizei- und Ordnungsbehördengesetz ausschließlich der Polizei zugewiesen ist. Ferner konnte die Ortsgemeinde auch nicht die Zuständigkeit für die Verfolgung der Ordnungswidrigkeit der Müllablagerung geltend machen, da dies der zuständigen Ordnungsbehörde obliegt. Zwar handelt es sich bei der kommunalen Abfallwirtschaft auch um die Wahrnehmung einer Aufgabe im öffentlichen Interesse (§ 21 Abs. 1 S. 1 Nr. 1 LDSG) und die Videoüberwachung kann zugleich dem Schutz des Eigentums vor Vandalismus dienen (§ 21 Abs. 1 S. 1 Nr. 3 Var. 1 LDSG). Vorrangiger Zweck der Videoüberwachung war jedoch, die Verhütung und Verfolgung von Ordnungswidrigkeiten und Straftaten zu begünstigen. Nachdem der LfDI die Ortsgemeinde aufgrund seiner Bewertung anwies, die Videoüberwachung zu beenden, stellte diese die Videoüberwachung ein und verhüllte die Kamera.

Im zweiten Fall betrieb eine Ortsgemeinde eine Videoüberwachungsanlage zur Sicherung von Glas- und Altkleidercontainern. Der Zweck der Videoüberwachung wurde darin gesehen, illegale Müllablagerungen zu verhindern. Jedoch konnte auch hier bereits die Gefahrensituation nicht belegt werden. Auch diese Ortsgemeinde beendete die Videoüberwachung und entfernte die Kamera, nachdem der LfDI sie zur Beendigung der Videoüberwachung anwies.

3.4 Videoüberwachung an der Schule

Gerade an Schulen führt das Thema Videoüberwachung schnell zu Diskussionen. Ein Vater beschwerte sich beim LfDI darüber, dass der Hausmeister der Schule sein Kind während einer Abendveranstaltung auf dem Schulgelände angesprochen habe, als es den Bereich der Veranstaltung verlassen wollte. Daher vermutete der Vater eine heimliche Videoüberwachung des Schulgeländes.

Auf Anfrage teilte die Schule mit, dass tatsächlich Kameras an der Schule angebracht seien. Diese würden allerdings nur den Privatbereich des Hausmeisters erfassen, der in einer angemieteten Wohnung auf dem Schulgebäude wohne. Es handele sich also nicht um die Überwachung eines öffentlichen Bereichs.

Da der Privatbereich des Hausmeisters vom öffentlichen Schulgelände optisch nur schwer zu unterscheiden war, wurde der Hausmeister vom LfDI auf Folgendes hingewiesen:

Kameras, die öffentliche Bereiche wie Schulen und Kitas aufnehmen – zum Beispiel zur Vandalismusprävention –, sollen nur außerhalb der Schul- oder Betriebszeiten aktiviert werden. Auch während schulischer Abendveranstaltungen müssen solche Systeme deaktiviert werden. Unabhängig davon, ob es sich um Kameras in öffentlichen oder privaten Bereichen handelt, besteht eine Kennzeichnungspflicht durch das Anbringen entsprechender Hinweisschilder.

4. WIRTSCHAFT

4.1 DSK verabschiedet neuen Beschluss zu Asset Deals

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) hat mit Beschluss vom 11. September 2024 für die Übermittlungen personenbezogener Daten an die Erwerberin oder den Erwerber eines Unternehmens im Rahmen eines Asset Deals überarbeitete datenschutzrechtliche Hinweise verabschiedet.

Hiermit ersetzt und konkretisiert die DSK den vormaligen Beschluss vom 24. Mai 2019 zum Thema Asset Deal, um den zusätzlichen datenschutzrechtlichen Herausforderungen, mit denen insbesondere Einzelkaufleute, Handwerksbetriebe und Personengesellschaften im Falle eines Betriebsübergangs konfrontiert sind, zu begegnen.

Der Beschluss unterscheidet inhaltlich zwischen der Übermittlung personenbezogener Daten vor Abschluss eines Asset Deals und in Bezug auf die Daten von Kundinnen und Kunden zwischen den verschiedenen Stadien einer Vertragsanbahnung, einer laufenden vertraglichen Beziehung sowie einer vollständig erfüllten oder beendeten vertraglichen Beziehung. Darüber hinaus enthält er spezifische Empfehlungen zum Umgang mit bestimmten weiteren Fallgruppen (z. B. Werbung durch den Erwerber, besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO, Bankdaten, offene Forderungen, Beschäftigtendaten etc.).

Während die Datenübermittlung vor Abschluss eines Asset Deals grundsätzlich unzulässig ist und nur aufgrund einer im Einzelfall vorliegenden freiwillig erteilten Einwilligung der betroffenen Personen erfolgen darf, kann im Falle der Vertragsanbahnung die Datenverarbeitung gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO im Rahmen einer Widerspruchslösung gestattet sein. Bei laufender vertraglicher Beziehung, insbesondere bei noch bestehenden Mängelgewährleistungsansprüchen, der Vertragsübernahme oder einer Schuldübernahme, die nicht mit der Erfüllungsübernahme zu verwechseln ist, ergibt sich die Verarbeitungsbefugnis aus Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO. Altdaten dürfen demgegenüber nur zur Erfüllung der gesetzlichen Aufbewahrungsfristen nach Abschluss eines Vertrages über eine Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO und unter Trennung zu den Daten der Kundinnen und Kunden mit einer laufenden vertraglichen Beziehung (sog. Zwei-Schrank-Lösung) verarbeitet werden. Für die Nutzung zu eigenen Zwecken benötigt der Erwerber die Einwilligung der Kundinnen und Kunden. Besonderheiten bestehen für Kleinst- oder Kleinunternehmen, die unter Beendigung ihrer eigenen wirtschaftlichen Tätigkeit Kundendaten an ein ebensolches Unternehmen verkaufen. Diese dürfen ausnahmsweise einmalig im Wege einer Widerspruchslösung ausschließlich die Postadressen auf Grundlage von Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO in Verbindung mit Erwägungsgrund 13 Satz 4 DS-GVO übermitteln.

Der vollständige Beschluss ist auf der Website der DSK unter **www.datenschutzkonferenz-online.de** in der Infothek unter Beschlüssen veröffentlicht und abrufbar.

Überdies hat der Europäische Datenschutzausschuss (EDSA) im September 2024 auf deren Website einen Datenschutzleitfaden (sog. Data Protection Guide for Small Business) speziell für kleine Unternehmen in 18 Sprachen veröffentlicht: **www.s.rlp.de/edpb-smallbusinesses**

4.2 Auskunftsrecht

Fragen rund um das Auskunftsrecht haben den LfDI auch im Jahr 2024 beschäftigt. So wurde

u.a. die Möglichkeit genutzt, ausgewählte Unternehmen insbesondere des Inkassobereichs und Kreditinstitute im Rahmen der vom Europäischen Datenschutzausschuss (EDSA) initiierten europaweite Aktion „Coordinated Enforcement Framework (CEF)“ zur praktischen Umsetzung des Auskunftsrechts auf Grundlage der Leitlinie 01/2022 on data subject rights – Rights of access (**www.s.rlp.de/edpb-roa**) zu befragen (vgl. Kapitel I.4.2 dieses Tätigkeitsberichts).

4.3 Kreditwirtschaft

4.3.1 Legitimation von Betreuer:innen

Oftmals sind sich Betreuer:innen unsicher, welche Daten sie gegenüber einem Kreditinstitut in ihrer Funktion als Betreuer:in für einen Bankkunden angeben müssen.

Legitimationspflichten für Betreuer:innen ergeben sich zum einen aus der Abgabenordnung (AO) und zum anderen aus dem Geldwäschegesetz (GwG):

Nach § 154 AO gilt das Prinzip der Kontenwahrheit: Danach haben sich Kreditinstitute vor Vertragsabschluss Gewissheit über die Person des Kontoinhabers und des ggf. wirtschaftlich Berechtigten, wozu auch Betreuer:innen gehören, zu vergewissern. Nach § 154 Abs. 2a AO ist grundsätzlich auch die Steueridentifikationsnummer zu erheben. Gemäß § 154 Abs. 2d AO können die Finanzbehörden für bestimmte Fallgruppen jedoch Erleichterungen bei der Identifikation zulassen. Diese Erleichterungen ergeben sich aus Nr. 11.1 des Anwendungserlasses zur Abgabenordnung (AEAO) zu § 154 AO hinsichtlich der Verfügungsberechtigten. Danach kann für Verfügungsberechtigte auf die Identifizierung, die Aufzeichnung, die Herstellung der Auskunftsbereitschaft und die Erhebung der steuerlichen Ordnungsmerkmale verzichtet werden, wenn es sich bei dem Verfügungsberechtigten um einen rechtlichen Betreuer handelt (Nr. 11.1 Satz 1 b AEAO zu § 154 AO).

Folglich ist ein Kreditinstitut nicht grundsätzlich verpflichtet, die Steueridentifikationsnummer des Betreuers zu erheben. Da es sich um eine Kann-Vorschrift handelt, kann dies im Einzelfall anders zu bewerten sein. Da aber der Grundsatz der Datenminimierung gilt (Art. 5 Abs. 1 lit. c DS-GVO), müsste die Bank im Einzelfall begründen, warum sie die Daten entgegen der Erleichterungen im Anwendungserlass dennoch erheben will.

Auch muss das Kreditinstitut die Sorgfaltspflichten beachten, die sich aus dem Geldwäschegesetz ergeben. Danach hat im Rahmen der allgemeinen Sorgfaltspflichten gem. § 10 Abs. 1 Nr. 1 GwG die Identifizierung des Vertragspartners und ggf. der für ihn auftretenden Person nach Maßgabe des § 11 Abs. 4 und des § 12 Abs. 1 und 2 GwG zu erfolgen. Zudem muss eine Prüfung, ob die für den Vertragspartner auftretende Person hierzu berechtigt ist, vorgenommen werden. Gemäß den Auslegungs- und Anwendungshinweisen zum Geldwäschegesetz der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (Stand: November 2024) sind als identifizierungspflichtige auftretende Personen auch Betreuer:innen anzusehen (vgl. Ziff. 5.1.2).

Die gemachten Angaben sind anhand eines gültigen amtlichen Ausweises, der ein Lichtbild der Inhaberin bzw. des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, zu überprüfen, also in der Regel anhand des Personalausweises (§ 12 Abs. 1 GwG). Dabei müssen dann auch die Art, die Nummer und die Behörde, die das zur Überprüfung der Identität vorgelegte Dokument ausgestellt hat, aufgezeichnet werden. Hier besteht das Recht und die Pflicht, das vorgelegte Ausweisdokument vollständig zu kopieren oder es vollständig optisch digital zu erfassen (§ 8 Abs. 2 GwG).

Für die ordnungsgemäße Identifizierung ist die persönliche Vorlage des Ausweispapieres erforderlich oder ein anderes geeignetes Verfahren, das zur geldwäscherechtlichen Über-

prüfung der Identität geeignet ist und ein Sicherheitsniveau aufweist, das dem der persönlichen Vorlage und Inaugenscheinnahme gleichwertig ist (z.B. das Videoidentverfahren, § 13 GwG). Die Vorlage letztlich nur einer Kopie des Ausweises reicht nicht, da die verpflichtete Bank die Identität der Person durch Inaugenscheinnahme prüfen muss und nicht lediglich die Angaben im Ausweisdokument (vgl. BGH, Urteil vom 20.04.2021 – XI ZR 511/19).

Das Geldwäschegesetz sieht jedoch, anders als die Abgabenordnung, nicht die Erhebung der Steueridentifikationsnummer vor, da diese für den Rechtskreis der Steuererhebung, nicht jedoch für die Geldwäschebekämpfung erheblich ist. Folglich findet die Erhebung dieses Datums keine Rechtgrundlage im Geldwäschegesetz.

4.3.2 Onlinebanking

Im Bereich des Onlinebankings kommt es zu Irritationen, wenn Bankkunden in ihrem Onlinebanking-Portal auch Konten einsehen können, die sie nicht innehaben, für die aber eine Vollmacht besteht, z.B. bei Vereins- oder Firmenkonten. Dies kann bei Betroffenen zu der Fehleinschätzung führen, dass z.B. auch andere Vereinsmitglieder oder Beschäftigte, die Vollmacht für das Vereins- oder Firmenkonto haben, auch die Privatkonten des anderen bevollmächtigten Mitglieds einsehen könnten.

Ein Onlinebanking-Zugang und damit auch das elektronisches Postfach wird immer und ausschließlich (nur) einer natürlichen Person zugeordnet und nicht einer juristischen Person (z.B. Arbeitgeber, Verein). Im elektronischen Postfach werden alle persönlichen Dokumente eingestellt, die die Geschäftsbeziehung des Kunden betreffen. Dies können Vertragsunterlagen, Kontoauszüge oder Abrechnungen sein. Dieses elektronische Postfach ist dem personalisierten Onlinebanking-Bereich des Kunden zugeordnet, d. h. ausschließlich dieser in seinem persönlichen Onlinebanking angemeldete Kunde kann die dort hinterlegten Dokumente einsehen.

Dies bedeutet, dass der Kunde über seinen persönlichen Onlinebanking-Zugang alle Konten und Informationen einsehen kann, für die er eine Berechtigung hat.

Wenn also eine Vollmacht für ein anderes Konto besteht, sei es für eine natürliche Person (z.B. ein Verwandter) oder eine juristische Person (z.B. Arbeitgeber, Verein), werden diese Konten ebenfalls im persönlichen Onlinebanking-Bereich angezeigt und Handlungen bzw. Verfügungen sind im Rahmen der Vollmacht möglich. Aber auch im Onlinebanking müssen die Aktionen aktiv angestoßen werden und Informationen zum Konto werden nicht aufgedrängt.

Umgekehrt heißt dies aber auch, dass andere Personen, die auch auf das Konto z.B. des Arbeitgebers oder des Vereins zugreifen könnten, nicht auch die Daten weiterer für das fragliche Konto Berechtigter sehen.

Falls persönliche Zugangsdaten an Dritte weitergegeben werden (z.B. an Verwandte oder weitere Vereinsmitglieder), erhalten diese Dritten selbstverständlich Einsicht in die persönlichen Daten der Person, die die Zugangsdaten weitergegeben hat. Dann liegt seitens der betreffenden Person ein Verstoß gegen die Bedingungen des Onlinebanking vor, nach denen die persönlichen Zugangsdaten zum personalisierten Onlinebanking niemals weitergegeben werden dürfen.

