Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

TÄTIGKEITSBERICHT ZUM DATENSCHUTZ 2022

www.datenschutz.rlp.de

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

August 2023

INHALT

VORWORT


Prof. Dr. Dieter Kugelmann

Das Jahr 2022 war ein Jahr, in dem manche Entwicklungen abgeklungen sind und andere Entwicklungen an Fahrt gewonnen haben. Abgeklungen ist – zumal zum Ende des Jahres hin – die Pandemie mit ihren vielfältigen Konsequenzen für Wirtschaft, Gesellschaft und auch den Datenschutz, auch wenn es immer noch viele Schwierigkeiten zu bewältigen galt. Aus der Sicht des Datenschutzes waren die Anfänge des Jahres durchaus noch von vielen offenen Fragen gekennzeichnet, die nach und nach konkretisiert und bearbeitet werden konnten. So konnten Rechtssicherheit und Verlässlichkeit in der datenschutzrechtlichen Bewältigung der Pandemie gesteigert werden. Abgeklungen sind auch die unmittelbaren Auswirkungen des Inkrafttretens der Datenschutz-Grundverordnung (DS-GVO). Zwar treten immer wieder neue Herausforderungen und Fragen auf, viele Grundfragen und Aspekte sind jedoch bearbeitet und in grundsätzlich sichere Bahnen überführt. Diese Entwicklungen haben auch die Arbeit der Behörde des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz im Jahr 2022 geprägt.

Im Hinblick auf die Datenschutz-Grundverordnung hat sich manches eingependelt. Die Grundfesten des Datenschutzes stehen. Die Zahl der Beschwerden steigt nicht in erheblichem Maße weiter an. Bei vielen Verantwortlichen in Verwaltung und Wirtschaft sind die Grundlagen für rechtmäßige Datenverarbeitungen gelegt, so dass möglicherweise Beschwerden nicht mehr notwendig sind. Ein hohes Niveau hält weiterhin der Bereich der Meldungen von Datenschutzverletzungen, die sog. Datenpannen. Dies ist auf die erschreckend hohe Zahl von Angriffen auf Computersysteme zurückzuführen. Cybersicherheit und Datenschutz rücken enger aneinander. Insgesamt ist im Zusammenhang mit der Anwendung der DS-GVO eine grundsätzliche Konsolidierung zu verzeichnen. Konsolidiert haben sich die Antworten auf eine Reihe von Rechtsfragen, auch wenn selbstverständlich immer wieder neue Konstellationen neue Antworten erfordern. Konsolidiert hat sich aber auch die Art und Weise des Umgangs mit der DS-GVO durch Verantwortliche in Wirtschaft und Verwaltung. Sorge bereitet allenfalls, dass an mancher Stelle ein Nachlassen der Aufmerksamkeit einzutreten scheint. Das Datenschutzmanagement insgesamt ist aber vielerorts gut aufgestellt und auch auf Fragen der Aufsichtsbehörde vorbereitet.

Neue Dynamik und neue Herausforderungen für unser Arbeitsfeld bringt hingegen insbesondere die Gesetzgebung der Europäischen Union mit sich. Einige neue Rechtsakte traten bereits 2022 in Kraft, andere liegen im Entwurf vor und werden heftig diskutiert. Diese rechtlichen Rahmenbedingungen für Wirtschaften im Internet, für die Plattformökonomie oder für den Einsatz von KI-Systemen werfen zahlreiche neue Fragen auf. Diesen Fragen muss sich auch die Behörde des Landesbeauftragten stellen. Als Leiter der TaskForce KI der deutschen Datenschutzaufsichtsbehörden habe ich hier eine besondere Rolle und Verantwortung, die ich sehr gerne wahrnehme, weil es um Zukunftsfragen für die gesamte digitale Gesellschaft geht. Das Jahr 2022 markierte insoweit eher den Anfang entsprechender Diskussionen und Entwicklungen als deren Ende. Denn die Rechtsakte treten nach und nach in Kraft, sind anzuwenden und in Einklang mit dem bereits geltenden Datenschutzrecht zu bringen (mehr dazu unter I.3).

Um diesen neuen Tendenzen und Herausforderungen gerecht zu werden, entwickelt sich auch die Datenschutzkonferenz weiter. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat dazu schon 2020 einen Arbeitskreis auf Leitungsebene eingerichtet, der die entsprechenden Entwicklungen begleiten soll und Änderungen in der Arbeitsweise der DSK vorbereitet. Ich habe die Leitung dieses Arbeitskreises, des AK DSK 2.0, seit Januar 2022 inne. Diese verantwortungsvolle Position bietet Gelegenheit, Kooperationen zwischen den deutschen Behörden in Richtung auf die Verantwortlichen in Wirtschaft und Verwaltung, aber auch in Richtung auf die Zusammenarbeit auf europäischer Ebene neu zu gestalten. Dank der hervorragenden Vorarbeit, die der sächsische Vorsitz des Arbeitskreises zuvor geleistet hat, ist es im Jahr 2020 gelungen, weitreichende Maßnahmen wie etwa die Erleichterung des Treffens von Mehrheitsentscheidungen zu verwirklichen. Das Jahr 2022 war insoweit auch ein Jahr der Neuausrichtung der DSK. Dieser Prozess ist gerade angesichts der zunehmenden Notwendigkeiten, sich mit anderen Behörden abzustimmen, längst nicht abgeschlossen.

Für die Behörde des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz war 2022 zudem ein besonderes Jahr des Einschnitts. Zum Oktober dieses Jahres ist Helmut Eiermann aus dem Dienst ausgeschieden, um den Ruhestand zu genießen. Genau 30 Jahre hat er der Behörde in verschiedensten Funktionen angehört. Als Stellvertreter des LfDI hat Helmut Eiermann in den letzten Jahren wesent-

liche Umgestaltungen mitgeprägt. Ich möchte ihm auch an dieser Stelle dafür herzlich danken. Ich freue mich zudem, dass es gelungen ist, mit Frau Dr. Daniela Franke eine Stellvertreterin zu gewinnen, die nunmehr die weiteren Fortentwicklungen der Behörde mitgestalten wird. Ich bin zuversichtlich, dass der LfDI Rheinland-Pfalz im Rahmen seiner Möglichkeiten und Zuständigkeiten auch in Zukunft eine tragende und prägende Rolle in Rheinland-Pfalz, Deutschland und Europa spielen kann.

Die Digitalisierung im Allgemeinen und die Entwicklungen auf dem Gebiet des Datenschutzes im Besonderen stellen stetig neue Herausforderungen. Ich und meine Behörde nehmen diese Herausforderungen gerne an, weil es uns darum geht, für die Bürgerinnen und Bürger in Rheinland-Pfalz und darüber hinaus einen angemessenen Schutz ihrer Rechte und Freiheiten zu sichern. Dies haben wir uns auf die Fahnen geschrieben und wir werden nicht nachlassen, dieses Ziel weiter mit Augenmaß und Nachdruck zu verfolgen.

I.
DER LFDI RHEINLAND-PFALZ IN DEUTSCHLAND UND EUROPA

I. DER LFDI RHEINLAND-PFALZ IN DEUTSCHLAND UND EUROPA

1. VORSITZ DES ARBEITSKREISES DSK 2.0

Die Datenschutzkonferenz (DSK) ist seit ihrem Gründungsjahr 1978 ein Gremium, das sich für die Wahrung und den Schutz der Datenschutzgrundrechte einsetzt. Es hat sich zur Aufgabe gemacht, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Dazu hat die DSK sich in den vergangenen Jahrzehnten stetig gewandelt. Seit der Geltung der Datenschutz-Grundverordnung (DS-GVO) hat die Vernetzung der Datenschutzaufsichtsbehörden noch einmal europaweit Auftrieb gewonnen. Die DSK stellt dies vor die Aufgabe, ihre Abstimmungsprozesse zu optimieren. Der Schlagtakt ist schneller, der rechtliche Abstimmungsbedarf aufgrund der einheitlichen gesetzlichen Grundlagen höher, die Anforderungen der Wirtschaft werden lauter und drängender geäußert. In der politischen Debatte der letzten Jahre hat dies – die Problematik verkürzend – zu einer Zentralisierungsdiskussion im Hinblick auf die Datenschutzaufsicht geführt. Beispiele dafür sind der Bericht der Datenethikkommission vom Oktober 2019 und der Beschluss der Wirtschaftsministerkonferenz vom 30. November 2020.

Gründung und Ergebnisse des AK DSK 2.0

Im Juni 2020 richtete die DSK zur Optimierung ihrer Arbeit einen Arbeitskreis DSK 2.0 auf Leitungsebene der Aufsichtsbehörden ein, der die derzeitige Zusammenarbeit der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder einschließlich der Arbeitsweise der DSK evaluieren und ggf. Vorschläge für eine Neugestaltung erarbeiten sollte. Der Vorsitz dieses Arbeitskreises ist im Januar 2022 von Sachsen auf Rheinland-Pfalz übergegangen.

Der AK DSK 2.0 konnte in der Kürze der Zeit seiner Tätigkeit bereits wesentliche Änderungen in der Arbeitsweise der Datenschutzkonferenz erreichen, die zu einer stärkeren Festlegung der internen Verfahren, zu einer besseren Abstimmung und Zusammenarbeit und zu einem stärkeren, geeinten und einheitlichen Auftreten gegenüber der Öffentlichkeit, der Gesellschaft, den Verantwortlichen und den betroffenen Personen führen:

Jour fixe der DSK

Zur besseren Abstimmung ihrer Schritte führt die DSK wöchentlich eine Videokonferenz auf Leitungsebene durch. Verantwortlich für die Durchführung ist der Vorsitz. Die Videokonferenz dient dem Austausch zu aktuellen Themen und zur Information über geplante öffentlichkeitswirksame Aktivitäten der einzelnen Aufsichtsbehörden. Beschlüsse werden nicht gefasst.

Gutachten „Rechtliche Möglichkeiten zur Stärkung und Institutionalisierung der Kooperation der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK 2.0)“ von Prof. Dr. Indra Spiecker gen. Döhmann und Prof. Eike Richter

Die DSK hat einen Auftrag für die Erstellung eines Gutachtens erteilt, um die rechtlichen Möglichkeiten zur Stärkung und Institutionalisierung der Kooperation innerhalb der Datenschutzkonferenz auszuloten. Ein Gegenstand

der Untersuchung war dabei insbesondere die Frage, ob und auf welche Weise eine Verbindlichkeit von Beschlüssen der Datenschutzkonferenz und die Errichtung einer Geschäftsstelle der Datenschutzkonferenz geregelt werden können.

Die im Rahmen des Gutachtens erörterten Spielräume für die Gestaltung der Fortentwicklung und Institutionalisierung wurden seitens des AK DSK 2.0 weiter elaboriert und in Unterarbeitskreisen zu „Verbindlichen Mehrheitsentscheidungen" und „Errichtung einer Ständigen Geschäftsstelle" operationalisiert.

Bindende Mehrheitsentscheidungen der Datenschutzkonferenz

Die DSK ist sich einig darin, eine einheitliche Rechtsanwendung unter Wahrung ihrer Unabhängigkeit zu fördern und ihre Zusammenarbeit dafür zu stärken. Die Pflicht zur harmonisierenden Anwendung der DS-GVO führt zum Erfordernis, eine stärkere Abstimmung der Aufsichtspraxis der Aufsichtsbehörden untereinander zu erreichen, insbesondere dann, wenn in einem Mitgliedstaat mehrere Aufsichtsbehörden bestehen, die eine einheitliche Anwendung gewährleisten müssen. Zu diesem Zweck wurde ein auf Freiwilligkeit beruhendes Kooperationssystem der deutschen Datenschutzaufsichtsbehörden etabliert, in dem unter bestimmten Voraussetzungen bindende Mehrheitsentscheidungen getroffen werden können, aber zugleich die notwendige Unabhängigkeit der einzelnen Aufsichtsbehörden gewahrt wird. Auf Grundlage des in dem AK DSK 2.0 verabschiedeten „Eckpunktepapier Bindende Mehrheitsentscheidungen" wurde die Geschäftsordnung der Datenschutzkonferenz unter Ziffer 3 dahingehend geändert, dass nunmehr Beschlüsse mit einer Mehrheit von mindestens 12 Stimmen (2/3) verabschiedet werden. Sie haben für die Mitglieder der DSK im Wege der Selbstbindung bindende Wirkung. Sie dienen nicht dem Schutz Dritter und begründen keine einklagbaren Rechte. Jedes Mitglied der DSK, das der Mehrheitsentscheidung nicht zustimmt, kann zusätzlich zu seiner Stimmabgabe erklären, dass es sich dieser Bindung nicht unterwirft. Diese Erklärung wird zusammen mit dem Beschluss veröffentlicht. Jedes Mitglied kann die Aufhebung oder Abänderung bindender Beschlüsse beantragen.

Errichtung eines Präsidiums der DSK

Für das Jahr 2023 wurde erstmalig als Pilotprojekt ein Präsidium bestehend aus vorherigem, aktuellem und nächstjährigem Vorsitz der DSK sowie den beiden Vertreter:innen des Europäischen Datenschutzausschusses (EDSA) gebildet. Das Präsidium stellt ein Gremium zur Unterstützung des DSK-Vorsitzes in operativen und strategischen Fragen dar. Insbesondere vor dem Hintergrund des jährlichen Vorsitzwechsels soll zudem Kontinuität geschaffen werden. Durch die Beteiligung der Vertreter:innen der deutschen Datenschutzaufsichtsbehörden im EDSA soll die Schnittstelle und der Anschluss zu selbigem weiter gestärkt werden.

Durchführung einer jährlichen Klausurtagung

Die Datenschutzkonferenz kommt einmal jährlich in einer Klausurtagung zusammen. Diese soll dem Austausch, der Bewusstseinsbildung und der gemeinsamen Beratung und Willensbildung zu strategischen (Grundsatz-)Fragen dienen, welche die Ausrichtung der Datenschutzkonferenz und des Datenschutzrechtes betreffen. Die erste Klausurtagung fand vom 28. bis 30. Juli 2023 unter meiner Leitung in Rheinland-Pfalz statt.

Einrichtung einer Ständigen Geschäftsstelle der Datenschutzkonferenz

Der AK DSK 2.0 formulierte in seinem Zwischenbericht, der im Nachgang der zweiten Sitzung des Arbeitskreises im Dezember 2020 erstellt wurde, das Ziel, zur Institutionalisierung und Effektivierung der (Zusammen-)Arbeit der DSK eine Geschäftsstelle der DSK einzurichten. Die Geschäftsstelle soll vorwiegend administrative und den Vorsitz unterstützende Aufgaben übernehmen, die im Zusammenhang mit der Organisation der Sitzungen, Veranstaltungen (wie des Europäischen Datenschutztags) und der Sitzungsdurchführung der DSK anfallen. Darüber hinaus soll die Geschäftsstelle den Vorsitz und die DSK bei regelmäßigen und dauerhaften Aufgaben im Umfeld der DSK unterstützen. Die Geschäftsstelle soll der umfassenden Weisungsbefugnis des jeweiligen Vorsitzes der DSK unterliegen. Rechtsgrundlage zur Einrichtung der Ständigen Geschäftsstelle soll eine Verwaltungsvereinbarung zwischen dem Bund und den Ländern sein. Ein entsprechender Entwurf wird derzeit erarbeitet.

Ausblick

Die Datenschutzkonferenz hat sich als wichtiges, national und international anerkanntes Experten- und Aufsichtsgremium fortentwickelt und immer stärker institutionalisiert, um bei den drängenden Fragen des Datenschutzes und der Digitalisierung seitens der Wirtschaft, des öffentlichen Sektors und nicht zuletzt der Gesellschaft schnelle und fundierte Antworten geben zu können. Dieser Prozess setzt sich stetig fort, denn der durch Gesetze, Verordnungen und Technologien vorangetriebene Wandel wird weitere Anpassungen erfordern, z.B. aufgrund der Rechtsakte zur Digitalisierung, die derzeit auf EU-Ebene verhandelt und verabschiedet werden. Die Datenschutzkonferenz stellt sich diesen Herausforderungen, indem sie auf der Grundlage der erreichten Erfolge ihre Kooperation weiter fortentwickelt. Diesen Prozess möchte ich weiter als Vorsitz des AK DSK 2.0 unterstützen und voranbringen.

2. DIE KOORDINIERTE DATENSCHUTZAUFSICHT ÜBER EUROPOL WECHSELT IHR GEWAND

Die europäische Agentur Europol hat die Aufgabe, die Mitgliedstaaten bei der Verhütung und Bekämpfung aller Formen von schwerer internationaler und organisierter Kriminalität, Cyberkriminalität und Terrorismus zu unterstützen. Dazu ist sie auf Informationen der Polizeibehörden der Mitgliedstaaten angewiesen und fungiert als sog. Information Hub. Die datenschutzrechtliche Aufsicht über Europol liegt beim Europäischen Datenschutzbeauftragten (EDSB), während die Datenschutzaufsichtsbehörden der Mitgliedstaaten die Datenschutzaufsicht über die nationalen Polizeibehörden

innehaben, wenn diese Unterstützung von Europol in Anspruch nehmen. Eine effektive datenschutzrechtliche Kontrolle erfordert Koordination und Kooperation der Datenschutzaufsichtsbehörden untereinander. Dazu wurde mit Inkrafttreten der Europol-Verordnung das Europol Cooperation Board gegründet. Wie bereits im 26. Tätigkeitsbericht berichtet, habe ich darin die Landesdatenschutzaufsichtsbehörden Deutschlands vertreten neben dem BfDI als Gemeinsamem Vertreter.

