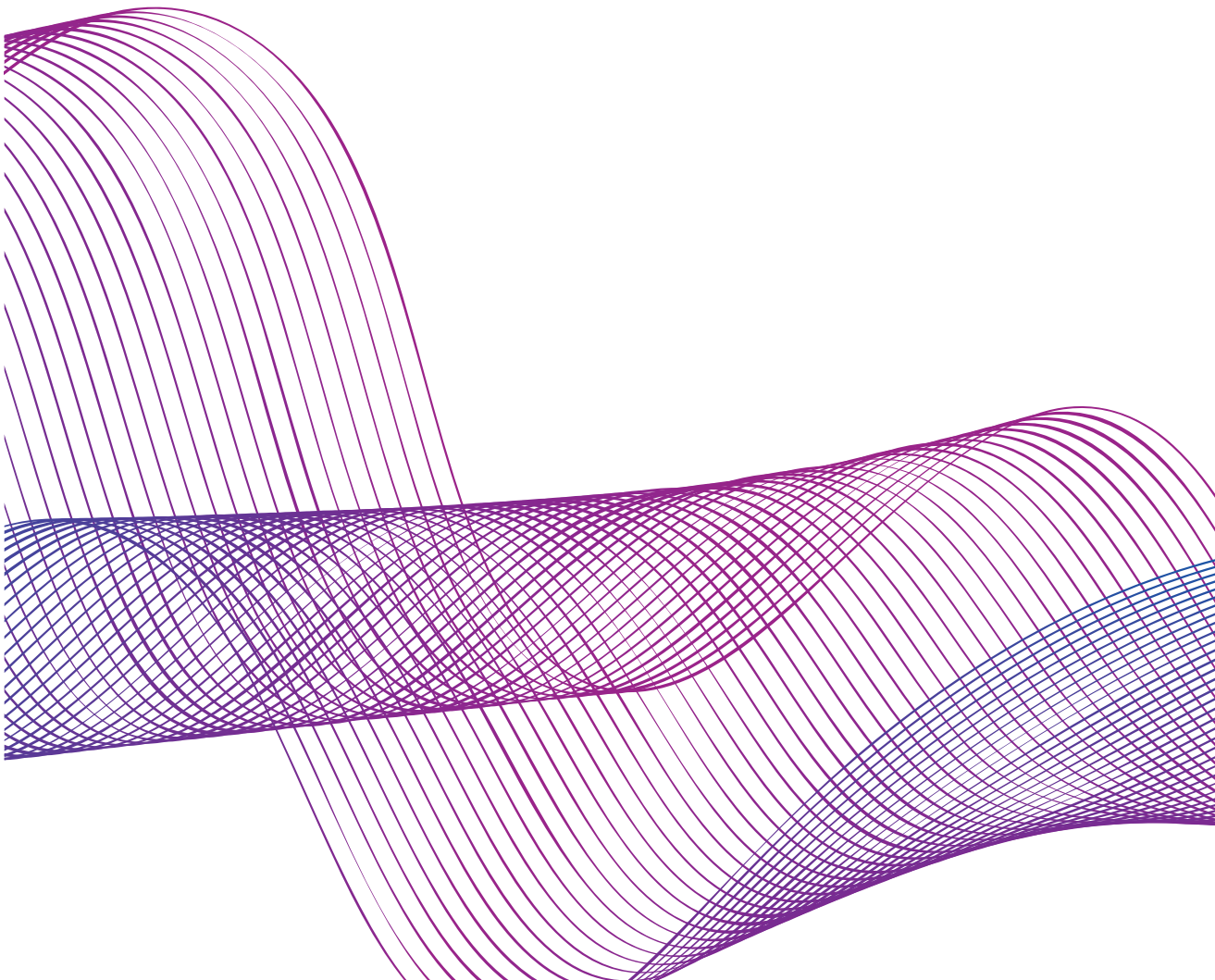
Der Landesbeauftragte für
den **DATENSCHUTZ** und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

TÄTIGKEITSBERICHT ZUM DATENSCHUTZ 2023



HERAUSGEBER
Der Landesbeauftragte
für den Datenschutz und die
Informationsfreiheit Rheinland-Pfalz
Hintere Bleiche 34 | 55116 Mainz
Postfach 30 40 | 55020 Mainz
Telefon +49 (0) 6131 8920 - 0
Telefax +49 (0) 6131 8920 - 299
poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

August 2024

INHALT

VORWORT

Prof. Dr. Dieter Kugelmann

Das Jahr 2023 war ebenso spannend wie ereignisreich. Dies gilt für den Datenschutz insgesamt und für mich im Besonderen. Im Hinblick auf das Datenschutzrecht ist viel in Bewegung gewesen. Verhandlungen auf Bundesebene zur Änderung des Bundesdatenschutzgesetzes wurden intensiv von den Datenschutzaufsichtsbehörden begleitet. Wir haben dabei versucht unsere Punkte zu setzen, um im politischen Raum einzuwirken. Parallel dazu ist die Diskussion um Künstliche Intelligenz in exponentiellem Maße angewachsen. Beide Themen beschäftigen gerade auch den LfDI Rheinland-Pfalz, weil wir in entsprechenden Gremien Leitungspositionen innehaben. Über diese strategischen Themen darf aber nicht in Vergessenheit geraten, dass wir insbesondere für die Bürgerinnen und Bürger in Rheinland-Pfalz da sind. Manchmal sind es die scheinbar einfachen und kleinen Fälle, die Menschen am meisten bewegen. Auch hier haben wir versucht, zielorientiert und vernünftig zu handeln. Damit ist der Bogen gespannt von den großen und überwölbenden strategischen Themen bis zum Einzelfall. Dies kennzeichnet die Tätigkeit des Landesbeauftragten.

Für mich persönlich war 2023 ein besonderes Jahr, weil ich wiedergewählt wurde. Ich danke dem Landtag Rheinland-Pfalz, der mich mit großer Mehrheit in meinem Amt bestätigt hat und mir eine zweite Amtszeit gewährt hat. Die erste Amtszeit war geprägt von der Einführung der Datenschutz-Grundverordnung, Umstellungen in der Behörde, neuen Auslegungen und Verständnissen von Fragen des Datenschutzrechts auf der Grundlage anderer und geänderter Rechtsgrundlagen. Zuletzt konnten wir dann auf der Basis des Erreichten konsequent und zielführend weiterarbeiten.

In der nunmehr zweiten Amtszeit möchte ich versuchen, Prioritäten zu setzen, die über den Tag hinausweisen. Dies betrifft zum einen die Verwaltungsdigitalisierung. Bürgerinnen und Bürger wollen ihre Behördengänge auch digital erledigen können. Dabei soll nicht vergessen werden, dass es auch viele gibt, die die unmittelbare Kommunikation in der Behörde vor Ort wollen oder brauchen. Andererseits soll es natürlich auch

möglich sein, Anträge online zu stellen und auch entsprechend zu bearbeiten. Umstellungen in diesem Bereich betreffen gerade auch die Kommunen, die ohnehin über eine große Arbeitslast zurecht klagen. Hier wollen wir Hilfestellungen im Rahmen unserer Möglichkeiten geben, um sinnvolle und notwendige Umstellungen zu erleichtern. Damit wollen wir zum einen den Behördenmitarbeitenden und zum anderen den Bürgerinnen und Bürgern unterstützend zur Seite stehen.

Eine zweite Priorität betrifft die Biotechnologie. Rheinland-Pfalz profiliert sich als Standort für Biotechnologie – und das mit großem Erfolg. Neue Ansiedlungen gerade auch von Start-ups, Erweiterungen durch bestehende Unternehmen und technologische Fortschritte insbesondere in der Forschung sind bereits zu verzeichnen und sollen und werden fortgesetzt werden. Dabei möchte ich unterstützen. In der Forschung, aber dann auch in der konkreten Marktfähigkeit von entsprechenden Produkten gibt es immer wieder digitale Bezüge. Es geht um die Nutzung von Daten, um die digitale Vermarktung und um weitere, die Lebenswelt der einzelnen Bürgerinnen und Bürger ganz konkret betreffende Fragen. In meiner Behörde baue ich daher einen dialogorientierten Schwerpunkt zur Biotechnologie auf. So stellen wir sicher, dass wir jederzeit kompetent und zielführend sowohl Unternehmen und öffentliche Stellen als auch Bürgerinnen und Bürger beraten können.

Die dritte, in der Öffentlichkeit sehr präsente Priorität ist die Befassung mit Künstlicher Intelligenz. Ohnehin gilt hier das Datenschutzrecht und wir beschäftigen uns bereits gegenwärtig mit der Technologie, ihrer Anwendung durch Verwaltung und Wirtschaft sowie ihrer Fortentwicklung. Zugleich geht es darum, die Entwicklung im Rahmen des Datenschutzrechts in die Richtung einer menschenzentrierten und grundrechtsschonenden Nutzung von Systemen Künstlicher Intelligenz zu lenken. Dabei will ich unterstützen. Dies erfolgt zum einen durch die entsprechenden Gremien und Mitwirkungen auf deutscher und europäischer Ebene. Zum anderen muss ich die Positionierung der Behörde im Blick halten und für ihre nötige Ausstattung sorgen. Wir brauchen Ressourcen, um uns konstruktiv mit der innovativen Zukunftstechnologie auseinanderzusetzen und sie datenschutzgerecht zu entwickeln.

Die Weichen sind 2023 gestellt worden. Ich hoffe sehr, dass es mir gelingt, die Brücke vom Einzelfall zur strategischen Ausrichtung weiter

erfolgreich zu schlagen. Dabei weiß ich mich im Einklang mit den Mitarbeitenden meiner Behörde, die diesen Weg mitgehen. Ohne mein engagiertes und fachkundiges Team ließe sich dies nicht verwirklichen.

Damit sind einige der Aspekte vorgestellt, die in diesem Tätigkeitsbericht eine Rolle spielen. Mein Ziel, Datenschutz konstruktiv in die Tat umzusetzen, werde ich weiter mit Nachdruck verfolgen.

Prof. Dr. Dieter Kugelmann

I.
DER LFDI RHEINLAND-PFALZ IN DEUTSCHLAND UND EUROPA

I. DER LFDI RHEINLAND-PFALZ IN DEUTSCHLAND UND EUROPA

1. FORTENTWICKLUNG DER DATENSCHUTZKONFERENZ DURCH DEN ARBEITSKREIS DSK 2.0

Im Jahr 2023 hat der Arbeitskreis DSK 2.0 unter meiner Leitung die Arbeiten des vergangenen Jahres (siehe **https://s.rlp.de/tb31**, Kapitel I.1) fortgeführt und neue Impulse aufgegriffen, um die Fortentwicklung der Datenschutzkonferenz und die effektive Zusammenarbeit der Datenschutzaufsichtsbehörden des Bundes und der Länder weiter voranzutreiben.

Gemeinsame Tatkraft statt hemmende Zersplitterung

Die Datenschutzaufsichtsbehörden des Bundes und der Länder müssen sich regelmäßig dem Vorwurf aus Wirtschaft und Politik stellen, uneinheitlich zu agieren und nicht geschlossen aufzutreten. In Wirklichkeit arbeiten sie eng und intensiv zusammen und gelangen regelmäßig zu gemeinsamen Sichtweisen. Die zahlreichen Publikationen der Datenschutzkonferenz (siehe **https://datenschutzkonferenz-online.de/**) zeigen auf, dass Meinungspluralität nicht zu einer Zersplitterung führt, sondern als Ressource aufzugreifen ist und den Datenschutzaufsichtsbehörden zu Tat- und Schlagkraft verhilft. Nicht zuletzt hat die Datenschutzkonferenz sich durch ihre Fortentwicklung aus eigener Kraft zu einem national und international anerkannten Expertinnen- und Expertengremium fortentwickelt. Mit einem im Arbeitskreis DSK 2.0 erarbeiteten Positionspapier wurden die ersten Meilensteine, die zur Fortentwicklung der Datenschutzkonferenz und zur Effektivierung der Zusammenarbeit erreicht wurden, politischen Entscheidungsträgern publik gemacht. Dazu zählen die Mehrheitsentscheidungen und andere eingeführte Instrumente zur verbesserten Kooperation, wie z.B. der wöchentliche Jour fixe und die jährliche Sommerklausur.

Fachlicher und strategischer Austausch auf der Sommerklausur 2023

Ende Juli 2023 durfte ich zu der ersten Sommerklausur der DSK auf Leitungsebene in Speyer einladen. Die Klausurtagungen der DSK sollen dem Austausch, der Bewusstseinsbildung und der gemeinsamen Beratung und Willensbildung zu strategischen (Grundsatz-) Fragen dienen, welche die Ausrichtung der Datenschutzkonferenz und des Datenschutzrechts betreffen. Das Format ist auf den offenen und vertrauensvollen internen Austausch ausgerichtet. Dabei waren u.a. die Themen „Anforderungen europäischer Rechtsakte an die deutschen Datenschutzaufsichtsbehörden“ und „Anonymisierung und Pseudonymisierung“ Gegenstand des Austauschs. Im Gegensatz zu den Datenschutzkonferenzen werden keine Festlegungen oder Beschlüsse gefasst.

Eine ständige Geschäftsstelle zur Sicherstellung von effektiver Zusammenarbeit und Kontinuität

Als nächsten, vordringlichen Schritt zur Institutionalisierung der DSK hat der Arbeitskreis DSK 2.0 das Projekt „Ständige Geschäftsstelle“ der DSK weiter ausgearbeitet und insbesondere die Aufgabenbereiche und die Verortung weiter konzeptualisiert. Die ständige Geschäftsstelle soll ein administratives Instrument zur

Institutionalisierung der DSK werden. Sie soll der weiteren Steigerung der Einheitlichkeit und der administrativen Entlastung des Vorsitzes der Datenschutzkonferenz dienen. Zu diesem Zweck soll sie bei der Organisation und Durchführung der Konferenzen mitwirken und die Durchführung der Umlaufbeschlüsse sowie die Abstimmung anderer interner Entscheidungen der DSK erleichtern. Zur Effizienzsteigerung und Vereinfachung der Meldeprozesse soll bei der Geschäftsstelle zudem ein Meldeportal angesiedelt werden, durch das zentralisiert Meldungen von Datenschutzbeauftragten oder von Datenpannen, die möglicherweise mehrere Bundesländer betreffen, empfangen und an die zuständigen Datenschutzaufsichtsbehörden verteilt werden sollen.

Zudem bietet die Geschäftsstelle Potential, als Kooperationsschnittstelle für Informationsaustausch und Abstimmungsprozesse zwischen den für die EU-Digitalrechtsakte (DDG, NIS-2 u.a.) zuständigen Fachbehörden und den Datenschutzbehörden von Bund und Ländern zu fungieren. Dieses Feld und die damit verbundenen kooperationsrechtlichen Fragestellungen werden im AK DSK 2.0 noch weiter behandelt.

Die Einrichtung der ständigen Geschäftsstelle soll durch eine Verwaltungsvereinbarung zwischen Bund und Ländern erfolgen, die derzeit erarbeitet wird. Maßgebliche Unterstützung könnte das Vorhaben durch eine Grundlegung im Bundesdatenschutzgesetz erfahren.

Novellierung des BDSG als Chance für die Institutionalisierung der DSK?

Der Prozess zur Novellierung des Bundesdatenschutzgesetzes hat im Jahr 2023 begonnen und die Datenschutzkonferenz konnte eine erste Stellungnahme abgeben. Als Vorsitz des Arbeitskreis DSK 2.0 habe ich die Erstellung der Stellungnahme federführend begleitet und konnte wichtige Impulse zur Fortentwicklung der Datenschutzkonferenz setzen. Denn durch eine Regelung im Bundesdatenschutzgesetz soll das im Koalitionsvertrag verbriefte Vorhaben der Institutionalisierung der Datenschutzkonferenz vollzogen werden. Die darin vorgeschlagene Regelung blieb und bleibt jedoch weit hinter den möglichen und notwendigen gesetzlichen Rahmenbedingungen zurück. Die Datenschutzkonferenz hat sich deswegen für eine stärkere Konturierung der Datenschutzkonferenz und insbesondere auch eine Erwähnung der ständigen Geschäftsstelle ausgesprochen und hervorgehoben, dass eine ständige Geschäftsstelle einen Gewinn an Professionalität und eine Steigerung der Kontinuität im Handeln der DSK zur Folge hätte.

Über den Fortgang dieses wichtigen Vorhabens und über die zukünftigen Arbeiten des Arbeitskreises DSK 2.0 halte ich Sie gerne auf dem Laufenden.

2. KÜNSTLICHE INTELLIGENZ

Künstliche Intelligenz (KI) hat in den letzten Jahren eine große gesellschaftliche Präsenz erlangt. Im Rahmen unterschiedlicher informationstechnologischer Systeme findet KI bereits heute Anwendung sowohl bei öffentlichen Stellen als auch im Privatsektor. Spätestens seit Ende 2022 erfreuen sich sogenannte Large Language Models (LLM), die häufig in Form von Chatbots angeboten werden, großer Beliebtheit. Mit dem Dienst ChatGPT und den dazugehörigen Sprachmodellen GPT bis GPT-4 stand und steht der breiten Öffentlichkeit erstmals ein unkomplizierter Zugriff auf KI zur Verfügung. Da ChatGPT unter anderem auf der automatisierten Verarbeitung personenbezogener Daten beruht und jedenfalls auch Personen in der Europäischen Union angeboten wird, findet die Datenschutz-Grundverordnung (DS-GVO) gemäß Art. 2 Abs. 1 und Art. 3 Abs. 2 Anwendung.

Als Leiter der im Jahr 2019 ins Leben gerufenen „Taskforce KI“ habe ich mich am 20. April 2023 in einer koordinierten Aktion mit weiteren Landesdatenschutzbehörden mit einem ausführlichen Fragebogen an das hinter ChatGPT stehende US-amerikanische Unternehmen OpenAI, L.L.C. gewandt, um unterschiedliche Fragestellungen im Zusammenhang mit der Verarbeitung personenbezogener Daten durch ChatGPT zu klären. Ziel des gemeinsamen Vorgehens in der Taskforce KI war es, die Verfahren der deutschen Datenschutzaufsichtsbehörden gegenüber OpenAI zu koordinieren und zu vereinheitlichen.

Obwohl OpenAI den ersten Fragebogen Ende Juni 2023 kooperativ und umfangreich beantwortete, bestand noch Bedarf an konkretisierenden Nachfragen. Deshalb legten die deutschen Aufsichtsbehörden, wiederum in der Taskforce KI koordiniert, im Oktober 2023 einen zweiten Fragenkatalog nach. Die gestellten Fragen dienen der vertieften Prüfung, ob die Verarbeitung personenbezogener Daten in ChatGPT rechtmäßig erfolgt. Dabei stehen auch die besonderen Datenkategorien nach Art. 9 DS-GVO im Fokus, also jene Daten, die speziellen Schutz genießen und beispielsweise Angaben zur Religion, zur Gesundheit oder zur sexuellen Orientierung betreffen. Auch die Verwirklichung der Rechte betroffener Personen auf Auskunft sowie Berichtigung und Löschung personenbezogener Daten wird besonders geprüft.

Innerhalb der Taskforce KI habe ich die Erarbeitung eines Handlungsleitfadens für den Einsatz von KI-Systemen initiiert und geleitet. Besonderes Augenmerk wurde dabei auf die Zielgruppe der öffentlichen Stellen sowie kleine und mittlere Unternehmen (KMU) gelegt werden. Ziel ist es, Verantwortliche auf spezifische datenschutzrechtliche Fallstricke aufmerksam zu machen und bei der Einhaltung der sich daraus ergebenden datenschutzrechtlichen Anforderungen zu unterstützen. Nachdem die Taskforce KI bereits im Jahre 2019 die „Hambacher Erklärung zur Künstlichen Intelligenz“ sowie „Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen“ erarbeitet hat, soll Verantwortlichen nun ein weitergehender Leitfaden an die Hand gegeben werden. Dieser Handlungsleitfaden sollte im Frühjahr 2024 fertiggestellt und durch die Datenschutzkonferenz beschlossen werden. Der Zeitplan wurde eingehalten.

3. INTERNATIONALER DATENVERKEHR

EU-U.S. Data Privacy Framework

Das Jahr 2023 markierte eine entscheidende Entwicklung im Bereich der Datenübermittlung in die USA. Gem. Art. 45 Abs. 1 DS-GVO darf die Übermittlung personenbezogener Daten an ein Drittland ohne eine besondere Genehmigung vorgenommen werden, wenn die Europäische Kommission beschlossen hat, dass das betreffende Drittland ein angemessenes Schutzniveau bietet. Seit dem Jahr 2020 war der Einsatz von Diensten US-amerikanischer Anbieter ohne zusätzliche Schutzmaßnahmen wegen des Schrems-II-Urteils des Europäischen Gerichtshofs (EuGH-Urteil C-311/18) unzulässig, das die damalige Entscheidung der Europäischen Kommission für ungültig erklärte. Am 10. Juli 2023 nahm nunmehr die Europäische Kommission den Angemessenheitsbeschluss für den Datenschutzrahmen EU-USA – das sog. EU-U.S. Data Privacy Framework (EU-U.S. DPF) – an und schuf somit eine neue Rechtsgrundlage für derartige Übermittlungen.