4.3.3 Kontenkontrolle

Kundinnen und Kunden vor Kreditinstituten wenden sich an den LfDI, weil sie von ihrem Institut auf bestimmte Transkationen angesprochen werden und kritisieren, dass man ihre Zahlungsdaten offensichtlich auswertet. Dies hängt mit der Verpflichtung von Sparkassen

und Banken und anderen Unternehmen im Finanzsektor zusammen, den Missbrauch des Finanzsystems durch Verschleierung und Verschiebung von Vermögenswerten legaler Herkunft sowie Finanzierung von Terrorismus zu verhindern. Hierfür müssen Geldinstitute über ein wirksames Risikomanagement verfügen, das eine Risikoanalyse und interne Sicherungsmaßnahmen umfasst. Entsprechende Verpflichtungen ergeben sich zum einen aus dem Geldwäschegesetz, zum anderen aus dem Kreditwesengesetz (KWG), hier § 25 h KWG. Nach dieser Vorschrift müssen Geldinstitute über ein angemessenes Risikomanagement sowie über interne Sicherungsmaßnahmen verfügen, die der Verhinderung von strafbaren Handlungen, die zu einer Gefährdung des Vermögens des Instituts führen können, dienen. Sie haben dafür angemessene geschäfts- und kundenbezogene Sicherungssysteme zu schaffen und zu aktualisieren sowie Kontrollen durchzuführen. Hierzu gehört auch die Aufdeckung von Transaktionen für Zwecke der Geldwäsche und der Terrorismusfinanzierung.

Nachdem der Gesetzgeber den Straftatbestand der Geldwäsche (§ 261 Strafgesetzbuch – StGB) im Jahr 2021 ausgeweitet hat, sind nunmehr alle Vergehen und Verbrechen als taugliche Vortaten der Geldwäsche anzusehen. So können im Rahmen der gesetzmäßig vorgesehenen Sicherungssysteme z.B. die Teilnahme an Onlineglücksspielen oder der Schusswaffenerwerb auffallen. Dies führt dann in der Regel dazu, dass die Geldinstitute auf die Kundinnen und Kunden zugehen, um auszuschließen, dass hier illegal gehandelt wurde.

Solche Maßnahmen sind datenschutzrechtlich nicht zu beanstanden.

5. LEBEN DIGITAL

5.1 Neue Verhaltensregeln für die Prüf- und Speicherfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien

Der Verband „Die Wirtschaftsauskunfteien e.V." mit Sitz in Wiesbaden hat am 25. Mai 2024 neue Verhaltensregeln für die Prüf- und Speicherfristen von personenbezogenen Daten veröffentlicht, die vom zuständigen Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) genehmigt wurden. Grund für die Anpassungen in den Verhaltensregeln war die unionsrechtswidrige Einstufung einzelner Regelungen, insbesondere zur Speicherfrist, im Urteil des Europäischen Gerichtshofs vom 7. Dezember 2023 in der verbunden Rechtssache C-26/22 und C-64/22 (vgl. 32. Tätigkeitsbericht 2023, S. 33, Abschnitt 5.2).

Zu den wesentlichen Änderungen gehören das Einführen eines Glossars und die genaue Festlegung des Speicherbeginns und -endes für verschiedene Datenarten. Außerdem wurden die Fristen für nachträglich beglichene Forderungen, für alle Insolvenzdaten sowie für Daten über die Restschuldbefreiung und über die ihr zugrundeliegenden Forderungen verkürzt. Die Verhaltensregeln stellen klar, dass Anschriftendaten nur noch zum Zwecke der Zuordnung bzw. Identifizierung gespeichert werden dürfen, soweit dies erforderlich und angemessen ist, und nicht mehr zum Zweck des Scorings. Darüber hinaus enthalten die Verhaltensregeln keine Speicherregelungen mehr zu Positivdaten und zu Kontomissbrauchsdaten.

Zu beachten war, dass zwei Verpflichtungen der Verhaltensregeln erst ab dem 1. Oktober 2024 bzw. ab dem 1. Januar 2025 galten (siehe die Nebenbestimmungen im Rahmen der Genehmigung der Verhaltensregeln für die Prüf- und Speicherfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien vom 25. April 2024, **www.s.rlp.de/gen-verhaltensregeln**). Bis dahin galten die betreffenden Regelungen der Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien vom 25. Mai 2018 in der Fassung vom 1. Januar 2020 fort. Seit dem 1. Januar 2025 gelten nun die neuen Verhaltensregeln im vollen Umfang.

5.2 Zulässigkeit der Übermittlung personenbezogener Daten an Inkassounternehmen

Bürger:innen tragen nach wie vor viele Anfragen und Beschwerden zur Übermittlung personenbezogener Daten von Unternehmen an Inkassodienstleister an den LfDI heran, da sie hierin automatisch einen Verstoß gegen das Datenschutzrecht vermuten (vgl. 32. Tätigkeitsbericht, S. 33, Abschnitt 5.1).

Der LfDI weist die Betroffenen deshalb immer wieder darauf hin, dass die Prüfung, ob der geltend gemachte Anspruch begründet oder etwa die Zahlung durch Betroffene korrekt erfolgt ist, nicht in den Zuständigkeitsbereich des LfDI fällt. Betroffene können hiergegen zivilrechtlich vorgehen und sich dazu an die Verbraucherzentrale oder eine Rechtsanwältin bzw. einen Rechtsanwalt für Zivilrecht wenden.

Ausführliche Hinweise finden Sie auf der Webseite des LfDI unter **www.datenschutz.rlp.de/themen/inkassounternehmen**.

5.3 Datenverarbeitung im Zusammenhang mit funkbasierten Zählern

ZuDie digitale Erhebung und Verarbeitung der Kaltwasser-, Strom-, Heizungs- bzw. Warmwasserzählern wird nach und nach flächendeckend funkgesteuert und fernablesbar umgesetzt. Den Bürger:innen soll mit dieser Technik die Einsparung von Energie dadurch erleichtert werden, dass sie ihre Energiever-

bräuche genauer im Blick behalten können und nicht erst durch eine jährliche Abrechnung ihres Versorgers von diesen Verbräuchen Kenntnis erlangen. In der Praxis des LfDI lässt sich allerdings bereits feststellen, dass bei den Bürger:innen im Hinblick auf Datenverarbeitungen im Zusammenhang mit funkbasierten Zählern Unsicherheiten z. B. darüber bestehen, welche Daten verarbeitet werden, wie häufig sie verarbeitet werden dürfen, welche Stelle sie verarbeitet und ob man sich gegen den Einbau der Zähler und/oder gegen die Datenverarbeitung selbst wehren kann. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat daher eine Orientierungshilfe veröffentlicht, die mehr Klarheit bzgl. der Rechtmäßigkeit dieser Datenverarbeitungen für Bürger:innen schaffen soll. Die Orientierungshilfe ist auf der Webseite der DSK veröffentlicht: **www.s.rlp.de/dsk-OH-zaehler**

5.4 Aktualisierung der Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressent:innen

Vor der Vermietung von Wohnraum erheben Vermieter:innen, Makler:innen oder Hausverwaltungen bei Mietinteressent:innen personenbezogene Daten, die bei der Entscheidung über den Vertragsschluss berücksichtigt werden sollen. Auch bei der Verarbeitung dieser Daten muss allerdings das Datenschutzrecht beachtet werden. Es dürfen daher nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Auf Basis einer Interessenabwägung muss auch das Recht der Mietinteressent:innen auf informationelle Selbstbestimmung Beachtung finden. Welche Daten zur Zweckerfüllung erforderlich sind, richtet sich nach verschiedenen Phasen im Rahmen der Vertragsanbahnung bzw. des Vertragsschlusses. Bezüglich der Datenerhebung kann zwischen bis zu drei Zeitpunkten differenziert werden:

1. Besichtigungstermin;
2. Vorvertragliche Phase, in welcher die Mietinteressent:innen den künftigen Vermieter:innen mitteilen, eine konkrete Wohnung anmieten zu wollen;
3. Entscheidung der künftigen Vermieter:innen für eine:n bestimmte:n Mietinteressent:in (Erstplatzierte:r).

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat im Berichtszeitraum die bestehende Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressenten“ aktualisiert, die hinsichtlich der Frage, welche personenbezogenen Daten, zu welchem Zeitpunkt verarbeitet werden dürfen, mehr Klarheit für die datenverarbeitenden Stellen schaffen soll. Die Orientierungshilfe ist auf der Webseite der DSK veröffentlicht: **www.s.rlp.de/dsk-OH-mietinteresse**

6. BESCHÄFTIGTENDATENSCHUTZ

6.1 Auskunftsanspruch im Stellenbesetzungsverfahren

Das Arbeitsgericht Mainz beschäftigte sich in einem Urteil vom 8. April 2024 (Az. 8 Ca 1474/23) u.a. mit der Frage, ob und inwieweit die Auswahlentscheidung des Arbeitgebers im Rahmen eines Stellenbesetzungsverfahrens ein personenbezogenes Datum der Bewerberin und des Bewerbers darstellt.

Anlass für die Befassung des Gerichts mit dieser datenschutzrechtlichen Fragestellung war die Klage eines Bewerbers, der sich erfolglos um eine ausgeschriebene Stelle bei der Beklagten beworben hatte und daraufhin von seinem Auskunftsrecht aus Art. 15 Abs. 1 und 3 DS-GVO Gebrauch gemacht hatte. Der Kläger forderte in diesem Zuge insbesondere die Herausgabe der Auswahlentscheidung des Arbeitgebers, da er der Ansicht war, der Ablehnungsgrund stelle eine Information dar, die sich auf ihn als betroffene Person beziehe.

Das Gericht war hier jedoch anderer Auffassung: Zwar definiere Art. 4 Nr. 1 DS-GVO personenbezogene Daten sehr weit als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Der Grund, weshalb sich ein Arbeitgeber für eine bestimmte Bewerberin oder einen bestimmten Bewerber entscheide, beziehe sich jedoch nicht auf die hiervon betroffenen Bewerber:innen. Vielmehr beziehe sich die Auswahlentscheidung auf den Arbeitgeber als Entscheider, da sie seine – unter Umständen auch schlicht nach Bauchgefühl vorgenommenen – Erwägungen widerspiegele.

Das Arbeitsgericht vertrat darüber hinaus die aus Sicht des LfDI zutreffende Auffassung, dass das Recht auf Erhalt einer Kopie nach Art. 15 Abs. 3 DS-GVO ausgeschlossen ist, wenn der Verantwortliche – außer den vom Bewerber selbst übermittelten Bewerbungsunterlagen – über keine weiteren Informationen des Bewerbers verfügt. Nach Auffassung des Gerichts besitzt der Betroffene damit bereits die „Originale", so dass dem Begehren nach Erteilung einer „originalgetreuen Kopie" im Sinne von Art. 15 Abs. 3 DS-GVO der Einwand des Rechtsmissbrauchs (§ 242 BGB) entgegensteht.

Der LfDI wird diese Rechtsauffassung im Rahmen der Beschwerdebearbeitung künftig berücksichtigen.

6.2 GPS-Überwachung des Fuhrparks

Im Berichtszeitraum erreichten den LfDI vermehrt Beschwerden wegen des Einbaus von Ortungsgeräten in Firmenfahrzeugen. Die hierfür vorgebrachten Gründe sind vielfältig:

- zur Verhinderung oder Aufklärung von Diebstählen;
- zur genaueren Abrechnung der eingesetzten Fahrzeuge gegenüber einem Auftraggeber durch den Verantwortlichen;
- zur effizienten Planung von Arbeitseinsätzen;
- zur Überwachung von Wartungsintervallen der Fahrzeuge.

Auf dem Markt sind Softwareprodukte erhältlich, die eine Reihe weiterer Funktionen unterstützen, z.B. GPS-Ortung in Echtzeit, detaillierter Fahrtenverlauf und Routenwiedergabe, Auswertung des digitalen Fahrtenschreibers auf Verstöße des Fahrers, tagesaktuelle Führerscheinkontrolle, Geofencing-Systeme, die darüber informieren, wenn Beschäftigte eine definierte Zone erreichen oder verlassen, sowie Geschwindigkeitsüberschreitungen und Anzeige ungeplanter Aktivitäten, usw.

Da eine Einwilligung im Beschäftigungsverhältnis in aller Regel nicht freiwillig erteilt wird,

kann der Einsatz von Ortungssystemen nur auf ein „berechtigtes Interesse“ im Sinne des Art. 6 Abs. 1 lit. f DS-GVO gestützt werden. Arbeitgeber haben vor dem Einsatz dieser Überwachung eine konkrete Zweckbestimmung festzulegen. Je weitreichender dabei in die Datenschutzrechte der Betroffenen eingegriffen wird, desto eher wird auch eine besondere Rechtmäßigkeitsprüfung in Form einer sogenannten Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO zu fordern sein.

Das Verwaltungsgericht Wiesbaden (Urteil vom 17.01.2022, Az. 6 K 1164/21) hat hierzu ausgeführt, dass zwischen anlasslosen präventiven Kontrollmaßnahmen zur Überprüfung der Einhaltung von bestehenden arbeitsrechtlichen Pflichten und anlassbezogenen Mitarbeiterkontrollen bei Bestehen eines konkreten zu dokumentierenden Anfangsverdachts zu unterscheiden sei.

Aus datenschutzrechtlicher Sicht darf es daher zu keiner Verknüpfung der Ortungsdaten mit den personenbezogenen Daten des Fahrpersonals kommen. Auswertungsfunktionen, die nur der allgemeinen persönlichen Überwachung von Beschäftigten dienen können (wie Geschwindigkeitsaufzeichnungen, Dauer von Fahrtunterbrechungen, usw.), sind daher technisch zu unterbinden. Geofencing-Systeme würden einen permanenten Kontrolldruck erzeugen und sind daher ebenfalls unzulässig.

Die DS-GVO sieht in Art. 13 und Art. 14 vorherige Informationspflichten des Arbeitgebers gegenüber den Beschäftigten vor. Das bedeutet, dass die Beschäftigten über die Datenverarbeitungsvorgänge, die im Zusammenhang mit der GPS-Ortung stehen, insbesondere die Möglichkeiten einer Verhaltens- und Leistungskontrolle vorab zu informieren sind. Ist eine private Nutzung der Firmenfahrzeuge gestattet, müssen die Beschäftigten die Möglichkeit haben, die Ortung abzuschalten. Die Möglichkeit der Beschäftigten, eine Fahrt manuell als „Privatfahrt“ zu deklarieren und damit das Tracking zu unterbinden, läuft aber dann ins Leere, wenn das Kilometerlimit für Privatfahrten aus steuerrechtlichen Gründen begrenzt ist.

Offenbar als Reaktion auf eine Beschwerde beim LfDI stellte ein rheinland-pfälzisches Unternehmen die GPS-Überwachung umgehend ein und kam auch seiner Verpflichtung nach, einen Datenschutzbeauftragten zu bestellen.