Im Berichtsjahr wurde diese koordinierte Aufsicht nunmehr umgestaltet. Am 27.06.2022 ist die Verordnung (EU) 2022/991 des Europäischen Parlaments und des Rates vom 8. Juni 2022 zur Änderung der Verordnung (EU) 2016/794 in Bezug auf die Zusammenarbeit von Europol mit privaten Parteien, die Verarbeitung personenbezogener Daten durch Europol zur Unterstützung strafrechtlicher Ermittlungen und die Rolle von Europol in Forschung und Innovation in Kraft getreten. Infolge der Änderungen wurde Art. 45 Europol-Verordnung, der die Etablierung des Europol Cooperation Boards geregelt hatte, gestrichen. Stattdessen wird die Zusammenarbeit des Europäischen Datenschutzbeauftragten und der nationalen Datenschutzaufsichtsbehörden im Einklang mit Artikel 62 der Verordnung (EU) 2018/1725 im Rahmen des Coordinated Supervision Committee gewährleistet werden. Dieses ist zuständig für die koordinierte und wirksame Aufsicht über IT-Großsysteme und über Organe, Einrichtungen und sonstige Stellen der Union. Darunter fallen neben Europol noch die koordinierte Aufsicht über das Internal Market Information System (IMI), die European Union Agency for Criminal Justice Cooperation (Eurojust), das European Public Prosecutor's Office (EPPO) und jüngst das Schengener Informationssystem (SIS). Ich werde dort weiterhin als Ländervertreter für die Themen, die Europol betreffen, fungieren und freue mich auf die weitere Zusammenarbeit.

3. NEUE HERAUSFORDERUNGEN UND ENTWICKLUNGEN DURCH EUROPÄISCHE RECHTSAKTE

Die Gesetzgebung auf europäischer Ebene hat im Jahr 2022 zu ersten konkreten Ergebnissen für den Bereich der Digitalisierung im Zusammenhang von Marktwirtschaft und Wirtschaftswachstum geführt. Mit dem Ziel, den digitalen Binnenmarkt in der EU zu stärken, ist die Europäische Kommission angetreten und hat eine Datenstrategie im Jahr 2022 vorgelegt. Auf deren Grundlage hat die Europäische Kommission eine Reihe von Vorschlägen für Rechtsakte erarbeitet. Im Jahr 2022 sind mit dem Rechtsakt zu digitalen Märkten, dem Rechtsakt zur Data Governance und dem Rechtsakt zu den digitalen Diensten die ersten davon im Amtsblatt der Europäischen Union veröffentlicht worden und damit in Kraft. Mit Übergangsfristen werden sie nach und nach auch Wirksamkeit entfalten. Zudem sind weitere Rechtsakte im Verfahren, die weitreichende Folgen haben werden.

Der Rechtsakt zur Data Governance zielt auf die erleichterte Zugänglichkeit von Informationen der öffentlichen Verwaltung für die Wirtschaft. Dieses Ziel wird auch dadurch erreicht, dass Datentreuhänder und zwischengeschaltete Einrichtungen mit Regeln ausgestattet werden, die ein entsprechendes Zugänglichmachen unter dem Ausgleich anderer berechtigter Interessen möglich machen sollen. Der Rechtsakt zu den digitalen Märkten zielt insbesondere auf die Sicherung freien Wettbewerbs vor dem Hintergrund, dass große Technologieunternehmen insbesondere aus den Vereinigten Staaten von Amerika zu bändigen sind. Auch der Rechtsakt zu den digitalen Diensten zielt nicht zuletzt darauf ab, die Oligopole und starken Stellungen von Technologieunternehmen aus Staaten außerhalb der Europäischen Union einzuhegen. Ziel der Europäischen Union ist es, die

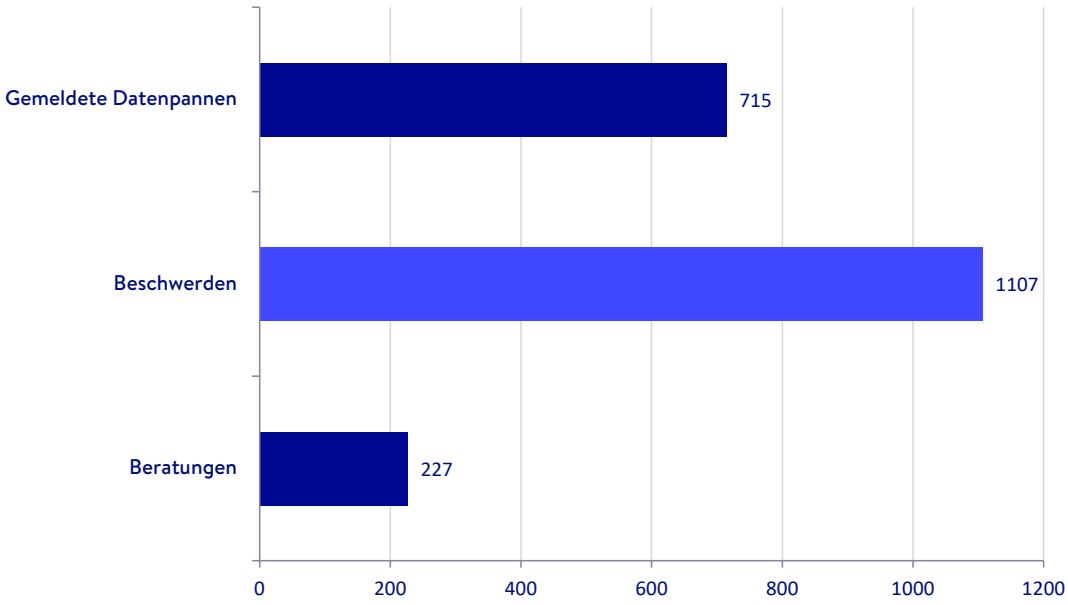
europäische Wirtschaft zu stärken und dabei einen soliden und gerechten Rahmen herzustellen, der zugleich die Eindämmung der Rolle großer Technologieunternehmen bewirkt.

Noch im Entwurf sind der Rechtsakt zu Rahmenbedingungen für die vernetzte Wirtschaft, der die erleichterte Zugänglichkeit von im Wirtschaftsverkehr vorhandenen Daten für andere Wirtschaftsunternehmen zum Inhalt hat. Zu diesem Zweck soll die Rolle der Bürger:innen, die entsprechende Daten zur Verfügung stellen, gestärkt werden. Von erheblicher Bedeutung wird die Verordnung über den Einsatz künstlicher Intelligenz sein. Im Entwurf werden insbesondere Hochrisikosysteme besonders geregelt, um die Rechte und Freiheiten der Einzelnen zu gewährleisten. Die Position der Datenschutzaufsichtsbehörden kann anknüpfen an die Hambacher Erklärung aus dem Jahr 2019, die unter meinem Vorsitz verabschiedet wurde. Der Mensch muss im Mittelpunkt stehen. Ausgangspunkt und Rahmen ist die Menschenwürde, unabhängig von technischen und informatorischen Möglichkeiten.

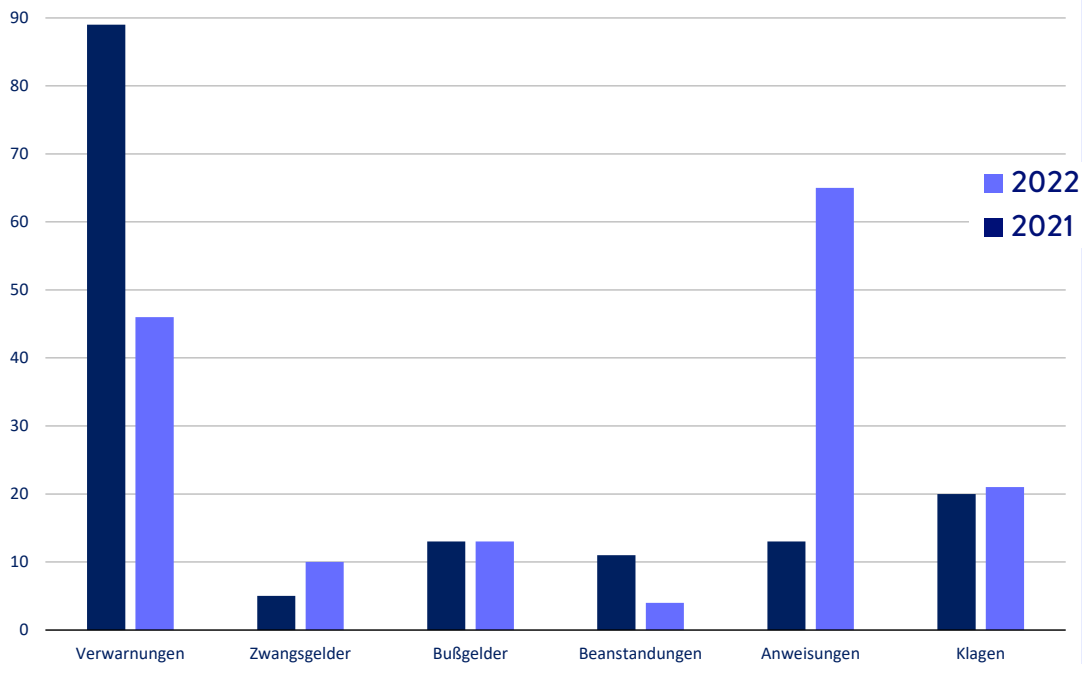
Diese und weitere Rechtsakte beeinflussen die Rolle der Datenschutzaufsichtsbehörden. In all diesen Rechtsakten sind Aufsichtsbehörden vorgesehen, die von den Mitgliedstaaten benannt werden können. So werden künftig etwa die Bundesnetzagentur oder auch die Wettbewerbsbehörden erweiterte Befugnisse im Zusammenhang mit der Digitalisierung und der Nutzung von Daten innehaben. Eine Kooperation mit den Datenschutzaufsichtsbehörden ist damit zwingend erforderlich. Auf diese Kooperation müssen sich die Datenschutzaufsichtsbehörden und damit auch der LfDI vorbereiten. Es kann zudem dazu kommen, dass die Rechtsakte, die noch ausstehen, in zeitlicher Nähe den Datenschutzaufsichtsbehörden zusätzliche Aufgaben zuerkennen werden. Der Aufgabenkreis erweitert sich und damit auch die Notwendigkeit, personell und organisatorisch auf die Erfüllung der entsprechenden Aufgaben vorbereitet zu sein. Für die Bürger:innen sind die inhaltlichen Änderungen und Gegebenheiten von großer Bedeutung. Für Wirtschaft und Verwaltung geht es um die Anforderungen an Datenverarbeitung auf dem digitalen Markt oder beim Einsatz von KI-Systemen. Für mich wird es darum gehen, diese Prozesse effektiv, konstruktiv und zukunftsorientiert zu begleiten.

II.
ZAHLEN UND FAKTEN

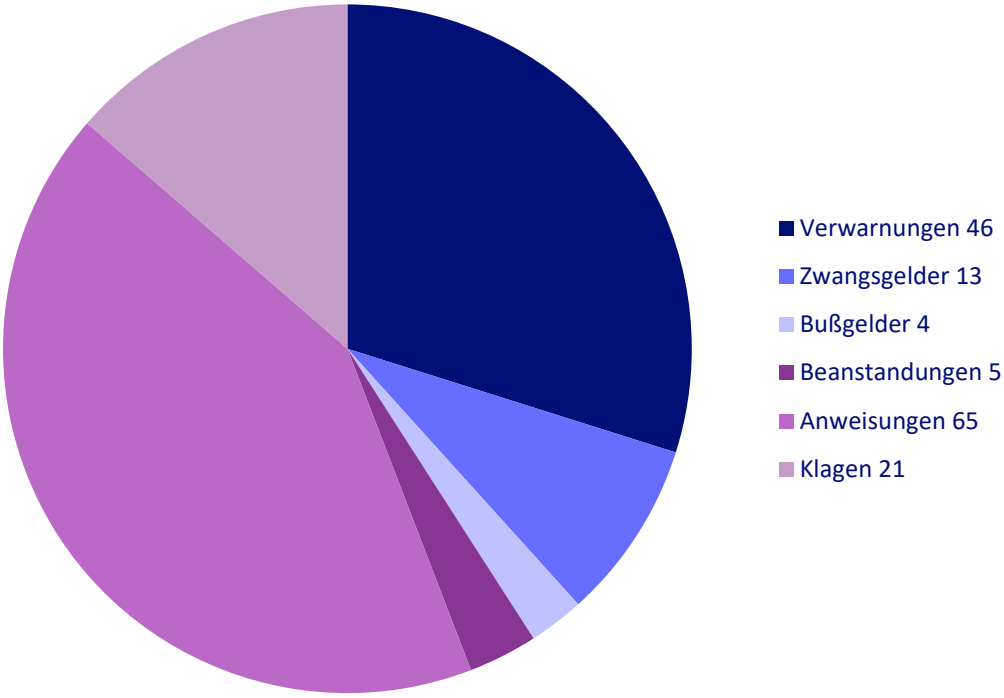
1. Geschäftsstatistik 2022



2. Ausgeübte Befugnisse 2021 und 2022



3. Ausgeübte Befugnisse 2022



III.
SACHGEBIETE

II. SACHGEBIETE

1. SICHERHEIT

1.1 Zuverlässigkeitsüberprüfungen bei (Groß-)Veranstaltungen

Bereits in den vergangenen Tätigkeitsberichten hat der LfDI zu der Thematik berichtet (**https://s.rlp.de/datenschutzttigkeitsberichte**, hier: 2016/2017, 2018). Auf die nachdrücklichen Forderungen des LfDI hin hat der rheinland-pfälzische Gesetzgeber eine bereichsspezifische Rechtsgrundlage zur Zuverlässigkeitsüberprüfung geschaffen. Seit Ende des Jahres 2020 sind mit den §§ 67 f. Polizei- und Ordnungsbehördengesetz (POG) Regelungen zur Zuverlässigkeitsprüfung für Veranstaltungen im POG in Kraft.

Im Berichtszeitraum wurden nach der Corona-Pandemie erstmals wieder (Groß-)Veranstaltungen durchgeführt und damit auch erstmalig Zuverlässigkeitsüberprüfungen – gestützt auf die nunmehr bestehenden Regelungen im POG – vorgenommen sowie der LfDI im Rahmen der in § 67 Abs. 1 S. 3 POG und § 68 Abs. 1 S. 2 POG geregelten Anhörungsverfahren beteiligt. Zuverlässigkeitsüberprüfungen führen zu einer hohen Anzahl von tiefgreifenden Datenerhebungen und -abgleichen bei Nichtstörern. Angesichts dessen ist das Instrument der Zuverlässigkeitsüberprüfung einerseits auf Anlässe zu beschränken, in denen es geeignet, erforderlich und angemessen ist, sowie andererseits in einer Art und Weise zu verwenden, welche die Grundrechte der betroffenen Personen nur in einem absolut erforderlichen Maß beeinträchtigt, sowohl was den Umfang der Überprüfung als auch den betroffenen Personenkreis betrifft, und dabei größtmögliche Transparenz bietet. Darauf wirkte der LfDI im Rahmen seiner Beteiligung hin und konnte bereits Lösungen für die folgenden Problemstellungen erreichen:

- Weitreichende Transparenz gegenüber den betroffenen Personen

Die Vorschriften zu den Zuverlässigkeitsüberprüfungen sehen vor, die von der Zuverlässigkeitsüberprüfung betroffenen Personen über die konkreten Abläufe und Inhalte der Überprüfung vor der Erteilung ihrer Zustimmung in die Zuverlässigkeitsüberprüfung zu informieren. Insoweit sah der LfDI Anpassungsbedarf bzgl. der verwendeten landeseinheitlichen Datenschutzerklärungen. Sie informierten beispielsweise über einen Regelabgleich der erhobenen personenbezogenen Daten der betroffenen Personen mit den Datenbeständen des Verfassungsschutzes. Das POG sieht jedoch vor, dass zum Datenabgleich zunächst einmal grundsätzlich nur polizeiliche Datenbestände einzubeziehen sind, soweit sich nicht schon sachbezogen die Erforderlichkeit ergibt, auf Datenbestände des Verfassungsschutzes zurückzugreifen. Ansonsten ist eine Abfrage beim Verfassungsschutz nur noch aus Gründen, die in der Person liegen, möglich. Da dies zum Zeitpunkt der Zustimmungserteilung noch nicht absehbar ist, die betroffene Person jedoch zu diesem Zeitpunkt informiert werden muss, empfahl der LfDI, die Datenschutzerklärung dahingehend zu ändern, dass zwischen keiner Abfrage, einer sachbezogenen Abfrage und einer potentiell möglichen personenbezogenen Abfrage zu unterscheiden ist, um größtmögliche Transparenz für die betroffene Person zu erreichen.