Datenexporteure aus der EU haben jedoch zu beachten, dass kein generelles angemessenes Datenschutzniveau für Übermittlungen an Organisationen in den USA vorausgesetzt werden

kann. Sie müssen zunächst vorab prüfen und sicherstellen, dass der Datenimporteur, an den übermittelt wird, unter dem EU-U.S. DPF zertifiziert ist. Eine Selbstzertifizierung steht bisher nur U.S.-Organisationen offen, die der Aufsicht der Federal Trade Commission oder des U.S. Department of Transportation unterliegen. Eine Liste der zertifizierten Stellen ist auf der Website des U.S. Department of Commerce veröffentlicht (**https://s.rlp.de/DPF**).

Sollte der Datenimporteuer in den USA nicht unter dem EU-U.S. DPF zertifiziert sein, sind weitere Übermittlungsinstrumente und ggf. zusätzliche Maßnahmen erforderlich (Art. 46 ff. DS-GVO).

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat am 4. September 2023 Anwendungshinweise zum EU-U.S. DPF (**https://s.rlp.de/dsk-DPF**) veröffentlicht. Die Anwendungshinweise enthalten Informationen für die Datenexporteure, also die Verantwortlichen und Auftragsverarbeiter, die Daten in die USA übermitteln möchten. Andererseits informieren sie betroffene Personen darüber, welche Rechtsschutz- und Beschwerdemöglichkeiten sie haben.

Nachdem bereits die vorangegangenen Angemessenheitsbeschlüsse der Europäischen Kommission („Safe Harbor-Abkommen“ und „EU-US Privacy Shield“) gerichtlich überprüft wurden, ist damit zu rechnen, dass der Europäische Gerichtshof auch über die Rechtmäßigkeit des EU-U.S. DPF zu entscheiden haben wird. Ich empfehle daher, dass funktionierende alternative Übermittlungsinstrumente beibehalten und fortentwickelt werden.

Überarbeitete EDSA-Empfehlungen für Binding Corporate Rules

Verbindliche interne Datenschutzvorschriften, sog. Binding Corporate Rules (kurz: BCR) gemäß Art. 47 DS-GVO, können unter den Voraussetzungen des Art. 46 Abs. 1 DS-GVO eine geeignete Garantie für die Übermittlung personenbezogener Daten in Drittländer darstellen (Art. 46 Abs. 2 lit. b DS-GVO). BCR sind vor allem für international tätige Unternehmensgruppen mit Datentransfers in Drittländer empfehlenswert.

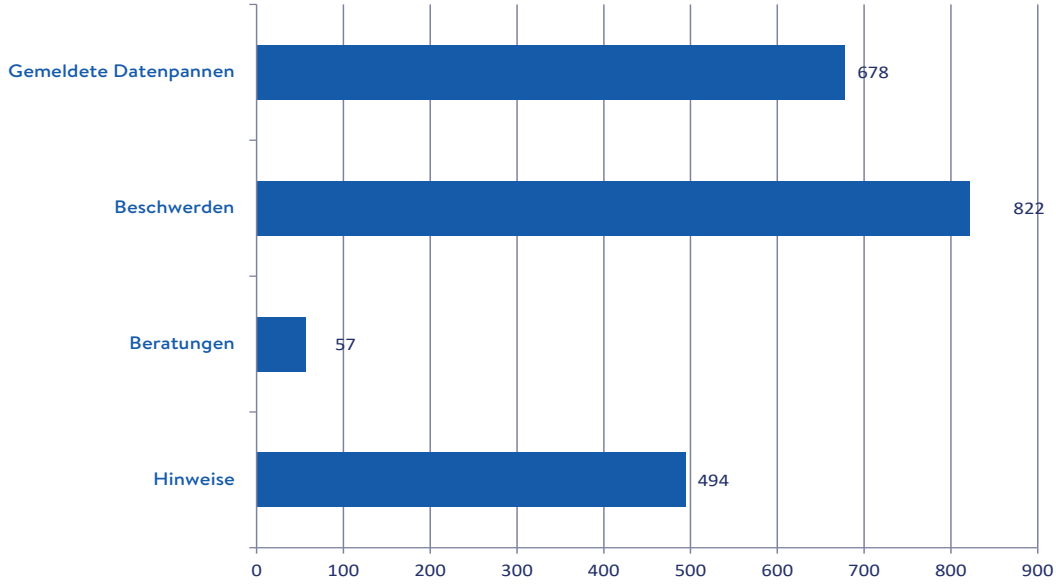
Die Genehmigung der BCR erfolgt gemäß des Kohärenzverfahrens nach Art. 63 DS-GVO durch die zuständige Aufsichtsbehörde (Art. 47 Abs. 1 DS-GVO). Der Europäische Datenschutzausschuss (EDSA) hat Arbeitspapiere bestätigt, die das Koordinierungsverfahren der europäischen Aufsichtsbehörden erläutern und Empfehlungen für Verantwortliche und Auftragsverarbeiter zur Genehmigung von BCR beinhalten.

Am 21. Juni 2023 hat der EDSA überarbeitete Empfehlungen zur Beantragung der Genehmigung und zu den Bestandteilen und Grundsätzen verbindlicher interner Datenschutzvorschriften für Verantwortliche (Binding Corporate Rules for Controllers, BCR-C) verabschiedet. Diese ersetzen das bisherige Arbeitspapier WP264. Die neuen Empfehlungen beinhalten Änderungen der Antragsdokumente und wesentliche inhaltliche Anforderungen an BCR-C. Verantwortliche haben spätestens mit der jährlichen Aktualisierung 2024 ihre bestehenden BCR-C entsprechend zu überarbeiten, ohne dass es einer erneuten Genehmigung durch die zuständige Aufsichtsbehörde bedarf (Ziffer 1.15. der Empfehlungen).

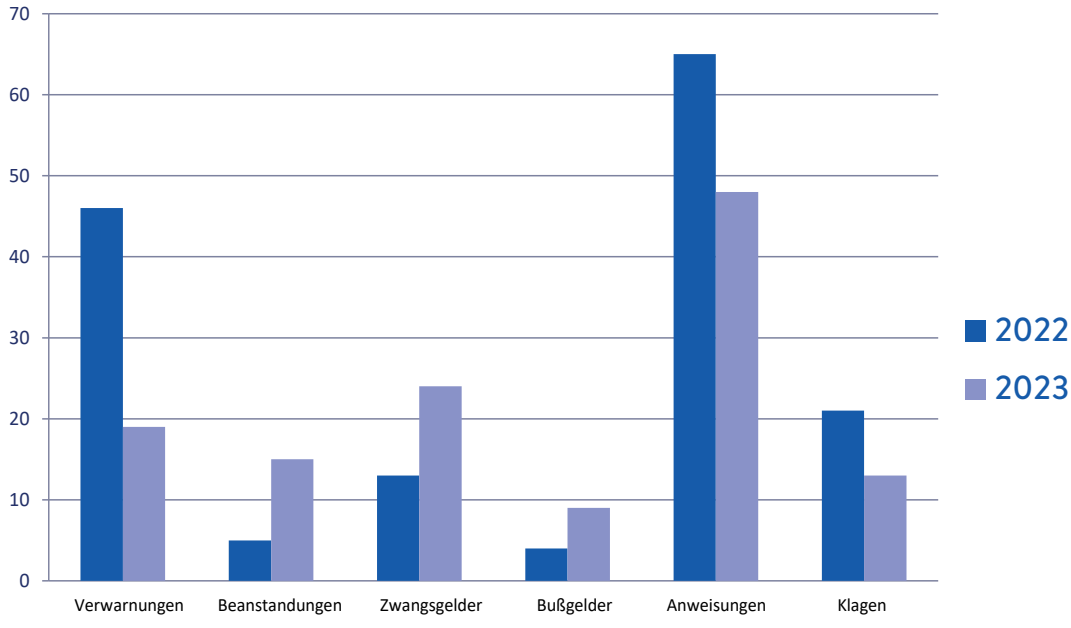
Die Empfehlungen – Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) – sind auf der Website des EDSA im Dokumentenbereich abrufbar: **https://edpb.europa.eu/**.

II.
ZAHLEN UND FAKTEN

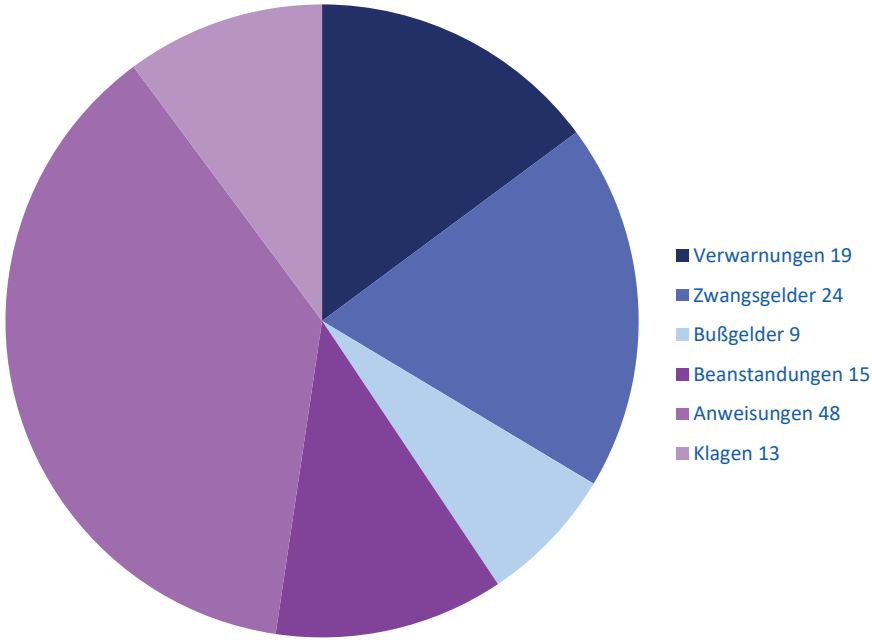
1. Geschäftsstatistik 2023



2. Ausgeübte Befugnisse 2022 und 2023



3. Ausgeübte Befugnisse 2023



III.
SACHGEBIETE

II. SACHGEBIETE

1. SICHERHEIT

1.1 Datenschutzrechtliche Kontrollen und Prüfungen des LfDI

1.1.1 Datenschutzrechtliche Kontrolle der Datenverarbeitung gemäß RED-G und ATDG

Gemäß § 11 des Rechtsextremismus-Datei-Gesetzes (RED-G) und § 10 des Antiterrordateigesetzes (ATDG) obliegt es dem LfDI, in regelmäßigen Abständen die Durchführung des Datenschutzes zu überprüfen. Diese Kontrollen dienen dem Zweck, die Einhaltung der Datenschutzbestimmungen sicherzustellen und damit die informationelle Selbstbestimmung und die Privatsphäre der Bürger:innen zu schützen.

In einer Zeit, in der personenbezogene Daten in einem beispiellosen Umfang gesammelt, verarbeitet und genutzt werden, ist es von entscheidender Bedeutung sicherzustellen, dass dies in Übereinstimmung mit den Datenschutzgesetzen geschieht. 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.

Ende 2023 hat der LfDI einen Informationsbesuch beim Landeskriminalamt Rheinland-Pfalz durchgeführt. Dabei hat sich der LfDI einen Überblick über die grundlegenden Aspekte der Datenverarbeitung verschafft, die gemäß RED-G und ATDG durch die Landespolizei in Rheinland-Pfalz durchgeführt werden.

Für die vertiefende datenschutzrechtliche Kontrolle im Berichtszeitraum 2024 beabsichtigt der LfDI, Protokolldaten zu beiden Dateien anzufordern und stichprobenartig Einzelfälle auf Datenschutzkonformität zu überprüfen. Dazu wird der LfDI im nächsten Tätigkeitsbericht berichten.

1.1.2 Datenschutzrechtliche Kontrolle nach § 47 Abs. 5 Polizei- und Ordnungsbehördengesetz (POG)

Gemäß § 47 Abs. 5 POG soll der LfDI alle zwei Jahre besonders eingriffsintensive – insbesondere heimliche – Datenerhebungen (§ 33-36, 38, 39, 41, 42 Abs. 2 und 44 POG) der Polizei Rheinland-Pfalz nach dem Polizei- und Ordnungsbehördengesetz überprüfen. Die Kontrolle dient dem kompensatorischen Grundrechtsschutz der betroffenen Personen, deren Individualrechtsschutz aufgrund der Heimlichkeit der Maßnahmen erschwert wird. Vor diesem Hintergrund wurde ein besonderer Fokus auf die Benachrichtigungen gemäß § 48 Abs. 1 POG gelegt, die grundsätzlich im Nachgang der Maßnahmen gegenüber den betroffenen Personen ergehen müssen.

Dazu wurden im Berichtszeitraum bei zwei Polizeipräsidien die entsprechenden Prüfungen vorgenommen. Die Prüfungen konzentrierten sich dabei auf die Plausibilität der Unterlagen, die Überprüfung der Rechtmäßigkeit der Maßnahmen sowie auf die ordnungsgemäße Erfüllung der Benachrichtigungspflichten, sowohl was die Verpflichtung an sich als auch die Art und Weise ihrer Umsetzung betraf.

Die überprüften Maßnahmen waren überwiegend rechtmäßig in Bezug auf die Eingriffsschwellen und Verfahrensanforderungen und anhand der Dokumentation und ergänzenden Informationen, die im Rahmen der Vor-Ort-Kontrolle mitgeteilt wurden, nachvollziehbar. Mängel wurden dagegen im Hinblick auf die Benachrichtigungspraxis festgestellt. So wurde in vereinzelten Fällen nicht oder nur münd-

lich über die Maßnahme informiert. In anderen Fällen wurde ein Vordruck genutzt, dem aber wichtige Angaben fehlten. Zudem wurden Benachrichtigungen zurückgestellt, jedoch verspätet überprüft, ob die Zurückstellung aufrechterhalten werden durfte.

Im Nachgang der Prüfungen wurden deswegen die folgenden Empfehlungen an die Polizeipräsidien und an das Ministerium des Innern und für Sport adressiert:

Überarbeitung der Benachrichtigungspraxis und des Benachrichtigungsformulars

Die gesetzlich verankerten Benachrichtigungspflichten im Hinblick auf besonders eingriffsintensive Maßnahmen haben eine bedeutsame Funktion. Denn sie sollen sicherstellen, dass den betroffenen Personen eine nachträgliche Rechtmäßigkeitsüberprüfung ermöglicht wird von Maßnahmen, die ohne deren Wissen und mit einer erheblichen Eingriffsintensität in Bezug auf ihre Grundrechte erfolgt sind. Dies gibt ihnen die Möglichkeit, gegebenenfalls eine nachträgliche gerichtliche oder datenschutzrechtliche Kontrolle zu initiieren, und trägt zur Verhältnismäßigkeit der Maßnahmen bei. In Anwendung dieser Grundsätze ist es entscheidend, adressatengerecht eine klare und einfache Sprache zu verwenden und in präziser, verständlicher und leicht zugänglicher Form zu benachrichtigen (§ 1a S. 3 POG i.V.m. § 47 Abs. 1 LDSG). Dies erfordert, dass die Benachrichtigung in jedem Fall schriftlich erfolgen muss. Auf diese Weise ist zugleich eine sorgfältige und transparente Dokumentation sichergestellt, die einer Kontrolle zugänglich ist. Das landesweit vorgesehene Benachrichtigungsformular erfüllt diese Anforderungen nicht, da es nur auf die Rechtsgrundlagen der zugrundeliegenden Maßnahmen hinweist, darüber hinaus jedoch keine Erläuterungen bzw. Erklärungen der Maßnahmen und der damit einhergehenden Datenverarbeitungen enthält, die jedoch für das Verständnis der betroffenen Personen, die in der Regel Laien sind, erforderlich sind. Zudem fehlen die oben genannten Angaben zur Speicherdauer der Verarbeitung, zu den Empfängern der Daten, zu den Kontaktdaten der Datenschutzbeauftragten sowie zu weiteren Betroffenenrechten und dem Beschwerderecht beim LfDI Rheinland-Pfalz. In der Folge sind bei der Neugestaltung des Formulars die Mindestanforderungen an die Benachrichtigung zu beachten, wie sie sich aus § 48 Abs. 2 POG und § 1a S. 3 POG i. V.m. § 44 Abs. 1 LDSG ergeben.

Intensive Schulungen zur Benachrichtigungspflicht

Nach Aussagen der Mitarbeitenden der Polizeipräsidien lassen sich die festgestellten Defizite einerseits auf fehlende Erfahrung im Hinblick auf die eingriffsintensiven Maßnahmen und die damit einhergehenden Benachrichtigungspflichten zurückführen, andererseits auf unzureichende Kenntnisse der rechtlichen – insbesondere datenschutzrechtlichen – Anforderungen. Dies ist auch dem Umstand geschuldet, dass die überprüften Maßnahmen aus dem Jahr 2020 und 2021 stammen. In diesem Zeitraum wurde das Polizei- und Ordnungsbehördengesetz gerade in diesem Bereich umfangreich novelliert. Infolgedessen sollte eine nachhaltige Sensibilisierung und gezielte Schulung der Mitarbeitenden erfolgen, insbesondere der Organisationseinheiten, die üblicherweise Verfahren bearbeiten, in denen eingriffsintensive Maßnahmen verwendet werden. Diese Schulungen würden dazu beitragen, die erforderlichen rechtlichen Kompetenzen zu vertiefen und eine effektive und verfahrenssichere Umsetzung der datenschutzrechtlichen Anforderungen zu gewährleisten.

Fristenkontrolle

Um sicherzustellen, dass Benachrichtigungspflichten bei polizeilichen Maßnahmen nicht versäumt werden, wird dringend empfohlen, eine effektive technische Fristenkontrolle zu implementieren. Mit Blick auf die bevorstehende Einführung des neuen polizeilichen Vorgangsbearbeitungssystems @rtus sollten geeignete Softwarelösungen eingesetzt werden, die automatisch an bevorstehende Fristen erinnern und so eine zeitgerechte Einhaltung sicherstellen. Bis zur vollständigen Einführung von @rtus mit entsprechender technischer Fristenkontrolle müssen geeignete Garantien eingeführt werden, die auch im derzeit bestehenden Vorgangsbearbeitungssystem POLADIS die Überwachung und Einhaltung von Fristen gewährleisten. Parallel dazu wird empfohlen, eine Fachaufsicht zu etablieren, die als zusätzliches Kontrollorgan agiert. Diese Fachaufsicht sollte regelmäßig die Einhaltung der Benachrichtigungspflichten überprüfen und sicherstellen, dass die technische Fristenkontrolle ordnungsgemäß funktioniert. Durch klare Zuständigkeitsregelungen kann die Fachaufsicht sicherstellen, dass sämtliche Schritte im Benachrichtigungsprozess ordnungsgemäß ausgeführt werden.

Angesichts der Einsicht und Kooperation der Mitarbeitenden der Polizeipräsidien vor Ort besteht Zuversicht, dass im Rahmen der Kontrolle 2025/2026 solche Defizite nicht mehr festgestellt werden.

1.2 Zuverlässigkeitsüberprüfungen von (Groß-)Veranstaltungen

Die gesetzlichen Regelungen in §§ 67 und 68 POG verfolgen den Zweck, die Sicherheit bei Veranstaltungen zu gewährleisten. Insbesondere dienen sie dazu, potenzielle Gefahrensituationen frühzeitig zu erkennen und zu verhindern sowie eine effektive Kontrolle über die Personen zu ermöglichen, die an solchen Veranstaltungen sicherheitsrelevante Tätigkeiten durchführen oder in sicherheitsrelevanten Bereichen eingesetzt werden.

Vereinheitlichung des Verfahrens der Zuverlässigkeitsüberprüfung

Bereits im 31. Tätigkeitsbericht (Ziffer II, 1.1 S. 24 ff.) wurde über die neu geschaffenen gesetzlichen Regelungen der Zuverlässigkeitsüberprüfung berichtet. Seitdem hat der LfDI im Rahmen seiner Anhörungspflicht eine Reihe von Zuverlässigkeitsüberprüfungen datenschutzrechtlich geprüft. Die daraus resultierenden Hinweise des LfDI an die durchführenden Stellen haben zu einer Vereinheitlichung der Konzepte bei den Polizeipräsidien geführt. Insbesondere bei der Neukonzeptionierung der verwendeten Formulare sind die datenschutzrechtlichen Hinweise des LfDI eingeflossen. Unter anderem wurde die Datenschutzerklärung an die gesetzlichen Vorgaben angepasst. Beispielsweise war es nicht mehr Bestandteil der Datenschutzerklärung, dass ein Abgleich mit den Dateien des Verfassungsschutzes der Regelfall ist. Des Weiteren konnte Klarheit bezüglich der Speicherung der Verfahrensunterlagen geschaffen werden. Diese werden nun einheitlich bei dem jeweiligen Polizeipräsidium zentral gespeichert, das die Zuverlässigkeitsüberprüfung durchführt. Durch diese zentrale Speicherung wird nicht nur eine einheitliche Verwaltung gewährleistet, sondern auch den betroffenen Personen eine Erleichterung geboten, wenn sie von ihren Rechten Gebrauch machen und die Verfahrensunterlagen etwa zu Zwecken der Rechtmäßigkeitsprüfung sichten möchten.

Verwaltungsgerichtliche Überprüfung des Verfahrens

Mit dem Urteil des Verwaltungsgerichts Koblenz vom 08.05.2023 - 3 K 834/22.KO war die Zuverlässigkeitsüberprüfung gemäß § 68 POG erstmals Gegenstand einer gerichtlichen Überprüfung. In dem Verfahren wehrte sich ein Veranstalter u.a. gegen die ordnungsbehördliche Anordnung, alle auf dem Veranstaltungsgelände eingesetzten Mitarbeiter:innen einer Zuverlässigkeitsüberprüfung zu unterziehen. Dies betraf alle Dienstleistenden inklusive der eingesetzten Wachpersonen gewerblicher Wachunternehmen.