Doch längst nicht immer sind Beschwerden im Zusammenhang mit der Fahrzeugüberwachung berechtigt. In einem anderen Fall wurde an den LfDI herangetragen, die Fahrzeuge eines Kurierdienstes seien mit einer Kamera ausgestattet, welche die Fahrer während der ganzen Fahrt überwachen würde. Tatsächlich handelte es sich dabei lediglich um eine sogenannte Dash-Cam, die nur bei Unfällen aufzeichnet und vom Fahrer auf freiwilliger Basis vor der Fahrt manuell aktiviert werden kann. Der Verantwortliche konnte nachweisen, die Beschäftigten vorab ordnungsgemäß hiervon unterrichtet zu haben.

6.3 Löschung von Bewerbungsunterlagen nach Zurückziehen der Bewerbung

Im Berichtszeitraum erreichten den LfDI wiederholt Eingaben Betroffener, die sich darüber beschwerten, dass Unternehmen ihnen nicht die unverzügliche Löschung ihrer Bewerbungsunterlagen bestätigten, obwohl sie ihre Bewerbung zurückgezogen hatten.

Richtig ist, dass nach Art. 17 Abs. 1 Buchst. a DS-GVO die betroffene Person das Recht hat, von dem Verantwortlichen zu verlangen, dass die sie betreffenden personenbezogenen Daten unverzüglich gelöscht werden, sofern die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Hiervon gibt es aber Ausnahmen: So gilt die Löschverpflichtung des Verantwortlichen etwa

dann nicht, wenn die Verarbeitung für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist, vgl. Art. 17 Abs. 3 Buchst. e DS-GVO.

Öffentliche und private Stellen müssen nach den Bestimmungen des Allgemeinen Gleichbehandlungsgesetzes (AGG) nachweisen, dass kein Verstoß gegen die Bestimmungen zum Schutz vor Benachteiligung vorgelegen hat (§ 22 AGG). Ansonsten müssen sie Entschädigung und Schadensersatz an die Person leisten (§ 15 AGG). Solange der Verantwortliche mit dem Vorwurf der Diskriminierung rechnen muss, darf er die Bewerbungsunterlagen aufbewahren. Eine Aufbewahrungsfrist von sechs Monaten ist dabei – auch bei einem Rückzug der Bewerbung – datenschutzrechtlich nicht zu beanstanden:

§ 15 Abs. 4 AGG sieht eine Frist von zwei Monaten zur Geltendmachung des Anspruchs einer Diskriminierung vor; die dreimonatige Frist des § 61b Abs. 1 Arbeitsgerichtsgesetz schließt sich an die Geltendmachung dieses Anspruchs an. Für die Abwicklung des Verfahrens ist ein weiterer Monat hinzuzurechnen.

Würden die Bewerbungsunterlagen nach einer Rücknahme der Bewerbung unverzüglich gelöscht, könnte die Person im Nachgang behaupten, die Bewerbung nur deshalb zurückgezogen zu haben, weil sie sich diskriminiert gefühlt habe. Das Unternehmen oder die öffentliche Stelle hätte dann keine Möglichkeit mehr, die Diskriminierungsfreiheit der Auswahlentscheidung zu beweisen.

Hinzu kommt, dass nicht nur die Betroffenen, sondern auch andere Bewerber:innen den Vorwurf der Diskriminierung im Bewerbungsverfahren erheben können. Daher hat der Verantwortliche auch gegenüber diesen ein berechtigtes Interesse daran, die Auswahlentscheidung insgesamt bis zum Ablauf der Sechsmonatsfrist zu dokumentieren.

7. MEDIEN UND WERBUNG

7.1 Webdienste, Apps und Social Media

Die Anzahl von Hinweisen und Beschwerden im Hinblick auf Internetdienste, Apps und Social Media bleibt auch im Jahr 2024 hoch und betrifft weiter eine breite Palette an Themen. Hierbei zeigt sich regelmäßig, dass die Digitalisierung des Lebens in nahezu alle gesellschaftlichen Bereiche vorgedrungen ist. Veröffentlichungen in Social-Media-Netzwerken spielten ebenso eine Rolle wie Privatpersonen, die sich in Nachbarschaftsstreitigkeiten gegenseitig mit dem Smartphone filmten. Auch der Einsatz von Cookies und anderen Trackingtechnologien auf Webseiten und in Apps wird weiterhin regelmäßig durch Hinweisgeber:innen bemängelt, wenn auch nicht mehr in so starkem Ausmaß wie in vergangenen Jahren. Immer wieder beschweren sich Personen, dass ihre Grundstücke oder auch öffentliche Bereiche durch fliegende Drohnen gefilmt werden.

Vermehrt sind in 2024 Fälle an den LfDI herangetragen worden, in denen Personen Leistungsbescheide von Ausländer- und Sozialbehörden in Social-Media-Netzwerken oder Messenger-Gruppen veröffentlichen, offenbar um anzuprangern, dass Menschen in Asylverfahren hohe Leistungen beziehen würden. Abfotografierte Leistungsbescheide werden zum Beispiel in Facebook-Profile eingestellt oder im WhatsApp-Status versendet. Sie enthalten in der Regel die Namen der Leistungsempfänger und stellen daher für diese durch die unzulässige Verarbeitung ihrer personenbezogenen Daten auch ein Risiko dar, in ihrem örtlichen Lebensbereich oder online zum Ziel von Anfeindungen zu werden. Neben Leistungsbescheiden werden auch andere behördliche Dokumente und gerichtliche Entscheidungen o.Ä. in Social-Media-Netzwerken und Messengern veröffentlicht, üblicherweise vor dem Hintergrund persönlicher Konflikte, die auf diese Weise vor Publikum ausgetragen werden. Der LfDI geht allen diesen Fällen nach. Die Veröffentlichung von Leistungsdaten oder anderer amtlicher Dokumente anderer Personen an einen großen Empfängerkreis ohne deren Zustimmung stellt einen schweren Datenschutzverstoß dar und kann mit empfindlichen Bußgeldern geahndet werden.

Ein weiterer Schwerpunkt lag auf einer Webseite in Rheinland-Pfalz, die verschiedene Dienste gegen Gebühr vermittelt, die eigentlich kostenfrei zu erhalten sind, z.B. die Terminbuchung beim Standesamt oder die Ummeldung beim Gebührenservice für den Rundfunkbeitrag. Die Webseite ist so gestaltet, dass einige Personen sie für die Webseite des jeweilig gewünschten Dienstes halten und erst nach Vertragsschluss bemerken, dass sie für eine kostenlose Verwaltungs-oder Dienstleistung einen kostenpflichtigen Vertrag geschlossen haben. Die Beschwerdeführer begründen eine Beschwerde beim LfDI dann mit Auskunfts- (Art. 15 DS-GVO) oder Löschungsanträgen (Art. 17 DS-GVO), da der Verantwortliche auf diese nicht reagiert. Das zugrundeliegende Problem, der Streit über den kostenpflichtigen Vertrag, liegt hier im Zivilrecht und außerhalb der Prüfungskompetenz des LfDI begründet. Der LfDI kann daher nicht dafür sorgen, dass betroffene Personen ihr Geld zurückerhalten. Der LfDI geht aber selbstverständlich insbesondere den Beschwerden aufgrund nicht erfüllter Auskunftsansprüche nach. Internetnutzende sollten sich vor dem Abschluss eines Vertrages auf einer Webseite anhand des Impressums davon überzeugen, dass sie es mit der Institution zu tun haben, bei der sie eine Leistung erhalten möchten (z.B. dem Standesamt oder dem Gebührenservice für den Rundfunkbeitrag).

7.2 Werbung

Der Schwerpunkt im Bereich der Werbung lag im Jahr 2024 erneut auf unerwünschter

Werbung in Form von Newslettern. Der überwiegende Teil richtete sich gegen per E-Mail verschickte Newsletter. Es wurden aber auch postalisch versendete Newsletter moniert. Insbesondere meldeten sich Personen beim LfDI, die trotz Abmeldeversuch beim Absender weiterhin Newsletter erhielten.

Werbung per E-Mail ist nur zulässig, wenn die Empfänger:innen dieser zugestimmt haben oder es sich um Werbung an Bestandskunden handelt und Produkte betrifft, die den von den Kund:innen bereits erworbenen Produkten ähneln.

Empfänger:innen von Newslettern ist zu raten, selbst gegen unerwünschte Werbung vorzugehen. Zunächst kann die Einwilligung zum Erhalt von Newslettern oder Werbung per E-Mail widerrufen werden, sofern vorher eine Einwilligung vorlag. Bei Werbung an Bestandskund:innen können betroffene Personen von ihrem Recht nach Art. 21 Abs. 2 DS-GVO Gebrauch machen und der Werbung mit Wirkung für die Zukunft widersprechen.

Werbung per Post ist grundsätzlich bis zum Widerspruch der betroffenen Person möglich, sofern die Adressdaten in zulässiger Weise erhoben wurden.

Hat eine betroffene Person der Werbung widersprochen oder die Einwilligung widerrufen, darf das Unternehmen keine Werbung mehr zusenden. Wird seitens des Unternehmens dem Werbewiderspruch oder dem Widerruf der Einwilligung nicht nachgekommen, können betroffene Personen gegen Unternehmen mit Sitz in Rheinland-Pfalz Beschwerde gegen diese beim LfDI einlegen.

Im Jahr 2024 leitete der LfDI viele Verfahren wegen Werbezusendungen trotz Widerspruch bzw. Widerruf der Einwilligung ein. Die Unternehmen werden in diesem Zusammenhang regelmäßig auf die rechtlichen Anforderungen hingewiesen und zur schnellstmöglichen Umsetzung der Werbewidersprüche aufgefordert. Die Verantwortlichen kommen der Aufforderung des LfDI in der Regel zügig nach.

7.3 Informationskampagnen zu Newslettern, Gastbestellungen und WhatsApp

Der LfDI hat im Jahr 2024 im Themenfeld Medien und Werbung drei Informationskampagnen durchgeführt. Ziel der Aktionen war es, Unternehmen und Kultureinrichtungen im Bundesland proaktiv auf die datenschutzrechtlichen Voraussetzungen hinzuweisen und die Anzahl von Verstößen zu verringern.

Die erste Informationskampagne klärte Verantwortliche über die datenschutzrechtlichen Voraussetzungen auf, die für den Versand von Newslettern und E-Mail-Werbung gelten. Hierzu wurden 30 rheinland-pfälzische Unternehmen und Kultureinrichtungen aus verschiedenen Branchen angeschrieben, um deren Aufmerksamkeit auf das Thema zu lenken und die geltenden Vorschriften zu erklären. Die angeschriebenen Verantwortlichen wurden nicht ausgewählt, weil bei ihnen selbst Verstöße festgestellt wurden, sondern in erster Linie als Werbetreibende, die diese Art der Kommunikation regelmäßig nutzen.

Die zweite Informationskampagne bezog sich auf die datenschutzrechtliche Notwendigkeit eines Gastzugangs bei Online-Shops. Dazu wurden mehr als 100 Unternehmen zuvor im Rahmen einer Stichprobe auf das Vorhandensein von Gastzugängen in ihren Online-Shops hin überprüft. Erfreulich war, dass der LfDI nur bei 13 Unternehmen Mängel feststellten konnte. Diese Verantwortlichen wurden mit Informationsschreiben auf die Notwendigkeit der Bereitstellung von Gastzugängen für den Bestellprozess hingewiesen. Ein großer Anteil der angeschriebenen Verantwortlichen stellte unmittelbar im Anschluss an das Schreibend es LfDI Gastzugänge in ihren Online-Shops bereit.

Die dritte Informationskampagne zielte auf die datenschutzrechtliche Aufklärung der Nutzung von WhatsApp ab. Hierzu wurden 25 Unternehmen angeschrieben. Da etwa 80% aller deutschen Bürger:innen WhatsApp nutzen und der Meta-Dienst somit der meistgenutzte Messenger-Dienst in Deutschland ist, war es dem LfDI ein besonderes Anliegen, auf die datenschutzrechtlichen Probleme hinzuweisen, die mit der Nutzung von WhatsApp einhergehen. In diesem Zusammenhang gab der LfDI den Verantwortlichen eine Checkliste an die Hand, die beim Einsatz von WhatsApp beachtet werden sollte.

Ausführliche Hinweise zu den o.g. Themen finden sich auf der Webseite des LfDI unter:

datenschutz.rlp.de/themen/direktwerbung-und-newsletter

datenschutz.rlp.de/themen/online-shops-gastbestellungen

datenschutz.rlp.de/themen/whatsapp

8. GESUNDHEIT

8.1 Datenschutz im Gesundheitsamt

Im Berichtszeitraum stand die Sicherstellung des Datenschutzes in den rheinland-pfälzischen Gesundheitsämtern im speziellen Fokus der Arbeit des LfDI: So wurde die Begleitung des durch das Ministerium für Wissenschaft und Gesundheit koordinierten Projekts zur landesweiten Digitalisierung des Öffentlichen Gesundheitsdienstes weiter fortgesetzt, daneben führte der LfDI anlassbezogene Prüfungen zum Datenschutz in vier ausgewählten Gesundheitsämtern vor Ort durch. Hintergrund für diese Schwerpunktsetzung war eine im November 2023 veröffentlichte Presserecherche zu vermuteten IT-Sicherheitslücken in den Gesundheitsämtern in Rheinland-Pfalz (vgl. dazu 32. TB 2023, 8.2).

Im Rahmen der Kontrollen deckte der LfDI diverse datenschutzrelevante Mängel auf, die zum Teil auch Gegenstand der Presseberichterstattung waren, teilweise zuvor aber auch nicht aufgefallen waren. Bei den vorgefundenen Missständen war zwischen softwarebedingten Defiziten und Mängeln bei der Umsetzung der datenschutzrechtlichen Vorgaben durch die Kommunalverwaltungen zu unterscheiden. So verfügte die eingesetzte IT-Anwendung weder über eine datenschutzkonforme Protokollierungsfunktion noch über die gebotene Unterstützung für eine hinreichende Verschlüsselung der Datenbanken. Auch hatte die Software im Auslieferungszustand das Prinzip der datenschutzfreundlichen Voreinstellungen nicht ausreichend beachtet. Auf der Seite der Kreisverwaltungen wiederum entsprach das Datenschutzmanagement häufig nicht den rechtlichen Anforderungen. Zudem waren die zum Schutz der Daten gebotenen technisch-organisatorischen Vorkehrungen nur rudimentär oder gar nicht dokumentiert, so dass bei einigen Maßnahmen unklar blieb, ob diese tatsächlich in der Praxis umgesetzt wurden.