- Speicherung der Verfahrensunterlagen

Unklarheiten bestanden darüber, durch welche Stelle die konkreten Verfahrensunterlagen, insbesondere die Zustimmungserklärungen und Identitätsnachweise der betroffenen Personen zu speichern sind. Nach Auffassung des LfDI sind Zustimmungserklärung und Kopien der Ausweisdokumente durch die Polizei zu speichern. Sie darf eine Zuverlässigkeitsüberprü-

fung zur Person nur dann durchführen, wenn die betroffene Person zuvor der Überprüfung zugestimmt hat. Die vorherige Zustimmung der betroffenen Personen ist als Verfahrensvoraussetzung zu begreifen, deren Einhaltung die Polizei zu überprüfen und nachzuweisen hat. In der Folge sind die Zustimmungserklärungen daher durch die Polizei zu speichern und zu löschen. Auf diese Weise ist zudem sichergestellt, dass die personenbezogenen Daten unter ausreichenden Sicherheitsvorkehrungen aufbewahrt werden.

- Umfang des einzubeziehenden Personenkreises

Der LfDI machte in den Anhörungsverfahren deutlich, dass die Zuverlässigkeitsüberprüfungen im Umfang der davon betroffenen Personen auf das unbedingt notwendige Maß zu beschränken sind. So ist eine Zuverlässigkeitsüberprüfung von Personen aus dem Dienstleistungssektor nur zulässig, wenn die beiden Voraussetzungen – a) privilegierter Zutritt b) zu einer besonders gefährdeten Veranstaltung – erfüllt sind. Im Anhörungsverfahren war daher darzulegen, welche besonderen Gefahren für die Veranstaltung drohen, die sich gerade durch einen privilegierten Zugang realisieren können. Es muss ein besonderer Gefahrenzusammenhang zwischen der Anwesenheit von Personen im Sicherheitsbereich und der Veranstaltung vorliegen, der erst Anlass für die Zuverlässigkeitsüberprüfung gibt. An die Gefährdungsbewertung sind im Vergleich zur Zuverlässigkeitsüberprüfung des Ordnungsdienstes höhere Anforderungen zu stellen („besonders gefährdete Veranstaltung“). Im Vorfeld einer Veranstaltung bestimmt sich daher die Erforderlichkeit einer Zuverlässigkeitsüberprüfung von Personen des Dienstleistungssektors auch danach, für welche Aufgabe bzw. in welchem Einsatzbereich oder an welchem Einsatzort sie eingesetzt werden. Denn der zu überprüfende Personenkreis kann je nach Veranstaltung eine Vielzahl von Personen betreffen.

- Inanspruchnahme von Auftragsverarbeitern

Der LfDI bewertet die Inanspruchnahme von Auftragsverarbeitern durch die Veranstalter zur Erfüllung von Aufgaben und Pflichten, die mit der Akkreditierung und dazu erfolgenden Zuverlässigkeitsüberprüfungen anfallen, kritisch. Insbesondere dann, wenn damit eine Kenntnisnahme übermittelter besonders sensibler Daten i.S.d. § 67 Abs. 5 S. 1 Nr. 1-5 POG einhergeht. Daher hat der LfDI im Austausch mit dem Ministerium des Innern Rheinland-Pfalz empfohlen, eine Auftragsverarbeitung in diesem grundrechtlich sensiblen Bereich per se auszuklammern oder unter hohe Anforderungen zu stellen. Insbesondere sind die Regelung des Art. 28 DS-GVO bzw. § 54 LDSG bzgl. der Rechte und Pflichten des Verantwortlichen und des Auftragsverarbeiters zu beachten.

Die Feststellungen des LfDI führten dazu, dass die den Zuverlässigkeitsüberprüfungen zugrunde liegende polizeiliche Rahmenkonzeption novelliert wird. An deren Entwurf soll der LfDI im Stellungnahmeverfahren beteiligt werden.

1.2 MonoCam – KI-Anwendung zur Detektierung von Ablenkungsverstößen

In Rheinland-Pfalz wurde im Berichtszeitraum die Nutzung des Verfahrens MonoCam pilotiert und probeweise verwendet. Dies ist ein Kamerasystem, welches mittels einer KI-Software automatisiert Ablenkungsverstöße, die durch die Nutzung von Smartphones verursacht werden, erkennt und festhält. Nach dem Aufbau und der Kalibrierung der Kamera erfolgt eine Echtzeitübertragung der durch das „Analysefeld“ durchfahrenden Fahrzeuge mit Hilfe von 25 Bildern pro Sekunde (keine Videoschleife) auf einen Auswerte-Laptop. Dabei erfasst das System mit Beginn der Echtzeitübertragung sämtliche Fahrzeuge und somit auch personen-

bezogene Daten (insb. Kennzeichen und Fahrzeuginsassen). Eine Verpixelung der personenbezogenen Daten vor der Feststellung eines Verstoßes ist nach Angaben des Herstellers nicht möglich.

Anschließend sucht das System mittels künstlicher Intelligenz zunächst nach dem Kennzeichen des Fahrzeugs und überprüft dessen Herkunft anhand des EU/UN-Unterscheidungszeichens am linken Kennzeichenrand, um die einschlägige Seite des Fahrzeugführenden auswählen zu können (Unterscheidung zwischen „Rechtslenkern" aus Großbritannien und „Linkslenkern" aus den übrigen Staaten). In einem weiteren Schritt sucht das System nach der Windschutzscheibe sowie einem möglichen Mobiltelefon im Bereich des Fahrzeugführenden. Hierbei wird neben einem Mobiltelefon auch eine entsprechende Handbewegung bewertet. Grundlage dieser auf künstlicher Intelligenz basierenden Erkennung sind typische Abmessungen sowie Formen und Farben von Mobiltelefonen, die dem System mit über zwei Millionen Vergleichsbildern „antrainiert" wurden. Erkennt das System eine Zugehörigkeit zwischen Mobiltelefon, Handbewegung und Handhaltung, wird ein potentieller Treffer generiert. Hierfür benötigt die Software einen technisch nicht bestimmbaren Zeitraum, der in der Fachsprache mit einer „technischen Sekunde" beschrieben wird und somit von einer äußerst geringen Dauer ist.

Sämtliche potentielle Treffer werden im Anschluss unmittelbar durch das Auswertepersonal geprüft und auf ihre Tatbestandsmäßigkeit verifiziert. Falsch positive Treffer (z.B. Erkennung einer Zigarettenschachtel als Mobiltelefon oder Mobiltelefon in einer entsprechenden Halterung) werden manuell sowie spurenlos gelöscht.

Gegenstand der Beratungen des LfDI im Vorfeld des Pilotversuchs waren u.a. die Frage der Rechtsgrundlage für die Nutzung des Verfahrens. Dabei wurde angeführt, dass grundsätzlich bereits die der eigentlichen Datenspeicherung vorausgehende Datenerhebung via Livestream einer Rechtsgrundlage bedarf. Die Polizei Rheinland-Pfalz hat auf die gefahrenabwehrrechtliche Natur der Maßnahme abgestellt und § 29 Abs. 2 S. 1 Nr. 3 POG als Rechtsgrundlage angeführt. Dieser erlaubt die Erhebung personenbezogener Daten dann, wenn eine konkrete Gefahr für den Straßenverkehr besteht. Diese Gefahr wäre in der konkreten Fallkonstellation erst dann zu bejahen, wenn ein Treffer vorliegen würde. Durch den Livestream werden dagegen bereits zuvor personenbezogene Daten (unverpixelt) erhoben. In seiner Entscheidung zur automatisierten Kennzeichenerfassung hat das Bundesverfassungsgericht (BVerfGE 150, 244-309) dagegen entschieden, dass eine automatisierte Kraftfahrzeugkennzeichenkontrolle Eingriffe in das Grundrecht auf informationelle Selbstbestimmung aller Personen begründet, deren Kennzeichen in die Kontrolle einbezogen werden, auch wenn das Ergebnis zu einem „Nichttreffer" führt und die Daten sogleich gelöscht werden (Abweichung von BVerfGE 120, 378). Insofern ist fraglich, ob die Datenerhebungsgeneralklausel diesem Eingriff gerecht wird, insbesondere vor dem Hintergrund, dass anlasslos Unbeteiligte erfasst werden.

Bestimmte Anforderungen, die der LfDI gefordert hat und auch umgesetzt wurden, sollen das Eingriffsgewicht in Bezug auf die Erfassung personenbezogener Daten Unbeteiligter abschwächen:

- die beabsichtigte Datenverarbeitung dauert im Falle eines Nichttreffers nur wenige Sekunden an;
- die Auswertung des Livestreams erfolgt lediglich automatisiert;
- eine Speicherung wird erst im Verdachtsfall vorgenommen;
- es erfolgt unverzüglich eine Überprüfung des Treffers und eine

spurenlose Löschung im Fall eines falsch-positiven Treffers;

- die Datenverarbeitung ist vorerst lediglich im Rahmen eines Pilotprojektes zeitlich befristet und auf bestimmte Strecken beschränkt vorgesehen;
- die Datenerhebung erfolgt offen aufgrund der Nutzung eines Hinweisschildes und entsprechender Informationen im Internet.

Nach dieser Maßgabe war das Vorgehen auf Grundlage der Datenerhebungsgeneralklausel des § 29 Abs. 2 Satz 1 Nr. 3 POG (zeitlich befristet für die Dauer des Pilotversuches) als hinnehmbar bewertet worden. Dabei ist jedoch darauf hingewiesen worden, dass bereits die Existenz des § 30 Abs. 1 POG als spezielle Rechtsgrundlage zur Datenerhebung mit technischen Mitteln die Anwendung der Datenerhebungsgeneralklausel ausschließen könnte. Des Weiteren wurde im Zusammenhang mit dem bestehenden rechtlichen Risiko, welches insbesondere durch die im Rahmen des Pilotversuches für notwendig erachtete Ahndung von Verstößen eintritt, die Heranziehung der Datenerhebungsgeneralklausel als kritisch bewertet.

Im Ergebnis hat der LfDI einem halbjährigen Pilotbetrieb auf der Grundlage der Generalklausel zugestimmt, dabei jedoch deutlich gemacht, dass für einen verstetigten Einsatz über sechs Monate hinaus eine eigenständige Rechtsgrundlage geschaffen werden muss. Vor diesem Hintergrund soll voraussichtlich im Jahr 2023 das Polizei- und Ordnungsbehördengesetz novelliert werden.

1.3 Programm Polizei 20/20 – Proof of Concept Datenkonsolidierung

Infolge der sog. Saarbrücker Agenda der Innenminister des Bundes und der Länder wurde das Programm Polizei 20/20 gegründet. Es hat zum Ziel, die polizeiliche IT-Architektur in Deutschland umzustrukturieren und die bislang heterogene IT-Landschaft zu harmonisieren und zu modernisieren. Dabei werden drei Kernziele des Programms herausgehoben: die Verbesserung der Verfügbarkeit polizeilicher Informationen, die Erhöhung der Wirtschaftlichkeit und die Stärkung des Datenschutzes durch Technik. Das Programm steht unter der Leitung des Bundeministeriums des Innern und für Heimat (BMI). Es sind alle 20 deutschen Polizeien beteiligt, so auch die Polizei des Landes Rheinland-Pfalz. Das Programm organisiert sich im Rahmen von zahlreichen Unterprojekten, die bestimmte Programmteilnehmer als Themenführer leiten. Der LfDI Rheinland-Pfalz ist sich der Bedeutung und Tragweite des Programms bewusst und begleitet es sowohl im Rahmen des Arbeitskreises Sicherheit der DSK als auch bilateral im Austausch mit den Programmverantwortlichen in Rheinland-Pfalz.

Das Landeskriminalamt des Landes Rheinland-Pfalz ist gemeinsam mit zwei weiteren Ländern Projektverantwortlicher des Projekts „Proof of Concept Datenkonsolidierung“, welches als Teilprojekt in das Programm Polizei 20/20 eingegliedert wurde. Bei dem PoC handelt es sich um eine Machbarkeitsstudie für ein Informationssystem, das unterhalb der Verbundschwelle des §§ 29 f. BKAG einen Austausch von Erkenntnissen zunächst zwischen den Polizeibehörden der beteiligten drei Bundesländer ermöglichen soll. Intendiertes Ziel ist unter anderem, das bisherige Verfahren zu sog. Erkenntnisabfragen zu ersetzen sowie die Feststellung einer etwaigen Verbundrelevanz von Daten zu erleichtern. Im Erfolgsfalle der Machbarkeitsstudie wurde seitens der Polizei eine bundesweite Ausweitung des Systems angestrebt.

Das Konzept wurde dem Landesdatenschutzbeauftragten Rheinland-Pfalz im Jahr 2018 vorgestellt und seitdem begleitet. Infolgedessen hat der LfDI zu dem Konzept im Jahr 2020 Stellung genommen und erhebliche Bedenken gegen die Funktionsweise des PoC geäußert. Bei einer erneuten Vorstellung des aktuellen Stands des Projekts in einem Workshop des BMI und der Kerngruppe Datenschutz des Programms Polizei 20/20 im November 2021 wurde aufgezeigt, dass den geäußerten Bedenken der zuständigen Landesdatenschutzbeauftragten seitens der Polizei bisher nicht ausreichend Rechnung getragen wurde. Des Weiteren wurde signalisiert, das erarbeitete Verbundsystem nunmehr mit Echt-Daten in Betrieb nehmen zu wollen. Aus diesen Gründen hat der LfDI – abgestimmt mit den beiden weiteren zuständigen Landesdatenschutzaufsichtsbehörden – eine Warnung gem. § 42 Abs. 1 Satz 5 LDSG gegen die geplante Funktionsweise des „Proof of Concept Datenkonsolidierung“ dahingehend ausgesprochen, dass das beabsichtigte Datenverarbeitungsverfahren in der Form, wie es am 08.11.2021 vorgestellt wurde, voraussichtlich gegen die einschlägigen datenschutzrechtlichen Vorschriften verstößt. Dies betraf insbesondere die Ausgestaltung des Verfahrens, das infolge des Abrufs eine zunächst teilnehmerübergreifende Übermittlung von Grunddaten vorsieht und dem abrufenden Teilnehmer im Anschluss daran Zugang zu weiteren bei den anderen Teilnehmern gespeicherten täter- oder tatbezogenen Informationen gewährt, ohne dass die gesetzlichen Voraussetzungen hierfür vorliegen. Die Prüfung der zuständigen Landesdatenschutzaufsichtsbehörden hat ergeben, dass die geplante Funktionsweise nicht im Einklang mit den Grundsätzen des Bundesverfassungsgerichts zur sog. hypothetischen Datenneuerhebung und diese umsetzenden rechtlichen Grundlagen steht.

Infolge der Warnungen wurde der beabsichtigte Echt-Betrieb vorerst gestoppt, bis eine Klärung der rechtlichen Fragestellungen erfolgt. Das Landeskriminalamt hat eine ausführliche Stellungnahme zu den Problemstellungen abgegeben, die jedoch weiterhin zu keinem Konsens führte.

Gleichwohl hat der Austausch zum PoC auch ohne Echt-Betrieb sowohl die beteiligten Datenschutzaufsichtsbehörden als auch die Projektverantwortlichen zu grundlegenden Fragestellungen in Bezug auf die hypothetische Datenneuerhebung weitergebracht und konnte in weiterführenden Teilprojekten zu begrüßenswerten Ergebnissen führen. Dazu kann voraussichtlich im nächsten Tätigkeitsbericht mehr berichtet werden.

2. JUSTIZ

2.1 Verarbeitung von personenbezogenen Daten aus der Corona-Kontaktdatenerfassung durch Strafverfolgungsbehörden

Nach den pandemiebedingten sogenannten Lockdowns war es wichtig, u.a. die Gastronomie wieder zur Teilnahme am Geschäftsleben zu befähigen und gleichzeitig das Infektionsrisiko weiterhin zu managen. Ein Instrument dazu war die Pflicht zur Kontaktdatenerfassung der Gäste, die sich in den betreffenden Einrichtungen aufhielten. Der LfDI hat sich dabei stets dafür stark gemacht, dass nur die erforderlichen Daten erfasst werden und diese ausschließlich zum Zwecke der Kontakterfassung verwendet werden. Schließlich wurde auch in § 28 a Abs. 1 Nr. 17, Abs. 4 S. 3, 6 Infektionsschutzgesetz (IfSG) alte Fassung diese enge Zweckbindung festgeschrieben. Zu Beginn des Berichtsjahres hat der LfDI von der Verarbeitung personenbezogener Daten aus der Corona-Kontaktdatenerfassung durch Strafverfolgungsbehörden zu Ermittlungszwecken Kenntnis erlangt und umgehend aufsichtsrechtliche Verfahren eingeleitet. Hintergrund war folgender Sachverhalt:

In Abstimmung mit der Staatsanwaltschaft Mainz haben die Ermittlungsbeamten der Polizei Mainz das Gesundheitsamt der Kreisverwaltung Mainz-Bingen zwecks Ermittlung potentieller Zeugen im Rahmen eines Ermittlungsverfahrens aufgrund eines Vorfalls, der sich in der Nacht auf den 30.11.2021 in der Nähe einer Mainzer Gastwirtschaft ereignete, um die Übermittlung der über die Luca-App erfassten Kontaktdatenliste der zu dem Unfallzeitpunkt in der Gastwirtschaft anwesenden Gäste ersucht. Nach Bereitstellung der entsprechenden Kontaktdatenliste in Form einer passwortgeschützten Excel-Datei durch das Gesundheitsamt, die die Personendaten von 48 Personen enthielt, haben die Ermittlungsbeamten der Polizei Mainz einen Teil dieser Gäste kontaktiert, wobei die gesamte Vorgehensweise mit der Staatsanwaltschaft Mainz abgestimmt gewesen ist. Zeitgleich sicherten Ermittlungsbeamte der Polizei nach vorheriger Zustimmung der zuständigen Staatsanwaltschaft in der Gastwirtschaft die Kopien der Gäste-Kontaktlisten des Tatabends, wobei es sich um 21 Kontaktformulare handelte.