Das Gericht entschied, dass § 68 Abs. 1 POG keine Grundlage zur Durchführung einer Zuverlässigkeitsüberprüfung aller auf dem Veranstaltungsgelände eingesetzten Mitarbeitenden bietet. Die Einbeziehung von gewerblichen Wachpersonen in die Zuverlässigkeitsüberprüfung lief nach Ansicht des Gerichts der gesetzlichen Regelung des § 68 Abs. 1 Satz 1 HS. 1 POG zuwider, da die Polizei nur dann eine Zuverlässigkeitsüberprüfung durchführen kann, wenn keine bundesrechtlichen oder besonderen landesrechtlichen Vorschriften eine solche vorsehen. Da Wachpersonen bereits gemäß § 34a der Gewerbeordnung überprüft werden, war eine zusätzliche polizeiliche Überprüfung nicht erforderlich.

Ebenfalls beanstandete das Gericht die Überprüfung aller auf dem Veranstaltungsgelände eingesetzten sonstigen Mitarbeitenden unabhängig von Art und Ausmaß der Zugangsmöglichkeiten, auch wenn es sich um eine besonders gefährdete Veranstaltung handelt. Denn nach dem Wortlaut der Vorschrift ist eine Zuverlässigkeitsüberprüfung nur in Bezug auf Mitarbeitende zulässig, die über einen privilegierten Zutritt zu der Veranstaltung verfügen. Dieser ist abzugrenzen vom allgemeinen Zugang, wie er den regulären Besucher:innen zur Verfügung steht. Diese erweiterten – privilegierten – Zutrittsmöglichkeiten können zeitlich (außerhalb der Öffnungszeiten des Veranstaltungsgeländes für jedermann) und/oder räumlich sein (zum Beispiel Zugang zu Bühnen, zum Backstage-Bereich, zu Strom-, Wasser- und sonstigen Versorgungseinrichtungen, zu pyrotechnischen Einrichtungen, zur Veranstaltungszentrale und zu ähnlichen sicherheitsrelevanten Bereichen). Dies ist nach Auffassung des Gerichts bei Mitarbeitenden, die sich in denselben Bereichen wie Besucher bewegen, nicht der Fall.

Schließlich führte das Gericht aus, dass es im Ermessen der Behörde liege, ob Ordnungsdienstkräfte, die keine Wachpersonen eines gewerblichen Bewacherunternehmens sind, oder Personen, für die ein privilegierter Zutritt vorgesehen ist, zuverlässigkeitsüberprüft werden. Die Ermessensentscheidung und deren Erwägungen müssen im Auflagenbescheid nachvollziehbar dargelegt werden.

Im konkreten Verfahren zum Festival Nature One hatte sich der LfDI bereits im Vorfeld gegenüber dem beteiligten Polizeipräsidium kritisch zu den strittigen Punkten geäußert und war in den Austausch mit dem Ministerium des Innern und für Sport Rheinland-Pfalz getreten, um eine grundsätzliche Klärung zu den Bedenken des LfDI in diesem Verfahren, aber auch zu weiteren datenschutzrechtlich relevanten herbeizuführen (vgl. 31. Tätigkeitsbericht a.a.O.). Das Verwaltungsgericht Koblenz hat letztlich die Rechtsauffassung des LfDI bestätigt, indem es feststellte, dass die Regelungen zur Zuverlässigkeitsüberprüfung keine Grundlage für eine solche umfassende Überprüfung bieten. Dies hat dazu geführt, dass die Konzepte der Polizei entsprechend angepasst wurden, um den gesetzlichen Vorgaben und den datenschutzrechtlichen Erfordernissen gerecht zu werden.

1.3 Informationsaustausch mit den behördlichen Datenschutzbeauftragten bei den Polizeipräsidien

Im Rahmen seines proaktiven Ansatzes ist es stets ein Anliegen des LfDI, mit den für die Gewährleistung von Datenschutz relevanten Akteur:innen in den Austausch zu treten und Theorie und Praxis zusammenzuführen. Zu diesem Zweck erfolgte ein Treffen zwischen dem LfDI und den behördlichen Datenschutzbeauftragten der Polizeipräsidien, des Landeskriminalamtes und der Hochschule der Polizei.

Betonung der Rolle der Datenschutzbeauftragten

Ein wesentliches Ziel der Tagung war es, die Rolle der Datenschutzbeauftragten als primäre Ansprechpartner:innen für datenschutzrechtliche Belange zu betonen. Als direkte Verbindung zwischen den datenschutzrechtlich Verantwortlichen und der Aufsichtsbehörde gemäß § 39 Abs. 1 S. 1 Nr. 2 LDSG spielen sie eine Schlüsselrolle bei der Gewährleistung der Einhaltung der Datenschutzbestimmungen.

Diskussion aktueller datenschutzrechtlicher Themen

Darüber hinaus diente der Informationsaustausch dazu, aktuelle datenschutzrechtlich relevante Themen zu diskutieren. Die Auswahl der Themen erfolgte sorgfältig unter Berücksichtigung ihrer aktuellen und praktischen Relevanz für die Aufsichtstätigkeit des LfDI. Dabei wurden nicht nur theoretische Aspekte betrachtet, sondern auch die praktische Erfahrung und Expertise der Teilnehmenden eingebunden. Diese Tagung ermöglichte es dem LfDI, wichtige Einblicke in die Herausforderungen und Entwicklungen im Bereich des Datenschutzes im Kontext polizeilicher Tätigkeiten zu gewinnen. So ist man zu aktuellen Entwicklungen im Auskunftsrecht, zum Thema „Polizeiliche Datenanalysen und KI“ und zu aktuellen Ergebnissen aus Datenschutzkontrollen in den Austausch getreten.

Fortführung des Dialogs und Intensivierung der Zusammenarbeit

Dieser Dialog wird fortgesetzt und die Zusammenarbeit mit den Datenschutzbeauftragten der Polizeipräsidien weiter intensiviert, um den Datenschutz der Sicherheitsbehörden – einem Bereich, der die Rechte und Freiheiten der Bürger:innen besonders berührt – bestmöglich zu fördern.

2. JUSTIZ

2.1 Dezentrale Fortbildung für die behördlichen Datenschutzbeauftragten der Amts- und Landgerichte sowie der Staatsanwaltschaften beim Pfälzischen Oberlandesgericht Zweibrücken

Im Bereich der Justiz sind hinsichtlich des Datenschutzes Besonderheiten zu beachten. Zum einen prallen verschiedene Datenschutzregime aufeinander: Während in der Zivil- und Verwaltungsgerichtsbarkeit die Datenschutz-Grundverordnung gilt, finden im Rahmen der Arbeit der Strafgerichte und Staatsanwaltschaften zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung die Gesetze zur Umsetzung der Richtlinie (EU) 2016/680 Anwendung.

Zum anderen sind die justiziellen Tätigkeiten der Gerichte gem. Art. 55 Abs. 3 DS-GVO bzw. § 41 Abs. 2 LDSG von der ordentlichen behördlichen Datenschutzaufsicht ausgeschlossen. Hintergrund ist das Rechtsstaatsprinzip, welches die Gewaltenteilung zwischen Gesetzgebung, Verwaltung und Rechtsprechung vorsieht und bezüglich der Rechtsprechung in Art. 97 GG die richterliche Unabhängigkeit festlegt. Die Staatsanwaltschaften unterliegen dieser Freistellung dagegen nicht und unterfallen somit der Zuständigkeit der Datenschutzaufsichtsbehörden.

Am 25. Oktober 2023 hat der LfDI im Rahmen einer dezentralen Fortbildung für die behördlichen Datenschutzbeauftragten der Amts- und Landgerichte sowie Staatsanwaltschaften im Bezirk des Pfälzischen Oberlandesgerichts Zweibrücken diese Abgrenzungsfragen und die in dem Arbeitsalltag der Teilnehmer:innen auftretende Thematik der Datenpannen, wie beispielsweise der Verlust oder der Fehlversand von Akten oder Hacking-Angriffe, behandelt. Zudem erhielten die Teilnehmer:innen einen Überblick über die Reichweite des Auskunftsrechts im Lichte der EuGH-Rechtsprechung. Im Anschluss wurden die behandelten Themen anhand der von den Teilnehmer:innen vorgestellten Praxisfälle gemeinsam mit den Referent:innen besprochen.

Der Austausch mit der Praxis geht auch aus Sicht des LfDI immer mit einem immensen Erkenntnisgewinn für dessen aufsichtsbehördliche Arbeit einher, sodass die Fortbildung mit den interessierten und sachkundigen Teilnehmer:innen für alle Beteiligten auch im Jahr 2023 sehr gewinnbringend war.

2.2 Veröffentlichung einer nicht anonymisierten gerichtlichen Entscheidung in Fachportalen

Datenschutzverletzungen, auch als Datenpannen bezeichnet, können auch bei der Verarbeitung personenbezogener Daten im Arbeitsalltag der Gerichte und Staatsanwaltschaften eine Rolle spielen, etwa im Fall des Versands von Schriftsätzen/Akten an die falschen Empfänger:innen oder im Fall der Betroffenheit von einer Schadsoftware.

In einem solchen Fall ist zu prüfen, ob gem. Art. 33 DS-GVO, § 54 LDSG eine Meldepflicht an den LfDI als Aufsichtsbehörde besteht. Diese steht im unmittelbaren Zusammenhang mit dem Transparenzgebot. Die Meldung soll dem LfDI insbesondere ein Lagebild über die vorhandenen Bedrohungen und Fehlerquellen bei der Verarbeitung personenbezogener Daten vermitteln, um somit wiederrum seine Beratungsfunktion sicherstellen zu können.

Im Rahmen des Berichtsjahres wurde dem LfDI die Veröffentlichung einer nicht hinreichend anonymisierten gerichtlichen Entscheidung in mehreren einschlägigen Fachportalen gemeldet.

Grundsätzlich ist die Anonymisierung einer gerichtlichen Entscheidung der justiziellen Tätigkeit des zuständigen Richters/ der zuständigen Richterin zuzuordnen und fällt damit unter die Bereichsausnahme des Art. 55 Abs. 3 DS-GVO, § 41 Abs. 2 LDSG, sodass eine Zuständigkeit des LfDI zu verneinen ist.

Der LfDI Rheinland-Pfalz verfolgt dabei eine restriktive Auslegung des Begriffs der justiziellen Tätigkeit; lediglich die originär rechtsprechende Tätigkeit der Gerichte einschließlich deren Vorbereitung und Durchführung sind in diesem Sinne umfasst.

Kennzeichen rechtsprechender Tätigkeit ist die letztverbindliche Klärung der Rechtslage in einem Streitfall. Die Bereichsausnahme erstreckt sich auf sämtliche Tätigkeiten, die mit der Entscheidungsfindung im Zusammenhang stehen, aber auch auf Verarbeitungsvorgänge der Gerichte, deren Kontrolle durch die Aufsichtsbehörde mittelbar oder unmittelbar die Unabhängigkeit der Mitglieder oder der Entscheidungen der Gerichte beeinflussen könnte (vgl. EuGH-Urteil vom 24. März 2022, C 245/20).

Vor diesem Hintergrund ist die Bereichsausnahme beim Versand der nicht anonymisierten Entscheidung für eine Veröffentlichung nicht einschlägig, sodass eine Zuständigkeit des LfDI zu bejahen ist und eine Meldepflicht bestand.

Die betreffende Entscheidung wurde durch das Gericht umgehend von den Fachportalen entfernt. Da es nachgewiesenermaßen bereits zu Abrufen der Entscheidung kam, wurde die betroffene Person gem. § 55 Abs. 1 LDSG über die Datenschutzverletzung benachrichtigt.

3. VIDEOÜBERWACHUNG

Im Jahr 2023 hat sich die Zahl der Eingaben zu Videoüberwachung im nachbarschaftlichen Bereich auf einem konstant hohen Niveau eingependelt. So gab es gut 350 Verfahren und 80 schriftliche Beratungen. Hinzu kam eine hohe Anzahl telefonischer Anfragen, sowohl von betroffenen Personen als auch von Verantwortlichen. Da inzwischen bei fast allen Kameramodellen die Erfassungsbereiche softwareunterstützt angepasst werden können, ist eine Einschätzung des Aufnahmebereichs von außen quasi nicht mehr möglich. Ebenso wenig kann dauerhaft sichergestellt werden, dass keine Änderungen vorgenommen werden. Dies führt auch bei der Aufsichtsbehörde dazu, dass weitere Ermittlungsmöglichkeiten in vielen Fällen ausgeschlossen sind. Da die Aufsichtsbehörde keine Entfernung von Kameras anordnen kann (möglich ist hier nur eine Verarbeitungsbeschränkung), bleibt Betroffenen oftmals nur der Zivilrechtsweg.

Im gewerblichen Bereich erreichten den LfDI 29 Beschwerden und 35 Hinweise. Hierbei ging es in den meisten Fällen um Videoüberwachung in Gastronomiebetrieben oder Geschäften. Verstärkt ist festzustellen, dass Fitnessstudios auf eine umfassende Videoüberwachung setzen, um so Personal einzusparen. Eine lückenlose Überwachung, gerade auch im Trainingsbereich, sieht der LfDI aufgrund des damit einhergehenden starken Eingriffs in die Persönlichkeitsrechte sehr kritisch, auch wenn hier mit Gefahrenabwehr, Gesundheitsschutz und Schutz vor Diebstählen argumentiert wird.

Die Eingaben zur Videoüberwachung durch öffentliche Stellen (16 Verfahren) betrafen die Bereiche Müllablagerungen, Parkraumbewirtschaftung und Schulen. Neben Beratungsanfragen zum Einsatz von Videotechnik bei Veranstaltungen gab es größere Beratungsprojekte zur Nutzung von Bodycams im Schienenpersonennahverkehr und zur Verkehrsraumüberwachung im Rahmen des ÖPNV. Hier zeigt sich verstärkt, dass die Abwägung von Sicherheitsinteressen und Persönlichkeitsrechten alle Beteiligten vor große Herausforderungen stellt. Der Einsatz künstlicher Intelligenz in diesem Bereich wird in Zukunft unausweichlich sein, aber ggf. neue Problemfelder mit sich bringen.

4. WIRTSCHAFT

4.1 Dauerbrenner Auskunftsrecht

Das in Art. 15 DS-GVO vorgesehene Auskunftsrecht beschäftigte den LfDI auch in diesem Berichtszeitraum. So fällt auf, dass Anträge auf Auskunft von den betroffenen Personen häufig mit der Forderung nach Löschung verbunden werden. Dies führt in der Praxis hin und wieder dazu, dass Verantwortliche bestätigen, die Löschung der Daten sei wunschgemäß erfolgt, dann aber die Auskunft nicht mehr erteilen können, weil die Daten nicht mehr vorhanden sind. Verantwortliche sollten daher zunächst die Auskunft erteilen, ob und welche Daten vorhanden sind, und dann erst zur Löschung schreiten.

Auch wird gerne übersehen, dass in jedem Fall den Antragstellenden zu antworten ist, auch wenn keine Daten vorhanden sind.

Häufig wird von den betroffenen Personen angezweifelt, dass die Auskunft vollständig ist. Für den LfDI ist es schwierig, dies festzustellen. Zwar kann die Aufsichtsbehörde prüfen, ob die in Art. 15 Abs. 2 DS-GVO genannten Informationen enthalten sind, ob aber tatsächlich alle konkreten personenbezogenen Daten mitgeteilt wurden, kann nicht rechtssicher festgestellt werden. Hier ist es aber hilfreich, wenn die Auskunftsersuchenden so konkret wie möglich darlegen, weshalb sie davon ausgehen, dass noch weitere Daten vorhanden sein müssten.

Die in Art. 15 Abs. 3 DS-GVO genannte Kopie meint nicht lediglich, wie von einigen Verantwortlichen angenommen, eine Liste oder sonstige schriftliche Zusammenstellung der gespeicherten personenbezogenen Daten. Das Recht auf Kopie umfasst vielmehr die originalgetreue und verständliche Reproduktion der personenbezogenen Daten der betroffenen Person, also Kopien von Auszügen aus Dokumenten oder ganze Dokumente, die u.a. die entsprechenden personenbezogenen Daten enthalten. Denn es lässt sich teilweise nur im Kontext des gesamten Dokuments verstehen, wie die Daten verarbeitet werden. Dieses Verständnis kann aber erforderlich sein, um der betroffenen Person die wirksame Ausübung ihrer Betroffenenrechte zu ermöglichen.

4.2 Auskunft zu Sprachaufzeichnungen insbesondere im Bereich der Kreditwirtschaft

Bei telefonischen Kontakten mit Kreditinstituten werden häufig Sprachaufzeichnungen gefertigt. Im Bereich des Wertpapierhandels sind die Finanzinstitute gesetzlich dazu verpflichtet. Für den Umgang mit solchen Aufzeichnungen gibt es hinreichende Regelungen. Aber auch außerhalb des Wertpapierhandels werden oftmals Gespräche aufgezeichnet, da die Institute auch Dritte im Rahmen der Auftragsverarbeitung einsetzen, um die Kommunikation mit den Kund:innen zu managen. Die Aufzeichnungen dienen dazu, die Qualität und das korrekte Verhalten dieser Dritten, in der Regel Callcenter, überprüfen zu können. Verantwortlich bleibt hier die einzelne beauftragende Bank.

Grundsätzlich sind auch solche Sprachaufzeichnungen vom Auskunftsanspruch gem. Art. 15 DS-GVO umfasst. Diese Aufzeichnungen sind in der Regel auch im Audioformat zu beauskunften, also als „Kopie“ gem. Art. 15 Abs. 3 DS-GVO. Die betroffene Person und der Verantwortliche können sich jedoch darauf einigen, dass die Auskunft in Form einer Transkription erteilt wird. Art. 15 Abs. 4 DS-GVO schränkt das Recht auf Erhalt einer Kopie dahingehend ein, dass dadurch nicht die Rechte und Freiheiten anderer Personen beeinträchtigt werden dürfen. Im Falle von Sprachaufzeichnungen können das die Rechte und Freiheiten des Gesprächspartners, in der Regel der Mitarbeitenden sein. Sollten diese Rechte beeinträchtigt sein, könnte die Aufzeichnung der Mitarbeiten-

den soweit unkenntlich gemacht werden, dass die Beeinträchtigung ausgeschlossen werden kann. Ob eine Beeinträchtigung vorliegt, muss der Verantwortliche prüfen. Er trägt letztlich die Beweislast, dass dem so ist.

4.3 Kopieren von Ausweispapieren

In vielen Wirtschaftsbereichen wird zur Identifikation oftmals die Vorlage des Personalausweises verlangt und dieser dann auch gerne kopiert oder fotografiert, vorgeblich zu Dokumentationszwecken.

Das Fotokopieren, Fotografieren und Einscannen von Personalausweisen wird in § 20 Abs. 2 Personalausweisgesetz (PAuswG) geregelt. Die Vorschrift lautet: „Der Ausweis darf nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Ausweisinhabers tun. Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt."

Die Anfertigung und Speicherung einer Ausweiskopie muss im Einzelfall erforderlich sein. Dies ist dann nicht der Fall, wenn der Personalausweis vor Ort vorgezeigt und eingesehen werden kann. Zusätzlich kommt ein schriftlicher Vermerk darüber in Frage, dass die betroffene Person die Identität durch Vorlage des Ausweises nachgewiesen hat.

Selbst wenn eine Kopie erforderlich ist, muss im Hinblick auf den Grundsatz der Datenminimierung zum Zweck der Identifizierung grundsätzlich nur der Vor- und Nachname, die Anschrift und gegebenenfalls auch die Gültigkeitsdauer erhoben werden. Die übrigen Daten dürfen und sollen auf der Kopie geschwärzt werden (zum Beispiel die Zugangs- und Seriennummer, die Staatsangehörigkeit, die Größe, die Augenfarbe, das Lichtbild und die maschinenlesbare Zone).

Die Angabe des Geburtsdatums und gegebenenfalls -ortes kann nur erforderlich sein, wenn trotz der vorgenannten Angaben eine Personenverwechslung möglich ist und das Unternehmen in seinem bisherigen Datenbestand überhaupt das Geburtsdatum oder den -ort als Referenzdatum gespeichert hat.

Anderes gilt für Verantwortliche, die nach dem Geldwäschegesetz verpflichtet sind, Sorgfaltspflichten einzuhalten und Personen zu identifizieren. Hier besteht das Recht und die Pflicht, das vorgelegte Ausweisdokument vollständig zu kopieren oder es vollständig optisch digital zu erfassen (§ 8 Abs. 2 GwG). Verpflichtete sind insbesondere Kreditinstitute, aber u.a. auch andere Finanzdienstleister, Versicherungen, Rechtsanwält:innen, Wirtschaftsprüfer:innen, Immobilienmakler:innen und Veranstalter von Glücksspielen.