In den im Juli 2024 übersandten Prüfberichten benannte der LfDI die jeweiligen Defizite und forderte die Kreisverwaltungen auf, diese zu beseitigen, soweit dies ihrerseits möglich war. Insbesondere das in drei von vier geprüften Verwaltungen bemängelte unzureichende Datenschutzmanagement stellt aus Sicht des LfDI ein großes Hindernis auf dem Weg zur Gewährleistung eines effektiven Datenschutzes auf kommunaler Ebene dar. Gerade den Kreisverwaltungen mit der Vielzahl der dort zu erfüllenden Sachaufgaben kommt in diesem Zusammenhang eine herausragende Bedeutung und nicht zuletzt eine Vorbildfunktion zu. Spätestens nach Wirksamwerden der Datenschutz-Grundverordnung im Jahre 2018 müssen die Kreisverwaltungen angesichts der in Art. 38 Abs. 2 DS-GVO normierten Unterstützungspflicht der Verantwortlichen und der in Art. 39 DS-GVO enthaltenen umfassenden Aufgaben die dort zu benennenden Datenschutzbeauftragten angemessen auswählen und ausstatten. Dass mehr als sechs Jahre später immer noch für die Aufgabenwahrnehmung ungenügende zeitliche Ressourcen bei kommunalen Datenschutzbeauftragten und unzureichende Einbindungen in datenschutzrelevante Verwaltungsabläufe festgestellt werden müssen, ist nicht hinnehmbar. Der LfDI wird sich deshalb nachdrücklich für eine Beseitigung dieser festgestellten Defizite einsetzen.

Der im Rahmen der örtlichen Feststellungen bestätigte Softwareeinsatz in den Gesundheitsämtern ohne datenschutzkonforme Protokollierungsfunktion war schließlich Gegenstand förmlicher Beanstandungen, die der LfDI gegenüber den geprüften Verwaltungen aussprach. Letztendlich betraf dieser Mangel aufgrund der landesweiten Verbreitung der IT-Anwendung sämtliche Gesundheitsämter in Rheinland-Pfalz, so dass sich die ausgesprochenen Beanstandungen inhaltlich im Ergebnis an alle 24 Kreisverwaltungen adressierten. In einem Fall kam neben dem Protokollierungsdefizit als Beanstandungsgrund auch das Feh-

len einer vertraglichen Vereinbarung zwischen der betroffenen Kreisverwaltung und dem IT-Dienstleister hinzu, der trotz fehlender Beauftragung konkrete Datenverarbeitungen zum Zwecke von Support und Fernwartung vorgenommen hatte. Die betroffenen Kreisverwaltungen sicherten in ihren Stellungnahmen zu, die sanktionierten Defizite zeitnah zu beseitigen.

Im Hinblick auf das landesweite Digitalisierungsprojekt sprach der LfDI zugleich gegenüber dem federführenden Ministerium für Wissenschaft und Gesundheit des Landes Rheinland-Pfalz folgende konkrete Empfehlungen zur datenschutzkonformen Digitalisierung des Öffentlichen Gesundheitsdienstes in Rheinland-Pfalz aus:

- Die Digitalisierung des öffentlichen Gesundheitsdienstes in Rheinland-Pfalz setzt ein funktionierendes internes Datenschutzmanagement bei den Gesundheitsämtern bzw. den diese tragenden Kreisverwaltungen voraus.

- Bei Auswahl und Einsatz von IT-Anwendungen im Öffentlichen Gesundheitsdienst sind die Anforderungen an die Datensicherheit (Art. 24/Art. 32 DS-GVO) und die Grundsätze von privacy by design und privacy by default (Art. 25 DS-GVO) zwingend zu beachten. Software-Produkte müssen die Umsetzung dieser Anforderungen technisch unterstützen.

- Aufgrund der besonderen Schutzbedürftigkeit der im Öffentlichen Gesundheitsdienst verarbeiteten Gesundheitsdaten der Bürgerinnen und Bürger muss jederzeit gewährleistet sein, dass diese innerhalb der Verwaltungen nur von denjenigen Beschäftigten zur Kenntnis genommen und verarbeitet werden können, die diese zur Erfüllung der ihnen zugewiesenen Aufgaben benötigen („Need-to-know-Prinzip“).

- Durch technisch-organisatorische Maßnahmen muss sichergestellt werden, dass die Einhaltung der Anforderungen an den Datenschutz und die Datensicherheit in den Verwaltungen dauerhaft dokumentiert ist und intern und extern überprüft werden kann. Hierzu gehören interne Konzepte zur Nutzerverwaltung, der Vergabe von Zugriffsrechten, der Datensicherung, der IT-Sicherheit, der Protokollierung und der Löschung sowie die Nachvollziehbarkeit ihrer jeweiligen Umsetzung.

- Der Einsatz von Dienstleistern, die personenbezogene Daten von Bürgerinnen und Bürgern beispielsweise im Rahmen der Fernwartung oder des IT-Supports zur Kenntnis nehmen können, setzt ausnahmslos das Vorhandensein einer vertraglichen Vereinbarung im Sinne von Art. 28 Abs. 3 DS-GVO voraus.

- Im Rahmen des Digitalisierungsprojekts sollten die Gesundheitsämter bei der Umsetzung der datenschutzrechtlichen Anforderungen so weit wie möglich durch das Land bzw. die im Projekt vorgesehene Leitstelle unterstützt werden. Hierzu gehören u.a. Festlegungen mit dem Hersteller der im ÖGD vorgesehenen Fachanwendungen zur Gewährleistung von Datenschutz und Datensicherheit in dessen IT-Produkten sowie eine landesweite Klärung der in den Gesundheitsämtern anzusetzenden Aufbewahrungsfristen. Auch an die einzelnen Kommunalverwaltungen gerichtete Handreichungen können hier ein geeignetes Mittel sein. Diese Handreichungen sollten konkrete Hinweise und Anleitungen enthalten, um eine effektive Verwirklichung der Anforderungen vor Ort sicherzustellen.

Die Umsetzung dieser Empfehlungen wird sowohl von der Landesregierung als auch den beteiligten Kommunalverwaltungen befürwor-

tet. Ob dies gelingt, bleibt abzuwarten. Der LfDI wird den weiteren Prozess der Digitalisierung des Öffentlichen Gesundheitsdienstes in Rheinland-Pfalz kritisch und konstruktiv begleiten.

8.2 Gültigkeitsdauer von Einwilligungen

Im Zusammenhang mit der Datenverarbeitung in medizinischen Registern wurde der LfDI um eine Stellungnahme gebeten, ob darauf gerichtete Einwilligungserklärungen von Patient:innen einer bestimmten Gültigkeitsdauer unterliegen. Hintergrund der Anfrage waren offensichtliche Schwierigkeiten bei der Einholung der für die Registertätigkeit notwendigen Informationen. So hatten wohl wiederholt Arztpraxen ihre Auskunfts- und Kooperationsbereitschaft mit dem Argument eingestellt, die von den Patient:innen abgegebenen Einwilligungen seien älter als fünf Jahre und deshalb nicht mehr gültig.

In seiner Stellungnahme verwies der LfDI auf die eindeutige Rechtslage. Datenschutzrechtliche Einwilligungen unterliegen den rechtlichen Anforderungen des Art. 7 DS-GVO sowie ggf. bestehender bereichsspezifischer Besonderheiten. Die Befristung der Gültigkeit von Einwilligungserklärungen ist hiernach regelmäßig nicht vorgesehen, so dass diese sich lediglich aus dem Text der jeweiligen Einwilligungserklärung selbst ergeben könnte. So sieht beispielsweise der im Rahmen der Medizin-Informatik-Initiative bereitgestellte Mustertext einer Patienteneinwilligung eine Gültigkeitsdauer der Einwilligung von fünf Jahren vor.

Eine Verweigerung der Datenverarbeitung mit dem Hinweis auf das Alter der zugrundeliegenden Einwilligungserklärung ist somit aus datenschutzrechtlicher Sicht nicht haltbar, wenn nicht eine zeitliche Befristung der Gültigkeit in der Erklärung selbst enthalten ist. Im Interesse der betroffenen Personen hält es der LfDI allerdings grundsätzlich für begrüßenswert, wenn zumindest bei Einwilligungserklärungen, die sich auf eine zeitlich unbegrenzte Verarbeitung besonders schutzbedürftiger Daten im Sinne des Art. 9 DS-GVO beziehen, die betroffenen Personen in regelmäßigen Intervallen von den Verantwortlichen auf die von ihnen abgegebenen Erklärungen und deren Relevanz aufmerksam gemacht werden. Dies dient dem in Art. 5 Abs. 1 DS-GVO verankerten Grundsatz der Transparenz der Datenverarbeitung und stärkt die informationelle Selbstbestimmung der Betroffenen.

8.3 Neues aus der Initiative „Mit Sicherheit gut behandelt“: Monatliche Praxistipps

Datenschutz ist ein zentrales Thema in Arzt- und Psychotherapiepraxen. Aus diesem Grund versucht die seit mehr als zehn Jahren bestehende und bundesweit einmalige Initiative „Mit Sicherheit gut behandelt“, der neben dem LfDI auch die Kassenärztliche Vereinigung Rheinland-Pfalz sowie die im Lande ansässigen Landesärzte- und Landespsychotherapeutenkammern angehören, mit unterschiedlichen Aktivitäten die Umsetzung des Datenschutzes durch die Praxisinhaberinnen und -inhaber zu unterstützen. Hierzu gehörten neben der zentralen Webseite **www.mit-sicherheit-gut-behandelt.de** in der Vergangenheit zahlreiche Fortbildungs- und Informationsveranstaltungen, in denen neben praktischen Hilfestellungen zum Umgang mit datenschutzrechtlichen Anforderungen auch übergeordnete Zusammenhänge in einem größeren Rahmen diskutiert wurden (vgl. hierzu beispielsweise den Beitrag im 32. Tätigkeitsbericht unter 8.1 zur Fachtagung „Was passiert mit unseren Gesundheitsdaten? – Möglichkeiten und Grenzen der digitalen Nutzung von Gesundheitsdaten“, die am 13. November 2023 erfolgreich in Mainz stattfand).

Für das Jahr 2025 will die rheinland-pfälzische Initiative den Behandelnden mit monatlich veröffentlichten Praxistipps konkrete und aktuelle Hilfestellung geben, wie sie die gesetzlichen Vorgaben in ihren Arbeitsalltag integrieren können. Die Planungen dazu fanden im letzten Quartal des Jahres 2024 statt. Danach sollen die Praxistipps auf der Webseite der Initiative jeweils eine im Praxisbetrieb relevante datenschutzrechtliche Frage mit dazugehöriger Antwort vorstellen. Zusätzlich ist geplant, den Behandelnden Hinweise zu den jeweils maßgeblichen Rechtsgrundlagen zu geben und über weiterführende Links Hintergrundinformationen bereitzustellen. Zum Zwecke einer besseren Nutzbarkeit verständigten sich die Kooperationspartner darauf, die veröffentlichten Tipps als druckbare PDF-Dateien zum Herunterladen anzubieten.

Den Auftakt machten zu Beginn des Jahres 2025 drei Tipps rund um den datenschutzrechtlichen Auskunftsanspruch von Patient:innen (**www.s.rlp.de/msgb-praxistipps**). Hierzu besteht nach den Erfahrungen des LfDI weiterhin ein großer Klärungsbedarf. Die weiteren Tipps sollen sich u.a. mit Fragen zur datenschutzkonformen Kommunikation von Heilberufspraxen per E-Mail, den Anforderungen an eine wirksame Einwilligung, den Rahmenbedingungen zur Nutzung sozialer Medien sowie zur Einbindung von Dienstleistern zur Terminverwaltung befassen.

Die Initiative hofft, durch innovative und praxistaugliche Instrumente bei den Inhaber:innen von Heilberufspraxen mehr Verständnis für datenschutzrechtliche Anliegen zu erzeugen. Zugleich verstehen sich die Kooperationspartner in diesem Zusammenhang als Dienstleister für die von den Vorgaben des Datenschutzes betroffenen Praxen. Es besteht jederzeit die Möglichkeit, sich mit kreativen Ideen und Ansätzen in die Arbeit der Initiative einzubringen.

9. UMWELT UND BIOTECHNOLOGIE

9.1 Umwelt: Datenschutzbeauftragte im Bereich Jagdgenossenschaften

Datenschutzrechtliche Fragestellungen aus dem Bereich der Jagdgenossenschaften haben den LfDI im Berichtszeitraum wiederholt beschäftigt. Dabei ging es regelmäßig um die Frage, ob Jagdgenossenschaften zur Benennung von eigenen Datenschutzbeauftragten verpflichtet sind. Gemäß Art. 37 Abs. 1 lit. a DS-GVO hat jede Behörde oder öffentliche Stelle einen Datenschutzbeauftragten zu benennen. Jagdgenossenschaften sind als Körperschaften des öffentlichen Rechts öffentliche Stellen im Sinne des Datenschutzrechts und daher unabhängig von ihrer Größe zur Benennung von eigenen Datenschutzbeauftragten verpflichtet.

Ausnahmen von dieser bestehenden Benennungspflicht sind nicht vorgesehen. Allerdings hat der Gesetzgeber auch kleinere und finanziell weniger stark ausgerüstete öffentliche Stellen berücksichtigt. Denn gemäß Art. 37 Abs. 3 DS-GVO kann für mehrere öffentliche Stellen abhängig von ihrer Organisationsstruktur und Größe ein gemeinsamer Datenschutzbeauftragter benannt werden. So ist es beispielsweise möglich, dass mehrere Jagdgenossenschaften einen gemeinsamen Datenschutzbeauftragten bestellen oder Datenschutzbeauftragte von naheliegenden Kommunalverwaltungen als eigene Datenschutzbeauftragte benennen. Im Austausch mit einer Jagdgenossenschaft wurde auch die Möglichkeit diskutiert, einen externen Datenschutzbeauftragten unter Vertrag zu nehmen. Der LfDI ist dafür vor dem Hintergrund des Art. 37 Abs. 6 DS-GVO ebenfalls offen.

Weitere Informationen zu behördlichen Datenschutzbeauftragten stehen im Internet-Angebot des LfDI unter **www.s.rlp.de/bDSB** zur Verfügung.

9.2 Biotechnologie

Rheinland-Pfalz hat sich spätestens nach der Corona-Pandemie als bedeutender Standort der Biotechnologie etabliert. Hierzu gehören nicht nur die Ansiedlung global agierender innovativer Unternehmen, sondern auch die im Lande bestehenden idealen Voraussetzungen für eine Vernetzung von Wissenschaft und Wirtschaft in diesem zukunftsträchtigen Feld.