Die durch die Staatsanwaltschaft Mainz autorisierten Erhebungen und Nutzungen der Kontaktdaten in Form der Kontakterfassungsbögen sowie der aus der Luca-App stammenden Kontaktdaten waren rechtswidrig. Denn in § 28 a Abs. 1 Nr. 17, Abs. 4 S. 3, 6 IfSG in Verbindung mit § 160 Abs. 4 Strafprozessordnung (StPO) und dem in seinem Regelungsgehalt gleichlautenden § 3 Abs. 4 S. 6 der 29. rheinland-pfälzischen Corona-Bekämpfungsverordnung (29. CoBeLVO) war ein ausdrückliches Verwendungsverbot zu anderen Zwecken als der Nachverfolgung und Unterbrechung von Infektionsketten normiert. Die Verwendung der Kontakterfassungsdaten zu Strafverfolgungszwecken stellte daher eine unrechtmäßige Zweckänderung und damit einen ungerechtfertigten Eingriff in das nach Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG gewährleistete Recht auf informationelle Selbstbestimmung dar.

Im Ergebnis hat der LfDI einen Verstoß gegen § 28 Abs. 2 Ziff. 1 Landesdatenschutzgesetz (LDSG) i.V.m § 26 Abs. 1 LDSG i.V.m. § 160 Abs. 4 StPO i.V.m. § 28 a Abs. 1 Nr. 17, Abs. 4 S. 3, 6 IfSG alte Fassung i.V.m. mit § 3 Abs. 4 S. 6 der 29 rheinland-pfälzischen Corona-Bekämpfungsverordnung (29. CoBeLVO) festgestellt, den er gegenüber dem Ministerium der Justiz des Landes Rheinland-Pfalz beanstandet hat.

Der LfDI nahm dies außerdem zum Anlass, erneut für das Thema zu sensibilisieren. Die Generalstaatsanwaltschaft Koblenz hat in diesem Zusammenhang die rheinland-pfälzischen Staatsanwaltschaften auf die rechtlichen Voraussetzungen für einen Datenzugriff hingewiesen und auch die Präsidenten der jeweiligen Polizeipräsidien unterrichtet. Durch die Ab-

kehr von der Verpflichtung zur Kontakterfassung und der Kündigung des Kooperationsvertrages mit den Betreibern der Luca-App sind vergleichbare Vorfälle künftig nicht mehr zu erwarten.

2.2 Elektronische Kommunikation

Die Kommunikation erfolgt heutzutage größtenteils digital, etwa mittels E-Mail. Sobald dabei aber personenbezogene Daten enthalten sind, sind die datenschutzrechtlichen Anforderungen an die Datensicherheit zu beachten. Der LfDI hat in dem Berichtszeitraum aufgrund von mehreren Beschwerden insbesondere bei Berufsgeheimnisträger:innen (z.B. Rechtsanwält:innen) diesbezüglich bestehende Unsicherheiten festgestellt.

Nach Artikel 32 DS-GVO haben Verantwortliche für ein angemessenes Schutzniveau geeignete technische und organisatorische Maßnahmen zu ergreifen. Nach Art. 5 Abs. 1 lit. f DS-GVO müssen Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Hierzu gehört etwa der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen. In der Konsequenz müssen Berufsgeheimnisträger:innen daher E-Mail-Kommunikation, die personenbezogene Daten enthält, dem Stand der Technik entsprechend datensicher organisieren.

E-Mails, die personenbezogene Daten enthalten, sollten daher mindestens mit einer „Transportverschlüsselung“ versendet werden. Bei besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO und damit besonders sensiblen Daten, wie Gesundheitsdaten, sollte zudem eine „Ende-zu Ende“-Verschlüsselung vorgenommen werden. Denn auf diese Weise wird neben dem Transportweg auch der Inhalt der E-Mail geschützt. Bei der Beurteilung eines angemessenen Schutzniveaus der elektronischen Kommunikation muss damit immer auf die Inhalte der jeweiligen E-Mails abgestellt werden.

Hinsichtlich der einzelnen technischen Anforderungen an die Verschlüsselung kann insbesondere die Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021 (Stand 16.07.2021) herangezogen werden (**https://s.rlp.de/email**).

2.3 Insolvenzverwalter:innen als datenschutzrechtlich Verantwortliche

Im Rahmen einer an den LfDI herangetragenen Beschwerde wurde eine datenschutzrechtliche Verantwortlichkeit von Insolvenzverwalter:innen infrage gestellt.

Der LfDI ist in Einigkeit mit den deutschen Datenschutzaufsichtsbehörden allerdings der Auffassung, dass Insolvenzverwalter:innen spätestens mit Eröffnung des Insolvenzverfahrens als eigenständige Verantwortliche gem. Art. 4 Nr. 7 DS-GVO anzusehen sind. Denn nach Art. 4 Nr. 7 DS-GVO ist „Verantwortliche“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. In datenschutzrechtlicher Hinsicht maßgeblich ist damit der Zeitpunkt der tatsächlichen und rechtlichen Entscheidungshoheit bezüglich der berührten Datenverarbeitungsvorgänge. Ausschlaggebend ist insoweit vorrangig die Entscheidungsbefugnis über den Zweck, also das Ob, Wofür und Wieweit einer Datenverarbeitung. Für eine entsprechende Auslegungsweise des Begriffs „Verantwortliche“ spricht auch der Sinn und Zweck des Art. 4 Nr. 7 DS-GVO, einen wirksamen und umfassenden Schutz der betroffenen

Personen zu gewährleisten.

Mit der Eröffnung des Insolvenzverfahrens geht die Verwaltungs- und Verfügungsbefugnis über das schuldnerische Vermögen auf den Insolvenzverwalter über (§ 80 Abs. 1 InsO), wodurch der Insolvenzverwalter gleichsam Einflussmöglichkeiten im Hinblick auf massebezogene Datenverarbeitungsvorgänge erhält. Dem Schuldner verbleibt ab dem Zeitpunkt des Eröffnungsbeschlusses dagegen keine entsprechende Entscheidungshoheit mehr.

3. VIDEOÜBERWACHUNG

Das Jahr 2022 war erneut von Beschwerden aus dem nachbarschaftlichen Bereich geprägt. Da der LfDI nicht überprüfen kann, ob sich die Videoüberwachung verändert (z.B. durch Änderung der Ausrichtung der Videokameras), wird in diesen Fällen häufig auf den Zivilrechtsweg verwiesen. Im Jahr 2022 wurden insgesamt fast 400 Verfahren eingeleitet und 78 schriftliche Beratungen durchgeführt. Hieran lässt sich erkennen, dass die Überprüfung der Videoüberwachung weiterhin stetig zunimmt. Ursächlich dafür ist die Tatsache, dass vermehrt die Anbringung einer Videokamera durch Verantwortliche als effektivstes Mittel zum Schutz des Eigentums bzw. zum Schutz vor Straftaten gesehen wird, gleichzeitig jedoch immer mehr Personen eine Anbringung einer Videokamera und einer vermeintlichen dauerhaften Überwachung ihrer Umgebung widersprechen. In diesem Zusammenhang konnte insbesondere bei der Überprüfung von Videokameras im nachbarschaftlichen Kontext bemerkt werden, dass die abschließenden Feststellungen und die datenschutzrechtlichen Bewertungen des LfDI sowohl auf Seiten der Verantwortlichen als auch auf Seiten der Beschwerdeführer:innen hinterfragt wurden und zu erneuten Überprüfungen angeregt wurde.

Des Weiteren fiel auf, dass einige Verantwortliche davon ausgingen, eine Klingelkamera zu verwenden, wobei sich im Rahmen der Überprüfung herausstellte, dass es sich tatsächlich um eine Videokamera handelte, die ein Monitoring durchführte. In diesen Fällen erfolgten vermehrt weitere Erläuterungen zu Klingelkameras. So darf eine Türklingelkamera u.a. nur anlassbezogen durch das Klingeln aktiviert werden und nur den unmittelbaren Nahbereich vor der Tür erfassen.

Die zahlreichen Eingaben im Bereich der Videoüberwachung führten ferner dazu, dass, insbesondere zur Ermittlung der verantwortlichen Stelle, die Hilfe anderer Behörden oder Stellen hinzugezogen werden musste.

Im gewerblichen Bereich erreichten den LfDI vermehrt Hinweise bzgl. potenzieller Videoüberwachungen in Gastronomiebetrieben. Als Zweck für die Videoüberwachung wird vereinzelt der Schutz des Eigentums (Mobiliar der Gaststätten) oder die Feststellung der Anzahl der anwesenden Kund:innen genannt. Dass der Besuch einer Gaststätte auch der Freizeitgestaltung zugeordnet wird und demnach die Entfaltung der Persönlichkeit betroffen ist, scheint in die Entschließung, eine Videoüberwachung durchzuführen, kaum einbezogen zu werden. Ebenso verhält es sich mit der Tatsache, dass grundsätzlich auch die Erfassung der Beschäftigten stattfindet bzw. stattfinden kann.

Prinzipiell wird bei den Überprüfungen deutlich, dass die Verantwortlichen auch hinsichtlich der Voraussetzung der Erforderlichkeit der Videoüberwachung zu sensibilisieren sind. Mildere Mittel zur Videoüberwachung werden selten vor der Anbringung der Videokameras in Betracht gezogen.

In den meisten Fällen entsprachen auch die Hinweisschilder nicht den Anforderungen an die Informationspflichten gem. Art. 12, Art. 13 DS-GVO, sodass auf eine Nachbesserung der Hinweisschilder hingewirkt und die Verantwortlichen bzgl. ihrer Pflichten sensibilisiert werden mussten. Die Bitte an die Verantwortlichen, die benötigten Informationen (insbesondere die Kontaktdaten) in das Hinweisschild einzubeziehen, traf bei einigen Verantwortlichen auf Unverständnis.

Durch öffentliche Stellen finden Beratungsanfragen weiterhin in großem Umfang statt. Die Zwecke für die geplanten Videoüberwachungen öffentlich zugänglicher Bereiche waren auch in diesem Jahr überwiegend die Vandalismusbekämpfung und das Verhindern bzw. die Verfolgung illegaler Müllablagerungen.

Im Ergebnis wurden auch die öffentlichen Stellen dazu angehalten, mildere Mittel in Betracht zu ziehen und konkretere Angaben (z.B. zur Schadenshöhe) nachzureichen.

Ferner ist festzustellen, dass auch vermehrt Eingaben hinsichtlich potenzieller Videoüberwachungen an Veranstaltungen eingehen. Dies beruht vermutlich darauf, dass aufgrund der Lockerung der im Rahmen der Pandemie getroffenen Maßnahmen wieder vermehrt Veranstaltungen stattfinden

4. WIRTSCHAFT

4.1 Datenverarbeitung durch Private in Zeiten von Corona

In den Tätigkeitsberichten für die Jahre 2020 (vgl. 29. Tb. Tz. 4.1) und 2021 (vgl. 30. Tb. Tz. 4.1) wurde ausführlich über die datenschutzrechtlichen Anforderungen an die verschiedenen Coronaschutzmaßnahmen berichtet. Ab dem Frühjahr 2022 jedoch entfiel neben Abstandsgebot, Kapazitäts- und Kontaktbeschränkungen auch die Verpflichtung, Kontaktdaten von Besucher:innen zu erheben, die bis zuletzt noch in bestimmten Einrichtungen des Gesundheitsbereichs bestand. Dies bedeutete, dass sich aus der Corona-Bekämpfungsverordnung (in Verbindung mit dem Infektionsschutzgesetz) keine Rechtsgrundlage und damit auch keine Verpflichtung mehr dafür ergab, die Kontaktdaten von Gästen, Kund:innen oder Besucher:innen zu erheben und vorzuhalten.

In der Folge gab es lediglich einzelne Hinweise, dass die erhobenen Kontaktdaten evtl. zweckentfremdet für Werbemaßnahmen genutzt wurden. Die Verantwortlichen wurden vom LfDI darauf hingewiesen, dass eine solche Nutzung unzulässig ist und die Daten unverzüglich zu löschen sind.

4.2 Online-Handel

Die Datenschutzkonferenz hat im März 2022 Hinweise zur Einrichtung von Gastkonten im Online-Handel beschlossen (vgl. Beschluss der Datenschutzkonferenz vom 24. März 2022 „Hinweise der DSK – Datenschutzkonformer Online-Handel mittels Gastzugang“).

Hintergrund ist, dass Online-Händler oftmals Bestellungen nur ermöglichen, wenn ein dauerhaftes Kundenkonto angelegt wird. Dies hat zur Folge, dass oftmals mehr personenbezogene Daten für einen längeren Zeitraum vorgehalten und auch genutzt werden als für eine einmalige Bestellung erforderlich sind. Dies widerspricht dem Grundsatz der Datenminimierung. Die Datenschutzkonferenz fordert daher die Möglichkeit, als Gast zu bestellen, wenn man kein Kundenkonto einrichten möchte. Die entsprechenden Hinweise sind abrufbar unter **https://s.rlp.de/gastkonto**.

4.3 Das Auskunftsrecht und die Auskunftspflicht

Das in Art. 15 DS-GVO vorgesehene Auskunftsrecht beschäftigt den LfDI dauerhaft. Hieran knüpfen sich zahlreiche Fragen, wie etwa Inhalt und Umfang der Auskunft, das Recht auf Kopie oder die Identifizierung des Auskunftsberechtigten. Auch gibt es mittlerweile eine umfangreiche, aber teilweise auch recht uneinheitliche Rechtsprechung zu diesen Fragen.

Nach Auffassung des LfDI ist der Auskunftsanspruch nach Art. 15 DS-GVO weit und damit besonders betroffenenfreundlich auszulegen. Davon sind auch zum Beispiel interne Vermerke und E-Mailkommunikation erfasst. Darüber hinaus sind grundsätzlich die erforderlichen Unterlagen in Kopie zur Verfügung zu stellen, sofern sie Informationen zu der betroffenen Person enthalten. Dies bedeutet, dass auch bereits bekannte Korrespondenz (z.B. Schreiben und E-Mails) zu übermitteln sind. Seine Grenze findet der Anspruch auf Auskunft bei rein rechtlichen Analysen und Beurteilungen (vgl. BGH Urteil vom 15.06.2021 – VI ZR 576/19, Randnummern 26, 28, 29, 32).

Grundsätzlich kann die Auskunft in einem gestuften Verfahren erteilt werden, insbesondere dann, wenn die Informationen umfangreich sind. Zunächst wird der betroffenen Person ein Überblick gegeben und sie sodann um weitere Präzisierung gebeten, so dass in einem zweiten Schritt die konkreten Informationen beauskunftet werden können.

Die erteilte Information muss vollständig sein, es sei denn, die betroffene Person grenzt ihr Auskunftsbegehren ein. Zudem müssen die Informationen richtig und aktuell sein.

Alle Informationen nach Art. 15 Abs. 1 DS-GVO sind konkret auf die betroffene Person bezogen zu erteilen, der Verweis auf die allgemeinen Informationen gem. Art. 13 und 14 DS-GVO reicht nicht aus.

4.4 Auskunft durch Kreditinstitute

Im Bereich der Kreditinstitute gibt es immer wieder Sonderfragen insbesondere zum Umfang der Auskunft.

Vom Auskunftsanspruch gegen ein Kreditinstitut sind „persönliche Informationen wie Identifikationsmerkmale (z.B. Name, Anschrift und Geburtsdatum), äußere Merkmale (wie Geschlecht, Augenfarbe, Größe und Gewicht) oder innere Zustände (z.B. Meinungen, Motive, Wünsche, Überzeugungen und Werturteile), als auch sachliche Informationen wie etwa Vermögens- und Eigentumsverhältnisse, Kommunikations- und Vertragsbeziehungen und alle sonstigen Beziehungen der betroffenen Person zu Dritten und ihrer Umwelt“ (AG Bonn Urteil vom 30.07.2020 – 118 C 315/19, RN 30) erfasst. „Auch solche Aussagen, die eine subjektive und/oder objektive Einschätzung zu einer identifizierten oder identifizierbaren Person liefern, weisen einen Personenbezug auf. Der Auskunftsanspruch umfasst in Ansehung dieser Grundsätze daher mehr als nur die Stammdaten“ (AG Bonn Urteil vom 30.07.2020 – 118 C 315/19, RN 30).

Danach sind auch Kontobewegungen vom Auskunftsanspruch erfasst. „Diese stellen sachliche Informationen im Hinblick auf die Eigentums- und Vermögensverhältnisse des Betroffenen dar“ (AG Bonn Urteil vom 30.07.2020 – 118 C 315/19, RN 30).

Auch wenn betroffene Personen bereits Kenntnis der Kontobewegungen über die ihnen zur Verfügung gestellten Kontoauszüge haben, erlischt der Anspruch nach Art. 15 DS-GVO nicht. Denn das Bereitstellen der Auszüge erfüllt eine zivilrechtliche, also bankenrechtliche Pflicht aus dem Zahlungsdienstevertrag, aber nicht die datenschutzrechtliche Verpflichtung zur Auskunft gem. Art. 15 DS-GVO.