4.4 Auswertung von Kundendaten zu Werbezwecken durch die Kreditwirtschaft

Kreditinstitute haben nach wie vor großes Interesse daran, die bei ihnen vorhandenen Kundendaten, insbesondere die Zahlungsverkehrsdaten, auszuwerten und so ihre Kundschaft zielgenau ansprechen zu können. An der datenschutzrechtlichen Zulässigkeit solcher Anliegen hat sich seit den Ausführungen im Tätigkeitsbericht 2019 (vgl. 28. Tb., Tz. 5.2) nichts geändert: Die Auswertung der Zahlungsverkehrsdaten, also z.B. Informationen zu den Zahlungsempfängern und den Verwendungszwecken, bedarf der Einwilligung der betroffenen Person und kann nicht auf Art. 6 Abs. 1 lit. f DS-GVO

gestützt werden, da die schutzwürdigen Interessen der Kund:innen am Ausschluss der Verarbeitung oder Nutzung das Interesse des Kreditinstituts überwiegen. Die Einwilligung muss in informierter Weise erfolgen, ist freiwillig und die Verweigerung hat keinen Einfluss auf die Kontoführung. Insbesondere dieser letztgenannte Punkt wird in der praktischen Umsetzung nicht immer deutlich.

4.5 Andere Auswertungen durch Kreditinstitute

Kreditinstitute überprüfen Kontobewegungen auch aufgrund gesetzlicher Verpflichtungen: So sind Sparkassen und Banken neben anderen Unternehmen im Finanzsektor verpflichtet, 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, hier § 25 h KWG.

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. Im Rahmen dieser gesetzmäßig vorgesehenen Sicherungssysteme kann dann z.B. auffallen, dass ein Kontoinhaber oder eine Kontoinhaberin am möglicherweise illegalen Glücksspiel teilnimmt oder Waffen kauft. Dies kann zu Maßnahmen des Geldinstituts führen von der Kundennachfrage bis zur Kündigung des Kontos. Da solche Überprüfungen in der Regel durch separate Stellen innerhalb der Bank vorgenommen werden, ist nicht davon auszugehen, dass andere Mitarbeitende hiervon Kenntnis erlangen bzw. diese Durchsicht der Konten vornehmen. Da diese Datenverarbeitungen aufgrund gesetzlicher Vorgaben gerechtfertigt sind, ist das datenschutzrechtlich nicht zu beanstanden.

4.6 Mitarbeiterexzesse

Manchmal kann ein datenschutzrechtliches Fehlverhalten dem Unternehmen oder Betrieb nicht vorgeworfen werden, nämlich dann, wenn Beschäftigte Daten zu eigenen privaten Zwecken und nicht zumindest in der Annahme, im Interesse des Arbeitgebers zu handeln, verarbeiten. Das kann z.B. dann der Fall sein, wenn Bankmitarbeiter:innen, die privat eine Wohnung vermieten, die Möglichkeit einer Bonitätsabfrage nutzen, um die Bonität eines möglichen Mieters abzufragen. Für solche Handlungen ist nicht mehr der Arbeitgeber verantwortlich, sondern die oder der Beschäftigte wird selbst zum Verantwortlichen und kann Adressat:in aufsichtsbehördlicher Maßnahmen werden. Bei der Verhängung entsprechender Maßnahmen spielt es für den LfDI auch eine Rolle, welche insbesondere arbeitsrechtlichen Maßnahmen der Arbeitgeber bereits ergriffen hat.

5. LEBEN DIGITAL

5.1 Zulässigkeit der Übermittlung personenbezogener Daten an Inkassounternehmen

Den LfDI erreichen nach wie vor Anfragen und Beschwerden zu der Übermittlung personenbezogener Daten von Unternehmen an Inkassodienstleister. Oftmals vermuten die Betroffenen (hier: die potentiellen Schuldner:innen) einen Verstoß gegen das Datenschutzrecht (vgl. 27. Tb., Tz. 5.3).

Die Zulässigkeit der Übermittlung personenbezogener Daten an ein Inkassounternehmen richtet sich nach Art. 6 Abs. 1 Satz 1 lit. b und f DS-GVO.

Im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO besteht das berechtigte Interesse des übermittelnden Unternehmens darin, dass die (vermeintlich) offene Forderung vom Schuldner beglichen wird. Hierzu kann es sich der Hilfe Dritter, nämlich eines Inkassounternehmens bedienen. Hierbei ist erforderlich, dass das Inkassounternehmen die Informationen erhält, die die Forderung begründen und die einen Einzug durch das Inkassounternehmen ermöglichen. Dies gilt auch dann, wenn das Bestehen oder die Höhe der Forderung zwischen den Parteien strittig ist. Die Einwilligung der betroffenen Person ist gerade nicht erforderlich.

In diesem Zusammenhang weist der LfDI darauf hin, dass der LfDI für die Prüfung, ob der geltend gemachte Anspruch begründet oder etwa die Zahlung durch Betroffene korrekt erfolgt ist, nicht zuständig ist, da es sich dabei nicht um datenschutzrechtliche Sachverhalte handelt. Hiergegen müssen Betroffene zivilrechtlich vorgehen.

.

5.2 Löschfristen bei Daten über Restschuldbefreiung aus dem öffentlichen Insolvenzregister

Private Wirtschaftsauskunfteien erfassen und speichern in ihren eigenen Datenbanken Informationen aus öffentlichen Registern, insbesondere solche über Restschuldbefreiungen aus dem öffentlichen Insolvenzregister. Bisher löschten die privaten Auskunfteien diese Informationen nach Ablauf einer Frist von drei Jahren nach der Eintragung gemäß den Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien vom 25. Mai 2018 (in der Fassung vom 1. Januar 2020), die in Deutschland vom Verband der Wirtschaftsauskunfteien ausgearbeitet und von der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen genehmigt wurden.

In den verbundenen Rechtssachen C-26/22 und C-64/22|SCHUFA Holding (Restschuldbefreiung) hat der EuGH entschieden, dass private Auskunfteien Daten über eine Restschuldbefreiung jedenfalls nicht länger speichern dürfen als das öffentliche Insolvenzregister. Das heißt, dass Informationen zur Restschuldbefreiung aus dem öffentlichen Insolvenzregister nach Erreichen der Speicherdauer des öffentlichen Insolvenzregisters auch aus dem Datenbestand der Auskunftei gelöscht werden müssen. Nach diesem Zeitraum kann die Speicherung dieser Daten durch eine Wirtschaftsauskunftei aus einem öffentlichen Insolvenzregister nicht mehr auf Art. 6 Abs. 1 lit. f DS-GVO gestützt werden, sodass eine Rechtsgrundlage für die Verarbeitung fehlen würde.

Das hat zur Folge, dass Wirtschaftsauskunfteien ihre bisherigen Löschfristen anpassen müssen. Informationen zur Restschuldbefreiung müssen nach sechs Monate gelöscht werden.

Die Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien vom 25. Mai 2018 (in der Fassung vom 1. Januar 2020) gem. Art. 40 DS-GVO, die in Deutschland vom Verband der Wirtschaftsauskunfteien ausgearbeitet wurden, werden ebenfalls angepasst.

5.3 Erstellung und Verwendung eines Scorewertes ist automatisierte Entscheidung im Sinne von Art. 22 Abs. 1 DS-GVO

Zum Scoring direkt finden sich keine Vorgaben in der Datenschutz-Grundverordnung. Wenn Entscheidungen ausschließlich auf den errechneten Scorewert gestützt werden, handelt es sich um eine automatisierte Entscheidung. Dies hat auch der der Europäische Gerichtshof (EuGH) so gesehen: Er hat in der vorgelegten Rechtssache C-634/21|SCHUFA Holding (Scoring) festgestellt, dass die Erstellung und Verwendung eines Scorewertes als automatisierte Entscheidung über den Kredit angesehen wird, sofern ihm die Kreditgeber „eine maßgebliche Rolle im Rahmen der Kreditgewährung beimessen". Folglich verstößt das Scoring gegen die DS-GVO, wenn dieses eine maßgebliche Rolle bei der Entscheidung über den Vertragsschluss bzw. die Kreditvergabe spielt.

Eine solche automatisierte Entscheidung im Sinne von Art. 22 Abs. 1 DS-GVO ist grundsätzlich unzulässig und darf gemäß Art. 22 Abs. 2 DS-GVO nur bei Erforderlichkeit für den Abschluss oder die Erfüllung eines Vertrags (lit. a), aufgrund einer gesetzlichen Erlaubnis (lit. b) oder mit ausdrücklicher Einwilligung (lit. c) getroffen werden.

§ 31 BDSG könnte eine solche gesetzliche Erlaubnis darstellen. Nach dieser Regelung zum „Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften" gilt, dass nur Daten verwendet werden dürfen, die wissenschaftlich nachgewiesen für die Berechnung des Wahrscheinlichkeitswerts erheblich sind. Zudem dürfen danach Anschriftendaten nicht ausschließlich den Scorewert bestimmen. Werden diese neben anderen Informationen in das Scoring einbezogen, sind die Betroffenen zuvor darüber zu unterrichten.

In seinem Urteil hat der EuGH jedoch auch seine Zweifel an der Vereinbarkeit der Regelung mit dem Unionsrecht geäußert. Es sei nun Sache des vorlegenden Gerichts zu prüfen, ob § 31 BDSG als Rechtsgrundlage im Sinne von Art. 22 Abs. 2 lit. b DS-GVO qualifiziert werden kann.

5.4 Online-Seminar „Datenschutz im Verein"

Der LfDI beteiligte sich auch im Jahr 2023 wieder am Projekt „Digital in die Zukunft" der Landesregierung, welches von der Leitstelle Ehrenamt und Bürgerbeteiligung in der Staatskanzlei zusammen mit medien+bildung.com, einer Tochter der Medienanstalt Rheinland-Pfalz, umgesetzt wird. Im Rahmen der Reihe von Online-Fortbildungen zu aktuellen Vereinsthemen wurden die Grundlagen des Datenschutzrechts erläutert und spezifische Praxishinweise, Hilfestellungen sowie Tipps für Vereine gegeben.

6. BESCHÄFTIGTENDATEN-SCHUTZ

6.1 Beihilfebescheide bei getrennt lebenden Ehegatten

Eine Beschwerdeführerin berichtete, sie sei über ihren getrennt lebenden Ehemann beihilfeberechtigt. In der Vergangenheit sei es wiederholt vorgekommen, dass die Beihilfestelle Bescheide zu ihren Anträgen an ihren Ehegatten gesandt hatte. Sie habe daher darum gebeten, die Bescheide an ihre Anschrift zu senden, und auch eine Vollmacht ihres Ehegatten vorgelegt. In dieser Vollmacht habe ihr Ehemann als Beihilfeberechtigter ihr die Vollmacht erteilt, selbst Anträge zu stellen und direkter Adressat der Bescheide zu sein.

Es liegt in der Natur der Sache, dass medizinische Daten nicht an den getrennt lebenden Ehegatten übermittelt werden sollten. Der LfDI wandte sich daher an die Beihilfestelle und bat um eine Stellungnahme.

Diese räumte ein, aufgrund individueller Fehler die Vollmacht nicht beachtet zu haben. Sie sicherte zugleich zu, die Vordrucke zu überarbeiten, um das Verfahren für bevollmächtigte Angehörige verbindlicher und transparenter zu gestalten.

6.2 Leiterin des Personalreferats als BEM-Beauftragte

Werden Beschäftigte in einem Zeitraum von zwölf Monaten länger als sechs Wochen (ununterbrochen oder wiederholt über mehrere Fehlzeiten verteilt) krank, hat der Arbeitgeber ein betriebliches Eingliederungsmanagement (BEM) durchzuführen. Zweck des betrieblichen Eingliederungsmanagements ist es, den Ursachen von Arbeitsunfähigkeitszeiten nachzugehen und nach Möglichkeiten zu suchen, künftig Arbeitsunfähigkeitszeiten zu vermeiden oder zumindest zu verringern.

Dem LfDI wurde aufgrund einer Beschwerde bekannt, dass bei einer größeren Landesbehörde die Personalleiterin auch gleichzeitig als BEM-Beauftragte tätig war. Der LfDI wies die Behörde darauf hin, dass der Gesetzgeber mit der Einführung des BEM eine Trennung zwischen Personalverwaltung einerseits und BEM-Verfahren andererseits erreichen wollte. Denn das BEM-Verfahren hat die Wiedereingliederung und Erhaltung der dauerhaften Arbeitsfähigkeit des Betroffenen zum Ziel, während es im Bereich der Personalverwaltung auch um eine Beendigung des Arbeitsverhältnisses gehen kann. Die Inhalte von BEM-Gesprächen sind daher kein zulässiger Gegenstand einer Personalakte. Wenn Mitarbeitende der Personalabteilung in leitender Funktion gleichzeitig als BEM-Beauftragte oder Mitglieder eines BEM-Teams tätig werden, besteht die Gefahr, dass Informationen aus dem BEM-Verfahren zweckwidrig auch für Personalmaßnahmen verwendet werden. Es bedürfte schon der sprichwörtlichen „Schere im Kopf“, um dies zu verhindern.

Eine solche Interessenkollision dürfte sich auf die Bereitschaft von Beschäftigten, ein BEM-Verfahren durchzuführen, nachteilig auswirken und damit der eigentlichen Zielsetzung des BEM zuwiderlaufen. Denn Betroffene, die befürchten müssen, dass sich die freiwillig gemachten Angaben zu gesundheitlichen Beeinträchtigungen nachteilig auf ihr berufliches Fortkommen auswirken, werden das BEM ablehnen oder nicht alle Informationen offenbaren. Der LfDI sprach daher die Empfehlung aus, die innerbetriebliche Organisation künftig so zu gestalten, dass eine Person außerhalb des Personalbereichs als BEM-Beauftragte tätig wird.

6.3 Veröffentlichung von Gehaltszetteln bei Facebook

Ein Vertriebsdienst hielt es für eine gute Form der Eigenwerbung, mehrere Gehaltszettel auf Facebook zu veröffentlichen, mit dem Zusatz: „Es gibt keine Grenze bei uns; jeder mit bisschen Disziplin kann sein Gehalt selbst gestalten“.

Zwar wurde der Name auf den Gehaltsabrechnungen geschwärzt, aber Angaben zu Geburtsdatum, Eintrittsdatum, Krankenkassennummer, Steuer-ID sowie Brutto- und Nettolohn waren nach wie vor ersichtlich. Von einer hinreichenden Anonymisierung konnte daher keine Rede sein. Ein Schreiben des LfDI genügte, dass die Daten umgehend auf Facebook gelöscht wurden.

6.4 Videoüberwachung durch Kollegen

Der Kassenverwalter einer Kommune hatte den Verdacht, dass eine Kollegin Stornobuchungen vornahm, um Geld aus der Kasse zu entwenden. Mit Einverständnis der übrigen Beschäftigten, aber ohne die Behördenleitung zu informieren, installierte er eine Überwachungskamera, deren Aufzeichnungen den Verdacht erhärteten. Der Mitarbeiterin wurde fristlos gekündigt.

Der LfDI vertrat die Auffassung, dass vorliegend nicht die Kommune, sondern der Kassenverwalter als datenschutzrechtlich Verantwortlicher anzusehen ist. Eine heimliche Videoüberwachung des Arbeitsplatzes ist nur als ultima ratio zulässig, d.h. nur dann, wenn keine milderen Maßnahmen möglich sind. Vorliegend hätte das pflichtwidrige Verhalten der Kollegin möglicherweise auch anhand der Protokolldaten belegt werden können. Daher war zumindest fraglich, ob tatsächlich keine anderen, weniger einschneidenden Möglichkeiten zur Aufklärung des Sachverhalts zur Verfügung standen. Unstreitig lag hier keine Einwilligung der Betroffenen vor. Dass die anderen Mitarbeitenden in der Abteilung eingewilligt haben, spielte insofern keine Rolle. Ohnehin ist in einem Abhängigkeitsverhältnis die Freiwilligkeit einer Einwilligung grundsätzlich in Frage zu stellen.

Die ehemalige Mitarbeiterin könnte in einem arbeitsgerichtlichen Verfahren die Kündigung anfechten und dabei ein Verwertungsverbot der Aufnahmen geltend machen. Denn die Videoaufzeichnung wurde hier von einer dazu nicht befugten Person initiiert und dürfte sich bei genauer Prüfung als unverhältnismäßig erweisen.

Mit der eigenmächtigen Videoüberwachung hatte der Kassenverwalter zumindest gegen datenschutzrechtliche und personalvertretungsrechtliche Vorschriften verstoßen. Ob und ggfs. welche dienstlichen Konsequenzen die Kommune aus dem Vorfall ziehen, blieb der Behördenleitung überlassen.

7. MEDIEN UND WERBUNG

7.1 Webseiten

Die in den vorigen Jahren zu verzeichnende hohe Zahl von Hinweisen auf Webseiten, die die datenschutzrechtlichen Anforderungen im Bereich Cookies und Tracking nicht erfüllen, ist in 2023 deutlich zurückgegangen. Zwar wurden weiterhin regelmäßig Hinweise zu diesem Themenbereich an den LfDI herangetragen, die Anzahl der Hinweise war jedoch mit den Vorjahren nicht vergleichbar. Ein Hintergrund dieser Entwicklung dürfte sein, dass im Juli 2023 die EU-Kommission den neuen Angemessenheitsbeschluss für die Übermittlung personenbezogener Daten in die USA (EU-U.S. Data Privacy Framework – EU-U.S. DPF) erlassen hat. Seit diesem Zeitpunkt sind eingebundene Dienste auf Webseiten und in Apps nicht schon deshalb datenschutzwidrig, weil sie überhaupt personenbezogene Daten in die USA übermitteln. Viele der zuvor eingegangenen Hinweise hatten sich gerade darauf gestützt, dass Webseiten und Apps US-amerikanische Dienste verwenden, obwohl damals durch das Urteil des Europäischen Gerichtshofs (EuGH) zum Privacy-Shield-Beschluss keine Rechtsgrundlage für eine Übermittlung in die USA bestanden hatte. Seit dem Vorliegen des neuen Angemessenheitsbeschlusses können US-amerikanische Dienste wieder in Webseiten eingebunden werden, sofern sich die Diensteanbieter dem EU-U.S. DPF unterworfen haben und wirksame Einwilligungen der betroffenen Personen (in der Regel mittels Einwilligungsbanner) durch die Webseitenbetreiber:innen eingeholt werden.

Ein weiterer Hintergrund dürfte sein, dass die Regelung des § 25 des Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG), insbesondere dessen Abs. 2 Nr. 2, zu einer gewissen Klarheit der Rechtslage geführt hat und immer mehr Webseitenbetreiber:innen sich bemühen, die Anforderungen zu erfüllen. Auf vielen Webseiten finden sich inzwischen Einwilligungsbanner, die den datenschutzrechtlichen Anforderungen entsprechen und daher wirksame Einwilligungen in das Setzen und Auslesen von Cookies oder den Einsatz anderer Dienste, die Nutzungsdaten verarbeiten, ermöglichen. Allerdings besteht auch weiterhin auf vielen Webseiten noch Nachbesserungsbedarf hinsichtlich des Themas „Cookies und Tracking“. Ausführliche Hinweise für Webseitenbetreiber:innen finden sich auf der Webseite des LfDI unter **https://www.datenschutz.rlp.de/themen/cookies-und-einwilligungsbanner** und in der „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien“ unter **https://s.rlp.de/dsk-OHTelemedien**.

7.2 Social Media

Social-Media-Dienste wie Facebook, Instagram, X oder TikTok sind zu ständigen Begleitern im beruflichen und privaten Informations- und Kommunikationsverhalten vieler Menschen geworden. Häufig vertrauen die Nutzer:innen den Betreiber:innen dieser Dienste sehr persönliche Informationen an. Die Vielfalt der Informationen, die innerhalb eines Netzwerks aktiv eingestellt oder über die Nutzer:innen erhoben werden, ermöglicht teilweise tiefe Einblicke in persönliche Angelegenheiten.

Bei Social-Media-Diensten handelt es sich häufig um mehrstufige Anbieterverhältnisse, bei denen Profile bzw. Seiten zum Beispiel von einem Unternehmen oder einer Behörde auf einer Plattform angeboten werden, die wiederum von einem weiteren Plattformbetreiber bereitgestellt wird, der die Daten der Nutzer:innen im Rahmen eigener Geschäftszwecke verarbeitet. Dies macht Social-Media-Dienste aus Nutzer:innenperspektive schwer durchschaubar und aus rechtlicher Sicht häufig problematisch, gerade im Hinblick auf Verantwortlichkeiten.

Unternehmen und öffentliche Stellen, die Profile in Social-Media-Diensten anbieten, müssen den datenschutzrechtlichen Anforderungen Rechnung tragen. Den LfDI erreichten auch im Jahr 2023 zahlreiche Anfragen öffentlicher und privater Stellen, die sich nach den Anforderungen an den datenschutzkonformen Betrieb von Social-Media-Kanälen erkundigten, in der Regel von Drittstaaten-Anbietern wie Meta (Facebook, Instagram), X (früher Twitter) oder TikTok. Die Erfahrung der Aufsichtsbehörden zeigt, dass der Schutz der Privatsphäre von den Betreiber:innen der Social-Media-Plattformen nicht immer hinreichend beachtet wird.

Der EuGH stellte mit Urteil vom 5. Juni 2018 (C-210/16, „Wirtschaftsakademie“) fest, dass die Betreiber:innen von Facebook-Fanpages und der Anbieter Meta Platforms gemeinsame Verantwortliche gemäß Art. 26 DS-GVO sind. Hieraus ergeben sich Pflichten, die von beiden Verantwortlichen eingehalten werden müssen.