Der LfDI hat es sich zur Aufgabe gemacht, den in Rheinland-Pfalz ansässigen Akteur:innen der Biotechnologie-Szene frühzeitig und praxisnah seine Expertise in Sachen Datenschutz zur Verfügung zu stellen. Auch wenn grundsätzlich denkbare Unterstützungsangebote wie zum Beispiel die Einrichtung einer Beratungssprechstunde speziell für Firmengründer:innen und Start-ups oder die Bereitstellung geeigneter Instrumentarien zur Klärung der Datenschutzkonformität von Anwendungen, die biotechnologische Produkte begleiten, an den derzeit noch fehlenden Personalressourcen scheitern, haben sich im Berichtsjahr konkrete Kooperationsmöglichkeiten zur Stärkung des Datenschutzes im Bereich Biotechnologie ergeben. Gemeinsam mit dem in Mainz ansässigen Unternehmen BioNTech wird der LfDI im Jahr 2025 eine Webinar-Reihe zum Thema „Datenschutz im Biotech-Unternehmen“ auflegen, die sich speziell an Akteur:innen im Bereich der Biotechnologie richtet. Ziel ist es, Umsetzung und Einhaltung der datenschutzrechtlichen Vorgaben auf anschauliche Weise näher zu bringen. In vier quartalsweise angebotenen Webinare sollen nicht nur Grundlagen zum Datenschutz vermittelt werden, sondern abhängig von den im Vorfeld geäußerten Bedarfen auch spezielle Themen wie z.B. Forschung mit Gesundheitsdaten, Beschäftigtendatenschutz und Datensicherheit behandelt werden.

Der LfDI sieht in der von ihm beabsichtigten Unterstützung der Biotechnologie-Szene ein zukunftsweisendes Tätigkeitsfeld, das die Aufgaben der Datenschutzaufsichtsbehörde im Hinblick auf einen proaktiven Datenschutz

konstruktiv ergänzt. Die im Berichtsjahr zu diesem Ansatz erhaltenen ermutigenden Rückmeldungen aus Politik und Wirtschaft deuten darauf hin, dass insoweit ein klarer Unterstützungsbedarf besteht. In welchem Maße der LfDI diesem nachkommen kann, bleibt nicht zuletzt von den ihm zur Verfügung gestellten Ressourcen abhängig.

10. SOZIALES

10.1 Datenaustausch zwischen Sozialleistungsträgern und Vermietern

Sofern beantragte Sozialleistungen auch die Übernahme von Mietkosten beinhalten sollen, besteht regelmäßig ein Dreiecksverhältnis zwischen den Hilfebedürftigen, der Sozialbehörde und den Vermietern. Immer wieder kommt es in diesem Zusammenhang zu einem Datenaustausch zwischen Behörde und Vermietern, der Gegenstand von an die Datenschutzaufsicht gerichteten Beschwerden ist.

So hatte in einem an den LfDI herangetragenen Fall die für die Gewährung von Grundsicherungsleistungen zuständige Verwaltung den Vermieter der Antragstellerin wiederholt unmittelbar kontaktiert und Informationen zum Leistungsbezug mitgeteilt sowie Fragen zum Bestand des Mietverhältnisses und dem Zustand der Mietwohnung gestellt. Die hiervon betroffene Leistungsempfängerin hatte allerdings in die direkte Kontaktaufnahme nicht eingewilligt. Die Behörde erläuterte ihr zudem zu keinem Zeitpunkt, aus welchen Gründen, zu welchem Zweck und auf welcher Rechtsgrundlage der Vermieter von ihr befragt worden war. In einer an den LfDI gerichteten Beschwerde wandte sich die Betroffene gegen die aus ihrer Sicht datenschutzwidrige Vorgehensweise der Sozialverwaltung.

Die Kreisverwaltung bestätigte gegenüber dem LfDI die unmittelbare Kontaktaufnahme mit dem Vermieter. Hintergrund sei die von der Beschwerdeführerin mitgeteilte Kündigung des bisherigen Mietvertrags gewesen, die im Ergebnis zu der Beendigung des Leistungsbezugs geführt hätte. Mit der Kontaktierung des Vermieters habe die Verwaltung eine Information über die behauptete Kündigung erhalten wollen, um ggf. eine dadurch drohende Obdachlosigkeit der Beschwerdeführerin durch Ergreifen geeigneter Maßnahmen und Hilfsangebote abzuwenden. Die Sozialbehörde räumte allerdings ein, dass der Datenaustausch mit dem Vermieter nicht zu ihrer Aufgabenerfüllung erforderlich gewesen war. Vielmehr hätte es ausgereicht, bei der Beschwerdeführerin nachzufragen, ob die Kündigung erfolgt sei und ob sie ggf. weitere Hilfeleistungen benötige.

Der LfDI stellte im Ergebnis einen Verstoß gegen die Vorgaben des Sozialdatenschutzrechts fest und beanstandete diesen gegenüber der betroffenen Kreisverwaltung. Die von dem Vermieter erbetenen Informationen waren für die von der Verwaltung in Bezug auf den Sozialleistungsbezug der Beschwerdeführerin zu treffenden Entscheidungen nicht erforderlich gewesen. Diese hatte bereits selbst angegeben, aufgrund der Wohnungskündigung keine Unterkunftskosten mehr geltend zu machen, so dass der Sozialleistungsträger auch keine weiteren Leistungen gewähren musste. Sofern Zweifel an der Richtigkeit dieser Informationen bestanden haben sollten, hätte die Behörde die Beschwerdeführerin um Vorlage eines Nachweises der Kündigung bitten und zugleich auf den damit verbundenen Wegfall des Leistungsbezugs hinweisen können. Zudem hätte die Verwaltung ggf. den weiteren Hilfebedarf der Beschwerdeführerin im Falle der Kündigung des Mietverhältnisses abklären können. Eine unmittelbare Datenerhebung bei dem Vermieter war nach Einschätzung des LfDI dagegen nicht erforderlich.

Der Sachverhalt ist exemplarisch für die gerade im Sozialbereich verbreitete Haltung, Sozialdaten mit Dritten austauschen zu dürfen, wenn dies im vermuteten Interesse der betroffenen Personen steht. Auch wenn die dahinterstehende Absicht als ehrenhaft anzusehen ist, verkennt ein derartiges Vorgehen das auch Hilfebedürftigen zustehende Grundrecht auf informationelle Selbstbestimmung. Der „gute Zweck“ heiligt nicht alle Mittel. Vielmehr sollten die betroffenen Personen im Regelfall als vorrangige Ansprechpartner:innen respektiert und behandelt werden, wenn es um Datenver-

arbeitungen zum Zwecke der Bereitstellung von Hilfen und Unterstützungen geht. Nur in den gesetzlich zugelassenen Fällen darf hiervon abgewichen werden.

10.2 Dauerbrenner Datenverarbeitung durch Jobcenter: Die Anforderung von Kontoauszügen und die Anfertigung von Personalausweis-Kopien

Die Frage der datenschutzrechtlichen Zulässigkeit der Anforderung von Unterlagen durch Jobcenter im Rahmen der Grundsicherung für Arbeitssuchende beschäftigt den LfDI regelmäßig. In der Vergangenheit hatte sich der LfDI bereits wiederholt hierzu geäußert (vgl. z.B. Beitrag im 28. Tätigkeitsbericht 2019, Nr. 10, S. 61 ff., und 26. Tätigkeitsbericht 2016/20217, Nr. 6.3, S. 91f.).

Nach den gesetzlichen Vorgaben haben Antragsteller:innen von Grundsicherungsleistungen dem Jobcenter die erforderlichen Unterlagen vorzulegen, um das Vorliegen der Bewilligungsvoraussetzungen überprüfen zu können. Dies schließt die Überprüfung der Identität und Hilfebedürftigkeit der Leistungsempfänger:innen ein.

Nach der gefestigten Rechtsprechung des Bundessozialgerichts und der Auffassung der Datenschutzaufsichtsbehörden ist die Anforderung von Kontoauszügen der letzten drei Monate datenschutzrechtlich zulässig (vgl. BSG, Urteil vom 19.09.2008, Az. B 14 AS 45/07 R; BSG, Urteil vom 19.02.2009, Az. B 4 AS 10/08 R). Denn die Vorlage der Kontoauszüge dient dem Nachweis der Hilfebedürftigkeit der Antragsteller:innen sowie der von diesen im Leistungsantrag gemachten Angaben und ist damit zur Aufgabenerfüllung der Jobcenter erforderlich. Die antragstellenden Personen trifft insoweit eine Mitwirkungspflicht. Dies gilt ebenso für den Fall, dass die betroffene Person schon Leistungen bezogen hat und nun die Fortsetzung der Leistungsgewährung für Folgezeiträume geltend macht. Bei der Antragstellung müssen die Leistungsträger auf die Möglichkeit der Schwärzung nicht leistungserheblicher Informationen auf der Ausgabenseite hinweisen, soweit daraus besondere Arten personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO wie beispielsweise Angaben zur Parteizugehörigkeit oder des konfessionellen Bekenntnisses ersichtlich wären. Dies bedeutet allerdings nicht, dass Kontoauszüge, die keinerlei Buchungseingänge (Gutschriften) enthalten, nicht leistungserheblich sind. Vielmehr ermöglicht gerade das Nichtvorhandensein von Gutschriften Rückschlüsse auf die Einnahmeseite und ist damit für das Jobcenter im Rahmen der Prüfung der Leistungsbewilligung erforderlich.

Gesondert zu betrachten ist die Frage, ob und wie lange die angeforderten Kontoauszüge von den Jobcentern gespeichert werden dürfen. Der LfDI hatte bislang die Vorlage und Sichtung der Kontoauszüge und einen anschließenden Aktenvermerk ohne weitere Speicherung der Dokumente für ausreichend gehalten, sofern sich daraus nicht bislang unbekannte leistungsrelevante Inhalte ergeben haben. Nach der Rechtsprechung des Bundessozialgerichts (Urteil vom 14. Mai 2020) ist eine regelmäßige Speicherung der vorgelegten Unterlagen für einen Zeitraum von zehn Jahren nach Bekanntgabe der Leistungsbewilligung zulässig, soweit dies für die Aufgabenerfüllung erforderlich ist (vgl. § 67c Abs. 1 SGB X) und die Möglichkeit der Schwärzung eingeräumt wurde. Es kommt somit nicht darauf an, ob die Unterlagen im Rahmen der Weiterbewilligung der Leistungen vorgelegt wurden oder sich daraus leistungsrelevante neue Erkenntnisse ergeben. Das Bundessozialgericht begründet seine Entscheidung damit, dass bloße Aktenvermerke nicht alle Einnahmen im Leistungszeitraum dokumentieren würden und daher keinen hinreichenden Beweiswert bieten.

Der LfDI schließt sich nunmehr – wie auch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die anderen Datenschutzaufsichtsbehörden – dieser Rechtsauffassung an. Die Aufnahme von Kontoauszügen in die Verfahrensakten für einen Zeitraum von zehn Jahren nach Bekanntgabe der Leistungsbewilligung begegnet insoweit keinen datenschutzrechtlichen Bedenken mehr.

Zur Überprüfung der Identität der Antragsteller:innen dürfen die Jobcenter auch die Vorlage eines gültigen Personalausweises verlangen. Es besteht allerdings häufig Klärungsbedarf im Hinblick auf ein datenschutzgerechtes Vorgehen bezüglich der Anfertigung einer Personalausweiskopie und deren Ablage in die Leistungsakte.

Nach § 20 Abs. 2 S. 3 Personalausweisgesetz (PAuswG) ist sowohl die Anfertigung einer Ablichtung personenbezogener Daten aus dem Personalausweis als auch deren Speicherung nur zulässig, wenn der Ausweisinhaber bzw. die Ausweisinhaberin darin eingewilligt haben. Bei der Anfertigung und aktenmäßigen Speicherung von Personalausweiskopien sind allerdings neben den Vorgaben des Personalausweisgesetzes auch die allgemeinen datenschutzrechtlichen Anforderungen und damit der Grundsatz der Erforderlichkeit bzw. Datenminimierung zu beachten. Denn zum Nachweis der Identität ist es regelmäßig ausreichend, wenn der Personalausweis bzw. dessen Kopie nur vorgelegt und nach Sichtung ein entsprechender Vermerk über die erfolgte Vorlage in die Leistungsakte aufgenommen wird. Die Speicherung der Ausweiskopie selbst ist dagegen nicht erforderlich.

Nur in Ausnahmefällen ist die Anforderung der Kopie eines Ausweispapiers durch den Leistungserbringer erforderlich, sofern Zweifel an der Identität der Antragstellenden bestehen. In diesen Fällen sind die Antragstellenden ausdrücklich darauf hinzuweisen, dass Schwärzungen von Angaben, die für die Identifizierung im konkreten Fall nicht notwendig sind (etwa Seriennummer, Staatsangehörigkeit, das Lichtbild, Größe, Augenfarbe etc.), vorgenommen werden können.

Vor diesem Hintergrund hat der LfDI in dem Berichtszeitraum eine Beanstandung gegen eine Kreisverwaltung ausgesprochen, die eine Kopie der Vorder- und Rückseite des Personalausweises eines Antragstellenden zur Leistungsakte genommen hatte, obgleich weder Identitätszweifel bestanden noch eine Belehrung über bestehende Schwärzungsoptionen erfolgte. Zudem wurden die ungeschwärzten Ausweiskopien erst nach entsprechender Einschaltung des LfDI gelöscht.

10.3 Erreichbarkeit von Datenschutzbeauftragten der Sozialverwaltung

In einem Beschwerdeverfahren wurde die über den Einzelfall hinausgehende Frage aufgeworfen, ob die Einrichtung einer automatischen und für Bürger:innen nicht erkennbaren Weiterleitung des an die Funktionsadresse der Datenschutzbeauftragten einer Sozialbehörde gerichteten E-Mail-Verkehrs an andere Personen innerhalb der Verwaltung noch mit den Vorgaben des Datenschutzes vereinbar ist. Im konkreten Fall war die Weiterleitung nur vorübergehend für den Fall einer vorhersehbaren, zeitlich begrenzten Abwesenheit der behördlichen Datenschutzbeauftragten eingerichtet worden. Die über die Funktionsadresse eingehenden E-Mails wurden einer Person in der Verwaltung bereitgestellt, die als Datenschutzkoordinator:in Teil des behördlichen Datenschutzmanagements war und bereits über ein fundiertes datenschutzrechtliches Fachwissen verfügte. Die Absender der an die Funktionsadresse gerichteten Nachrichten wurden über die Einrichtung der Weiterleitung erst nach Versand der E-Mails informiert.

Die im Rahmen der Beschwerde geltend gemachten Bedenken gegen die Zulässigkeit einer derartigen automatischen Weiterleitung wurden seitens des LfDI im Ergebnis nicht geteilt.

Insbesondere konnte der LfDI keine Verletzung der Regelung des Art. 38 Abs. 4 DS-GVO feststellen. Hiernach haben von einer Datenverarbeitung betroffene Personen das Recht, den von der verantwortlichen Stelle benannten Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte im Zusammenhang stehenden Fragen zu Rate zu ziehen.