Beauskunftet werden können aber nur solche personenbezogenen Daten, die auch noch vorhanden sind, also gespeichert werden. In der Regel beträgt die Aufbewahrungsfrist zehn Jahre. Dies ergibt sich aus dem Handelsgesetzbuch und der Abgabenordnung. Laut § 257 des Handelsgesetzbuches ist jeder zur Aufbewahrung wichtiger Dokumente verpflichtet, der nach dem Steuer- und Handelsrecht zum Führen von Büchern und Aufzeichnungen angehalten ist. Demnach gilt für Banken nichts anderes als für jedes andere Handelsunternehmen auch: Neben Kontoauszügen müssen beispielsweise auch Handelsbücher, Bilanzen, Jahresabschlüsse sowie Lageberichte zehn Jahre lang aufbewahrt werden. Zudem gibt es nach § 147 der Abgabenordnung eine steuerrechtliche Aufbewahrungspflicht von Kontoauszügen von ebenfalls zehn Jahren.

4.5 Sonderfall: Auskünfte aus Gutachten

In Gutachten findet man zumeist personenbezogene Daten und andere Informationen wie z.B. Bewertungskriterien vermischt. Hier herrscht oft Unklarheit, über welche Informationen tatsächlich Auskunft erteilt werden muss, insbesondere dann, wenn eine Kopie verlangt wird. Dann fällt es Verantwortlichen oft schwer, zwischen personenbezogenen Daten und anderen Informationen, die nicht dem Auskunftsanspruch gem. Art. 15 DS-GVO unterfallen, zu unterscheiden mit der Folge, dass die Herausgabe des gesamten Gutachtens verweigert wird.

Zu den personenbezogenen Daten gehören auch „subjektive“ Informationen, Meinungen oder Beurteilungen, die für Entscheidungen herangezogen werden. Interne abstrakte Bewertungskriterien, die keine personenbezogenen Daten enthalten, und die ansonsten verwendete abstrakte Bewertungslogik sind nicht zu beauskunften. Folglich sind diejenigen Inhalte des Gutachtens zu beauskunften, die personenbezogene Daten darstellen. Sachdaten sind regelmäßig nicht erfasst.

Folglich darf der Verantwortliche nicht pauschal die Herausgabe verweigern, sondern muss einzelfallbezogen prüfen, welche Teile des Gutachtens er beauskunften muss und welche nicht. Selbstverständlich darf der Verantwortliche auch alle Daten herausgeben, also das gesamte Gutachten. Nur stehen hier meist Bedenken entgegen, weil so evtl. Geschäftsgeheimnisse offenbart werden könnten. Dies führt dann letztlich dazu, dass eine etwas aufwendigere Prüfung durchzuführen ist, um die Daten zu unterscheiden.

5. LEBEN DIGITAL

5.1 Einsicht in Unterlagen einer Wohnungseigentümergemeinschaft zwecks Nutzung zu Werbezwecken

Der LfDI erhielt im Jahr 2022 gehäuft Beschwerden und Anfragen von Wohnungseigentümer:innen, welche etwa von Makler:innen oder Miteigentümer:innen bezüglich etwaiger Verkaufsabsichten kontaktiert wurden. Häufig stellte sich im Rahmen der Ermittlungen heraus, dass die Kontaktsuchenden die Kontaktdaten der betroffenen Wohnungseigentümer:innen durch Einsicht in die Verwaltungsunterlagen der Wohnungseigentümergemeinschaft (WEG) erhalten haben. Ein solches Einsichtsrecht ergibt sich aus § 18 Abs. 4 Wohnungseigentumsgesetz (WEG). Danach kann jeder Wohnungseigentümer von der Gemeinschaft der Wohnungseigentümer Einsicht in die Verwaltungsunterlagen verlangen.

Nach Ansicht des LfDI ist die Nutzung von personenbezogenen Daten, welche im Wege des Einsichtsrechts nach § 18 Abs. 4 WEG erhoben worden sind, zu werblichen Zwecken, etwa der Einholung von Verkaufsinteressen, unzulässig.

Zwar kann gemäß § 18 Abs. 4 WEG jeder Wohnungseigentümer von der Gemeinschaft der Wohnungseigentümer Einsicht in die Verwaltungsunterlagen verlangen. Aufgrund des umfassenden Einsichtsrechts in die Verwaltungsunterlagen der WEG haben Miteigentümer auch einen Anspruch auf Übermittlung von Kontaktdaten der Miteigentümer, z.B. in Form einer Eigentümerliste. Umfasst von diesem Anspruch sind jedoch nur der Name und die Anschrift der Eigentümer, nicht jedoch deren E-Mail-Adresse und Telefonnummer.

Die Nutzung von personenbezogenen Daten, welche im Rahmen der Einsicht in die Verwaltungsunterlagen (z. B. die Eigentümerliste) erhoben worden sind, zu Werbezwecken ist in der Regel jedoch nicht zulässig, soweit hierfür keine ausdrücklichen Vereinbarungen oder Einwilligungen der Betroffenen vorliegen. In aller Regel dürfte der Zweck der Verarbeitung im Rahmen der WEG maßgeblich in der Verwaltung des gemeinschaftlichen Eigentums liegen. Eine Nutzung für Werbezwecke Einzelner ist in der Regel von diesem Zweck nicht gedeckt und erfolgt daher rechtswidrig. Der Hausverwaltung ist daher zu raten, bei der Einsichtnahme darauf hinzuweisen, dass die Daten nur für Verwaltungszwecke genutzt werden dürfen.

Diese Ansicht beruht auf folgenden Erwägungen:

Die Verarbeitung von personenbezogenen Daten ist nur dann zulässig, wenn hierfür eine einschlägige Rechtsgrundlage vorhanden ist. Sofern keine Einwilligung vorliegt, kann eine Verarbeitung etwa u.a. rechtmäßig sein, wenn diese gem. Art. 6 Abs. 1 lit. b DS-GVO zur Erfüllung eines Vertrages (z.B. Hausverwaltervertrag) oder gem. Art. 6 Abs. 1 lit. c DS-GVO aufgrund einer rechtlichen Verpflichtung (z.B. durch den Hausverwalter im Rahmen des Einsichtsrechts nach § 18 Abs. 4 WEG) oder gem. Art. 6 Abs. 1 lit. f DS-GVO zur Wahrung berechtigter Interessen erforderlich ist.

In Bezug auf Werbung kann als Rechtsgrundlage zwar vorliegend Art. 6 Abs. 1 lit. f DS-GVO in Betracht kommen, dieser dürfte im Ergebnis jedoch abzulehnen sein, so dass die Nutzung der Daten zu Werbezwecken in der Regel unzulässig ist.

Gemäß Art. 6 Abs. 1 lit. f DS-GVO ist die Verarbeitung rechtmäßig, wenn diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z.B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht. Dies ist in den meisten der einschlägigen Beschwerden jedoch nicht der Fall.

Auf jeden Fall wäre das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen. Eigentümer:innen müssen grundsätzlich nicht damit rechnen, dass ihre personenbezogenen Daten durch Miteigentümer:innen für die Werbung eigener Geschäftstätigkeit genutzt werden. Hierbei ist auch zu berücksichtigen, dass die Daten von der WEG bzw. der Verwaltung in der Regel ausschließlich zum Zwecke der ordentlichen Hausverwaltung erhoben worden sind. Gemäß Art. 5 Abs. 1 lit. b DS-GVO müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. In den vorliegenden Fallgestaltungen werden die Daten in der Regel zweckwidrig weiterverarbeitet, indem diese für Werbezwecke genutzt werden, die von dem ursprünglichen Zweck (Verwaltung) abweichen.

Dem Vorgehen, durch Geltendmachung des Einsichtsrechts nach § 18 Abs. 4 WEG personenbezogene Daten für Zwecke der Direktwerbung zu verarbeiten, stehen ebenso regelmäßig die Grundsätze einer fairen und transparenten Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 lit. a und Art. 12 Abs. 1 DS-GVO entgegen.

5.2 Übermittlung personenbezogener Daten durch Vermieter an Sozialhilfeträger

Den LfDI erreichten im Jahr 2022 mehrere Beschwerden von Mieter:innen, in denen deren Vermieter:innen Details zu dem Mietverhältnis zur Höhe des Mietzinses oder zur Höhe von vorgenommenen Mietminderungen an den Träger der Sozialhilfe übermittelten.

Die Übermittlung von Daten zur Höhe des Mietzinses bzw. zu erfolgten Mietminderungen erfolgten in einem Fall auf konkrete Anfrage des Sozialhilfeträgers und in einem anderen Fall aus eigener Initiative der Vermieterin heraus. Die betroffenen Mieter:innen hatten hierin weder eingewilligt noch wurden diese zuvor informiert.

Unabhängig davon, ob die Übermittlung auf Anfrage eines Sozialhilfeträgers oder auf eigene Initiative durch Vermieter:innen erfolgte, war diese in den vorliegenden Fällen rechtswidrig, da für die Übermittlung keine Rechtsgrundlage vorlag.

Die Übermittlung war insbesondere nicht gemäß Art. 5 Abs. 1 lit. a i.V.m. Art. 6 Abs. 1 lit. c DS-GVO aufgrund einer rechtlichen Verpflichtung, der der Vermieter unterliegt, erforderlich. Eine rechtliche Verpflichtung, die Vermieter:innen unaufgefordert dazu verpflichtet, Minderungen von Mieter:innen an den Sozialhilfeträger zu melden, besteht zumindest regelmäßig dann nicht, wenn die Auszahlung des Mietzinses nicht an den/die Vermieter:in erfolgt, sondern zunächst an den/die Mieter:in und diese/r dann den Mietzins an den Vermieter zahlt. Insbesondere greift die Auskunftspflicht nach § 117 Abs. 3 Satz 1 Fall 2 SGB XII nicht. § 117 Abs. 3 Satz 1

Fall 2 SGB XII regelt u. a.: „Wer jemandem, der Leistungen nach diesem Buch beantragt hat oder bezieht, […] oder für ihn Guthaben führt […], hat dem Träger der Sozialhilfe auf Verlangen hierüber sowie über damit im Zusammenhang stehendes Einkommen oder Vermögen Auskunft zu erteilen, soweit es zur Durchführung der Leistungen nach diesem Buch im Einzelfall erforderlich ist. § 21 Abs. 3 Satz 4 des Zehnten Buches gilt entsprechend." Im Rahmen eines Mietverhältnisses kann allenfalls dann eine solche Auskunftspflicht in Betracht kommen, wenn der Vermieter um Auskunft bezüglich eines für den Leistungsempfänger geführten Guthabens ersucht wird. Dies kann etwa dann der Fall sein, wenn Gegenstand der Anfrage Kautions- oder Betriebskostenguthaben sind. Dies war vorliegend nicht der Fall. Angaben zu Mietminderungen oder der Höhe des Mietzinses sind daher von o.g. Auskunftspflicht nach Auffassung des LfDI nicht erfasst.

Die Übermittlung war ebenso nicht gemäß Art. 5 Abs. 1 lit. a i.V.m. Art. 6 Abs. 1 lit. f DS-GVO rechtmäßig, da kein berechtigtes Interesse des Vermieters an der Übermittlung gegeben war. Das Vertragsverhältnis sowie der Anspruch auf Zahlung des Mietzinses bestand ausschließlich zwischen dem Vermieter und dem Beschwerdeführer. Insbesondere hatte die Übermittlung an den Sozialhilfeträger auch keinerlei Sachzusammenhang bezüglich einer ggf. strittigen Mietminderung, da diese ausschließlich zivilrechtlich zwischen den Vertragsparteien geklärt werden kann.

Zum Zeitpunkt der Übermittlung war auch kein berechtigtes Interesse des Sozialhilfeträgers erkennbar. Im vorliegenden Fall war dem Vermieter zum Zeitpunkt der Übermittlung nicht bekannt, ob der Sozialhilfeträger bereits Kenntnis von der Minderung hatte bzw. der Beschwerdeführer diese selbst melden würde und daher überhaupt ein Interesse dessen an der Übermittlung bestand. Ein mögliches Interesse des Sozialhilfeträgers war daher allenfalls rein spekulativ. Ebenso ist zu berücksichtigen, dass gemäß § 67a Abs. 2 Satz 1 SGB X Sozialdaten beim Betroffenen zu erheben sind. Der Sozialhilfeträger ist deswegen verpflichtet, die für die Prüfung von Leistungen für Unterkunft und Heizung nach § 22 SGB II benötigten Daten zunächst beim Betroffenen selbst zu erheben. Es liegt daher in der Regel gerade nicht im berechtigten Interesse des Sozialhilfeträgers, ohne weitere Ermittlungen Sozialdaten im Wege der Erhebung über Dritte zu erhalten.

5.3 Veröffentlichung von Details zu Inkassoverfahren auf einer Bewertungsplattform im Internet durch Inkassounternehmen

Im Mai 2022 wurde dem LfDI zur Kenntnis gebracht, dass ein Inkassounternehmen auf Bewertungen in einem Internet-Bewertungsportal unter Preisgabe von konkreten Details zu den jeweiligen Inkassoverfahren der bewertenden Personen antwortet. Die betroffenen bewertenden Personen waren in dem Bewertungsportal durch deren Nutzerkontonamen namentlich erkennbar. Wurde durch die Bewertenden etwa Kritik am Vorgehen des Unternehmens geäußert, so verwies das Unternehmen in der veröffentlichten Antwort z.B. auf das konkrete Aktenzeichen oder die Anzahl der offenen Forderungen oder Vollstreckungsbescheide.

Nachdem das Inkassounternehmen auf das Stellungsnahmeersuchen des LfDI mitteilte, in dem Vorgehen keinen Datenschutzverstoß zu sehen und künftig die Antworten allgemeiner zu formulieren, hörte der LfDI das Inkassounternehmen bezüglich einer beabsichtigten Maßnahme nach Art. 58 Abs. 2 lit. d DS-GVO an. Diese umfasste, das Inkassounternehmen anzuweisen, einige der bisher konkret veröffentlichten Details zu den Inkassoverfahren zu löschen bzw. löschen zu lassen, sowie es künftig zu unterlassen, konkrete Details zu Inkassoverfahren von Betroffenen wie etwa die Höhe der

ausstehenden Forderung, das Vorliegen von Vollstreckungsbescheiden, das Vorliegen von Titeln, das Aktenzeichen oder vergleichbare Informationen der Öffentlichkeit zugänglich zu machen, etwa durch Veröffentlichung auf der genannten Webseite, sonstigen öffentlich zugänglichen Internetseiten oder durch ähnliche Verarbeitungsvorgänge.

Dieses Vorgehen beruhte auf folgender rechtlichen Bewertung:

Die o.g. Veröffentlichung von Details zu Inkassoverfahren Betroffener stellt einen Datenschutzverstoß dar, da keine Rechtsgrundlage für die Veröffentlichung von Details zu Inkassoverfahren vorlag. Insbesondere war diese nicht aufgrund berechtigter Interessen gemäß Art. 6 Abs. 1 S. 1 lit. f DS-GVO zulässig. Die Veröffentlichung war schon nicht erforderlich, da zur Bearbeitung entsprechender Beschwerden ebenso effektiv auf die direkte Kommunikation etwa auf dem Postweg zurückgegriffen werden konnte. Im Übrigen überwiegen in der Regel die Interessen der Betroffenen die Interessen des Inkassounternehmens an einer derart detaillierten Antwort. Bei den Bewertungen der Betroffenen handelte es sich überwiegend um Bewertungen und Mitteilungen im Sinne einer Warnung bzw. eines Erfahrungsaustausches und nicht um konkrete an das Inkassounternehmen adressierte Fragen. Betroffene müssen daher regelmäßig nicht damit rechnen, dass auf diese Bewertungen mit teils sensiblen Details aus den konkreten Verfahren öffentlich geantwortet wird. Die Interessen der Betroffenen daran, dass Details zu den Inkassoverfahren nicht öffentlich werden, überwogen daher das Interesse des Inkassounternehmens an der Veröffentlichung konkreter Details zu den Inkassoverfahren. Insbesondere ist es zur Entkräftung etwaiger unberechtigter Vorwürfe nicht erforderlich, konkrete Details aus den Verfahren öffentlich zu machen.

Das Inkassounternehmen löschte die entsprechenden Interneteinträge daraufhin und teilte mit, es künftig zu unterlassen, die Bewertungen der Schuldner:innen mit Details aus Inkassoverfahren im o.g. Sinne oder vergleichbaren Informationen öffentlich zu kommentieren.

5.4 Anfertigung von Fotos von Verkehrsverstößen durch Bürger:innen zwecks Übermittlung an Ordnungsbehörden

Im März 2022 wandte sich ein Bürger mit seiner Beschwerde an den LfDI, dessen auf einer Grünfläche ordnungswidrig abgestellter PKW von einer passierenden Person fotografiert wurde. Das Foto wurde in der Folge offensichtlich an die zuständigen Ordnungsbehörden übermittelt, die daraufhin ein Verfahren gegen den Beschwerdeführer einleitete. Dieser beschwerte sich hiergegen beim LfDI, da er der Ansicht war, es handele sich hierbei um einen Datenschutzverstoß.