Die Taskforce Facebook-Fanpages der DSK stellte in ihrem Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages vom 10. November 2022 fest, dass einige dieser Pflichten, die den Verantwortlichen obliegen, nicht eingehalten werden. Für die Erfüllung der datenschutzrechtlichen Anforderungen durch die Facebook-Fanpage-Betreiber:innen wäre dabei eine Mitwirkung von Meta Platforms notwendig, die derzeit aber nicht vollständig gegeben ist. Datenschutzrechtlich problematisch sind u.a. folgende Aspekte:

- Die Fanpage-Betreiber:innen holen keine wirksame Einwilligung für das Speichern von Informationen in den Endeinrichtungen der Endnutzer:innen, sowie den Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, ein (§ 25 Abs. 1 TTDSG).
- Die Fanpage-Betreiber:innen können sich im Hinblick auf die Verarbeitung der auf Basis der gesetzten Cookies erhobenen personenbezogenen Daten der Webseitenbesucher:innen nicht auf eine Rechtsgrundlage nach Art. 6 DS-GVO berufen.
- Die Fanpage-Betreiber:innen können ihren Informationspflichten aus Art. 13 DS-GVO nicht hinreichend nachkommen, da Meta Platforms diesbezüglich die notwendigen Informationen nicht vollständig liefert.
- Zwischen den Betreiber:innen von Facebook-Fanpages und Meta Platforms wird keine gültige Vereinbarung im Sinne von Art. 26 Abs. 1 Satz 2 DS-GVO abgeschlossen.
- Nachdem der Privacy Shield im Jahr 2020 wegen des Schrems-II-Urteils des Europäischen Gerichtshofs (EuGH-Urteil C-311/18) für ungültig erklärt wurde, war eine Übermittlung auf dieser Grundlage nicht möglich. Am 10. Juli 2023 nahm die Europäische Kommission den Angemessenheitsbeschluss für den Datenschutzrahmen EU-USA – das sog. EU-U.S. Data Privacy Framework (EU-U.S. DPF) – an und schuf somit eine neue Rechtsgrundlage für derartige Übermittlungen. Meta Platforms ist unter dem EU-U.S. DPF zertifiziert. Folglich besteht nunmehr eine Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA. Die Absicherung durch zusätzliche Grundlagen für die Drittlandübermittlung gemäß Art. 44ff. DS-GVO ist jedoch zu empfehlen.

Die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ordnet den Betrieb einer Facebook-Präsenz derzeit gemäß des Beschlusses zur Task Force Facebook-Fanpages vom 23. März 2022 als datenschutzrechtlich nicht zulässig ein. Da Fanpage-Betreiber:innen als Verantwortliche die Rechtskonformität der Datenverarbeitung sicherstellen und nachweisen können müssen, ist

der rechtmäßige Betrieb von Facebook-Fanpages mangels Mitwirkung von Meta Platforms aktuell nicht möglich.

Der LfDI hat in der Vergangenheit gerade die Verantwortlichen im öffentlichen Bereich durch einen Handlungsrahmen zur datenschutzkonformen Nutzung von Social Media unterstützt (siehe https://www.datenschutz.rlp.de/themen/social-media). Die Anforderungen des Handlungsrahmens besitzen weiterhin Gültigkeit. Allerdings können sie nicht als ausreichend bewertet werden, um Social-Media-Profile datenschutzkonform anzubieten, da Profil-Betreiber:innen ohne weitere Maßnahmen der Plattformanbieter nicht in der Lage sind, die dargestellten Defizite der gängigen Social-Media-Plattformen auszugleichen. Ein rechtskonformer Betrieb einer Facebook-Fanpage ist derzeit auch bei Anwendung des Handlungsrahmens leider nicht möglich.

Die datenschutzrechtlichen Bewertungen in Bezug auf Meta Platforms sind zwar nicht automatisch auf andere Plattformen zu übertragen, vergleichbare Problemlagen dürften aber auch bei diesen vorhanden sein. Hier gilt es selbstverständlich, die technischen Entwicklungen der Plattformanbieter und die Fortentwicklung ihrer datenschutzrechtlichen Dokumente zu beobachten. Eine explizite gerichtliche Klärung gibt es derzeit nur für den Betrieb von Facebook-Fanpages.

7.3 Werbung

Im Bereich der Werbung lag der Schwerpunkt der aufsichtsrechtlichen Tätigkeit im Jahr 2023 auf unerwünschter Werbung und unerwünschten Newslettern, zumeist per E-Mail, aber auch per Post. Insbesondere wandten sich viele betroffene Personen an den LfDI, die sich bereits erfolglos mit dem Wunsch, keine Werbung mehr zu erhalten, an den Absender gewandt hatten.

Werbung per E-Mail ist nur unter zwei Voraussetzungen zulässig: Entweder liegt eine Einwilligung der Empfänger:innen in den Erhalt vor oder die Werbung geht an Bestandskund:innen und enthält Werbung für vergleichbare Produkte wie die bereits von den Kund:innen erworbenen. Betroffene Personen können und sollten zunächst selbst gegen unerwünschte Werbe-E-Mails und Newsletter vorgehen. Hatten sie zuvor eine Einwilligung in den Erhalt von Newslettern oder Werbung per E-Mail erteilt, können sie diese widerrufen. Bei zulässiger Bestandskund:innen-Werbung haben betroffene Personen nach Art. 21 Abs. 2 DS-GVO das Recht, Werbung per E-Mail gegenüber dem werbenden Unternehmen mit Wirkung für die Zukunft zu widersprechen. Oftmals lässt sich der Widerruf oder Widerspruch mit Anklicken des Abmeldelinks in der entsprechenden E-Mail tätigen. Sollte ein solcher nicht vorhanden sein, kann der Widerruf oder Widerspruch per E-Mail an das werbende Unternehmen gesendet werden.

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

Hat eine betroffene Person der Werbung widersprochen oder ihre Einwilligung in diese widerrufen, darf ihr das jeweilige Unternehmen keine Werbung mehr zusenden. Bereits vorbereitete und/oder versendete Werbung ist dann allerdings noch für einen kurzen Zeitraum hinzunehmen. Kommt ein Unternehmen dem Werbewiderspruch nicht nach oder ignoriert den Widerruf einer Einwilligung, können die Betroffenen gegen Unternehmen mit Sitz in Rheinland-Pfalz beim LfDI eine Beschwerde gegen das Unternehmen einlegen.

Viele Beschwerdeführer:innen wandten sich daher im Jahr 2023 an den LfDI und rügten die Zusendung von Werbe-Post oder Werbe-E-Mails und Newslettern durch Unternehmen.

Hierbei wurden die entsprechenden Unternehmen darauf hingewiesen, dass Werbe-Widersprüche schnellstmöglich, spätestens jedoch innerhalb eines Monats, umzusetzen sind. Die technische und organisatorische Umsetzung von Werbewidersprüchen und widerrufenen Einwilligungen bei den werbenden Unternehmen scheint dabei häufig nicht mit der gebotenen Sorgfalt angegangen zu werden. Bei wiederholten Verstößen drohen den Unternehmen Verwarnungen und Bußgelder, so dass ihnen ein funktionierendes Datenschutzmanagement dringend zu empfehlen ist.

7.4 Weitere Themen

Neben dem Bereich der Nutzungsdatenverarbeitung durch Webseitenbetreiber:innen waren im Berichtszeitraum zahlreiche weitere Themen relevant. Bürger:innen filmten sich gegenseitig mit Smartphones oder Helmkameras, Personen veröffentlichten Bilder oder andere Informationen über Dritte auf Webseiten, Unternehmen reagierten auf negative Bewertungen im Internet, indem sie in einer Antwort die personenbezogenen Daten der Bewertenden offenlegten, Kommunen veröffentlichten in ihren Social Media-Kanälen Fotos von Personen, die den örtlichen Weihnachtsmarkt besuchten. Vielerorts fehlt offenkundig das Bewusstsein dafür dass die personenbezogenen Daten anderer Personen nicht im Internet veröffentlicht werden sollten. Angesichts der immer leichter verfügbaren Techniken zum Veröffentlichen personenbezogener Daten ist davon auszugehen, dass Aufklärungsarbeit und Sensibilisierung Daueraufgaben bleiben werden – nicht nur, aber gerade auch bei jungen Menschen. Der LfDI setzt sich dafür zum Beispiel mit seinen Schülerworkshops ein.

8. GESUNDHEIT UND FORSCHUNG

8.1 Fachtagung „Was passiert mit unseren Gesundheitsdaten? Möglichkeiten und Grenzen der digitalen Nutzung von Gesundheitsdaten“ am 13. November 2023

Die datenschutzrechtlichen Anforderungen an die Primär- und Sekundärnutzung von Gesundheitsdaten zur Verbesserung der Gesundheitsversorgung sowie für Forschungszwecke waren im Berichtsjahr auf nationaler und europäischer Ebene ein hochaktuelles Thema, das in Politik, Medizin und Wissenschaft sowie von Datenschützern und Ethikern intensiv diskutiert wurde. Schon im November 2022 positionierte sich die DSK in der sog. Petersberger Erklärung inhaltlich und präzisierte im Berichtsjahr die sich daraus ergebenden Schlussfolgerungen in unterschiedlichen Zusammenhängen (siehe Kapitel 8.3). Auch der Verordnungsentwurf der EU-Kommission aus dem Mai 2022 und die Ausführungen des Deutschen Ethikrats aus dem März 2023 zur besseren Nutzung von Gesundheitsdaten (**https://s.rlp.de/ethikrat-gesundheitsdaten**) setzten wichtige Impulse. Angesichts der großen Potentiale der Digitalisierung des Gesundheitswesens gerade im Hinblick auf eine Weiterentwicklung der Medizin ist es nach Einschätzung des LfDI immer drängender, die Möglichkeiten und Grenzen der digitalen Nutzung von Gesundheitsdaten aus rechtlicher und ethischer Sicht verlässlich und einvernehmlich zu definieren.

Aufgrund der Aktualität und überragenden Bedeutung der Thematik führte der LfDI im Rahmen der Initiative „Mit Sicherheit gut behandelt“ zusammen mit der Kassenärztlichen Vereinigung Rheinland-Pfalz, der Landesärztekammer Rheinland-Pfalz und der Landespsychotherapeutenkammer Rheinland-Pfalz am 13. November 2023 hierzu eine Fachtagung in Mainz durch. Ziel der Veranstaltung war es, durch Expert:innen unterschiedlicher Disziplinen die in der bisherigen gesellschaftlichen und politischen Diskussion vertretenen jeweiligen Perspektiven zu beleuchten, in einen Gesamtkontext zu stellen und daraus ableitbare Lösungsoptionen gemeinsam zu identifizieren.

Im Anschluss an zwei grundlegende Impulsvorträge von Frau Prof. Dr. Ursula Klingmüller, Mitglied des Deutschen Ethikrats, und Herrn Prof. Dr. Jürgen Kühling von der Fakultät für Rechtswissenschaften der Universität Regensburg fanden insgesamt drei moderierte Fachgespräche zu den Themen „Recht und Ethik“, „Versorgungsqualität“ und „Medizin 2.0“ statt, an denen jeweils mehrere Expert:innen unterschiedlicher Einrichtungen und fachlicher Hintergründe teilnahmen. In den Panels konnten einzelne Aspekte der Digitalisierung fachlich beleuchtet und insbesondere bestehende Hürden auf dem Weg zu einer erfolgreichen digitalen Transformation identifiziert werden.

Mit über 120 Teilnehmenden im Plenarsaal des rheinland-pfälzischen Landtags in Mainz und mehr als 100 weiteren Zuschauenden per Livestream fand die Veranstaltung eine große Resonanz. Dies belegt die gesellschaftliche Relevanz des Themas und bestärkte die Organisator:innen in ihrer Überzeugung, die Perspektiven und Kompetenzen verschiedener Fachdisziplinen zugunsten einer tragfähigen Modernisierung des Gesundheitssystems zu bündeln. Credo der Fachtagung war die Erkenntnis, dass der Datenschutz frühzeitig eingebunden werden müsse und gemeinsam mit Ethik und Medizin durchaus tragfähige Lösungen gefunden werden können, um eine Digitalisierung des Gesundheitssektors zu gestalten, die der Gesundheit der Menschen dient, ohne ihre Rechte und Freiheiten unverhältnismäßig einzuschränken. Interdisziplinäres Vorgehen von der Projektidee bis zur Gesetzgebung ebenso wie umfassendes Vertrauen in die Sicherheit der Datenverarbeitung sind nach Überzeugung aller Beteiligten fundamental für den Erfolg der digitalen Transformation.

Die auf der Tagung diskutierten Lösungsansätze hat die Initiative „Mit Sicherheit gut behandelt“ Anfang Dezember 2023 in einem Positionspapier aufgegriffen. Das Papier beinhaltet acht Thesen, mit denen eine erfolgreiche und gesellschaftlich anerkannte Transformation der Gesundheitsversorgung in das digitale Zeitalter gelingen kann. So sollten z.B. immer noch bestehende Handlungsunsicherheiten bei der Umsetzung des Datenschutzes konsequent ausgeräumt werden. Auch die interdisziplinäre Begleitung von Digitalisierungsvorhaben unter Berücksichtigung rechtlicher, ethischer, technischer, medizinischer und psychotherapeutischer Expertise ist nach Überzeugung der Initiative ein Schlüssel zum Erfolg. Das Papier empfiehlt zudem die Entwicklung neuer Berufsbilder und Ausbildungswege hin zur Gesundheitsdatenmanagerin oder zum Datenlotsen. Das enorme Potential, das die Digitalisierung der Medizin zur Entwicklung neuer oder besserer Therapien und effektiverer Behandlungsmöglichkeiten bietet, kann und muss auf einem datenschutzrechtlich, ethisch und fachlich tragfähigen Fundament genutzt werden.

Der LfDI wird auch in Zukunft dafür werben, die in dem Positionspapier enthaltenen acht Thesen den weiteren Digitalisierungsschritten im Gesundheitswesen zugrunde zu legen.

Zum Positionspapier:
https://s.rlp.de/PPDigiGesund

8.2 Digitalisierung des öffentlichen Gesundheitsdienstes

Im Rahmen des Digitalpakts des Bundes zur Digitalisierung der Gesundheitsämter läuft in Rheinland-Pfalz seit Herbst 2022 das Projekt „Einheitliche EDV-Plattform für den Öffentlichen Gesundheitsdienst (ÖGD) in Rheinland-Pfalz“. Dabei soll unter Beachtung der datenschutzrechtlichen Vorgaben die im Lande bislang bestehende dezentrale, heterogene IT-Landschaft, die den organisatorischen Prinzipen einer Aufbauorganisation folgt und unterschiedliche proprietäre Softwarekomponenten primär eines Herstellers nutzt, harmonisiert und an die Anforderungen des digitalen Verwaltungshandelns angepasst werden. Im Projekt, das zunächst bis September 2024 angesetzt ist, soll die Spezifikation und Implementierung einer einheitliche Prozess- und Datenplattform sowie Kommunikations- und Kollaborationskomponenten für alle landesspezifischen Akteure des ÖGD vorgenommen werden. Darüber hinaus ist ein landesweites Portal geplant, welches insbesondere als zentrale Anlaufstelle für sämtliche Bürgeranfragen, die den öffentlichen Gesundheitsdienst betreffen, dient.

Der LfDI begleitet das vom Ministerium für Wissenschaft und Gesundheit Rheinland-Pfalz koordinierte Projekt im Rahmen der ihm zur Verfügung stehenden personellen Ressourcen. Auf seine Initiative hin wurde eine zusätzliche Arbeitsgruppe zur Umsetzung datenschutzrechtlicher Vorgaben geschaffen, die auch die kommunalen Datenschutzbeauftragten in das Projektintegrierte. Der LfDI erhält im Rahmen seiner Begleitung regelmäßig Statusberichte über den aktuellen Entwicklungsstand sowie den projektbezogenen Newsletter. Eine aktive Einbindung in die konkrete Projektarbeit erfolgt nicht. Lediglich bei anlassbezogenen datenschutzrelevanten Fragen konsultiert das Gesundheitsministerium den LfDI und bittet um Beratung.

Aus datenschutzrechtlicher Sicht sind bei der anstehenden landesweit harmonisierten Digitalisierung des ÖGD sowohl technisch-organisatorische Inhalte (z.B. Ausgestaltung des Software-Einsatzes in den Gesundheitsämtern, Meldeportal bei Schuleingangsuntersuchungen, Form der Datenhaltung) als auch rechtliche Aspekte wie die Festlegung von Löschfristen oder die Gewährleistung der Betroffenenrechte von Bedeutung. Ziel der Beratungstätigkeit des LfDI ist es, auf die umfassende Einhaltung der Regelungen der Datenschutz-Grundver-

ordnung und der anderen datenschutzrechtlichen Bestimmungen hinzuwirken. Dabei kommt dem lückenlosen Schutz der im ÖGD verarbeiteten Gesundheitsdaten eine herausragende Bedeutung zu. Inwieweit dies dann auch tatsächlich realisiert wird, liegt nicht mehr in den Händen des LfDI. Denn die Umsetzung der datenschutzrechtlich gebotenen Anforderungen obliegt letztendlich den einzelnen Akteuren im ÖGD: in erster Linie den einzelnen Kreisverwaltungen, bei denen die Gesundheitsämter angebunden sind, die als eigenständige datenschutzrechtlich Verantwortliche unstreitig Adressaten der Datenschutz-Vorgaben sind. Aber auch die Software-Hersteller sowie das projektkoordinierende Fachministerium tragen in diesem Kontext Verantwortung für eine datenschutzkonforme Datenverarbeitung.

Im Zusammenhang mit dem Digitalisierungsprojekt berichteten Presseberichte im November 2023 über mögliche IT-Sicherheitsdefizite in rheinland-pfälzischen Gesundheitsämtern. Dabei standen neben den Kreisverwaltungen und dem das Digitalisierungsprojekt koordinierenden Ministerium der Hersteller der im ÖGD eingesetzten Software und der LfDI Rheinland-Pfalz im Fokus. Der LfDI nahm die Berichterstattung zum Anlass, die darin beschriebenen Defizite sowie grundsätzlich den Stand der Datensicherheit in den rheinland-pfälzischen Gesundheitsämtern zu klären. Zu diesem Zweck wurden das zuständige Fachministerium, der Software-Hersteller und die 24 Kreisverwaltungen detailliert um Auskunft gebeten. Zudem wurde festgelegt, bis zur Jahresmitte 2024 vor Ort Prüfungen in ausgewählten Landkreisen durchzuführen.

Im Ergebnis stellten sich die in der Presse aufgekommenen Befürchtungen hinsichtlich einer unzureichenden IT-Sicherheit in den Gesundheitsämtern als weniger gravierend heraus als zunächst angenommen. Anhaltspunkte für ein unbefugtes Abfließen von Gesundheitsdaten der Bürger:innen an Stellen außerhalb der Verwaltung bestanden nicht. Allerdings deckte der LfDI im Rahmen seiner Prüfungen diverse datenschutzrelevante Schwachstellen auf, die zum Teil bereits Gegenstand der Berichterstattung in der Presse waren, teilweise aber auch zuvor 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 bislang 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 ist. Im Hinblick auf das landesweite Digitalisierungsprojekt sprach der LfDI zugleich gegenüber dem federführenden Ministerium für Wissenschaft und Gesundheit konkrete Empfehlungen zur datenschutzkonformen Digitalisierung des Öffentlichen Gesundheitsdienstes in Rheinland-Pfalz aus. Zudem ist beabsichtigt, den Austausch mit dem Hersteller der in den Gesundheitsämtern eingesetzten IT-Anwendung fortzusetzen.

8.3 Sekundärnutzung von Gesundheitsdaten als Top-Thema des Jahres 2023

Die sich im Vorjahr bereits abzeichnende Dynamik im Zusammenhang mit der Sekundärnutzung von Gesundheitsdaten setzte sich im Berichtsjahr eindrucksvoll fort. Dies prägte auch die Arbeit des LfDI, der sich in zahlreichen Zusammenhängen sehr intensiv mit den datenschutzrechtlichen Implikationen dieser Thematik befasste.

Unter der Sekundärnutzung von Gesundheitsdaten versteht man die Zweitverwertung medizinisch relevanter personenbezogener Informationen, die insbesondere aus dem System der Gesundheitsversorgung generiert werden, aber auch aus anderen Zusammenhängen wie z.B. medizinischen Registern, Präventionsprogrammen oder Lifestyle-Applikationen stammen können. Im Gegensatz zur Primärnutzung solcher Daten, die hauptsächlich im Rahmen der ambulanten oder stationären Heilbehandlung in niedergelassenen Praxen oder Krankenhäusern erfolgt, fehlt es bei der Sekundärnutzung regelmäßig an einem direkten Kontakt der datenverarbeitenden Stellen mit den betroffenen Personen. Zugleich steht aus der Perspektive der Patient:innen die sich an eine Heilbehandlung anschließende Weiterverwertung der sie betreffenden Gesundheitsdaten auch nicht in ihrem unmittelbaren Fokus. Sie haben die sie selbst betreffenden Informationen vielmehr zu dem Zweck den Behandlern offenbart, den eigenen Gesundheitszustand zu verbessern. Es bedarf aufgrund dieser Ausgangssituation einer sorgfältigen Abwägung zwischen den Rechten und Freiheiten der Personen, deren Gesundheitsdaten weiterverwendet werden sollen, und den mit der Sekundärnutzung verknüpften Anliegen, um einen rechtlich und ethisch vertretbaren Ausgleich zwischen allen von der Sekundärnutzung der Gesundheitsdaten tangierten Interessen zu erreichen.