Mit einer lediglich vorübergehenden Weiterleitung von E-Mails, die nicht persönlich, sondern nur funktional adressiert wurden, an im Umfeld der Datenschutzbeauftragten ernannte, datenschutzrechtlich qualifizierte Personen wird das aus Art. 38 Abs. 4 DS-GVO garantierte Recht der betroffenen Personen auf unmittelbaren Zugang zu den formell benannten Datenschutzbeauftragten und die damit einhergehende Vertraulichkeit der Kommunikation nicht unverhältnismäßig eingeschränkt. Vielmehr müssen betroffene Personen, die sich mit konkreten Anliegen über Funktionsadressen an behördliche Datenschutzbeauftragten wenden, damit rechnen, dass zeitweise ihre elektronischen Schreiben oder Nachrichten von anderen, dem Funktionsbereich des internen Datenschutzmanagements angegliederten Personen der Verwaltung zur Kenntnis genommen werden können.

Grundsätzlich steht den behördlichen oder betrieblichen Datenschutzbeauftragten im Interesse eines funktionierenden Datenschutzmanagements durchaus die Option zu, an ihre Funktion gerichtete Nachrichten im Falle einer planbaren vorübergehenden Abwesenheit zeitweise an Personen, die den Aufgaben der Datenschutzbeauftragten nahestehen, intern weiterzuleiten. Regelungen aus der Datenschutz-Grundverordnung, die dies untersagen, sind nicht ersichtlich. Auch eine Abwägung der Interessen der betroffenen Personen an einer vertraulichen Behandlung ihrer Anliegen mit dem Interesse an einem funktionierenden Datenschutzmanagement führt zu keinem anderen Ergebnis. Solange die an eine derartige Funktionsadresse gerichteten Nachrichten nicht an einen beliebigen Kreis von Empfänger:innen innerhalb einer Verwaltung weitergeleitet werden, sondern nur ausgewählten, organisatorisch dem internen Datenschutzmanagement zugeordneten und diesbezüglich besonders qualifizierten Personen zur Kenntnis gelangen, ist dies datenschutzrechtlich mit den Vorgaben des Art. 38 Abs. 4 DS-GVO vereinbar. Dem Interesse der Betroffenen an einer vertraulichen Kommunikation mit dem internen Datenschutzmanagement wird damit weiterhin ausreichend entsprochen. Zudem enthält die Rechtsordnung keine Anhaltspunkte dafür, dass eine entsprechende Erwartung der Betroffenen in eine ausschließliche und persönliche Kommunikation mit den Datenschutzbeauftragten über Funktionsadressen geschützt wird. Sofern die betroffenen Personen sich unmittelbar an einen bestimmten Mitarbeiter der Verwaltung wenden wollen, steht ihnen vielmehr alternativ zu der Funktionsadresse weiterhin die Option einer Versendung ihrer Anliegen an eine persönliche E-Mail-Adresse der gewünschten Person zur Verfügung.

11. KOMMUNALES

11.1 Netzwerktreffen mit den behördlichen Datenschutzbeauftragten rheinland-pfälzischer Kommunen

BRegelmäßig lädt der Landesbeauftragte für den Datenschutz und die Informationsfreiheit zum Informationsaustausch die behördlichen Datenschutzbeauftragten der rheinland-pfälzischen Gemeinden ein. Im Rahmen dieser Netzwerktreffen werden aktuelle datenschutzrechtliche Fragestellungen behandelt und zwischen den Teilnehmenden ausführlich diskutiert. Ziel ist es, für drängende Problemstellungen zu sensibilisieren und mögliche Lösungsansätze in der Breite zu kommunizieren.

Nachdem die vergangenen Netzwerktreffen pandemiebedingt ausschließlich online stattfanden, trafen sich Ende September 2024 die Vertreterinnen und Vertreter von rund 50 rheinland-pfälzischen Kommunen erstmals seit fünf Jahren persönlich vor Ort im Rathaus der Verbandsgemeinde Landstuhl.

Auf der Tagesordnung des Netzwerktreffens standen etwa der Datenschutz in der Schule, die Digitalisierung von Verwaltungsleistungen im Rahmen des Onlinezugangsgesetzes sowie die datenschutzrechtlichen Herausforderungen bei der kommunalen Wärmeplanung. Auch die datenschutzrechtlichen Rahmenbedingungen bei der Erbenermittlung wurden in den Blick genommen. Vertreter:innen der Kommunen berichteten über die Erfolge der bereits gelebten interkommunalen Zusammenarbeit im Bereich des Datenschutzes und stellten eine Software zum Datenschutzmanagement vor. Daneben gab es reichlich Raum für die Erörterung konkreter Datenschutzfälle aus Sicht der kommunalen Datenschutzbeauftragten und der Aufsichtsbehörde.

Der Verlauf der Veranstaltung sowie die individuellen Rückmeldungen haben einmal mehr gezeigt, dass der persönliche Kontakt zwischen den behördlichen Datenschutzbeauftragten und der Aufsichtsbehörde einen wichtigen Stellenwert genießt und wertvolle Impulse für die tägliche Arbeit auf beiden Seiten bieten kann.

11.2 Speicherung von Fotos zur Durchsetzung des Hausrechts

Im Jahr 2024 haben mehrere öffentliche Verwaltungen den Landesbeauftragten für den Datenschutz und die Informationsfreiheit kontaktiert und angefragt, ob es möglich ist, Lichtbildaufnahmen von mit einem Hausverbot belegten Personen zu speichern und zum Zwecke der Durchsetzung des Hausverbots zu verarbeiten.

In den angesprochenen Fällen gab es zuvor konkrete Bedrohungen gegen einzelne Mitarbeitende, weshalb in etlichen Fällen zum Schutz der Bediensteten Hausverbote ausgesprochen wurden. Um diese effektiv durchsetzen zu können, beabsichtigten die anfragenden Kommunen, Fotos der nicht zutrittsberechtigten Personen zu speichern.

Ausgehend von der Annahme, dass von den mit Hausverbot belegten Personen beim widerrechtlichen Betreten des Verwaltungsgebäudes eine nicht nur geringfügige Störung des Dienstbetriebs ausgeht, wird die Überwachung der Einhaltung des Hausverbots als eine im öffentlichen Interesse liegende Aufgabe betrachtet. Von daher ist es zulässig, wenn bestimmte Grunddaten betroffener Personen Mitarbeitenden gegenüber bekanntgegeben werden, um diese Personen eindeutig identifizieren zu können.

Insofern kann eine diesbezüglich notwendige Verarbeitung personenbezogener Daten grundsätzlich auf Art. 6 Abs. 1 lit. e, Absätze 2 und 3 DS -GVO i.V.m. § 3 Landesdatenschutzgesetz (LDSG) gestützt werden.

Im Rahmen der notwendigen Erforderlichkeitsprüfung sowie im Hinblick auf den Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DS -GVO ist hierbei allerdings festzustellen, inwiefern neben dem Namen auch die Verarbeitung von Lichtbildern notwendig ist und ob eine entsprechende Verarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt ist.

Die Notwendigkeit der Verarbeitung von Lichtbildern kann beispielsweise bejaht werden, wenn eine erhebliche Gefahr für die Mitarbeitenden durch die jeweilige Person ausgeht, weil diese bereits in der Vergangenheit durch Gewalt oder sonstige Bedrohungen inner- oder außerhalb der Behörde aufgefallen ist und es zwingend notwendig ist, die jeweilige Person schnellstmöglich zu identifizieren. Bei dieser Beurteilung sollte insbesondere der Grund für das ausgesprochene Hausverbot und die Schwere des Vergehens herangezogen werden, da die Verarbeitung von Lichtbildern und deren Verbreitung einen verhältnismäßig hohen Eingriff in das Persönlichkeitsrecht eines Einzelnen bedeutet.

Zudem ist es notwendig festzustellen, welchen Personen das ausgesprochene Hausverbot offenbart wird. In der Regel sollte es ausreichen, lediglich die üblicherweise besuchten Ämter zu informieren. Ist beispielsweise ein Bürger regelmäßig und ausschließlich im Sozialamt auffällig geworden, so sollte es genügen, auch nur die dort tätigen Kolleg:innen von dem Hausverbot in Kenntnis zu setzen.

Auch gegenüber einem zentralen Empfang kann die Offenbarung zulässig sein, wenn dieser die Funktion einer zentralen Einlasskontrolle übernimmt.

Eine generelle Bekanntgabe im Intranet, auf das alle Mitarbeitenden zugreifen können, wird hingegen in bestimmten Szenarien kritisch gesehen. Allerdings gilt auch hier der Grundsatz: Je größer die Bedrohungslage und das im Einzelfall vorhandene Risiko, desto größer darf der zu informierende Personenkreis sein.

Hinsichtlich des Ursprungs der Fotos hat der Verantwortliche im Übrigen offenzulegen, woher diese stammen. Erst mit dieser Angabe kann die Rechtmäßigkeit der Verarbeitung auch einwandfrei bestimmt werden. Ggf. ist in diesem Zusammenhang auch eine Prüfung dahingehend durchzuführen, ob die Voraussetzungen des § 7 LDSG (Verarbeitung zu anderen Zwecken) vorliegen. Auch ist die betroffene Person gem. Art. 13, 14 DS-GVO entsprechend zu informieren und die zuvor dargestellte Verarbeitung ist in das Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DS-GVO aufzunehmen.

11.3 Umfrage zum kommunalen Datenschutz

Im Berichtsjahr hat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit eine Umfrage zum behördlichen Datenschutz in rheinland-pfälzischen Kommunen gestartet: Wie stellt sich die Situation des behördlichen Datenschutzmanagements dar? Welches Zeitbudget steht den behördlichen Datenschutzbeauftragten für die Erledigung ihrer Aufgaben zur Verfügung? Städte, Gemeinden und Landkreise in Rheinland-Pfalz waren aufgerufen, diese und andere Fragen in einer Online-Umfrage zu beantworten.

Ziel der Umfrage war unter anderem die Feststellung, ob den Datenschutzbeauftragten vor Ort genügend Zeit für die Erledigung ihrer Aufgaben zur Verfügung steht. Auch sollte ein Eindruck davon gewonnen werden, welchen Stellenwert der Datenschutz in der Fläche genießt. Die Umfrage war daher als Unterstützung für diejenigen angelegt, die vor Ort täglich mit den unterschiedlichsten Aufgaben und Fragestellungen des Datenschutzes konfrontiert sind.

Die Umfrage wurde faktisch anonym durchgeführt, die Teilnahme war freiwillig und es waren keine unmittelbaren Rückschlüsse auf die Teilnehmenden bzw. die jeweiligen Kommunen möglich. Dies war mit Rücksicht auf den Beratungsgedanken auch nicht notwendig, denn vielmehr ging es darum, die Kommunen präventiv zu unterstützen, anstatt bei eventuellen Verstößen im Nachhinein sanktionierend tätig zu werden.

Welche konkreten Schlüsse aus der Umfrageergebnissen gezogen werden konnten und mit welchen Maßnahmen evtl. potentiell negativen Entwicklungen aktiv entgegengesteuert werden kann, soll unter Einbindung aller Beteiligten im Laufe des Jahres 2025 kommuniziert werden.

11.4 Digitalisierung der Verwaltung und Umsetzung des Gesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz, OZG)

Im 32. Tätigkeitsbericht zum Datenschutz 2023 merkten wir im Kapitel 10.4 kritisch an, dass die rechtlichen Rahmenbedingungen für eine datenschutzkonforme Datenverarbeitung eines länderübergreifenden Online-Dienstes, der nach dem „Einer für Alle (EfA)"-Prinzip entwickelt und bereitgestellt wird, noch nicht geschaffen waren, obwohl die Konferenz der unabhängigen Datenschutzaufsichtsbehörden die Erwartung an ein gesetzgeberisches Tätigwerden bereits im Herbst 2021 formuliert hatte. Dieser Kritikpunkt ist erfreulicherweise nicht mehr aktuell.

Das OZG-Änderungsgesetz (OZGÄndG) bzw. OZG 2.0 ist am 24. Juli 2024 nach einer Einigung im Vermittlungsausschuss in Kraft getreten und regelt in § 8a OZG die Rechtsgrundlagen der Datenverarbeitung in einem länderübergreifenden Onlinedienst, der wiederum in § 2 Abs. 8 OZG erstmals definiert wird. Außerdem werden Maßnahmen zur Beschleunigung der Verwaltungsdigitalisierung getroffen, darunter die Abschaffung der Schriftform und die Verankerung des „Once-Only"-Prinzips. Zudem wird die BundID zur DeutschlandID weiterentwickelt.

Der bisherige Arbeitsauftrag der Kontaktgruppe OZG 2.0 zur Beratung der am Gesetzgebungsverfahren beteiligten Stellen hat sich damit erledigt. Nach wie vor unter dem Vorsitz der Berliner Beauftragten für Datenschutz und Informationsfreiheit setzt die Kontaktgruppe, in der die Behörde des LfDI jetzt ebenfalls mitwirkt, die bewährte und hilfreiche Tätigkeit fort und behandelt konkrete datenschutzrechtliche Fragen, die sich aus der Umsetzung des OZG insbesondere zu den EfA-Projekten ergeben. Dazu zählt etwa die Standardisierung der Prüfung von EfA-Onlinediensten (Festlegung der 107. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder).

Bereits im November 2024 konnte eine Orientierungshilfe (Version 1.0) der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder veröffentlicht werden, die ausgewählte Fragestellungen des geänderten Onlinezugangsgesetzes behandelt und eine Anwendungshilfe für die Stellen sein soll, die (länderübergreifende) Onlinedienste nach OZG betreiben oder nutzen.

Die Orientierungshilfe steht unter **www.s.rlp.de/dskOHOZG** zur Verfügung und soll bei Bedarf ergänzt bzw. aktualisiert werden.

Die Behörde des LfDI hat bereits damit begonnen, die Orientierungshilfe im Rahmen von Netzwerktreffen mit behördlichen Datenschutzbeauftragten vorzustellen, und wird diese weiter kommunizieren.

Auf Landesebene ist die Teilnahme des LfDI an Sitzungen des IT-Kooperationsrats als beratendes Mitglied (§ 28 Abs. 2 S. 5 EGovG RP) erwähnenswert. Seit seiner konstituierenden Sitzung am 19. Januar 2024 tagt der IT-Koope-

rationsrat viermal jährlich. Er beschäftigt sich u.a. mit Umsetzungsregelungen für die Beschlüsse des IT-Planungsrats und somit auch mit Aspekten, die im Zusammenhang mit dem OZG stehen.