Der LfDI verneinte in diesem konkreten Fall einen Datenschutzverstoß sowohl durch die fotografierende Person als Hinweisgeber:in als auch durch die Ordnungsbehörde und vertritt die Auffassung, dass die fragliche Form der Übermittlung von Fotos grundsätzlich zulässig ist. Hierzu im Einzelnen:

Die Erhebung und Übermittlung von Fotos durch die hinweisgebende Person an eine Ordnungsbehörde ist zulässig, da diese gemäß Art. 5 Abs. 1 lit. a i.V.m. Art. 6 Abs. 1 lit. f. DS-GVO rechtmäßig ist. Gemäß Art. 5 Abs. 1 lit. a DS-GVO müssen personenbezogene Daten u.a. auf rechtmäßige Weise verarbeitet werden. Die Verarbeitung ist rechtmäßig, wenn mindestens eine der Bedingungen aus Art. 6 Abs. 1 S. 1 DS-GVO erfüllt ist. Die Übermittlung kann durch ein berechtigtes Interesse der hinweisgebenden Person gemäß Art. 6 Abs. 1 S. 1 lit. f DS-GVO gerechtfertigt sein. Danach ist eine Übermittlung rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen

des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Der Begriff des berechtigten Interesses ist seinem Schutzzweck nach weit auszulegen.

Er umfasst alle rechtlichen, wirtschaftlichen, tatsächlichen oder ideellen Interessen. Die hinweisgebende Person kann als berechtigtes Interesse in solchen Fällen anführen, dass es auch in ihrem Interesse ist, dass öffentliche Flächen nicht durch ordnungswidrig parkende Fahrzeuge beeinträchtigt werden. Insoweit ist von der Rechtsprechung etwa im Zivilrecht anerkannt, dass Verkehrsregelungen drittschützenden Charakter haben können (BGH, Urteil vom 14.06.2005 - VI ZR 185/04). Demzufolge besteht am Schutz dieser Regeln auch ein berechtigtes Interesse der/des Einzelnen.

Die Übermittlung eines Fotos ist auch zur Wahrung dieses Interesses erforderlich. Dies ist immer dann der Fall, wenn keine datenschutzfreundlichere, gleich wirksame Maßnahme möglich ist. Vorliegend wäre die einzig praktische Alternative, den Sachverhalt telefonisch der Ordnungsbehörde zu melden. Auch in diesem Fall hätte die hinweisgebende Person jedoch die gleichen personenbezogenen Daten übermittelt, welche durch ein Foto übermittelt worden wären (Fahrzeugtyp, Standort, Kennzeichen). In beiden Fällen wären also die gleichen personenbezogenen Daten übermittelt worden. Erfahrungsgemäß würde die Ordnungsbehörde dann in einem Folgeschritt ohnehin ein Beweisfoto fertigen. Ein Anruf wäre jedoch auch nicht gleich wirksam, da er die Dokumentation des Sachverhaltes zeitlich verzögert und damit das Risiko der nicht rechtzeitigen Dokumentation begründet.

Auch ist nicht ersichtlich, dass das Interesse an dem Schutz vor der Übermittlung des Fotos die Interessen der hinweisgebenden Person am Schutz einer öffentlichen Fläche überwiegt. Ein Kriterium hierfür ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Hier ist zu berücksichtigen, dass der Verantwortliche in diesen Fällen zumindest fahrlässig einen Verstoß im öffentlichen Verkehrsraum begangen hat. Es ist daher auch nicht überraschend, wenn dieser von passierenden Personen dokumentiert und an die Ordnungsbehörde übermittelt wird.

Es liegt hier auch keine vergleichbare Interessenslage zu Dashcams vor. Während bei Dashcams die anlasslose Aufzeichnung des öffentlichen Raumes problematisch ist, ist in dieser Konstellation eben keine anlasslose Aufzeichnung erfolgt, sondern nur ein bereits vorliegender Verstoß dokumentiert worden.

Bei der Übermittlung eines Fotos ist weiterhin der Grundsatz der Datenminimierung zu beachten. Auch müssen die berechtigten Interessen unbeteiligter Dritter geschützt werden. Daher müssen Fotos so angefertigt bzw. bearbeitet werden (Schwärzen, Verpixeln), dass nur die für die Ordnungsbehörde relevanten Daten ersichtlich sind, nicht aber personenbezogene Daten unbeteiligter Dritter.

Von der soeben erläuterten grundsätzlichen Zulässigkeit kann es im Einzelfall Ausnahmen geben. Zu denken ist hierbei an Fälle, in denen die hinweisgebende Person kein ernstliches Interesse an der Einhaltung von Verkehrsregelungen zeigt, sondern vielmehr in querulatorischer Absicht und ungefiltert in einer Vielzahl von Fällen Fotos fertigt und versendet. Auch sind diejenigen Fälle anders zu werten, in denen die gefertigten Aufnahmen über das Internet, insbesondere durch soziale Medien, verbreitet werden.

Hinsichtlich der Datenverarbeitung durch die Ordnungsbehörde liegt regelmäßig ebenso kein Datenschutzverstoß vor. Diese ist befugt, zum Zwecke der Durchführung eines Verwarnungsverfahrens personenbezogene Daten zu verarbeiten (§ 28 Abs. 1 Landesdatenschutzgesetz), soweit dies erforderlich ist. In diesem Zusammenhang spielt die Herkunft dieser personenbezogenen Daten, die als Beweismittel genutzt wurden, zunächst keine Rolle. Auch wenn diese datenschutzwidrig durch die hinweisgebende Person erhoben worden sein sollten, hat dies nicht zwangsläufig Auswirkungen auf die Verwertbarkeit im Rahmen der Beweiswürdigung der Ordnungswidrigkeitenbehörde. Der Verwertung bzw. Verarbeitung könnten gesetzlich geregelte Verwendungs- oder Verwertungsverbote entgegenstehen. Diese sind jedoch vorliegend nicht ersichtlich.

5.5 Online-Seminar „Datenschutz im Verein“

Der LfDI beteiligte sich auch im Jahr 2022 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 erläuterte ein Referent des LfDI am 17. März 2022 die Grundlagen des Datenschutzrechts und gab spezifische Praxishinweise, Hilfestellungen sowie Tipps für Vereine. Die Fragen der Teilnehmenden zeigten, dass die Vereine weiterhin sowohl die Lösung typischer Sachverhalte aus dem Vereinsalltag wie auch der Umgang mit der Pandemiesituation beschäftigen. Insbesondere die Veröffentlichung von Fotografien, das korrekte Einholen von Einwilligungen sowie Fragen im Zusammenhang mit der Verarbeitung des Impf- und Genesenenstatus waren auch diesmal wieder von Interesse.

Der LfDI beantwortet diese und viele weitere Fragen in seinem Online-Informationsangebot für Vereine:

http://www.datenschutz.rlp.de/de/themenfelder-themen/vereine/

6. BESCHÄFTIGTENDATEN-SCHUTZ

6.1 Die erfolgreiche, aber unzulässige Videoüberwachung am Arbeitsplatz

In einem dem LfDI bekannt gewordenen Fall hatte der Kassenverwalter einer Gemeinde den Verdacht, dass sich eine Kollegin durch einen „Griff“ in die Meldeamtskasse persönlich bereichert. Daher nahm er seine private Videokamera mit ins Büro und brachte diese so an, dass er das Verhalten der Mitarbeiterin überwachen konnte. Es konnte so nachvollzogen werden, dass sich die Mitarbeiterin im System einloggte, unrichtige Stornobuchungen vornahm und das Geld aus der Meldeamtskasse entnahm. Der Mitarbeiterin wurde fristlos gekündigt. Der Kassenverwalter hatte sich zuvor die Einwilligung der anderen Mitarbeitenden für die Überwachung eingeholt. Die Datenschutzbeauftragte der Gemeinde bat den LfDI um eine Einschätzung zu dieser Überwachungsmaßnahme.

Da die Gemeinde von der Videoüberwachung keine Kenntnis hatte, kam nur der Kassenverwalter als der datenschutzrechtlich Verantwortliche in Frage.

Eine heimliche Videoüberwachung ist nur als ultima ratio zulässig, d.h. nur dann, wenn keine milderen Maßnahmen möglich sind. Vorliegend hätte das pflichtwidrige Verhalten der Kollegin auch anhand der Protokolldaten der vorgenommenen Buchungen belegt werden können.

Unstreitig lag in dem fraglichen Fall keine Einwilligung der betroffenen Person vor. Dass die anderen Kollegen in der Abteilung eingewilligt haben, spielt insofern keine Rolle. Ohnehin ist in einem Abhängigkeitsverhältnis die Freiwilligkeit einer Einwilligung grundsätzlich in Frage zu stellen.

Der LfDI wies darauf hin, dass die betroffene Mitarbeiterin in einem arbeitsgerichtlichen Verfahren die Kündigung anfechten und dabei ein Verwertungsverbot der Aufnahmen geltend machen könnte. Denn die Videoaufzeichnung wurde von einer dazu nicht autorisierten Person initiiert und stellte bereits deshalb eine unzulässige Überwachungsmaßnahme dar. Gleichwohl hat sich die Gemeinde die Aufnahmen zu eigen gemacht und hierauf ihre Kündigung gestützt.

Ob die eigenmächtige Videoüberwachung für den Kassenverwalter dienstrechtliche Konsequenzen hatte, wurde dem LfDI nicht mitgeteilt. Der LfDI regte aber an, gemeinsam mit dem Personalrat eine Dienstvereinbarung zur Zulässigkeit von Videoaufnahmen in der Gemeinde abzuschließen. Hierin sollten der Zweck, Anlässe für Auswertungen, zu beteiligende Personen (z.B. behördlicher Datenschutzbeauftragter, Personalrat) und die Speicherdauer geregelt werden.

6.2 Abhandenkommen von Bewerbungsunterlagen

Ein Spaziergänger fand in einem Gebüsch interne Unterlagen aus einem Stellenbesetzungsverfahren einer öffentlichen Stelle, nahm Kontakt zu einer Bewerberin auf und übergab ihr das ganze Paket der aufgefundenen Dokumente.

Die Bewerberin wandte sich daraufhin an die öffentliche Stelle und bat um Aufklärung. Von dort teilte man ihr aber nur lapidar mit, es sei kein Verlust von Bewerbungsunterlagen zu verzeichnen. Daraufhin übergab die Bewerberin die aufgefundenen Dokumente im Rahmen ihrer Beschwerde dem LfDI. Dieser bat das Amt ebenfalls um eine Stellungnahme. Die daraufhin angestellten Aufklärungsbemühungen des Amtes konnten jedoch den Verlust der Unterlagen nicht erklären.

Unterlagen eines Bewerbungsverfahrens sind gemäß Art. 32 und Art. 5 Abs. 1 lit. f DS-GVO

in einer Weise zu verarbeiten, dass durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit der personenbezogenen Daten gewährleistet ist, einschließlich dem Schutz vor unbeabsichtigtem Verlust („Integrität und Vertraulichkeit“).

Das Abhandenkommen der Bewerbungsunterlagen sowie der Umstand, dass dies weder bemerkt noch aufgeklärt werden konnte, belegten, dass entsprechende angemessene organisatorische Maßnahmen seitens des Amtes nicht ergriffen worden waren.

Dies stellte einen Verstoß gegen Art. 32, 5 Abs. 1 lit. f DS-GVO i.V.m. § 20 LDSG dar und wurde gem. § 17 Abs. 1 LDSG beanstandet.

6.3 Verstoß gegen Vertraulichkeit von Gesprächen

Wiederholt musste sich der LfDI im Berichtszeitraum damit beschäftigen, dass der Name von hinweisgebenden Personen unzulässigerweise aus vertraulichen Gesprächen an die beschuldigte Person weitergegeben wurde.

So hatte eine Beschwerdeführerin in einem vertraulichen Gespräch mit ihrem Referatsleiter einen Fall von sexueller Belästigung am Arbeitsplatz angezeigt. Der Referatsleiter fertigte hiervon einen Vermerk und übersandte diesen an die Beschwerdeführerin mit der Bitte, diesen unterschrieben an ihn zurückzusenden. Ohne die Rückübersendung abzuwarten, informierte der Referatsleiter noch am selben Tag den Kollegen, der von der Beschwerdeführerin beschuldigt worden war, über die erhobenen Vorwürfe. Dieser suchte umgehend einen Rechtsanwalt auf, der die Beschwerdeführerin mit anwaltlichen Schreiben zur Abgabe einer Unterlassungs- und Verpflichtungserklärung aufforderte.

Ausweislich der in der Verwaltung geltenden Dienstvereinbarung hatten Personen, die sich sexuell belästigt fühlen, das Recht auf ein persönliches, vertrauliches Beratungsgespräch. Dort war ebenso geregelt, dass weiterführende Maßnahmen nur mit Einverständnis der betroffenen Person eingeleitet werden dürfen.

Zwar sah die Dienstvereinbarung auch die Unterrichtung der beschuldigten Person „unverzüglich, spätestens nach einer Woche nach Kenntnis des Vorfalls“ vor. Diese Unterrichtung hätte indes auch ohne namentliche Nennung der hinweisgebenden Person erfolgen können. Jedenfalls hing die namentliche Weitergabe von der Einwilligung der anzeigenden Person ab. Hiervon ging offenbar auch der Referatsleiter aus, weil er die Beschwerdeführerin ansonsten nicht zur Unterschrift des Vermerks aufgefordert hätte. Damit hatte er den Eindruck erweckt, dass weitere Schritte von dieser Autorisierung abhängen.

Die Anzeige und Bekämpfung von sexueller Belästigung am Arbeitsplatz würde leerlaufen, wenn die anzeigende Person stets damit rechnen müsste, gegenüber der beschuldigten Person nicht anonym bleiben zu können.

In den fraglichen Fällen lag daher ein Verstoß gegen Art. 5 Abs. 1 lit.c, Art. 6 Abs. 1 lit. a, Art. 9 Abs. 1 lit. a, 88 DS-GVO in Verbindung der Dienstvereinbarung vor, der vom LfDI formell beanstandet wurde.

6.4 Das uneinsichtige Personalratsmitglied

Im Berichtszeitraum beschäftigte ein besonderer Fall von Dreistigkeit den LfDI: Ein Personalratsmitglied fotografierte heimlich mit dem Privathandy eine Sitzungsniederschrift der vorangegangenen Personalratssitzung. Der Vorsitzende bemerkte dies und forderte das Mitglied auf, das Foto zu löschen. Das Personalratsmitglied weigerte sich jedoch und behauptete, es habe ein Recht auf Kopien von Sitzungsniederschriften. Der Vorstand des Personalrats bat um

eine Einschätzung des LfDI. Dieser wies darauf hin, dass die Protokolle von Personalratssitzungen vertraulich zu behandeln sind und nicht auf privaten Endgeräten von Personalratsmitgliedern gespeichert werden dürfen. Über Cloud-Synchronisationen könnten ansonsten Daten, die dem Personalaktengeheimnis unterliegen, dem Cloudanbieter oder sonstigen unbefugten Dritten bekannt werden. Mit dem eigenmächtigen Abfotografieren wurde gegen § 72 Abs. 2 Satz 1 und Satz 2 LPersVG und damit im Ergebnis auch gegen die Verschwiegenheitspflicht nach § 71 LPersVG verstoßen.

Im Rahmen eines Telefonats mit dem uneinsichtigen Personalratsmitglied erteilte der LfDI diesem die mündliche Anweisung, die Aufnahmen auf dem Privathandy und solche, die ggfs. in eine Cloud synchronisiert wurden, unverzüglich zu löschen. Dem kam das Mitglied zwar nach, behauptete aber im Nachgang wahrheitswidrig, der LfDI habe anlässlich des Telefonats seinen grundsätzlichen Anspruch auf eine Kopie der Sitzungsniederschrift anerkannt. Die Pflichtverletzungen des Personalratsmitglieds führten in der Folge zu dessen Ausschluss aus dem Gremium, der auch vor Gericht Bestand hatte.

7. MEDIEN

7.1 Telemediendienste, Cookies und Tracking

Der Schwerpunkt der Aufsichtstätigkeit des LfDI im Bereich der Telemediendienste lag im Jahr 2022 eindeutig auf der Durchsetzung des teilweise neuen Datenschutzrechts im Hinblick auf Cookies und Trackingdienste. Im Dezember 2021 war das neue „Telekommunikation-Telemedien-Datenschutz-Gesetz“ (TTDSG) in Kraft getreten, das insbesondere den Einsatz von Cookies auf Webseiten und in Apps regelt. Die Einführung des TTDSG wurde durch eine neue Orientierungshilfe der Datenschutzkonferenz (DSK) begleitet, die neben der Verarbeitung von Cookies auch die rechtlichen Voraussetzungen weiterer Dienste, insbesondere aus dem Bereich des Werbetrackings, aus Sicht der deutschen Datenschutzaufsichtsbehörden darstellte.

Gemäß § 25 TTDSG dürfen nur solche Cookies eingesetzt werden, die zum Betrieb des Telemediendienstes technisch erforderlich sind. Tracking-Dienste, die nicht unter § 25 TTDSG fallen, sind, soweit sie personenbezogene Daten verarbeiten, nach Art. 6 DS-GVO zu bewerten. Dienste, die zum Betrieb einer Webseite nicht technisch erforderlich sind, bedürfen in der Regel einer wirksamen Einwilligung der Nutzer:innen. Diese Einwilligung kann grundsätzlich mit sogenannten „Einwilligungsbannern“ oder auch „Cookie-Bannern“ eingeholt werden, dies aber nur dann, wenn die Banner so gestaltet sind, dass das Ablehnen der Einwilligung ebenso leicht möglich ist wie ihre Erteilung. Zahlreiche Banner waren im Jahr 2022 jedoch noch so gestaltet, dass sie das Ablehnen der Einwilligung deutlich erschwerten, so dass keine wirksamen Einwilligungen eingeholt werden konnten. Überdies stützten einige Webseiten den Einsatz von einwilligungsbedürftigen Diensten immer noch (unzulässig) auf Art. 6 Abs. 1 lit. f DS-GVO.