Doch warum bedarf es überhaupt einer solchen Sekundärnutzung? Schon vor der Digitalisierung der Gesundheitsversorgung war es unbestritten, dass medizinischer Fortschritt in weiten Teilen auch auf der Auswertung bisheriger Erfahrungen und Erkenntnisse aus der Patientenbehandlung basiert. Allerdings waren die hierzu benötigten Informationen überwiegend papiergebunden vorhanden, so dass deren Verfügbarkeit z.B. für externe wissenschaftliche Einrichtungen oder Forschungsverbünde nur sehr eingeschränkt bestand. Dies änderte sich grundlegend mit der auch im Versorgungsbereich mittlerweile standardmäßigen elektronischen Datenverarbeitung. Die in unterschiedlichen Kontexten digital gespeicherten Gesundheitsdaten können unabhängig von Quantität und Speicherort vielfältig zusammengeführt und ausgewertet werden. Forscher versprechen sich durch die Analyse großer und integrierter Mengen an Patientendaten neue und vor allem bessere und schnellere Erkenntnisse z.B. für die Gestaltung der Versorgungsprozesse oder die Entwicklung effizienter Therapien.

Vor diesem Hintergrund erklärt sich die zunehmende Bereitschaft der Politik, dem von zahlreichen Wissenschaftler:innen, Forscher:innen und Verbänden, aber auch der Industrie und der Wirtschaft verstärkt geäußerten Wunsch nach einem möglichst ungehinderten und dauerhaften Zugang zu Gesundheitsdaten und deren weiterer Verwendung nachzugeben. Auf nationaler Ebene ergibt sich dies nicht zuletzt aus dem Koalitionsvertrag und der darin beabsichtigten diversen Gesetzesvorhaben zur Nutzbarkeit von Gesundheitsdaten, auf EU-Ebene verfolgt der seitens der Kommission geplante Europäische Gesundheitsdatenraum (European Health Data Space – EHDS) ähnliche Ziele. Aus der Perspektive der Datenschutzaufsichtsbehörden gilt es, diese Bestrebungen ungeachtet der damit angestrebten gesellschaftlich berechtigten Ziele derart auszugestalten, dass sie mit den Grundsätzen des Datenschutzes und

den dahinterstehenden Persönlichkeitsrechten der betroffenen Personen in Einklang stehen.

Die seitens der DSK bereits im Jahre 2021 zu diesem Zweck eingerichtete Taskforce Forschungsdaten, an der auch der LfDI beteiligt ist, erwies sich im Berichtsjahr in diesem Zusammenhang als überaus konstruktiv und bereitete zahlreiche Dokumente der DSK vor, die den Zweck haben, bereits frühzeitig datenschutzrelevante Haltungen zu einzelnen Vorhaben oder politischen Diskussionen zu formulieren und für alle Stakeholder im Bereich des Gesundheitswesens sichtbar zu machen.

Stellungnahme der DSK vom 27. März 2023 zum Europäischen Gesundheitsdatenraum

Durch den Europäischen Gesundheitsdatenraum (EHDS) soll nach dem Willen der Europäischen Kommission eine Nutzung elektronischer Gesundheitsdaten zu Behandlungszwecken europaweit ermöglicht und vereinheitlicht werden. Dazu soll auf Informationen in den Systemen der Mitgliedstaaten gegenseitig zugegriffen werden können. Außerdem sieht der Verordnungsentwurf vom 3. Mai 2022 Regelungen zu diversen sekundären Nutzungszwecken vor, unter anderem zum Training künstlicher Intelligenz, für Zwecke der Forschung oder auch zu reinen Bildungszwecken. Bei dem EHDS handelt es sich um den ersten von mehreren im Rahmen der EU-Datenstrategie geplanten sektorenspezifischen Datenräume.

Die DSK fordert in ihrer Stellungnahme vom 27. März 2023 konkrete Nachbesserungen des Kommissionsentwurfs aus dem Mai 2022, damit das Datenschutzniveau der Datenschutz-Grundverordnung und der Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union nicht ausgehöhlt wird. Die DSK kritisiert insbesondere, dass der vorgelegte Entwurf das Grundrecht auf Datenschutz noch nicht mit den diversen Nutzungsinteressen der Stellen, die von den im EHDS angelegten Zugangsmöglichkeiten zu Gesundheitsdaten profitieren können, in einen angemessenen Ausgleich bringt. Kohärenz und Konsistenz von Begrifflichkeiten und Definitionen des EHDS-Verordnungsentwurfs zu anderen Rechtsakten der EU ist aus Sicht der DSK unerlässlich. Sie fordert sowohl im Zusammenhang mit der Datenverarbeitung zu Behandlungszwecken (Primärnutzung) als auch hinsichtlich der Sekundärnutzung der Gesundheitsdaten Verbesserungen in Bezug auf die Betroffenenrechte, die Transparenz der Datenverarbeitung, die Rechtsklarheit und die zur Schaffung eines durchgängigen Vertraulichkeitsniveaus erforderlichen technischen und organisatorischen Maßnahmen. Die vorgesehene Regelung zur Bereitstellung von Genomdaten sieht die DSK kritisch. Im Behandlungszusammenhang eingesetzte Geräte oder Software, die Patientendaten verarbeiten (sog. Electronic Health Record-Systeme), sollten aus Sicht der DSK vor Inbetriebnahme nur bei Gewährleistung der hohen Anforderungen an IT-Sicherheit und Datenschutz von unabhängigen Stellen zugelassen werden. In der Stellungnahme fordert die DSK zudem die standardmäßige Anwendung von Methoden zur Pseudonymisierung, Anonymisierung und Verschlüsselung von Daten bei der Sekundärnutzung von Gesundheitsdaten. Sie betont ausdrücklich die Bedeutung der einwilligungsbasierten Forschung. Je sensibler persönliche Daten sind, desto strenger müssen aus Sicht der DSK auch die Anforderungen an deren Verarbeitung sein.

Mit der Stellungnahme vom 27. März 2023 ergänzt die DSK die Kritik des Europäischen Datenschutzausschusses an dem am 3. Mai 2022 vorgelegten Verordnungsentwurf der Kommission. Im Dezember 2023 nahmen der Europäische Rat und das EU-Parlament zu dem Verordnungsentwurf der Kommission Stellung und forderten ebenfalls Nachbesserungen wie z.B. die Stärkung der Betroffenenrechte.

Zur Stellungnahme: **https://s.rlp.de/dsk-EHDS**

Stellungnahmen vom 10. und 14. August 2023 zum Referentenentwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten

Im Vorgriff auf die Pläne der EU zu einem Europäischen Gesundheitsdatenraum und in Umsetzung eines zentralen Gesetzgebungsvorhabens der Koalition legte die Bundesregierung im Sommer 2023 den Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG) vor. Der damalige Referentenentwurf war Gegenstand intensiver Erörterungen in der Taskforce Forschungsdaten und auf den Sitzungen der DSK. Zu dem Gesetzentwurf positionierte sich die DSK in ihrer Stellungnahme vom 14. August 2023. Zu der zugleich vorgesehenen weitreichenden Verlagerung von Aufsichtszuständigkeiten im Bereich des Datenschutzes von den Ländern zum Bund äußerten sich die unabhängigen Datenschutzaufsichtsbehörden der Länder in einer separaten Stellungnahme vom 10. August 2023.

Stellungnahme der DSK vom 14. August 2023

Nach Überzeugung der DSK braucht es für eine breite gesellschaftliche Akzeptanz der Nutzung von Gesundheitsdaten zu Forschungszwecken ausgewogene, mit den verfassungsrechtlichen Vorgaben in Einklang stehende Regelungen. Diese Anforderungen sah die DSK in dem Referentenentwurf vom 3. Juli 2023 nur unzureichend erfüllt. Zwar begrüßte die DSK das grundsätzlich mit dem Entwurf verfolgte Ziel, die rechtlichen Voraussetzungen für eine Forschung mit Gesundheitsdaten zu normieren. Allerdings sah die Konferenz aus datenschutzrechtlicher Sicht an mehreren Stellen noch dringenden Korrekturbedarf. Ausgehend von den in der Petersberger Erklärung im November 2022 formulierten Anforderungen an eine datenschutzkonforme Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung bemängelt sie in dem Entwurf das weitgehende Fehlen konkreter, spezifischer Maßnahmen und Garantien zur Wahrung der Rechte und Freiheiten der betroffenen Personen. Es reicht nach ihrer Überzeugung nicht aus, allein den Verantwortlichen allgemein aufzuerlegen, angemessene Maßnahmen zur Minimierung der Risiken für die Rechte und Freiheiten der betroffenen Personen zu treffen. Vielmehr müssen diese selbst im Gesetz enthalten sein. Die DSK vermisst im Gesetzentwurf normenklare Festlegungen z.B. zu den Anforderungen an eine sichere Verarbeitungsumgebung oder zur Bildung einer Forschungskennziffer. Auch das Verhältnis des GDNG zu den landesrechtlichen Forschungsregelungen für Krankenhäuser einschließlich Fragen zur Gesetzgebungszuständigkeit hält die DSK für ungeklärt. Sie bemängelt die lediglich eingeschränkte Gewährleistung von Betroffenenrechten in dem Gesetzentwurf, die in Widerspruch zu dem datenschutzrechtlichen Grundsatz der Transparenz der Datenverarbeitung steht. Die den Krankenkassen zuerkannte Befugnis zur datengestützten Auswertung gesundheitsbezogener Versichertendaten hält die DSK für schlicht unzulässig und fordert deren Streichung. Das damit den Kranken- und Pflegekassen ermöglichte Erstellen von Gesundheitsprofilen ihrer Versicherten birgt nach Auffassung der DSK ein hohes Diskriminierungsrisiko und überträgt den Krankenkassen Aufgaben aus dem Behandlungskontext, die aus guten Gründen den medizinischen Behandler:innen vorbehalten sind. Schließlich kritisiert die DSK die in dem Gesetzentwurf nur unzureichend vorgesehenen Möglichkeiten der Patient:innen zur Wahrnehmung ihrer Rechte im Zusammenhang mit der Übermittlung von Gesundheitsdaten aus der elektronischen Patientenakte an das Forschungsdatenzentrum. Schließlich betont die DSK die Bedeutsamkeit der Einführung eines strafbewährten Forschungsgeheimnisses.

Zur Stellungnahme vom 14. August 2023:
https://s.rlp.de/dskGDNG

Stellungnahme der unabhängigen Datenschutzaufsichtsbehörden der Länder vom 10. August 2023

Nach dem vom Bundesgesundheitsministerium vorgelegten Referentenentwurf sollte u.a. die datenschutzrechtliche Aufsichtszuständigkeit der Länder über die Kranken- und Pflegekassen und die Kassenärztlichen Vereinigungen auf den Bund übertragen werden. Gleiches war auch für alle Stellen vorgesehen, „die gesundheitsbezogene Sozialdaten im Sinne des § 67 SGB X verarbeiten". Dies hätte auch kommunale Jugend- oder Sozialämter erfasst. Hiergegen wandten sich die Aufsichtsbehörden der Länder in einer separaten Stellungnahme, in der sie die mit der beabsichtigten Verschiebung der Datenschutzaufsicht verbundenen erheblichen Nachteile offenlegten. Neben grundlegenden verfassungsrechtlichen Bedenken wiesen sie auf zu erwartende gravierende Unklarheiten und Abgrenzungsproblemen bei der Wahrnehmung der Aufsichtstätigkeit zwischen Bund und Ländern hin. Auch die mit dem Gesetzesvorhaben einhergehenden Gefahr des Rückgangs der aufsichtsbehördlichen Kontrolldichte und der fehlenden Präsenz als Ansprechpartner vor Ort sprachen aus Sicht der Länder gegen die geplante Regelung.

Zur Stellungnahme vom 10. August 2023:
https://s.rlp.de/laenderGDNG

Im weiteren Gesetzgebungsverfahren wurden einige der in den Stellungnahmen geforderten Anpassungen des Gesetzentwurfs aufgegriffen, andere datenschutzrechtlich als kritisch zu bewertende Inhalte dagegen bedauerlicherweise beibehalten. Während z.B. die zunächst beabsichtigte Zuständigkeitsverlagerung der Datenschutzaufsicht doch nicht weiterverfolgt und ein strafbewährtes Forschungsgeheimnis etabliert wurden, blieben aus Sicht der DSK nicht hinzunehmende Festlegungen weiter bestehen. So blieb es bei den den Krankenkassen ermöglichten Auswertungen von Versichertendaten oder dem Mangel an normenklaren Festlegungen zur Minimierung der mit einer Datenverarbeitung verbundenen Risiken. Der Gesetzentwurf passierte im Dezember 2023 den Bundestag. Das GDNG trat im März 2024 in Kraft.

Positionspapier zu cloudbasierten digitalen Gesundheitsanwendungen vom 6. November 2023

Mit Beschluss vom 6. November 2023 verabschiedete die DSK ein Positionspapier zu cloudbasierten digitalen Gesundheitsanwendungen. Mit dem Papier, an dem der LfDI wesentlich mitgewirkt hatte, sollen die spezifischen datenschutzrechtlichen Anforderungen an die Ausgestaltung und den Betrieb derartiger Anwendungen unabhängig davon, ob diese im Rahmen der gesetzlichen Krankenversicherung erstattungsfähig sind, hervorgehoben werden. Denn auch solche Anwendungen, die nicht von der Regelung des § 139e SGB V und der Digitalen Gesundheitsanwendungen-Verordnung (DiGAV) erfasst werden, verarbeiten regelmäßig besonders schutzbedürftige Gesundheitsdaten der Nutzer. Auch sie müssen datenschutzrechtliche Standards erfüllen. Das im November 2023 veröffentlichte Positionspapier soll den an der Herstellung und dem Betrieb digitaler Gesundheitsanwendungen beteiligten Stellen die in diesem Zusammenhang bestehenden Vorgaben des Datenschutzes bewusstmachen und deren Umsetzung erleichtern.

Zum Positionspapier:
https://s.rlp.de/dskCloudGesund

Entschließung „Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register“ vom 23. November 2023

Angesichts der im Koalitionsvertrag der Bundesregierung enthaltenen Festlegung, neben einem Gesundheitsdatennutzungsgesetz auch ein im Einklang mit der Datenschutz-Grundverordnung stehendes Registergesetz auf den Weg zu bringen, präzisierte die DSK in ihrer Entschließung vom 23. November 2023 die bei der Regulierung der Datenverarbeitung in medizinischen Registern zu berücksichtigenden datenschutzrechtlichen Anforderungen und Bedingungen. Vorausgegangen waren intensive Vorarbeiten der in der Taskforce Forschungsdaten hierzu eingerichteten Arbeitsgruppe.

Medizinische Register stellen ein wichtiges Instrument auf dem Weg zu einem besseren Verständnis der Ursachen einzelner Erkrankungen und der Bewertung und Entwicklung geeigneter Therapien dar. Hierzu sammeln sie Patientendaten in unterschiedlicher Menge und Häufigkeit. Je nach Registerzweck werden die vorgehaltenen Daten durch die Register selbst oder Dritte insbesondere zu wissenschaftlichen Zwecken weiterverarbeitet.

Die DSK begrüßt in der Entschließung die bereits in der Vergangenheit gemachten Überlegungen zur Schaffung eines bundesweiten Registerverzeichnisses und einer Zentralstelle für medizinische Register. Denn die Registerlandschaft in Deutschland ist sehr heterogen und vielfältig. Datenverarbeitungen basieren je nach Art und Ausgestaltung der Register auf unterschiedlichen Rechtsgrundlagen. Während z.B. die klinischen Krebsregister einer umfassenden Regulierung auf Bundes- und Landesebene unterliegen und dort die Einhaltung von Datenschutz und IT-Sicherheit im ausdrücklichen Fokus steht, gibt es andere, häufig auf persönliche Initiative hin gegründete Register, die rechtlich nicht geregelt sind und letztlich auf der Einwilligung der Patient:innen basieren. Die gesetzliche Regulierung bietet nach Ansicht der DSK die Chance, die Verarbeitung der in den Registern enthaltenen Gesundheitsdaten zu strukturieren und einheitliche datenschutzrechtliche Standards zu etablieren. Dies betrifft u.a. Fragen zu den Voraussetzungen für eine Übermittlung von Gesundheitsdaten aus dem Bereich der medizinischen Versorgung an medizinische Register, der Speicherung und Löschung dieser Daten in den Registern sowie deren Bereitstellung für Dritte. Auch das dem Verarbeitungsrisiko angemessene Schutzniveau bzw. die hierzu erforderlichen technisch-organisatorischen Maßnahmen sollten in einem Registergesetz festgelegt werden.

In der Entschließung sind die bei der anstehenden Gesetzgebung zu berücksichtigenden datenschutzrechtlichen Rahmenbedingungen aufgelistet. Ergänzend sind die in der Petersberger Erklärung der DSK aus dem November 2022 enthaltenen Hinweise zu beachten, sofern die Daten aus den Registern den Zwecken wissenschaftlicher Forschung dienen sollen.

Zur Entschließung:
https://s.rlp.de/dsk-medRegister

Entschließung „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken“ vom 23. November 2023

In der im Berichtsjahr geführten gesellschaftlichen und politischen Diskussion über die Rahmenbedingungen medizinischer Forschungsprojekte wurde deutlich, dass eine wesentliche Erschwernis für die zügige Durchführung derartiger Vorhaben die je nach Forschungsstandort unterschiedlichen datenschutzrechtlichen Anforderungen sind. Verantwortlich hierfür sind entgegen einer reflexartigen Annahme nicht die Datenschutzaufsichtsbehörden, sondern die im Einzelfall heranzuziehenden, teilweise beachtlich voneinander abweichenden bundes- und landesrechtlichen Vorgaben. Die

DSK griff die Thematik auf und forderte in einer Entschließung vom 23. November 2023 die zuständigen Gesetzgeber in Bund und Ländern auf, die jeweils geltenden gesetzlichen Regelungen besser aufeinander abzustimmen und damit den Schutz des informationellen Selbstbestimmungsrechts in der länderübergreifenden Forschung maßgeblich zu stärken.

Die Entschließung listet hierzu mehrere in der Taskforce Forschungsdaten vorbereitete Eckpunkte auf, die bei der gebotenen Harmonisierung der forschungsrelevanten datenschutzrechtlichen Vorgaben berücksichtigt werden sollten. Insbesondere fordert die DSK, auf eine inhaltliche Abstimmung und Verzahnung der jeweiligen Gesetze zu achten und jeweils angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und der Interessen der betroffenen Personen gesetzlich festzulegen. Die DSK bekräftigt den bereits in der Petersberger Erklärung aus dem November 2022 postulierten Grundsatz, dass desto umfangreicher und spezifischer Daten zu Forschungszwecken genutzt werden können, je höher der Schutz der betroffenen Personen durch geeignete Garantien und Maßnahmen sichergestellt wird.

Es bleibt abzuwarten, ob und ggf. in welcher Weise die Gesetzgeber in Bund und Ländern das mit der Entschließung verbundene Anliegen aufgreifen. Die DSK steht in diesem Zusammenhang für einen konstruktiven Dialog mit den jeweiligen Akteuren zur Verfügung.

Zur Entschließung:
https://s.rlp.de/dsk-medForschung

9. SOZIALES

9.1 Rechnungsprüfung im Jugendamt

Die datenschutzrechtliche Zulässigkeit der Bereitstellung von Akten des Jugendamtes zum Zwecke der Rechnungsprüfung beschäftigt den LfDI RP immer wieder. Auch im Berichtsjahr zeigte sich, dass das Spannungsfeld zwischen dem berechtigten Anliegen der internen oder externen Revision und dem gesetzlich verankerten Sozialgeheimnis die betroffenen Kommunalverwaltungen in beachtlichem Maße verunsichert, sofern im Rahmen laufender Prüfungen von den Jugendämtern die Herausgabe vollständiger Akten verlangt wird. Grund hierfür ist die aus Sicht der Sozialverwaltung unterschiedliche Schutzbedürftigkeit der bei den Jugendämtern vorgehaltenen Daten. Während Angaben über die Höhe der Kosten und der Effizienz im Einzelfall gewährter Beratungs- oder Unterstützungsleistungen eher eine fiskalische Aussagekraft besitzen und wenig über die Ursachen des jeweiligen Hilfebedarfs erkennen lassen, ist dies bei Daten aus dem Allgemeinen Sozialen Dienst (ASD) der Jugendämter anders. Er ist zentrale Anlaufstelle, wenn junge Menschen, Eltern und andere Familienangehörige oder auch Fachkräfte und Organisationen Hilfe und Unterstützung brauchen. Aufgrund dieser Funktion sind die dort verarbeiteten Daten im Regelfall für die Betroffenen sehr intim und schutzbedürftig. Deren Bereitstellung für Organisationseinheiten außerhalb des Jugendamts birgt latent die Gefahr des Vertrauensverlustes.

Zu der Thematik hatte sich der LfDI Rheinland-Pfalz bereits im 17. Tätigkeitsbericht im Jahre 1999 – damals vorwiegend in Bezug auf den Umgang mit sog. anvertrauten Daten – geäußert (https://s.rlp.de/tb17, dort unter Tz. 11.3.1 auf S. 72). Allgemein gilt, dass nach den Vorgaben des Datenschutzes eine Übermittlung von Sozialdaten aus dem Bereich der Jugendhilfe an die Rechnungsprüfungsbehörden (Rechnungsprüfungsämter, Rechnungshof) zur Überprüfung der Wirtschaftlichkeit der Sozialverwaltung zulässig ist, soweit die Daten für eine konkrete Prüfung erforderlich sind (vgl. §§ 35 Abs. 1 Satz 4 SGB I, 67c Abs. 3 Satz 1 und 69 Abs. 5 SGB X). Dem Rechnungshof wiederum sind die Unterlagen, die er zu seiner Aufgabenerfüllung für erforderlich hält, von den zu prüfenden Einrichtungen vorzulegen (§ 95 Abs. 1 LHO). Das skizzierte Spannungsfeld zwischen Rechnungsprüfung und Vertrauensschutz soll nach dem Willen der Rechtsordnung somit über die Frage der Erforderlichkeit der Daten für die Zwecke der Revision final gelöst werden.