12. BILDUNG

12.1 Fotos und Videos in Schulen und Kitas

Auch im Jahr 2024 konnte der LfDI vielen Schulen und Kindergärten beratend und helfend zur Seite stehen. Insbesondere Fragen zum Thema „Recht am eigenen Bild“ beschäftigten Schulen und Kitas gleichermaßen. Auch Eltern von Schul- und Kindergartenkindern sowie Schul- und Kita-Träger befassen sich vielfältig mit dieser Thematik und treten mit spezifischen Fragen an den LfDI heran. Immer wieder kommt die Frage auf, wie mit Fotos und Videoaufnahmen von Schüler:innen auf Schulhomepages umzugehen sei. Darf eine Schule ohne Weiteres Fotos vom Schulalltag oder auch von besonderen schulischen Anlässen veröffentlichen? Nein: Sofern nicht das Ereignis selbst, sondern einzelne Schüler:innen im Vordergrund stehen, ist vor der Veröffentlichung der Fotos bzw. Videos die Einwilligung der Betroffenen einzuholen.

Auch für den Unterricht werden vermehrt Videos durch Lehrkräfte angefertigt, die dann zu unterrichtlichen Zwecken herangezogen werden sollen. Nach dem Schulgesetz ist hier die Einwilligung der Schüler:innen bzw. je nach Alter die Einwilligung der Eltern notwendig (§ 67 Abs. 4 Schulgesetz). Wird die Einwilligung nicht erteilt, dürfen den Schüler:innen hierdurch keine Nachteile entstehen.

Ferner beschäftigt Kitas und Schulen die Frage, ob bei Festen Besucher:innen fotografieren dürfen. Auch hier konnte der LfDI aufkommende Fragen von Eltern, Kindern und Einrichtungen beantworten: Verantwortlich für die Anfertigung und Verarbeitung von Fotos bzw. Videos sind nicht die Einrichtungen, sondern die Besucher:innen, die die Fotos anfertigen. Demnach kann die Einrichtung im Vorfeld größerer Veranstaltungen darauf hinweisen, dass Fotos bzw. Videos nur für das eigene Familienalbum gemacht werden dürfen und dass Veröffentlichungen via Social Media ohne Einwilligung der abgebildeten Personen strafrechtlich geahndet werden können.

12.2 Kita-Webinar mit großer Resonanz

Auch im Jahr 2024 konnte der LfDI vielen Angesichts zahlreicher Anfragen von Bürger:innen sowie von Einrichtungen und Trägern stellt der LfDI seit Jahren einen großen Beratungsbedarf zu Datenschutzthemen in der Kita fest. Im Jahr 2024 veranstaltete der LfDI daher ein Webinar mit dem Titel „Kita-Datenschutz gut umgesetzt“. Zielgruppe waren die Erzieher:innen und Kita-Leitungen des Landes. Die Resonanz auf die Veranstaltung fiel außergewöhnlich hoch aus. Das Webinar, das im Rahmen der „Woche der Medienkompetenz 2024“ stattfand, zählte mehr als 500 Teilnehmer:innen. Diesen wurde in der 90-minütigen Veranstaltung ein Rundumblick über die wichtigsten Datenschutzthemen in der Kita vermittelt. Klassiker wie das Recht am eigenen Bild oder Datenschutz bei Kita-Festen waren hier von zentralem Interesse. Die Aufzeichnung des Webinars ist unter folgendem Link abrufbar: **www.s.rlp.de/kitawebinar**

12.2 Schülerworkshops – Nachfrage übersteigt Mittel

Die Datenschutz-Workshops des LfDI sind seit vielen Jahren fester Bestandteil der Medienkompetenzvermittlung für rheinland-pfälzische Schüler:innen. Im Jahr 2024 war die Nachfrage so groß, dass die zur Verfügung stehenden Mittel weit überschritten wurden und bereits früh aufgebraucht waren. Einzelne Schulen, die keine Workshops erhalten konnten, finanzierten die vom LfDI ausgebildeten Referent:innen mit eigenen Geldern über Fördervereine, um möglichst viele Kinder von dem Projekt profitieren zu lassen. Der LfDI hofft, zukünftig über mehr

Mittel für dieses Bildungsprogramm zu verfügen, um möglichst viele Schüler:innen über neue technologische Entwicklungen und Gefahren informieren und aufklären zu können. Von den rund 1600 Schulen im Land konnten im Jahr 2024 an insgesamt 103 Schulen Workshops für jeweils eine komplette Klassenstufe durchgeführt werden, was rund 330 Klassen entsprach.

12.4 Unterrichtsmaterialien zum Thema „Künstliche Intelligenz“

In seinen Schülerworkshops hat der LfDI das Thema „Künstliche Intelligenz“ (KI) als Lehrinhalt bereits fest integriert. Technologien wie Large-Language-Modelle (ChatGPT, Perplexity, Mistral etc.) oder Bildgeneratoren werden von den Schüler:innen mittlerweile für Hausaufgabenrecherchen oder für die Zusammenfassung von Texten über die vom Ministerium für Bildung des Landes Rheinland-Pfalz beschaffte Software „Fobizz“ (vgl. 32. Tätigkeitsbericht zum Datenschutz 2023, Tz. 11.2) regulär genutzt. Die Datenschutz-Workshops des LfDI vermitteln den Schüler:innen die Funktionsweise von KI-Systemen und tragen zu einem kritischen Blick auf den Umgang entsprechender KI-Tools mit personenbezogenen Daten der Nutzer:innen bei. Vom LfDI entwickelte Unterrichtsmaterialien ermöglichen es, das Thema in unterschiedlichem Umfang und für verschiedene Alters- und Zielgruppen aufzugreifen. Die Online-Materialien stehen auch interessierten Lehrkräften und Pädagogen kostenfrei zur Verfügung: **www.youngdata.de/vor-ort/rp/unterricht-ki**

12.5 Lehrkräftebildung

Die Digitalisierung in den Schulen verlangt von Lehrkräften immer mehr Kompetenzen zum sicheren Umgang mit Schülerdaten in verschiedensten Anwendungen (vgl. 30. Tätigkeitsbericht 2021, Tz. 11.4). Der LfDI verstetigt daher seine Zusammenarbeit mit dem Pädagogischen Landesinstitut und bietet seit dem Jahr 2024 jährlich drei Online-Fortbildungen für spezifische Lehrkräftegruppen an. In den Webinaren vor den Sommerferien, nach den Herbstferien und nach den Halbjahreszeugnissen werden Schulleitungen, schulische Datenschutzbeauftragte und neue Lehrkräfte mit den für sie relevanten datenschutzrechtlichen Informationen versorgt.

Ebenfalls an die Zielgruppe Lehrkräfte richtet sich die rheinland-pfälzische Bildungsmesse „iMedia“, zu deren Programm der LfDI auch im Berichtsjahr mehrere Workshops zu schulischen Datenschutzfragen und didaktischer Datenschutz-Medienkompetenz beisteuerte.

12.6 Kontrolle von Tablets bei der mündlichen Abiturprüfung

Tablets finden in der Schule immer mehr Verwendung und sind teils fester Bestandteil des Unterrichts. Die von der Schule oder dem Schulträger gestellten Geräte sind oft auch privat nutzbar. Dies kann sich auf Prüfungssituationen auswirken. In einem Fall verlangte eine Schule nach der mündlichen Abiturprüfung Einsicht in den Browserverlauf des Tablets eines Prüflings, da der Verdacht eines Täuschungsversuchs bestand. Die Eltern des Prüflings sahen darin einen unzulässigen Eingriff in die Persönlichkeitsrechte ihres Kindes.

Bei der Bewertung dieser Sachlage stellte sich die Frage, ob das Tablet auch für private Zwecke genutzt werden darf, was bei einem eigenen Endgerät selbstredend der Fall ist. Handelt es sich aber um ein geliehenes Gerät, kommt es darauf an, ob die Schule die außerschulische Nutzung des Tablets gestattet oder verboten hat. Für beide Szenarien stellte der LfDI vor geraumer Zeit Muster-Nutzungsordnungen für die Schulen bereit: **www.s.rlp.de/musterInKomSchule**

Ähnlich der Internetnutzung im Arbeitsverhältnis sind auch im schulischen Kontext die Voraussetzungen für Kontrollmaßnahmen höher, wenn auch die private Nutzung erlaubt ist. Konkret bedeutet dies, dass Kontrollmaßnahmen nur mit Einwilligung der Betroffenen zulässig sind.

Im vorliegenden Fall war lediglich die schulische Nutzung des schuleigenen Tablets gestattet, so dass aufgrund des Verdachts einer Täuschungshandlung das Gerät kontrolliert werden durfte.

Alternativ besteht in Prüfungssituationen die Möglichkeit, für die Dauer der Prüfung eine Monitoring-Software zu verwenden. Diese Software erlaubt es den Lehrkräften, die während der Prüfung aufgerufenen Seiten zu überwachen. Damit ist sichergestellt, dass keine unerlaubten Lern- und Hilfsmittel verwendet werden. Hierüber sind die Prüflinge vorab in Kenntnis zu setzen.

12.7 Verordnung für die Einrichtung eines zentralen Stammdatenservers

Im Zuge des Ausbaus der Lehr-Lernplattform „Bildungsportal RLP“ beabsichtigte das Ministerium für Bildung des Landes Rheinland-Pfalz die Einrichtung eines zentralen Stammdatenservers, um verschiedene dezentrale Dienste über einen einheitlichen Zugang erreichbar zu machen.

Hierzu sollten Daten aus dem Schulverwaltungssystem edoo.sys und weiteren Fachverfahren in einem Verfahren zusammengeführt werden, um den Zugriff über andere Dienste zu ermöglichen und so den Lehrkräften das Arbeiten zu erleichtern. Datenschutzrechtlich handelt es sich dabei um die Einrichtung eines automatisierten Abrufverfahrens in Bezug auf Stammdaten von Schüler:innen und Lehrkräften, so dass die rechtlichen und technischen Anforderungen höher sind als dies bei einer Übermittlung bzw. einem Datenexport der Fall wäre.

Da die gegenwärtige Rechtslage einen solchen Abruf für Zwecke des Identitätsmanagements nicht hergab, griff das Ministerium für Bildung den Hinweis des LfDI auf, mit der „Verordnung zur Verarbeitung personenbezogener Daten beim Einsatz zentraler digitaler Anwendungen“ eine tragfähige rechtliche Grundlage zu schaffen.

Mit dieser Verordnung soll der Grundregel zur Datenverarbeitung im schulischen Kontext in § 67 Abs. 1 S. 1 SchulG Rechnung getragen werden, wonach die Verarbeitung personenbezogener Daten unter dem Vorbehalt steht, dass sie „zur Erfüllung der durch Rechtsvorschrift zugewiesenen schulbezogenen Aufgaben erforderlich ist“.

13. ARCHIVWESEN

Über Sachverhalte aus dem Bereich des Archivwesens berichtet der LfDI eher selten, zuletzt im 28. Tätigkeitsbericht für das Jahr 2019, was auch Ausdruck des sensiblen Umgangs mit Archivgut seitens der Landesarchivverwaltung ist. Im Berichtsjahr beschäftigte sich die Behörde des LfDI mit verschiedenen Angelegenheiten aus diesem Bereich.

Im Rahmen einer geplanten Novellierung des Landesarchivgesetzes (LArchG) wurde der LfDI vom zuständigen Ministerium um eine Äußerung zu den datenschutzrechtlich relevanten Regelungen gebeten.

Archive können als gesetzlich erlaubte Form der Vorratsdatenspeicherung bezeichnet werden mit der Folge, dass Notwendigkeiten des Archivwesens mit den Grundsätzen des Datenschutzes zur Zweckbindung und zur Speicherbegrenzung (Art. 5 Abs. 1 lit. a und lit. e DS -GVO) über die Privilegierung gemäß Art. 89 DS-GVO in Einklang zu bringen sind.

Archivrecht als bereichsspezifisches Datenschutzrecht regelt als Besonderheit, dass die Übernahme von archivwürdigen Unterlagen in ein Archiv als Löschung gilt. Diese Vorgehensweise stellt, anders formuliert, eine Alternative bzw. ein Surrogat zur Löschung von personenbezogenen Daten dar.

Mit dem vorgelegten Entwurf zur Überarbeitung des Landesarchivgesetzes Rheinland-Pfalz soll dieses an das Bundesarchivgesetz sowie die Gesetze anderer Bundesländer angepasst und der Landesarchivverwaltung Möglichkeiten eingeräumt werden, auf die zunehmende Digitalisierung behördlichen Handelns zu reagieren. Gleichzeitig sollen die Änderungen einen leichteren Zugang zu Archivgut und die Stärkung der Rechte der Nachkommen bewirken.

Die Prüfung hat keine durchgreifenden rechtlichen Bedenken ergeben. Insbesondere zur künftig vorgesehenen Archivierung öffentlicher Social-Media-Accounts von anbietungspflichtigen Stellen und Amtsträger:innen in Ausübung ihres Amtes wurden datenschutzrechtliche Anmerkungen mitgeteilt.

Aus der Landesverwaltung wurde mit der Bitte um datenschutzrechtliche Bewertung auch der folgende Sachverhalt vorgetragen:

Die Landesarchivverwaltung hatte Digitalisate, d.h. Endprodukte der Digitalisierung analoger Gegenstände, des Bestandes der Akten der Geheimen Staatspolizei einer bestimmten Region aus dem Archivinformationssystem „Apertus“ herausgenommen. Eine Stichprobe aus den über 12.000 noch erhaltenen Akten hatte ergeben, dass diese Vorgänge detaillierte Beschreibungen von Gewaltdarstellungen und sexuellem Missbrauch sowie Fotos von Hinrichtungen während des 2. Weltkriegs enthalten, in denen sogenannte „beiläufige“ personenbezogene Daten vorkommen.

Zwar waren die Akten noch vor Ort im Lesesaal der Archivverwaltung analog einsehbar und nutzbar. Trotzdem wurde darin eine gravierende Beeinträchtigung der Wissenschaft, der historisch-politischen Bildungsarbeit und des öffentlichen Interesses gesehen.

Aus datenschutzrechtlicher Sicht ist hier ein Interessenausgleich zwischen dem Recht auf informationelle Selbstbestimmung und dem Informationsinteresse der Wissenschaft sowie der allgemeinen Öffentlichkeit (Bestandsdatenschutz) notwendig. Das Zugänglichmachen von Archivgut, das personenbezogene Daten enthält, ist als Datenübermittlung zu sehen und wird in erster Linie durch die Sperrfristen geregelt. Aber auch nach dem Ablauf der Sperrfristen ist die Benutzung von Archivgut nach § 3 Abs. 2 Nr. 2 LArchG einzuschränken oder zu versagen, soweit Grund zu der Annahme besteht, dass schutzwürdige Belange betroffener Personen oder Dritter entgegenstehen.