Hinzu kommt, dass seit dem sogenannten „Schrems-II-Urteil“ des EuGH keine allgemeine Rechtsgrundlage für Übermittlungen personenbezogener Daten in die USA mehr bestand. Zahlreiche weit verbreitete Tracking-Dienste übermitteln jedoch personenbezogene Daten in die USA oder an US-amerikanische Unternehmen. Fälschlicherweise stützen sich dabei viele Webseiten auf die in Art. 49 Abs. 1 DS-GVO normierten Ausnahmetatbestände, obwohl diese eng auszulegen sind und nur bei gelegentlich erfolgenden Übermittlungen in Betracht kommen (Erwägungsgrund 111 zu Art. 49 DS-GVO).

Unter diesen Voraussetzungen kam es ab Ende 2021 bis weit ins Jahr 2022 hinein zu einer großen Zahl von Hinweisen auf rheinland-pfälzische Webseiten, die die dargestellten Anforderungen nicht erfüllten. Aufgrund der Masse der Hinweise musste der LfDI diesbezüglich priorisieren, welche Hinweise direkt zu Prüfungsverfahren führten. Die Hinweise bezogen sich in der Mehrzahl der Fälle auf die Webseiten kleiner und mittelständischer Unternehmen. Diesen gegenüber wurde in der Regel konstruktiv darauf hingewirkt, dass die datenschutzrechtlichen Vorgaben in Zukunft erfüllt werden. Sanktionen oder andere formale aufsichtsrechtliche Maßnahmen wurden nur dann in Betracht gezogen, wenn eine Kooperation mit dem LfDI verweigert wurde. Die meisten Betreiber von Telemediendiensten haben sich schon auf die Hinweise des LfDI hin sehr bemüht, die gesetzlichen Anforderungen umzusetzen, so dass im Ergebnis von einem spürbaren Fortschritt bei der Durchsetzung des Datenschutzrechts auf Webseiten im Jahr 2022 gesprochen werden kann. Dieser Prozess wird aber voraussichtlich auch im Jahr 2023 noch andauern.

7.2 Werbung

Im Bereich der Werbung lag der Schwerpunkt der aufsichtsrechtlichen Tätigkeit im Jahr 2022 auf unerwünschter Werbung und unerwünschten Newslettern. Der Großteil der Beschwerden bezog sich dabei auf elektronische (E-Mail), ein kleinerer auf postalische Zusendungen.

Immer wieder tritt in diesem Zusammenhang das sog. „Lettershop-Verfahren" in unterschiedlichen Konstellationen auf. Die Idee des Lettershop-Verfahrens besteht grundsätzlich darin, dass ein Werbeanbieter selbst keine Adressen von Werbekund:innen sammelt und nutzt, sondern einen Werbeauftrag für bestimmte Zielgruppen bei einem Lettershop erteilt und das entsprechende Werbematerial liefert. Dieses Material wird dann vom Lettershop an passende Adressat:innen aus seiner Adressdatenbank verschickt. Auf diesem Weg verarbeitet der Werbeanbieter selbst keine personenbezogenen Daten. Hieraus ziehen viele Werbeanbieter den Schluss, sie seien selbst datenschutzrechtlich nicht für die Nutzung der Adressen verantwortlich. Hinzu kommt, dass viele Lettershops entweder keine wirksame Einwilligung der Personen in ihrer Adressdatenbank für die Nutzung ihrer Daten nachweisen können oder teilweise fälschlich davon ausgehen, die Verarbeitung könne auf Art. 6 Abs. 1 lit. f DS-GVO gestützt werden. Besonders problematisch wird es, wenn Online-Shops die Daten ihrer Bestandskund:innen nutzen, um als Lettershop für Werbeaktionen anderer Unternehmen zu agieren, ohne hierfür eine gesonderte Einwilligung ihrer Kund:innen einzuholen.

Der LfDI geht grundsätzlich davon aus, dass Werbeanbieter und die von ihnen beauftragten Lettershops hinsichtlich der Verarbeitung personenbezogener Daten für Werbezwecke nach Art. 26 DS-GVO gemeinsam verantwortlich sind. Es handelt sich nicht um eine reine Auftragsverarbeitung durch den Lettershop. Hieraus folgt, dass sie eine Vereinbarung schließen müssen, die den Anforderungen aus Art. 26 DS-GVO entspricht. Hieraus folgt außerdem, dass auch die Werbeanbieter in der Lage sein müssen (ggf. mit Hilfe ihres Lettershops), dem LfDI gegenüber die notwendigen Einwilligungen der Werbeempfänger:innen nachzuweisen.

Der LfDI geht weiterhin davon aus, dass gerade bei E-Mail-Werbung in der Regel eine Einwilligung der betroffenen Personen für die Nutzung ihrer personenbezogenen Daten im Lettershop-Verfahren notwendig ist. Gemäß § 7 Abs. 2 Nr. 2 i.V. mit Abs. 3 UWG ist E-Mail-Werbung ohne Einwilligung nur bei Bestandskund:innen und nur für eigene Waren möglich, die den von den Kund:innen bisher gekauften Waren ähnlich sind und nur soweit die Kund:innen nicht widersprochen haben. Diese Wertung des UWG ist auf Art. 6 Abs. 1 lit. f DS-GVO zu übertragen, so dass in allen anderen Fällen der E-Mail-Werbung eine Einwilligung erforderlich ist.

Diese Einwilligung ist auch dann vom Werbeanbieter nachzuweisen, wenn er selbst keine personenbezogenen Daten verarbeitet, sondern sich eines Lettershops bedient. Kann der Werbeanbieter die Einwilligung nicht (ggf. durch Nachfrage beim Lettershop) nachweisen, ist die Verarbeitung zu beenden.

8. GESUNDHEIT

Datenschutzkonforme Sicherstellung der Nachweispflichten von Corona-Testzentren im Rahmen der sog. Bürgertestungen

Eine Corona-Bekämpfungsstrategie stellte das Testen auf den Corona-Virus insbesondere in dafür vorgesehenen Corona-Testzentren dar. Bei den sog. Bürgertestungen wurden lange Zeit die anfallenden Kosten vom Staat übernommen. Mit Abnahme der Infektionszahlen wurde im Jahr 2022 die Test-Infrastruktur umgestellt und die in der Testverordnung (TestV) geregelten Rahmenbedingungen der Bürgertests geändert. Nunmehr wurden nur in Ausnahmefällen die Kosten für die Testungen erstattet. Lag ein solcher Anspruch vor, mussten die Testzentren sicherstellen, dies dem Land ggfs. nachweisen zu können.

Um diese Prozesse zu vereinfachen, wurde seitens des Landesamt für Soziales, Jugend und Versorgung (LSJV) ein Formular zur Selbstauskunft/Nachweis nach § 6 Abs. 3 Nr. 4 und 5 TestV (a.F.) zur Inanspruchnahme von Testungen nach § 4a TestV (a.F.) (Bürgertestungen) den Corona-Testzentren in Rheinland-Pfalz zur Verfügung gestellt. In diesem Formular waren zahlreiche personenbezogene Daten anzugeben; u.a. wurde zum Nachweis der Identität neben dem Namen, Geburtsdatum, Geburtsort und Anschrift der betroffenen Person auch die Angabe der Ausweisnummer verlangt. Die Angabe wurde nicht als freiwillig o.ä. gekennzeichnet. Zwar hat die damalige Regelung in der Testverordnung verlangt, dass bei den Bürgertestungen gegenüber dem Leistungserbringer zum Nachweis der Identität der zu testenden Person ein amtlicher Lichtbildausweis oder, soweit die zu testende Person das 18. Lebensjahr noch nicht vollendet hat, ein sonstiger amtlicher Lichtbildausweis vorzulegen war, nach Auffassung des LfDI war die Erhebung der amtlichen Ausweisnummer vor dem Hintergrund der gesetzlichen Regelung jedoch weder erforderlich noch zweckmäßig und damit rechtmäßig im datenschutzrechtlichen Sinne. So wurde in der Regelung lediglich die Vorlage des amtlichen Lichtbildausweises zum Identitätsnachweis verlangt und keine Erfassung oder Speicherung dieser Daten. Sollte der Zweck der Erfassung und Speicherung der Ausweisdaten sein, dass dadurch seitens des Leistungserbringers nachgewiesen werden kann, dass der Identitätsabgleich vorgenommen wurde, ist zudem fraglich, ob die Angabe der Ausweisnummer dazu überhaupt geeignet ist. Denn der überprüfenden Stelle ist eine Kontrolle der Ausweisnummer nicht möglich. Außerdem müssten die sehr engen Vorgaben des Personalausweisgesetzes (PAuswG) zur Verarbeitung personenbezogener Daten aus dem Personalausweis durch nichtöffentliche Stellen (§§ 20 PAuswG) berücksichtigt werden.

Diese Zweifel an der Rechtmäßigkeit der Erhebung der Ausweisnummern hat der LfDI dem LSJV mitgeteilt und empfohlen, dass auf dem Selbstauskunftsbogen ein Feld implementiert wird, in dem vermerkt wird, dass der Personalausweis vorgelegt und geprüft wurde, dagegen jedoch keine Ausweisnummer erfasst wird. So konnte der LfDI erreichen, dass das betreffende Formular geändert wurde und ein Hinweis an die Testzentren in Rheinland-Pfalz erfolgte, dass die Personalausweisnummer nicht mehr erhoben werden darf.

Auch wenn mit dem Rückgang des Corona-Virus das regelmäßige Testen und die damit einhergehenden Datenverarbeitungen der Vergangenheit angehören, ist es auch für zukünftige formularmäßige Datenerhebungen wichtig, nur den entsprechend des Zwecks der Datenerhebung erforderlichen Umfang zu verlangen und der LfDI konnte dazu das entsprechende datenschutzrechtliche Bewusstsein schaffen.

9. SOZIALES

Beteiligung des LfDI an der Tagung des Landesamtes für Soziales, Jugend und Versorgung für Fachkräfte der Wirtschaftlichen Jugendhilfe

Datenschutz hat in der Jugendhilfe eine wichtige Bedeutung. Denn er spielt eine zentrale Rolle für den Aufbau einer vertrauensvollen erziehenden, beratenden oder helfenden Beziehung zwischen den Einrichtungen der Jugendhilfe und den Bürger:innen, die konkreten Hilfebedarf haben. Vor diesem Hintergrund nahm der LfDI das Angebot des Landesjugendamtes gerne wahr, sich an der erstmals durchgeführten Fachtagung für Fachkräfte der Wirtschaftlichen Jugendhilfe am 31. Mai 2022 in Mainz zu beteiligen.

Nach einem Impulsvortrag von Professor Jan Kepert, der die mit dem 2021 in Kraft getretenen Gesetz zur Stärkung von Kindern und Jugendlichen (Kinder- und Jugendstärkungsgesetz – KJSG) einhergehenden umfassenden Neuerungen vorstellte, gestaltete der LfDI unter dem Titel „Sozialdatenschutz für die Wirtschaftliche Jugendhilfe“ eines der drei Fachforen.

Dabei wurden neben der Vorstellung der wichtigsten datenschutzrechtlichen Bestimmungen, die im Rahmen der Tätigkeit der Wirtschaftlichen Jugendhilfe zu beachten sind, insbesondere konkrete Fallszenarien mit den Teilnehmer:innen erörtert. Die engagierten Diskussionen zeigten, dass die Thematik eine hohe praktische Relevanz hat und landesweit der Bedarf nach Austausch und konkreter Wissensvermittlung besteht.

Vor diesem Hintergrund wird der LfDI zusammen mit dem Landesjugendamt nach Möglichkeiten suchen, die Jugendämter in Rheinland-Pfalz bei der Umsetzung der datenschutzrechtlichen Vorgaben praxisnah zu unterstützen.

10. FORSCHUNG

10.1 Beteiligung des LfDI an der TaskForce Forschungsdaten und Petersberger Erklärung

Der LfDI beteiligte sich im Berichtsjahr an der durch die DSK Ende 2021 neu eingerichteten TaskForce Forschungsdaten, die wegen bisheriger Schwerpunkte gemeinsam vom Hessischen Beauftragten für den Datenschutz (HBDI) als Vorsitzendem des AK Wissenschaft und Forschung und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) geleitet wird. Die TaskForce setzt sich u.a. aus Mitgliedern der Arbeitskreise Wissenschaft und Forschung, Gesundheit und Soziales, Internationaler Datenverkehr sowie Technik zusammen und soll als einheitlicher Ansprechpartner u.a. für die Technologie- und Methodenplattform für die vernetzte medizinische Forschung (TMF) dienen.

Damit sollen die Abstimmungsprozesse zwischen den Datenschutzaufsichtsbehörden zügiger gestaltet werden. Dafür fanden insgesamt fünf Hauptsitzungen der TaskForce sowie weitere Sondersitzungen in dem Berichtsjahr statt.

Für die Bearbeitung von Einzelthemen sowie der Erstellung von Positionspapieren wurden zudem Unterarbeitsgruppen innerhalb der TaskForce gegründet, wobei sich der LfDI intensiv in der Unterarbeitsgruppe zu der Bearbeitung des Themas „Registergesetz – Anforderungen an den Datenschutz“ einbrachte. Auch im Rahmen dieser Untergruppen fanden regelmäßig Sitzungen statt, wobei die darin erzielten Ergebnisse in den Hauptsitzungen mit allen Mitgliedern der TaskForce diskutiert und zur Abstimmung gestellt wurden.

Eine Beteiligung der nicht innerhalb der TaskForce vertretenen Aufsichtsbehörden wurde wiederum durch eine Übermittlung der getroffenen Ergebnisse an den Arbeitskreis Wissenschaft und Forschung sowie den Arbeitskreis Gesundheit und Soziales sichergestellt.

Die TaskForce wirkte in dem Berichtszeitraum u.a. maßgeblich an der Entstehung der Petersberger Erklärung der DSK mit. Darin hat die DSK Empfehlungen zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung aufgestellt.

Grundlage für eine effektive Gesundheitsdatenforschung sind danach neben einer weitreichenden Transparenz vor allem eine hohe Rechtsklarheit für alle Beteiligten sowie die Sicherstellung eines nachhaltigen Schutzes personenbezogener Daten mit der Beratung und Überwachung durch die Datenschutzaufsichtsbehörden. Zu den grundlegenden Garantien und Maßnahmen gehören danach zudem die Verschlüsselung, die Pseudonymisierung durch eine Vertrauensstelle und die frühestmögliche Anonymisierung.

Mithin ist die datenschutzrechtliche Verantwortlichkeit lückenlos zu regeln, insbesondere bei der Übermittlung zwischen Forschungseinrichtungen, um sicherzustellen, dass die betroffenen Personen ihre Datenschutzrechte ausüben können. Außerdem empfiehlt die DSK die Errichtung eines laufenden, zentralen Verzeichnisses der bestehenden Register im Gesundheitsbereich, um zunächst eine strukturierte Übersicht über vorhandene Daten zu bieten und somit Transparenz für alle Beteiligten zu schaffen sowie mehrfache Datensammlungen zu vermeiden. Dabei sind Qualitätsanforderungen verbindlich vorzugeben, zu prüfen und auszuweisen.

Weitergehende Informationen unter:
https://s.rlp.de/petersbergererklaerung

10.2 Forschung als vielfältiges datenschutzrechtliches Beratungsfeld

Die Datenerhebungen an Schulen im Rahmen von Forschungsvorhaben haben mit dem Auslaufen der Corona-Pandemie wieder „Fahrt aufgenommen". Als Erhebungsmittel gerade in Verbindung mit Qualifikationsmaßnahmen (z.B. Bachelor-, Master-, Examensarbeiten) werden insbesondere die Instrumente (Online-)Fragebogen, Test, Interview, Gruppendiskussion oder Beobachtung genutzt.

Aber auch die bundeslandübergreifenden Schulleistungsuntersuchungen, mit denen Kenntnisse und Fertigkeiten von Schüler:innen gemessen werden, um u.a. die Leistungen der Schulen zu evaluieren, kommen wieder in ihren Rhythmus, da sie vielfach mit mehrjähriger Laufzeit ausgelegt sind.

Hier einige Beispiele für entsprechende Studien:

- Kontinuität und Wandel der Schule in Krisenzeiten – KWiK
- Schule macht stark – SchuMaS
- Trends in International Mathematics and Science Study – TIMSS
- Inklusion in der Sekundarstufe I in Deutschland – INSIDE

Regelmäßig wird im Rahmen der beratenden Begleitung der Studien vom LfDI geprüft, ob der Grundsatz der Datenminimierung beachtet wird und die Texte und Inhalte der Informationsmaterialien für die Teilnehmer:innen korrekt sind. Gelegentlich werden auch die vorgelegten Prozedurenbeschreibungen und Datenschutzkonzepte inkl. der zum Einsatz kommenden technischen Hilfsmittel einer eingehenden Prüfung unterzogen.

Gerade bei Forschungsvorhaben zum Thema Gesundheit werden eingereichte Datenschutzkonzepte umfassend geprüft. So z.B. bei einer Studie zur Erfassung der SARS-CoV-2-Infektionen anhand eines Beobachtungs- und Frühwarnsystems für die Bevölkerungsgesundheit. Trotzdem gingen zu dieser Studie Beschwerden ein, die in diesem Kontext ausgesprochen selten sind und auch nicht begründet waren.