Zumindest bei den im ASD der Jugendämter vorgehaltenen Daten sind aufgrund ihrer hohen Schutzbedürftigkeit qualifizierte Anforderungen an deren Erforderlichkeit zur Rechnungsprüfung zu stellen. Ihrer Bereitstellung sollte eine strenge Prüfung der Erforderlichkeit der Daten vorausgehen. Dabei ist zu berücksichtigen, dass die der individuellen Hilfe dienenden und einem besonderen Vertrauensschutz unterliegenden Daten im Gegensatz zu den Akten über die wirtschaftliche Hilfe für die Verwaltung grundsätzlich keine Leistungspflicht nach sich ziehen und damit regelmäßig auch nicht für eine Rechnungsprüfung geeignet sind.

Daneben sind die Schranken des § 65 SGB VIII zu beachten, der für anvertraute Daten – also Daten, die einzelnen Mitarbeiter:innen eines Trägers der öffentlichen Jugendhilfe zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind – einen rechtlich verankerten besonderen Vertrauensschutz etabliert. Anvertraute Daten dürfen hiernach nur bei Vorliegen der ausdrücklich in der Bestimmung genannten Übermittlungstatbestände von den Mitarbeiter:innen, denen sie offenbart wurden, weitergegeben werden. Eine Übermittlung dieser Informationen zum Zwecke der Rechnungsprüfung ist demnach nur mit Einwilligung derjenigen, die die Daten anver-

traut haben, zulässig. Liegt diese nicht vor, sind die anvertrauten Daten vor Bereitstellung zur Rechnungsprüfung zu schwärzen (vgl. Hauck, Kommentar zum SGB VIII; Rnr. 8 zu § 65). Dementsprechend sollten bereits im Jugendamt selbst organisatorische Vorkehrungen zur Vermeidung einer solchen Überprüfung getroffen werden, d.h. die anvertrauten Daten im Sinne von § 65 SGB VIII sollten von der allgemeinen Leistungsakte körperlich getrennt aufbewahrt werden. Auch eine getrennte Aktenführung von wirtschaftlicher Jugendhilfe und ASD ist datenschutzrechtlich geboten. Vor einer beabsichtigten Bereitstellung von Akten an Rechnungsprüfungsbehörden sollte zudem geklärt werden, welche Bestandteile der im Jugendamt in den verschiedenen Bereichen geführten Akten tatsächlich zur Durchführung des Prüfungsauftrags benötigt werden und ob es ggf. nicht genügt, in diesem Zusammenhang zunächst anonymisierte Akten zu verwenden.

9.2 Auskunftsanspruch in der öffentlichen Jugendhilfe

Soweit im jugendhilferechtlichen Verfahren ein datenschutzrechtlicher Auskunftsanspruch nach Art. 15 DS-GVO geltend gemacht wird, richtet sich dessen Umsetzung inhaltlich nach den Vorgaben des § 83 SGB X in Verbindung mit den §§ 61 ff. SGB VIII. Fragen können sich in diesem Zusammenhang sowohl im Hinblick auf die Antragstellung als solche als auch bezüglich des Umfangs der Auskunftserteilung ergeben.

In Bezug auf die Wirksamkeit der Antragstellung ist zu klären, in welchem Namen der Auskunftsanspruch erhoben wird. Geht es der auskunftsbegehrenden volljährigen Person allein um die zu ihr verarbeiteten Daten, ist die Beantragung rechtlich unproblematisch und das Jugendamt hat sich an den Vorgaben des § 83 SGB X zu orientieren. Wird der Anspruch dagegen im Namen eines minderjährigen Kindes geltend gemacht, wird es komplizierter: Bei gemeinsamem Sorgerecht der nicht getrennt lebenden Sorgeberechtigten ist auf der Grundlage der familienrechtlichen Vorgaben der §§ 1626 ff. BGB davon auszugehen, dass die Antragstellung einvernehmlich und in gemeinsamer Ausübung des Sorgerechts erfolgt. Solange dem Jugendamt keine Anhaltspunkte für Meinungsverschiedenheiten im Sinne des § 1628 BGB vorliegen, ist ein nur von einem Sorgeberechtigten gestellter Auskunftsantrag daher als einvernehmlich und wirksam einzustufen. Leben die Sorgeberechtigten dagegen nicht nur vorübergehend getrennt und steht ihnen beiden das Sorgerecht für das minderjährige Kind zu, muss zunächst geklärt werden, ob bzw. unter welchen Voraussetzungen überhaupt ein wirksamer Auskunftsantrag vorliegt.

Maßgeblich ist in diesem Zusammenhang die Regelung des § 1687 Abs. 1 BGB. Hiernach bedarf es für Entscheidungen in Angelegenheiten, deren Regelung für das Kind von erheblicher Bedeutung ist, einer gemeinsamen einvernehmlichen Sorgerechtsausübung. Die Geltendmachung des datenschutzrechtlichen Auskunftsanspruchs stellt als Ausdruck der Wahrnehmung eines der betroffenen Person zustehenden Grundrechts grundsätzlich eine Angelegenheit von erheblicher Bedeutung dar, so dass eine einvernehmliche Antragstellung für das minderjährige Kind durch beide Sorgeberechtigten erforderlich ist. Dies erfolgt entweder durch eine gemeinsame Antragstellung oder durch eine einseitige Erklärung der nicht antragstellenden Person, dass sie mit der Geltendmachung des Auskunftsanspruchs für das minderjährige Kind durch den anderen Sorgeberechtigten einverstanden ist. Sofern das Kind selbst bereits in der Lage ist, die Bedeutung und Reichweite eines derartigen Auskunftsanspruchs einzuschätzen, sollten zudem dessen Haltung und Interessen dabei mitberücksichtigt werden. Soweit ersichtlich ist, dass die Auskunft nicht dem Wohl des Kindes dient, kann der Antrag – ausgehend von der gesetzlichen Wertung des § 1686 BGB – bereits als

offensichtlich unbegründet gemäß Art. 12 Abs. 5 S. 2 DS-GVO verweigert werden.

Falls es zu einer wirksamen Antragstellung kommt, sind im Hinblick auf die Erteilung von Auskünften die Vorgaben des § 83 SGB X in Verbindung mit den §§ 61 ff, SGB VIII, insbesondere zum Schutz der Vertraulichkeit anvertrauter Daten nach § 65 VIII, zu berücksichtigen. Dabei sind für die Praxis zwei Regelungen von besonderer Bedeutung:

Nach § 83 Abs. 1 Nr. 1 SGB X in Verbindung mit § 82a Abs. 1 Nr. 1 lit. a SGB X besteht die Pflicht zur Auskunftserteilung u.a. dann nicht, soweit dadurch die ordnungsgemäße Erfüllung der in der Zuständigkeit der auskunftserteilenden Stelle – also dem Jugendamt – liegenden Aufgaben gefährdet werden würde. In einem derartigen Fall unterbleibt die Auskunftserteilung, d.h. das Interesse der Antragsteller muss zugunsten des im konkreten Fall bestehenden überwiegenden Anliegens der Jugendhilfe zurücktreten. Konkret kann dies z.B. dann gegeben sein, wenn im Rahmen eines Auskunftsantrags die Identität von Hinweisgeber:innen offengelegt werden müsste.

Auskunftsanträge, die eine Preisgabe zum Zwecke persönlicher oder erzieherischer Hilfe einzelnen Mitarbeiter:innen von Jugendämtern anvertrauter Daten im Sinne des § 65 SGB VIII zur Folge hätten, haben nur Erfolg, wenn die in der Regelung enthaltenen Voraussetzungen für eine zulässige Weitergabe oder Übermittlung dieser Daten vorliegen. Die seitens des Gesetzgebers insoweit getroffene Abwägung zwischen der Effektivität der Jugendhilfe und dem familienrechtlich verankerten allgemeinen Informationsrecht der Sorgeberechtigten bleibt auch im datenschutzrechtlichen Zusammenhang bestehen. Ohne den über § 65 SGB VIII gewährleisteten Vertrauensschutz ist eine effektive Wahrnehmung der Aufgaben der Jugendämter nicht möglich, so dass die sich daraus ergebende Einschränkung des Auskunftsrechts datenschutzrechtlich hinnehmbar ist.

10. KOMMUNALES

10.1 Umgang mit personenbezogenen Daten von Hinweisgebenden und Informant:innen

Der LfDI hat sich bereits in der Vergangenheit damit befasst, wie mit personenbezogenen Daten von Hinweisgebenden und Informant:innen in der öffentlichen Verwaltung umzugehen ist. Die für die Praxis relevanten Informationen hierzu finden sich zum einen in der auf der Webseite des LfDI bereitgestellten Orientierungshilfe (**https://s.rlp.de/dsk-OHHinweisgeber**). Zum anderen enthalten der 12. Tätigkeitsbericht der Datenschutzkommission Rheinland-Pfalz unter Tz. 20.1 sowie der Tätigkeitsbericht zum Datenschutz 2022 unter Tz. 11.2 entsprechende Ausführungen.

Nach wie vor gilt in diesem Zusammenhang, dass die Identität von Hinweisgebenden und Informant:innen grundsätzlich vertraulich zu behandeln ist und die Identität nur dann weitergegeben werden darf, wenn

- der oder die Hinweisgebende ausdrücklich damit einverstanden ist,
- der Inhalt des Hinweises sich durch andere Aufklärungs- und Beweismittel nicht erhärten lässt, der Inhalt der Aussage des oder der Hinweisgebenden sich aber grundsätzlich als Beweismittel eignet und deshalb im überwiegenden Allgemeininteresse entsprechend genutzt werden muss,
- die Hinweise sich als falsche Anschuldigungen erweisen, denen mit erheblicher Wahrscheinlichkeit eine Beleidigungs- oder Schädigungsabsicht des oder der Hinweisgebenden zugrunde liegt.

Anders verhält es sich jedoch, wenn aufgrund des oder der Hinweisgebenden ein Ordnungswidrigkeitenverfahren eingeleitet wird. Dann gibt es durchaus Fallkonstellationen, in welchen die Identität preisgegeben werden muss.

Wird z.B. von betroffenen Personen Akteneinsicht in das laufende Verfahren nach § 49 OWiG beantragt, so entsteht die gesetzliche Pflicht des Verantwortlichen, dieser nachzukommen. Daneben besteht zudem auch das Akteneinsichtsrecht des Verteidigers oder der Verteidigerin nach § 147 StPO iVm § 46 Absatz 1 OWiG, welches ebenfalls eine rechtliche Verpflichtung des Verantwortlichen auslöst.

In diesen Fällen kann es notwendig sein, die Identität des oder der Hinweisgebenden zu offenbaren. Die Zulässigkeit ergibt sich im Falle der Einleitung eines Bußgeldverfahrens unmittelbar aus dem OWiG. Nach § 66 Abs. 1 Nr. 4 OWiG enthält nämlich der Bußgeldbescheid die Beweismittel. In dieser Hinsicht ergibt sich durch § 46 Abs. 1 OWiG in Verbindung mit § 222 Ab s. 1 Strafprozessordnung (StPO) auch die Pflicht zur Namhaftmachung von Zeuginnen und Zeugen, sodass die Identität gegenüber der angezeigten Partei bekanntgegeben werden kann.

Allerdings ist in diesem Zusammenhang auch der Grundsatz der Datenminimierung zu beachten, welcher sich wiederum aus Art. 5 Abs. 1 lit. c DS -GVO ergibt. Hiernach müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Sollten also einzelne personenbezogene Daten in diesem Kontext keine Relevanz besitzen (z.B. die private E-Mail-Adresse des Zeugen oder der Zeugin), so sind diese in den Akten auf geeignete Weise unkenntlich zu machen.

Es dürfen also nur solche Daten zugänglich gemacht werden, die dem Zweck der Gewährung einer Akteneinsicht – dies ist die Überprüfung des erhobenen Vorwurfs und die Abschätzung der Erfolgsaussicht eines Einspruchs gegen den Bußgeldbescheid – dient.

10.2 Veröffentlichung personenbezogener Daten im Internet

Regelmäßig kommt es zu Beschwerden aus der Bürgerschaft, weil deren personenbezogene Daten in einem kommunalen, aus dem Internet erreichbaren Bürgerinformationssystem veröffentlicht werden. Fast immer erfolgen solche Veröffentlichungen ohne wirksame Rechtsgrundlage und die jeweiligen Verstöße werden durch den LfDI mit aufsichtsrechtlichen Maßnahmen geahndet.

Die geschilderten Probleme entstehen meist dann, wenn personenbezogene Daten zwar grundsätzlich durch die Gemeinden verarbeitet und in Ratsprotokolle oder Vorlageberichte einfließen dürfen, die anschließende Veröffentlichung im Internet hiervon jedoch nicht mehr abgedeckt ist.

Im Berichtsjahr gab es in diesem Zusammenhang in mehreren Gebietskörperschaften Beschwerden aufgrund von Veröffentlichungen im Rahmen der 2023 durchgeführten Schöffenwahlen. Teilweise wurden hier umfangreiche personenbezogene Daten, die sich aus kompletten Lebensläufen von Kandidatinnen und Kandidaten um das Schöffenamt ergaben, ohne Kenntnis der betroffenen Personen online gestellt.

Diejenigen Probleme, welche rund um die Schöffenwahl entstehen, hatte der LfDI bereits im 27. Tätigkeitsbericht für das Jahr 2018 unter Rz. 3.1 thematisiert. Die damals vorgetragenen Ausführungen besitzen nach wie vor Gültigkeit, sodass im Ergebnis zusammengefasst werden kann, dass eine Veröffentlichung der im Rahmen von § 36 GVG erhobenen Daten im Internet ausschließlich über eine Einwilligung der betroffenen Personen zulässig ist. Nähere Ausführungen können dem genannten Tätigkeitsbericht entnommen werden.

Einen immer wiederkehrenden Fall stellt trotz mehrfacher Sensibilisierung durch den LfDI auch die Annahme von Spenden dar, welche durch die Gemeinderäte in öffentlicher Sitzung beschlossen werden.

Auch hier gilt, dass eine Veröffentlichung dieser Daten im Internet nur auf Grundlage einer Einwilligung möglich ist. Der LfDI empfiehlt daher, auf die Bekanntgabe von Spenderdaten im Internet verzichten, sofern keine Einwilligung der Spenderinnen oder Spender vorliegt. Stattdessen sollte lediglich darüber informiert werden, dass Spenden in einer bestimmten Höhe angenommen wurden, ohne personenbezogene Daten der Spenderinnen und Spender preiszugeben. Insoweit sei auch auf den Tätigkeitsbericht 2022 verwiesen.

10.3 Auftragsverarbeitung beim Abschluss von Fahrrad-Leasing-Angeboten

Um umweltfreundliche Fortbewegung zu fördern, gehen immer mehr Verwaltungen dazu über, ihren Bediensteten Leasingangebote für Fahrräder zu unterbreiten. Hierbei ist es in der Regel so, dass die Kommune ein Ausschreibungsverfahren startet und sich im Anschluss auf einen Anbieter festlegt. Mit diesem wird dann ein Leasing-Rahmenvertrag abgeschlossen, der grundsätzlich festlegt, dass Einzel-Leasingverträge zwischen der Kommune und dem Leasinganbieter zur leasinggebundenen Finanzierung von Fahrrädern geschlossen werden können. Entscheiden sich nun Bedienstete, das Angebot des Arbeitgebers anzunehmen, so schließt der Arbeitgeber mit dem Leasinggeber einen Einzelvertrag ab und gibt in diesem Zusammenhang die personenbezogenen Daten der Beschäftigten weiter.

Von Seiten mehrerer Gemeinden wurde die Frage aufgeworfen, ob es sich hierbei um eine Auftragsverarbeitung im Sinne des Art. 28 DS-GVO handelt und ob in der Folge entsprechende Verträge gem. Art. 28 Abs. 3 DS-GVO abzuschließen sind.

Auftragsverarbeiter ist gem. Art. 4 Nr. 8 DS-GVO „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet". Verantwortlicher wiederum ist „die natürliche oder juristische Person, Behörde […], die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet" (Art. 4 Nr. 7 DS-GVO).

Eines der wesentlichen Merkmale der Auftragsverarbeitung ergibt sich aus Art. 29 DS-GVO. Dieser sagt aus, dass Auftragsverarbeiter personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten. In der Folge sind Handlungen des Auftragsverarbeiters auch grundsätzlich dem Verantwortlichen zuzurechnen.

Auch ist zu berücksichtigen, dass bei einer Auftragsverarbeitung die Verarbeitung personenbezogener Daten die Kernaufgabe sein muss. Wenn die Datenverarbeitung lediglich im Zusammenhang mit der Erbringung einer Dienstleistung für einen anderen erfolgt, liegt keine Auftragsverarbeitung vor. Aus Erwägungsgrund 81 ergibt sich ferner, dass eine Auftragsverarbeitung in der Regel nur dann gegeben ist, wenn der Verantwortliche „einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will".

Da die Haupttätigkeit des Leasinggebers im Abschluss von Einzelleasingverträgen zwischen ihm und der jeweiligen Gemeinde liegt, verfolgt dieser insoweit eigene Interessen und bestimmt für die Durchführung seiner Tätigkeit Zwecke und Mittel der Verarbeitung. Die Übermittlung personenbezogener Daten von Beschäftigten durch die Gemeinde sowie die anschließende Verarbeitung durch den Leasinggeber bildet hierbei nicht die Kernaufgabe der Tätigkeit.

Vielmehr ist die Verarbeitung der personenbezogenen Daten lediglich ein Nebenbestandteil der Gesamttätigkeit. Im Sinne des Erwägungsgrunds 81 ist aus objektiven Gesichtspunkten regelmäßig nicht davon auszugehen, dass die betroffenen Kommunen die Auftragnehmer mit der Verarbeitung personenbezogener Daten betrauen wollen. Die Datenverarbeitung ist in diesem Fall als „unvermeidliches Beiwerk" bei der Erfüllung der eigentlichen Dienstleistungspflicht – nämlich des Abschlusses eines Einzelleasingvertrages – zu betrachten.

Vergleichbar ist dies z.B. mit der Übermittlung von Beschäftigtendaten bei der Buchung eines Hotels für eine Dienstreise. Auch hier werden Mitarbeiterdaten durch einen Dritten verarbeitet. Gleichwohl liegt keine Auftragsverarbeitung vor, da die Kerntätigkeit ebenfalls nicht auf der Verarbeitung personenbezogener Daten beruht.

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

Das oben genannte Thema wurde zuletzt im Tätigkeitsbericht 2021 (II.13.2) aufgegriffen.

In der derzeit noch gültigen Fassung des OZG werden die öffentlichen Verwaltungen verpflichtet, die 6.000 Verwaltungsleistungen, die zu 575 OZG-Leistungsbündeln in 14 Themenfeldern zusammengefasst wurden, bis Ende 2022 auch digital über entsprechende Verwaltungsportale anzubieten.

Dieser Termin ist längst verstrichen und es wartet auf Bund, Länder und Kommunen noch viel Arbeit. Schon aus diesem Grund hat sich die Notwendigkeit für eine Gesetzesänderung ergeben, mit der dieses Thema als Daueraufgabe für die Verwaltung mit hoher Priorität verankert wird.

Aus datenschutzrechtlicher Sicht war für das Erfordernis der Änderung des OZG insbeson-

dere maßgeblich, dass die rechtlichen Rahmenbedingungen für eine datenschutzkonforme Datenverarbeitung in einem nach dem „Einer für Alle (EfA)"-Prinzip entwickelten und bereitgestellten länderübergreifenden Online-Dienst noch nicht geschaffen waren und die Zuweisung der datenschutzrechtlichen Verantwortlichkeit für die Datenverarbeitung innerhalb eines Online-Dienstes auf Übergangsregelungen gestützt wurde.

Bereits im Herbst 2021 hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (Datenschutzkonferenz, DSK) die Erwartung an ein gesetzgeberisches Tätigwerden bis zum dritten Quartal 2022 formuliert. Während der Zwischenkonferenz der DSK im September 2022 traten die Aufsichtsbehörden daher gegenüber dem Bundesministerium des Innern und für Heimat (BMI) erneut dafür ein, alle erforderlichen Vorrausetzungen zu schaffen, damit die datenschutzrechtlichen Anpassungen des OZG so bald wie möglich in Kraft treten können.

Zu diesem Zweck stellte die DSK datenschutzrechtliche Expertise in Gestalt der Kontaktgruppe „OZG 2.0" unter dem Vorsitz der Berliner Beauftragten für Datenschutz und Informationsfreiheit bereit. Den im Rahmen intensiver Beratungen von der Kontaktgruppe vorgeschlagenen Änderungen stand das BMI offen gegenüber und hat datenschutzrechtlich maßgebliche Vorschläge in den Gesetzentwurf übernommen.

Auch der LfDI Rheinland-Pfalz hatte sich im Berichtszeitraum an der Länderabstimmung zum Entwurf eines Gesetzes zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz) beteiligt und sich im Rahmen seiner Möglichkeiten eingebracht.