Der wertausfüllende Begriff der „schutzwürdigen Belange“ verlangt eine Abwägung des Persönlichkeitsrechts einer betroffenen Person und des Stellenwerts, den die Offenlegung und Verwendung der Daten für sie hat, gegen die Interessen des Archivs als speichernder Stelle und der Benutzer:innen als Dritten, für deren Zwecke die Übermittlung erfolgt (vgl. BGH NJW 1986, S. 2505). Auf Seiten der Einsichtbegehrenden kommt es auf das Risiko eines Missbrauchs der Daten an, auf Seiten der betroffenen Person steigt die Schutzwürdigkeit ihres Geheimhaltungsinteresses mit der Sensibilität der Information (vgl. Koschmieder in Partsch, Hrsg., Handkommentar zu BArchG § 13 Rn 1, 20).

Unter diesen Voraussetzungen hat sich der LfDI dem Standpunkt der Landesarchivverwaltung angeschlossen, da bei einer digitalen Bereitstellung von Archivmaterial im Archivinformationssystem „Apertus“ weder eine Interessenabwägung im Einzelfall noch eine Bewertung des Risikos eines Missbrauchs von sogenannten „beiläufigen“ personenbezogenen Daten durch Einsichtbegehrende erfolgen kann.

Eine Rückäußerung der Landesverwaltung zu einer gleichzeitig beschriebenen alternativen Vorgehensweise liegt bisher nicht vor.

Schließlich ist auch die Beschwerde eines Bürgers beim LfDI eingegangen, mit der dieser geltend macht, dass seinem Antrag auf Löschung (Art. 17 DS-GVO) von Akten hinsichtlich der Nutzung von Archivgut bei der Landesarchivverwaltung nicht (vollständig) entsprochen worden sei.

Dem Recht auf Löschung einer betroffenen Person steht zunächst eine rechtliche Verpflichtung einer Behörde als Verantwortliche im Sinne von Art. 17 Abs. 3 lit. b Alt. 1 DS-GVO entgegen. Denn die Behörde hat Aufbewahrungs- und Dokumentationspflichten zu erfüllen. Dies stellt eine Ausnahme von der Löschungspflicht dar, d.h. eine ausnahmsweise Befugnis zur fortgesetzten Speicherung an sich zu löschender personenbezogener Daten.

Entsprechende Vorschriften, die die Aufbewahrungsdauer solcher Benutzerakten regeln, gibt es nicht. Die Erforderlichkeit der Dauer der Aufbewahrung ist dann zu messen an den Erfordernissen einer ordnungsgemäßen Dokumentation. Nicht mehr erforderlich ist die Aufbewahrung, wenn die Daten keine praktische Bedeutung mehr haben und deshalb ausgeschlossen werden kann, dass sie die Arbeit der zuständigen Behörde noch fördern können.

Die Landesarchivverwaltung hat dazu vorgetragen, dass Benutzerakten dem fachbezogenen Bereich zuzurechnen seien, für die grundsätzlich eine Aufbewahrungsfrist von fünf Jahren gelte. Allerdings könne nicht ausgeschlossen werden, dass auch (Teile von) Benutzerakten als „Unterlagen von bleibendem Wert“ bewertet und als Archivgut übernommen würden.

Das Verfahren konnte im Berichtszeitraum noch nicht beendet werden, ein Austausch bezüglich der Dauer von Aufbewahrungsfristen und der Bewertungskriterien zur Entscheidung über die Archivwürdigkeit von Vorgängen dauert noch an.

14. MELDEWESEN

14.1 Übermittlung von Daten Neugeborener

Aufgrund einer Beschwerde wurde der LfDI über die Praxis einer Kreisverwaltung informiert, von den Meldeämtern der Verbandsgemeinden im Kreis regelmäßig Daten von Eltern zu erhalten, die Nachwuchs bekommen haben. Die Eltern wurden sodann von der Kreisverwaltung in einem Anschreiben über Informationsangebote für junge Eltern im Landkreis informiert. Des Weiteren wurde auf einen „kostenlosen" Hausbesuch eines Vereins hingewiesen und angekündigt, dass sich ein Mitarbeiter des Vereins bei den Eltern zwecks Terminabsprache melden würde.

Die Kreisverwaltung räumte ein, dass es bei diesem Hausbesuch zumindest auch darum gehe, Hinweise für eine Kindeswohlgefährdung zu erhalten, so dass als Ausgangsnorm Art. 6 Abs. 1 lit. e DS-GVO („Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt") heranzuziehen war. Allerdings erfordern Art. 6 Abs. 2 und Abs. 3 DS-GVO für diesen Anwendungsfall Rechtsnormen, in denen die spezifischen Anforderungen für die Datenverarbeitung präziser bestimmt werden. Insoweit kamen die melderechtlichen Bestimmungen zur Anwendung. Denn hier wird insbesondere zwischen anlassbezogenen Übermittlungen, regelmäßigen Datenweitergaben und Datenabrufen differenziert.

§ 36 BMG schreibt vor, dass regelmäßige Datenübermittlungen einer bundes- oder landesrechtlichen Regelung bedürfen, in der Anlass und Zweck der Übermittlungen, der Empfänger und die zu übermittelnden Daten festgelegt sind.

Die Meldedatenlandesverordnung (MDLVO) stellt eine solche landesrechtliche Bestimmung dar. Im Hinblick auf die regelmäßige Weitergabe von Meldedaten durch die Meldeämter an die Kreisverwaltung sieht § 10 Abs. 1 MDLVO lediglich Datenübermittlungen für Jubiläumszwecke vor. Die MDLVO enthält darüber hinaus keine Bestimmungen zur regelmäßigen Übermittlung von Daten Neugeborener an die Kreisverwaltung. Insofern fehlte es bereits an einer rechtlichen Grundlage für die regelmäßige Übermittlung.

Hinzu kam, dass die Eltern in dem Anschreiben – entgegen Art. 14 DS-GVO – nicht informiert wurden, wie die Kreisverwaltung an die Daten gekommen war und wie sie damit verfuhr. Auch wurde den Eltern keine echte Wahlmöglichkeit eingeräumt, ob sie eine Beratung wünschten oder nicht. Sie mussten vielmehr selbst aktiv werden, um den Besuch abzusagen.

Schließlich wurde der eigentliche Anlass des Hausbesuchs (Kinderschutz) verschleiert, so dass der Eindruck entstand, Mitarbeitende des Vereins verschafften sich unter einem Vorwand Zutritt zur Wohnung. Von einer informierten und freiwilligen Entscheidung der Eltern konnte jedenfalls keine Rede sein. Auch war dieses Vorgehen mit dem grundgesetzlich verankerten Schutz der Unverletzlichkeit der Wohnung (Art. 13 Grundgesetz) nicht zu vereinbaren.

Der LfDI erteilte der Kreisverwaltung und den beteiligten Meldeämtern den Hinweis, dass die bisherige Praxis nicht datenschutzkonform sei, und schlug mit der sogenannten Datenmittlung eine datenschutzkonforme Alternative zur bisherigen Verfahrensweise vor:

Hierbei übergibt die Kreisverwaltung den Meldeämtern vorgefertigte Anschreiben an die Eltern und die Meldeämter übernehmen (gegen Kostenerstattung) die Übersendung an die Eltern. Da bei dieser Verfahrensweise keine Meldedaten an die Kreisverwaltung übermittelt werden, ist sie datenschutzrechtlich unproblematisch. Hierdurch wird auch sichergestellt, dass die Eltern selbst über eine Kontaktaufnahme zum Verein entscheiden können. Die

Kreisverwaltung überarbeitete daraufhin das Anschreiben und stimmte den Text mit dem LfDI ab.

In einem anderen Fall forderte ein Heimat- und Kulturverein von einer Verbandsgemeinde die Daten Neugeborener, um Obstbäumchen mit den Namen der Neugeborenen auf der „Storchenwiese“ zu pflanzen. Da auch hier keine rechtliche Grundlage für die Übermittlung von Meldedaten an den Verein vorhanden war, schlug der LfDI zur Erhaltung dieser Tradition die zuvor erwähnte Datenmittlung vor.

14.2 „Bitte melde dich“

Einer Verwaltung lag die Anfrage einer Fernsehproduktionsfirma für die TV-Sendung „Julia Leischik sucht: Bitte melde Dich” vor, die aus dem Einwohnermelderegister eine Anschrift übermittelt bekommen wollte. Das Meldeamt der Verwaltung fragte beim LfDI nach, wie man jetzt verfahren solle.

Die Erteilung einer sogenannten einfachen Melderegisterauskunft ist nach § 44 Bundesmeldegesetz (BMG) nur zulässig, wenn die Identität der Person, über die eine Auskunft begehrt wird, eindeutig festgestellt werden kann und die Daten nicht für Zwecke der Werbung oder des Adresshandels verwendet werden. Sofern die Daten für gewerbliche Zwecke verwendet werden, sind diese anzugeben.

Sind diese Anforderungen erfüllt und hat das Meldeamt keine Hinweise dafür, dass schutzwürdige Interessen der betroffenen Person durch die Auskunftserteilung beeinträchtigt werden (§ 8 BMG), darf im Rahmen dieser „einfachen Melderegisterauskunft“ die derzeitige Anschrift (also Haupt- und Nebenwohnungen) beauskunftet werden und – falls die Person verstorben ist – auch diese Tatsache.

Der gewerbliche Zweck (Fernsehsendung „Julia Leischik sucht: Bitte melde Dich”) wurde im vorliegenden Fall angegeben. Schutzwürdige Interessen der betroffenen Person konnten hier aber dadurch beeinträchtigt werden, dass beispielsweise ein Kamerateam unangemeldet vor der Wohnungstür der betroffenen Person stehen und filmen könnte. Der LfDI schlug daher vor, dass die betroffene Person vom Meldeamt über die Anfrage der Produktionsfirma informiert und ihr eine Kontaktadresse/Telefonnummer der Produktionsfirma mitgeteilt wird, so dass sie selbst darüber entscheiden kann, ob sie für die Fernsehsendung zur Verfügung steht oder nicht.

15. RECHTSDURCHSETZUNG

Das Jahr 2024 war durch eine Vielzahl von Verfahren zum Auskunftsrecht nach Art. 15 DS-GVO geprägt. Die überwiegende Anzahl der 69 erlassenen Anweisungen resultierte aus diesem Bereich. Für weitere festgestellte Datenschutzverstöße erließ der LfDI 15 Verwarnungen sowie zwölf Geldbußen mit einem Gesamtbetrag von 15.600 €. Gegenüber öffentlichen Stellen musste in elf Fällen eine Beanstandung ausgesprochen werden.

Weiterhin hoch ist die Zahl der Verantwortlichen, die auf ein Informationsersuchen der Aufsichtsbehörde mit der Anweisung, alle für die Aufgabenerfüllung des Landesbeauftragten erforderlichen Informationen bereitzustellen, erst nach Erinnerungen oder Zwangsgeldandrohungen reagieren. Aus diesem Grund drohte der Landesbeauftragte in 69 Fällen Zwangsgelder an und verhängte diese in 23 Fällen. Die durchschnittliche Höhe der Zwangsgelder betrug 500 €. In 15 Fällen läuft weiterhin ein Beitreibungsverfahren durch die Landeshauptkasse.

Auch in diesem Jahr führten Bürger:innen Klageverfahren gegen hoheitliche Maßnahmen. So wurden 2024 insgesamt 24 Klagen gegen den Landesbeauftragten erhoben. Dabei war der LfDI in drei Fällen von Berufungen zum OVG Koblenz beteiligt, ein Revisionsverfahren wird beim BVerwG geführt.

ABKÜRZUNGSVERZEICHNIS

AEAO	Anwendungserlass zur Abgabenordnung
AGG	Allgemeines Gleichbehandlungsgesetz
AK	Arbeitskreis
AO	Abgabenordnung
ATD	Antiterrordatei
ATDG	Antiterrordateigesetz
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BDSG	Bundesdatenschutzgesetz
BDSG-E	Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes
BGB	Bürgerliches Gesetzbuch
BKA	Bundeskriminalamt
BM	Ministerium für Bildung des Landes Rheinland-Pfalz
BMG	Bundesmeldegesetz
BNotO	Bundesnotarordnung
BSG	Bundessozialgericht
BT-Drs.	Bundestagsdrucksache
BVerwG	Bundesverwaltungsgericht
bzgl.	bezüglich

DS-GVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
EDSA	Europäischer Datenschutzausschuss
EGovGRP	Landesgesetz zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz
EU	Europäische Union
EuGH	Europäischer Gerichtshof
GG	Grundgesetz
ggf.	gegebenenfalls
GwG	Geldwäschegesetz
i.V.m.	in Verbindung mit
IHK	Industrie- und Handelskammer
KI-VO	Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-Verordnung)
KMU	Kleine und mittlere Unternehmen
KWG	Kreditwesengesetz
LArchG	Landesarchivgesetz
LDI	Landesbetrieb Daten und Information Rheinland-Pfalz
LDSG	Landesdatenschutzgesetz Rheinland-Pfalz

LfDI	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
LJVollzDSG	Landesjustizvollzugsdatenschutzgesetz
LKA	Landeskriminalamt
LT-Drs.	Landtagsdrucksache
MDLVO	Meldedatenlandesverordnung
OVG	Oberverwaltungsgericht
OWiG	Gesetz über Ordnungswidrigkeiten
OZG	Onlinezugangsgesetz
OZGÄndG	OZG-Änderungsgesetz
PAuswG	Personalausweisgesetz
POG	Polizei- und Ordnungsbehördengesetz
POLADIS	Polizeiliches Auskunfts -, Datenverarbeitungs- und Informationssystem Rheinland-Pfalz
POLIS	Polizeiliches Informationssystem Rheinland-Pfalz
RED	Rechtsextremismus-Datei
RED-G	Rechtsextremismus-Datei-Gesetz
RIVAR	Rheinland-pfälzisches Informations-, Vorgangsbearbeitungs-, Auswerte- und Recherchesystem
SchulG	Schulgesetz Rheinland-Pfalz

SGB	Sozialgesetzbuch
sog.	sogenannt
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
u.a.	unter anderem
z.B.	zum Beispiel

FOLGEN SIE UNS

Podcast Datenfunk

Unser Podcast Datenfunk versorgt Sie regelmäßig mit aktuellen datenschutzrechtlichen Hintergründen im Audio-Format.

www.datenschutz.rlp.de/themen/podcast

Newsletter

Der Newsletter des Landesbeauftragten für den Datenschutz und die Informationsfreiheit wird im Zwei-Monats-Rhythmus an die Abonnentinnen und Abonnenten versandt. Sie können sich für den Newsletter unter folgendem Link anmelden:

www.datenschutz.rlp.de/service/newsletter/anmeldung

Mastodon

Kennen Sie schon Mastodon, die datenschutzfreundliche Alternative zum Kurznachrichtendienst X? Auf **https://social.bund.de/@lfdi_rlp** gehen wir in den Dialog mit den Nutzerinnen und Nutzern und informieren tagesaktuell über unsere Aktivitäten und Veröffentlichungen. Folgen Sie uns – ganz ohne datenschutzrechtliche Bedenken und Fallstricke.

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