Mit den bekannten Fortschritten im Gesetzgebungsverfahren ist das Inkrafttreten eines OZG-Änderungsgesetzes nun in Kürze zu erwarten.

Aus der Sicht der Datenschutzaufsichtsbehörden dauerte die Weiterentwicklung und Änderung des OZG allerdings zu lange.

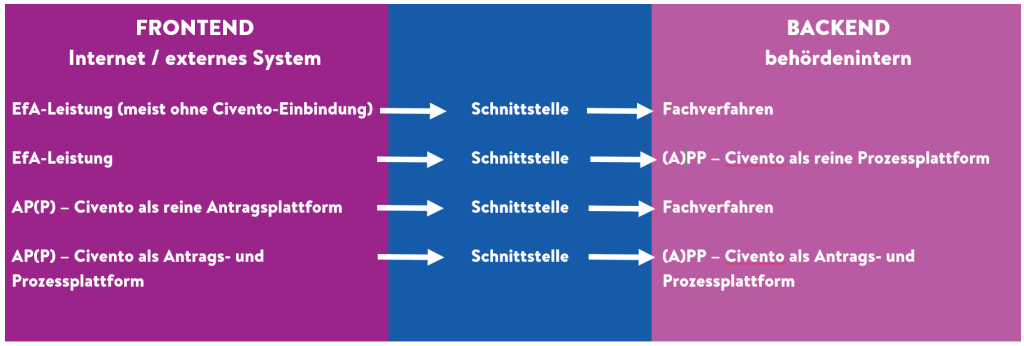
Um insbesondere die Umsetzung des OZG voranzutreiben, haben Hessen, das Saarland und Rheinland-Pfalz den OZG-Verbund Mitte gegründet. Kern der Kooperation ist der länderübergreifende Austausch von Onlineprozessen, die auf einer gemeinsamen technischen Plattform – der Antrags- und Prozessplattform (APP) Civento – entwickelt werden. In Rheinland-Pfalz und dem Saarland wird die APP vom Landesbetrieb Daten und Information (LDI) betrieben.

Die APP ist eine mandantenfähige Standardsoftware und ein Basisdienst gemäß 25 Abs. 4 Nr. 4 des Landesgesetzes zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz (EGovGRP). Mit der APP können Verwaltungsleistungen außerhalb der 14 Themenfelder des Leistungskataloges des OZG Bund digitalisiert werden. Mit der APP können Anträge, Datenfelder und Maskenprozesse konfiguriert und andere Basiskomponenten wie Nutzerkonto oder Bezahldienst integriert werden.

Die flächendeckende Anbindung für die 194 hauptamtlich geführten Kommunen in Rheinland-Pfalz startete im Mai 2022 und mit dem Fortschreiten des Einführungsprozesses der APP Civento fokussierte sich der LfDI darauf, sich die Funktionsweise der Software und deren Verwendungsmöglichkeiten zu erschließen.

Zu diesem Zweck fand ein Austausch mit den Datenschutzaufsichtsbehörden des Saarlandes und von Hessen statt. Letztere haben ein Informationsgespräch mit dem Rechenzentrum ekom21 organisiert, welches das Hosting der APP Civento für öffentliche Stellen in Hessen übernommen hat.

Mögliche Prozessgestaltung:



Fachverfahren (oder Fachanwendungen) sind Softwareprogramme für die Bearbeitung von Leistungen in der Verwaltung (z.B. Anträge). Fachverfahren werden ausschließlich im internen Netz der Behörde den Sachbearbeiter:innen zur Verfügung gestellt, nicht im Internet. Fachverfahren sind nicht zwingend mit einem Online-Dienst verbunden und lassen sich auch ohne diesen nutzen.

Weiterhin hatte sich eine Kommunalverwaltung dazu bereit erklärt, dem LfDI vor Ort eine mit der Civento APP digitalisierte Verwaltungsleistung innerhalb der Testumgebung „civento rlp sandbox kommunal“ vorzustellen.

Die Verarbeitungsleistungen, die mit der Civento APP digitalisiert werden können, sind zahlreich und vielfältig. Eine Kommunalverwaltung hat mehrere hundert dafür geeignete Verarbeitungstätigkeiten identifiziert. Nachfolgend einige Beispiele:

- Veranlagung zur Hundesteuer, Prozess von der Anmeldung eines Hundes bis zum abschließenden Versand eines Hundesteuerbescheids
- Anwohnerparkausweis beantragen
- Erteilung eines Jagdscheins
- Anträge für Leitungsverlegung beim Träger der Wegebaulast
- Organisation von Stadtführungen, Führungen im Tierpark o.ä.
- Anmeldung für Flohmarkt oder Ferienprogramm
- Ehrenamtsförderung

Die Abstimmung zwischen der Datenschutzaufsichtsbehörde des Saarlandes und dem LfDI zu verschiedenen datenschutzrechtlichen Fragestellungen wie ausreichende Mandantentrennung im LDI oder die Festlegung von Löschterminen innerhalb eines mit der APP Civento digitalisierten Verwaltungsleistung ist noch nicht abgeschlossen.

11. BILDUNG

11.1 Datenschutzfragen bei der Kita-Sozialarbeit

Bei der Kita-Sozialarbeit suchen Mitarbeitende verschiedener Träger eine Kita auf und bieten ihre Hilfe an. Im Vorfeld ist dabei die Frage aufgetaucht, ob Kita-Sozialarbeiter:innen Daten von Kita-Personal und Kita-Leitungen erhalten dürfen (z.B. über den Entwicklungsstand des Kindes, Verhaltensauffälligkeiten etc.), aber auch eigene Beobachtungen mitteilen können.

Bei der Kita-Sozialarbeit handelt es sich um ein freiwilliges Angebot, welches Eltern auch ablehnen können, beispielsweise weil sie keinen Bedarf sehen und möglichweise auch nicht möchten, dass das Verhalten ihres Kindes in der Kita von Externen beobachtet wird.

Anfragende Kommunen vertraten die Auffassung, dass die Daten der Kinder den geschützten Bereich des Sozialdatenschutzes nicht verlassen würden, weil alle beteiligten Akteur:innen selbst schweigepflichtig wären. Daher könne der gegenseitige Austausch auf eine gesetzliche Grundlage gestützt werden und bedürfe keiner Einwilligung der Eltern.

Der LfDI hielt es für fraglich, ob § 64 SGB VIII als rechtliche Grundlage für den Informationsaustausch herangezogen werden könne. Denn die Norm regelt auf den Einzelfall bezogene Datenübermittlungen und nicht einen pauschalen Datenaustausch verschiedener Stellen innerhalb eines Projektes. Auch enthält die Vorschrift spezielle Regelungen dazu, unter welchen Voraussetzungen die Kita dem Träger personenbezogene Daten von Kindern mitteilen darf. Die genannten Fallgruppen trafen auf das Projekt „Kita-Sozialarbeit“ nicht zu.

Außerdem ist den Bestimmungen des Kita-Zukunftsgesetzes zu entnehmen, dass die Bildungs- und Lerndokumentation, welche auch ohne Einwilligung der Eltern zu führen ist, Grundlage für die Aufgabenwahrnehmung der Kita sein soll (§ 3 Abs. 3 Kita-Zukunftsgesetz). Das Portfolio darf ohne ausdrückliche Einwilligung der Eltern nicht an Dritte weitergegeben werden. Datenverarbeitungen und -austausche mit externen Personen und Stellen, wie sie in dem vorliegenden Projekt beabsichtigt waren, können daher nicht auf diese Regelungen gestützt werden.

Hinzu kommt, dass individuelle Förderbedarfe als Gesundheitsdaten dem besonderen Schutz des Art. 9 DS-GVO unterliegen, so dass eine Verarbeitung dieser Informationen nur unter strengen Voraussetzungen möglich ist. Aus Sicht des LfDI sprach daher vieles dafür, dass die vorliegenden Datenverarbeitungsvorgänge lediglich auf der Grundlage einer informierten Einwilligungserklärung der Sorgeberechtigten und Kita-Beschäftigten zulässig sind. Insoweit musste auch darüber informiert werden, welche Folgen eine Weigerung bzw. ein Widerruf der Einwilligung hätte, zu welchem Zweck die Daten verarbeitet und wie lange diese bei welcher Stelle gespeichert werden. Außerdem sollten die Eltern informiert werden, bei welcher Stelle sie ihre Betroffenenrechte nach der DS-GVO wahrnehmen können. Die Kommunen passten ihre Formulare und Informationsschreiben auf der Basis dieser Bewertung an.

11.2 Künstliche Intelligenz (KI) an rheinland-pfälzischen Schulen

Der LfDI beriet das Ministerium für Bildung des Landes Rheinland-Pfalz (BM) im Zuge der Einführung der KI-Software Fobizz, die den Schulen zum zweiten Schulhalbjahr 2023/24 angeboten werden soll. Die Software ermöglicht es Schulen unter anderem, auf verschiedene Large-Language-Modelle wie „Chat-GPT“ zuzugreifen, ohne dass die Schüler:innen dazu individuelle Login-Accounts erstellen müssen. Das System verwendet einen Proxy, über den die Lehrkraft einen Raum erstellen kann, der

den Schüler:innen temporär den Zugriff auf verschiedene KI-Dienste ermöglicht.

Gegenüber dem BM regte der LfDI Rahmenbedingungen und Konfigurationen an, die den Einsatz der Anwendung datenschutzkonformer gestalten. Er wies zudem auf die Notwendigkeit der Erstellung einer Datenschutzfolgenabschätzung hin.

Der Anbieter der Software hat seinen Sitz in Hamburg, über Schnittstellen werden die Eingaben der Schüler jedoch – zumindest temporär – zur Herstellerfirma von Chat-GPT Open-AI übertragen. Die dort stattfindenden Datenverarbeitungsprozesse bedürfen noch der Klärung. Der LfDI befindet sich daher in einem fortlaufenden Austausch mit dem BM und Fobizz. Darüber hinaus erstellte das BM entsprechende organisatorische Hinweise für Lehrkräfte und Schüler:innen zum Umgang mit personenbezogenen Daten bei Eingaben in die KI-Software.

11.3 Mobile-Device-Management-System mit privaten Endgeräten

Der LfDI informierte sich über das Mobile-Device-System (MDM) Jamf, welches von vielen Schulträgern in Rheinland-Pfalz zur Administration von iPads verwendet wird. Der Fokus lag hierbei auf den Zugriffsberechtigungen und Zugriffsmöglichkeiten auf der administrativen Ebene.

Bei der Demonstration des Systems durch einen Schulträger im Echtbetrieb konnten sich die Mitarbeiter:innen des LfDI einen umfassenden Einblick in die Zugriffsberechtigungen in verschiedenen Rollen verschaffen. Da in das System auch eigene Geräte der Eltern und Schüler:innen eingebunden werden können („Bring Your Own Device“ / „BYOD“), war insbesondere die Trennung zwischen privat installierten Apps und den schulischen Apps des Schulträgers eine zentrale Fragestellung. Zwar ließ das System keinen Einblick in die Inhalte der einzelnen Apps zu, jedoch konnten sich die Administratoren der obersten Ebene die privat installierten Apps anzeigen lassen. Der LfDI sieht hierfür keine Erforderlichkeit, da bereits die Kenntnis des Vorhandenseins einer App Rückschlüsse auf sensible persönliche Informationen geben kann (beispielsweise Schwangerschafts-App, Ramadan-Kalender, queere Kommunikations-Apps, Dating-Apps, Abnehm-Apps). Als Lösung wurde auf eine Beschränkung der entsprechenden Rechte verwiesen, beispielsweise durch eine von den Administratoren unabhängige übergeordnete Funktionsstelle zur Rechtevergabe.

Hinsichtlich der Ortung des GPS-Standorts eines privaten Endgeräts im sog. „Lost-Modus“ bzw. der „Wo-ist-Funktion“ präsentierte der Träger einen datenschutzfreundlichen Ansatz. Der Modus kann nur auf schriftlichen Antrag durch die Eltern aktiviert werden, um eine „Kontrolle“ durch die Schule oder den Träger auszuschließen.

Ein weiterer Aspekt der Betrachtung des Systems war die Protokollierung. Hier zeigte sich, dass in der Standardkonfiguration seit Systembeginn protokolliert wurde und diese Protokolldaten auch Namen von Schüler:innen im Klartext enthielten. Im Rahmen eines Datenschutzkonzeptes empfahl der LfDI interne Regelungen zur Speicherdauer von Protokolldaten. Die hier festzulegenden Fristen sollten sich nach der zweckmäßigen Erforderlichkeit der vorgehaltenen Protokolldaten richten. Insofern scheint eine Speicherdauer von sechs Monaten angemessen.

11.4 Versetzung online

Den LfDI erreichten mehrere Beschwerden zum Portal „Versetzung online“, welches für versetzungsinteressierte Lehrkräfte die Möglichkeit bietet, sich nach offenen Stellen „umzusehen“.

Die Lehrkräfte problematisierten, dass bereits bei der Registrierung in dem oben genannten Portal eine Meldung für die Schulleitung ausgelöst wird. Dies habe dazu geführt, dass Schulleitungen die betroffenen Lehrkräfte auf ihren angeblichen Versetzungswunsch direkt angesprochen haben. Die Lehrkräfte wollten sich jedoch nur in dem Portal umschauen bzw. sich allgemein informieren, so dass die Konfrontation mit einem angeblichen Versetzungswunsch für sie als überraschend und unangenehm empfunden wurde.

Den Nutzungshinweisen auf der Startseite des Portals war hierzu kein Hinweis zu entnehmen.

Die Recherchen des LfDI ergaben, dass die Authentizität der Person, die sich anmeldet, durch Einbeziehung der Schulleitung sichergestellt werden sollte.

Aus technisch-organisatorischer Sicht war es jedoch nicht geboten, bei der Passwortvergabe für die Registrierung zum Portal die Schulleitungen zu beteiligen. So bestand beispielsweise die Möglichkeit, das Passwort per Brief an die Schule zu übersenden oder an eine dienstliche E-Mail-Anschrift des Anmeldenden, die im Registrierungsprozess abgefragt wird.

In der Folge wurde der Registrierungsprozess gemäß den Empfehlungen des LfDI datenschutzkonform umgestellt. Weiterhin wurde eine Schulleiterin vom LfDI dafür gerügt, dass sie Informationen aus dem Registrierungsprozess (Lehrerin L ist versetzungswillig) zweckwidrig verwendet und an Dritte weitergegeben hatte.

11.5 Youngdata.de

Youngdata.de ging vor 10 Jahren als Eigenentwicklung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI) an den Start. Die Seite hat zum Ziel, Jugendliche für einen sicheren Umgang mit ihren personenbezogenen Daten im Internet sowie in Apps und Social Media zu sensibilisieren. Seitdem hat sich viel getan:

Neben den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder wurde der Kanton Zürich Kooperationspartner, die Inhalte wurden stetig an neue Entwicklungen angepasst, interaktive Elemente sowie zahlreiche Videos und Cartoons wurden zur besseren Veranschaulichung zielgruppengerecht eingebettet. Der LfDI Rheinland-Pfalz hatte dabei stets die technische und redaktionelle Letztverantwortung für die gemeinsamen Teile des Portals.

Mittlerweile ist youngdata.de auch in Bildungskreisen etabliert und wird nicht nur in Schüler-Workshops, sondern auch von Lehrkräften, Ausbildern und „Silver Surfern“ zur Eigenfortbildung genutzt. Am 3. Dezember 2023 wurde die Webseite mit dem 3. Platz in der Kategorie „Jugendpreis Bildung“ des renommierten Kindersoftwarepreises TOMMI 2023 ausgezeichnet.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte im März 2022 den Relaunch der Seite beschlossen, um youngdata.de noch besser an die Nutzungspräferenzen der Zielgruppe anzupassen.

Am 11. Mai 2023 wurde **www.youngdata.de** im neuen Look vorgestellt. Die Administration der Seite hat ein Team aus Kolleg:innen der Datenschutzaufsichtsbehörden in Berlin, Hamburg, Mecklenburg-Vorpommern und Rheinland-Pfalz sowie des Bundesdatenschutzbeauftragten übernommen.

12. MELDEWESEN UND WAHLEN

Auch im zurückliegenden Berichtsjahr gab es zahlreiche Beschwerden über die Weitergabe von Meldedaten. Den Beschwerdeführenden ist oftmals nicht bekannt, dass sie selbst aktiv werden müssen, um bestimmte Informationsvorgänge zu unterbinden. Dies gilt namentlich für die Weitergabe von Jubiläumsdaten oder die Datenübermittlung an politische Parteien im Vorfeld von Wahlen.

Aber auch die Weitergabe von Meldedaten an den Beitragsservice ARD ZDF Deutschlandradio (früher „GEZ“) ist immer wieder Grund für erboste Schreiben an den LfDI.

Gemäß § 11 Abs. 4 des Rundfunkbeitragsstaatsvertrages kann die zuständige Landesrundfunkanstalt für Zwecke der Beitragserhebung sowie zur Feststellung, ob eine Beitragspflicht nach dem Rundfunkbeitragsstaatsvertrag besteht, personenbezogene Daten bei öffentlichen und nichtöffentlichen Stellen ohne Kenntnis des Betroffenen erheben, verarbeiten oder nutzen. Öffentliche Stellen in diesem Sinne sind insbesondere die Meldebehörden. Für die vorliegende Art der Datenverarbeitung besteht mithin ein gesetzlicher Erlaubnistatbestand im Sinne des Art. 6 Abs. 1 lit. e der DS-GVO, wonach eine Verarbeitung rechtmäßig ist, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Des Weiteren legt § 12 Abs. 1 der Meldedatenlandesverordnung Rheinland-Pfalz fest, dass die zuständige örtliche Meldebehörde zum Zwecke der Erhebung und des Einzugs der Rundfunkbeiträge nach dem Rundfunkbeitragsstaatsvertrag dem Südwestrundfunk oder der von ihm beauftragten Stelle unter anderem aus Anlass der An - oder Abmeldung personenbezogene Daten wie den Familiennamen und die Anschrift übermitteln darf.

13. RECHTSDURCHSETZUNG

In Fällen, in denen der LfDI Anhaltspunkte erhält, welche auf das Bestehen von Datenschutzverstößen hindeuten, ermittelt er zunächst den zugrundeliegenden Sachverhalt. Eine wesentliche Ermittlungsbefugnis sind hierbei Informationsersuchen, die sich an Verantwortliche oder Auftragsverarbeiter richten und die Anweisung zum Gegenstand haben, alle für die Aufgabenerfüllung des Landesbeauftragten erforderlichen Informationen bereitzustellen. Im Jahr 2023 kamen trotz bestehender Rechtspflicht nicht alle Adressaten dieser Aufforderung nach. Aus diesem Grund drohte der Landesbeauftragte in 71 Fällen Zwangsgelder an und verhängte diese in 24 Fällen. Die durchschnittliche Höhe der Zwangsgelder betrug 500 €.

Bei festgestellten Datenschutzverstößen machte der LfDI auch in diesem Jahr von Abhilfebefugnissen Gebrauch. So sprach er 15 Beanstandungen aus und verhängte 19 Verwarnungen. Um bestehende Mängel zu beseitigen, erließ die Behörde 48 Anweisungen. Der LfDI erließ zudem insgesamt neun Geldbußen mit einem Gesamtbetrag von 3.930 €.

Auch im Jahr 2023 erhoben Bürger:innen Klagen gegen hoheitliche Maßnahmen. In insgesamt elf Fällen war der Landesbeauftragte an Klageverfahren beteiligt. Hiervon waren acht Klageverfahren beim Verwaltungsgericht Mainz anhängig, drei Verfahren wurden vor dem Oberverwaltungsgericht Rheinland-Pfalz geführt.

ABKÜRZUNGSVERZEICHNIS

Arbeitskreis	AK
Antrags- und Prozessplattform	APP
Allgemeiner Sozialer Dienst der Jugendämter	ASD
Antiterrordateigesetzes	ATDG
Binding Corporate Rules	BCR
Binding Corporate Rules for Controllers	BCR-C
Betriebliches Eingliederungsmanagement	BEM
Bürgerliches Gesetzbuch	BGB
Ministerium für Bildung des Landes Rheinland-Pfalz	BM
Bundesministerium des Innern und für Heimat	BMI
bezüglich	bzgl.
Digitale Gesundheitsanwendungen-Verordnung	DiGAV
Datenschutz-Grundverordnung	DS-GVO
Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder	DSK
Der Europäische Datenschutzausschuss	EDSA
Europäischer Datenschutzbeauftragter	EDSB
Landesgesetz zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz	EGovGRP
European Health Data Space	EHDS
Europäische Union	EU
Europäischer Gerichtshof	EuGH

EU-U.S. Data Privacy Framework	EU-U.S. DPF
Gesundheitsdatennutzungsgesetz	GDNG
Grundgesetz	GG
gegebenenfalls	ggf.
Geldwäschegesetz	GwG
Kreditwesengesetz	KWG
Landesbetrieb Daten und Information Rheinland-Pfalz	LDI
Landesdatenschutzgesetz Rheinland-Pfalz	LDSG
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz	LfDI
Öffentlicher Personennahverkehr	ÖPNV
Onlinezugangsgesetz	OZG
Personalausweisgesetz	PAuswG
Polizei- und Ordnungsbehördengesetz	POG
Rechtsextremismus-Datei-Gesetz	RED-G
Sozialgesetzbuch	SGB
sogenannt	sog.
Telekommunikation-Telemedien-Datenschutz-Gesetz	TTDSG
zum Beispiel	z.B.

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