Anlass der Beschwerden war, dass zum Einschluss einer repräsentativen Bevölkerungsstichprobe in die Studie aus dem Einwohnermelderegister mehrerer Kommunen Auskünfte durch die Studienleitung beantragt und von den Einwohnermeldeämtern auch erfüllt wurden. Denn um mit möglichen Studienteilnehmer:innen Kontakt aufnehmen zu können, benötigt die Studienleitung entsprechende Kontaktdaten, für die es aber eine gesetzlich geregelte Verarbeitungserlaubnis gibt. Denn das Recht auf informationelle Selbstbestimmung ist kein uneingeschränktes Recht.

Bei dem Bundesmeldegesetz (BMG) handelt es sich um eine solche gesetzliche Verarbeitungserlaubnis. Die Einwohnermeldeämter bei den Städten und Gemeinden dürfen gemäß §§ 44 ff. BMG Auskünfte aus dem Melderegister erteilen. Hier erfolgte zum Zweck der wissenschaftlichen Forschung im öffentlichen Interesse eine Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Personen (sog. Gruppenauskunft) gemäß § 46 BMG.

Außer der Tatsache der Zugehörigkeit einer Person zu der Gruppe darf das Einwohnermeldeamt u.a. die derzeitige Anschrift mitteilen. Der Empfänger der Meldedaten darf diese aber nur für den besonderen Zweck verarbeiten und ist nach § 47 Abs. 1 BMG zur Löschung verpflichtet.

Auch über den Sachstand zur Einrichtung von sog. Datenintegrationszentren (DIZ) im Rahmen der Medizininformatik-Initiative (MII), die im Januar 2023 in eine Ausbau- und Erweiterungsphase starten, wurde der LfDI informiert und um Beratung u.a. hinsichtlich der Fragestellung gebeten, ob die Anonymisierung von

Patientendaten und die anschließende Weitergabe an das DIZ auf § 36 Abs. 2 S. 1 Nr. 3 i.V.m. § 37 Abs. 1 S. 2 Nr. 3 Landeskrankenhausgesetz (LKG) gegebenenfalls gestützt werden.

Weitere Informationen zu diesem bundesweiten, vom Bundesministerium für Bildung und Forschung geförderten Projekt, mit dem die medizinische Forschung gestärkt und die Patientenversorgung verbessert werden soll, sind unter **https://s.rlp.de/medinfo** im Internet abrufbar.

Weiter hat das Deutsche Kinderkrebsregister (DKKR) eine neue Initiative zum Datenabgleich mit den Datenbeständen des Krebsregisters Rheinland-Pfalz und denen in anderen Bundesländern gestartet. Informationen zur Bedeutung des 1980 gegründeten DKKR finden sich unter **https://s.rlp.de/dkkr**.

Bei einem Datenabgleich bzw. -austausch würden Daten vom DKKR an ein Landeskrebsregister (LKR) übermittelt, Daten von einem LKR erhoben und die erhobenen Daten dann vom DKKR gespeichert und wissenschaftlich verwendet.

Ein „Abgleich (oder die Verknüpfung)“ ist als Vorgang in der Aufzählung der Definition zur Verarbeitung personenbezogener Daten (Art. 4 Nr. 2 DS-GVO) enthalten. Unter einem Abgleich von Daten wird die Überprüfung verstanden, ob die in mehreren Dateisystemen über einen Betroffenen gespeicherten Daten konsistent (widerspruchsfrei) sind. Ein Abgleich liegt auch dann vor, wenn überprüft wird, ob bestimmte Daten in zwei unterschiedlichen Datei(system)en vorhanden sind. Werden Daten aus einem System im anderen hinzugefügt, um den anderen Datensatz zu vervollständigen, handelt es sich um eine Verknüpfung (Paal/Pauly/Ernst, 3. Aufl. 2021, DS -GVO Art. 4 Rn. 31).

Eine Verknüpfung von personenbezogenen Daten setzt im Regelfall mehrere Datenbestände voraus, die so zusammengeführt werden, dass Daten zu bestimmten Merkmalen oder bestimmten Personen verbunden werden, dass sich der Aussagewert der Daten deutlich erhöht (Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 4 Rn. 28).

Die Beratung und Begleitung der letztgenannten Vorhaben wird den LfDI weiter in Anspruch nehmen.

11. KOMMUNALES

11.1 Bekanntgabe personenbezogener Daten in Ratssitzungen und Ratsinformationssystemen

Schon im 26. Datenschutzbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI) für die Berichtsjahre 2016/2017 waren Rats- und Bürgerinformationssysteme und die damit oftmals ohne Ermächtigungsgrundlage einhergehende Veröffentlichung personenbezogener Daten ein großes Thema. Gleiches gilt für die Art und Weise, wie mit Bürgerdaten im Verlaufe einer Ratssitzung umgegangen wird.

Auch im Jahr 2022 gab es in diesen beiden Themenkreisen zahlreiche Beschwerden und Hinweise, weil sensible Informationen in unachtsamer Weise veröffentlicht wurden. Trotz umfassender Beratung und Sensibilisierung durch den LfDI scheint die Rechtslage noch nicht überall bekannt zu sein bzw. fehlt mitunter ein entsprechendes Gespür für datenschutzrechtliche Belange bei den zuständigen Mitarbeiter:innen in den jeweiligen Fachabteilungen der Kommunalverwaltungen.

11.1.1 Veröffentlichung einer Unterschriftenliste im Internet

U.a. erreichte eine erhebliche Zahl von Beschwerden den LfDI, nachdem in einem Rats- und Bürgerinformationssystem einer Verbandsgemeinde eine von 784 Personen unterzeichnete Unterschriftenliste gegen die Errichtung eines Industriegebietes veröffentlicht wurde. Enthalten waren die vollständigen Namen, Geburtsdaten, Adressen und Unterschriften der unterzeichnenden Personen.

Da keine Ermächtigungsgrundlage für die Veröffentlichung der Liste im Internet und damit zur Bekanntgabe personenbezogener Daten gegenüber einer unbestimmten Anzahl Dritter bestand, ahndete der LfDI den Verstoß mit einer förmlichen Beanstandung gem. § 17 Abs. 1 Landesdatenschutzgesetz (LDSG) wegen Verstößen gegen Art. 6 Abs. 1 i.V.m. Art. 5 Abs. 1 lit. a und lit. c DS-GVO bzw. § 3 LDSG (Nichtbeachtung der Grundsätze der Rechtmäßigkeit der Verarbeitung und der Datenminimierung).

11.1.2 Veröffentlichung von Spenderdaten

Eine ähnliche Problematik ergab sich in einigen Fällen bei der Annahme von Spenden, denn auch bei dieser Fallkonstellation gibt es keine Ermächtigungsgrundlage zur Veröffentlichung im Internet.

Nach den kommunalrechtlichen Vorschriften entscheidet über die Annahme oder Vermittlung von Spenden der Gemeinderat bzw. der Kreistag. Nach dem Grundsatz der Öffentlichkeit aus § 35 Abs. 1 GemO bzw. 28 Abs. 1 LKO sind solche Angelegenheiten auch grundsätzlich in öffentlicher Sitzung zu beschließen, es sei denn, die Beratung in nicht öffentlicher Sitzung ist aus Gründen des Gemeinwohls oder wegen schutzwürdiger Interessen Einzelner erforderlich.

Zu beachten ist jedoch zwingend der Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DS-GVO, welcher besagt, dass die Verarbeitung personenbezogener Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen.

Unter Berücksichtigung dieses Grundsatzes wird in der Regel die Bekanntgabe personenbezogener Daten der Spender:innen während der Sitzung neben der Höhe der Spende auf Name und Wohnort zu beschränken sein. Falls vorhanden, sind selbstverständlich auch anderweitige Beziehungsverhältnisse offenzulegen.

Diese Daten dürfen insoweit auch Eingang in die nach § 41 GemO bzw. § 34 LKO zu erstellende Niederschrift finden. Die Rechtsgrundlage hierfür ergibt sich insoweit aus Art. 6 Abs. 1 lit e, Abs. 2 und 3 DS-GVO i.V.m. den o.g. Rechtsgrundlagen aus den §§ 94 GemO bzw. 58 LKO.

Eine Online-Veröffentlichung des Abstimmungsergebnisses oder eines zuvor erstellten Vorlageberichts im Internet ist allerdings aus den eingangs genannten Gründen unzulässig.

11.1.3 Veröffentlichung von Haushaltsplänen und Stellenplänen

Probleme wegen einer fehlenden Ermächtigungsgrundlage nach Art. 6 Abs. 1 DS-GVO zur Veröffentlichung im Internet bestehen häufig auch bei der Aufstellung von Haushaltsplänen.

Personenbezogene Datenschutzproblematiken ergeben sich dabei insbesondere aus dem Stellenplan, der gem. § 96 Abs. 4 Nr. 4 GemO Bestandteil des Haushaltsplans ist. Darin können gerade bei sehr kleinteilig aufgegliederten Stellenplänen auch zumindest personenbeziehbare Angaben zu Teilzeit, Altersteilzeit, Entgeltgruppe, Dienstunfähigkeit, Elternzeit, Besuch des Angestelltenlehrganges o.ä. enthalten sein.

Ähnliche Problematiken können sich aber auch an anderer Stelle des Haushaltsplans ergeben. Gibt es z.B. in einer kleinen Ortsgemeinde nur eine Dienstwohnung, die z.B. – wie jedermann bekannt – vom Hausmeister der Gemeindehalle bewohnt wird, dann sollten die Mieteinnahmen im Haushaltsplan nur ganz allgemein als „Mieteinnahmen“ ohne nähere Bezeichnung der Immobilie und nicht als „Miete Hausmeisterwohnung Gemeindehalle“ benannt werden. Andernfalls wäre direkt für alle ersichtlich, welche Miete vom Betroffenen zu zahlen ist.

Die Regelungen zum Erlass der Haushaltssatzung und zu deren Veröffentlichung ergeben sich ausschließlich aus § 97 Gemeindeordnung (GemO) und diese sieht eben keine Veröffentlichung im Internet und damit eine Bekanntgabe gegenüber einer unbestimmt großen Anzahl von Personen vor.

Vielmehr ist der Entwurf der Haushaltssatzung nach Zuleitung an den Gemeinderat bis zur Beschlussfassung zur Einsichtnahme durch die Einwohner:innen verfügbar zu halten. In welcher Form dies geschieht, ist nicht festgeschrieben. Es bleibt also der Gemeinde überlassen, ob sie den Entwurf in herkömmlicher Weise als Druckwerk auslegt, im Internet verfügbar macht oder in sonstiger Weise ihren Einwohner:innen zur Einsichtnahme zur Verfügung stellt. Nach der öffentlichen Bekanntmachung der Haushaltssatzung ist der Haushaltsplan an sieben Werktagen bei der Gemeindeverwaltung während der allgemeinen Öffnungszeiten öffentlich auszulegen.

Sollte eine Online-Veröffentlichung innerhalb dieses Verfahrens vorgesehen sein, müssen zwingend Vorkehrungen zum Schutz personenbezogener Daten getroffen und ggf. der Stellenplan von einer Veröffentlichung im Internet ausgenommen werden oder (z.B. durch Schwärzen) zumindest so verändert werden, dass eine Personenbeziehbarkeit ausgeschlossen ist.

11.2 Bekanntgabe von Hinweisgeber:innen

Auch der Umgang der öffentlichen Verwaltung mit Anzeigenden und Hinweisgeber:innen bleibt ein Dauerthema. Die hierzu immer noch geltenden datenschutzrechtlichen Grundsätze wurden vom LfDI bereits im 12. Tätigkeitsbericht des Jahres 1989 kommuniziert. Zudem bietet der LfDI auf seiner Internetseite eine auf die derzeit geltende Rechtslage aktualisierte Orientierungshilfe an. Trotzdem gab das Thema wiederholt Anlass zu Beschwerden von Betroffenen, weshalb noch einmal grundsätzlich auf

diese Problematik hingewiesen wird.

In fast allen Zweigen der Verwaltung (auch außerhalb der Strafverfolgung, wo diese Problematik durch Verwaltungsvorschriften und Gesetze, insbes. die StPO, speziell geregelt ist) kommt es vor, dass Bürger:innen Hinweise auf vermeintlich rechtswidriges Verhalten oder rechtswidrige Zustände geben.

Die erlangten Informationen dürfen grundsätzlich von einer Behörde zur weiteren Klärung genutzt werden. Allerdings ist die Identität von Hinweisgeber:innen und Informant:innen vertraulich zu behandeln. Auch gegenüber dem Auskunftsanspruch des Betroffenen gem. Art. 15 DS-GVO und dem Akteneinsichtsanspruch des Beteiligten gem. § 29 Abs. 1 VwVfG ist das Geheimhaltungsinteresse in diesen Fällen grundsätzlich vorrangig (Art. 15 Abs. 4 DS-GVO, § 29 Abs. 2 VwVfG, vgl. BVerwG, Urteil vom 3. September 1991, NJW 92, 451; OVG Koblenz, Urteil vom 16. September 1997, Az. 7 A 12512/96 und 7 A 10004/97).

Der Schutz des Hinweisgebers ist nicht abhängig von einer Bitte um vertrauliche Behandlung. Eine solche Bitte verpflichtet aber die Verwaltung zu besonders sorgfältiger und restriktiver Prüfung, ob ein Ausnahmefall vorliegt, der die Nutzung und Weitergabe der personenbezogenen Daten von Hinweisgeber:innen zulässt.

Keinesfalls ist es erforderlich, den von Hinweisen Betroffenen zum Zweck der Stellungnahme die Identität des Hinweisgebers mitzuteilen. Hier reicht grundsätzlich die Formulierung „Nach Hinweisen aus der Bevölkerung …“ aus. Falls die Bekanntgabe der Identität des Hinweisgebers wesentlich ist, um dem Betroffenen eine Stellungnahme zu ermöglichen, ist zu prüfen, ob einer der nachfolgend aufgeführten Rechtfertigungsgründe für die Übermittlung vorliegt.

Dies ist zum einen dann der Fall, wenn der Hinweisgeber ausdrücklich damit einverstanden ist.

Auch wenn sich der Inhalt des Hinweises durch andere Aufklärungs- und Beweismittel nicht erhärten lässt, sich der Inhalt der Aussage des Hinweisgebers aber grundsätzlich als Beweismittel eignet, so kann die Identität im überwiegenden Allgemeininteresse entsprechend genutzt werden.

Letztendlich darf die Identität des Hinweisgebers auch dann bekanntgegeben werden, wenn sich die Hinweise als falsche Anschuldigungen erweisen, denen mit erheblicher Wahrscheinlichkeit eine Beleidigungs- oder Schädigungsabsicht des Hinweisgebers zugrunde liegt (Art. 6 Abs. 1 lt. e, Abs. 3 DS-GVO i.V.m. § 7 Abs. 1 Nr. 2 LDSG; für ein Verwaltungsverfahren: § 29 Abs. 1 Satz 1 i.V.m. Abs. 2 VwVfG).

12. BILDUNG

12.1 Smartwatches im Schulbetrieb

Aus Anlass der Einschulung, nach Weihnachten, Ostern oder Geburtstagen erhalten Kinder zunehmend sog. Smartwatch-Uhren als Geschenk. Neben der Uhrfunktion bieten diese auch die Möglichkeit, mit dem Gerät zu telefonieren oder den Standort des Kindes zu tracken. Daher häufen sich im Berichtszeitraum Anfragen von Schulen beim LfDI hinsichtlich der Nutzung dieser Smartwatches während des Schulbetriebs.

So berichteten Schulen, dass Eltern ihr Kind während des Unterrichts über die Uhr anriefen, um ihnen etwas mitzuteilen. In einem anderen Fall rief eine Mutter ihr Kind an, weil sie anhand der Trackingdaten sehen konnte, dass ihr Kind die Schule verlassen hatte. Dabei befand sich die Klasse nur auf dem Weg zum Sportplatz.

Einige Modelle der Smartwatches ermöglichen über eine SIM-Karte, dass die Uhr unbemerkt vom Träger eine bestimmte Telefonnummer anruft, so dass die Anrufer (also z.B. die Eltern) Gespräche im Unterricht mithören und die Gespräche sogar aufzeichnen können. Diese Geräte dürfen in Deutschland nicht verwendet werden. Der Nutzer einer solchen Uhr kann sich sogar nach § 201 StGB strafbar machen. Hiernach wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer das nichtöffentlich gesprochene Wort mit einem Abhörgerät abhört oder aufzeichnet.

Sofern die Schule Kenntnis davon hat, dass Eltern trotz von der Schule mitgeteilter Bedenken ihr Kind mit einer Smartwatch in die Schule schicken, die über eine unzulässige Abhörfunktion verfügt, können die Eltern darauf hingewiesen werden, dass die Schule im Wiederholungsfall die Polizei einschalten wird.

Geräte, die über keine unzulässige Abhörfunktion verfügen, sind Handys vergleichbar und können daher wie diese behandelt werden. Es bleibt der Schule vorbehalten, ob sie die Verwendung der Smartwatches als Uhr toleriert oder ob sie die gleichen Regeln wie für herkömmliche Handynutzung anwendet.

12.2 Telepräsenzroboter für langzeiterkrankte Kinder

Nach Corona kehrten die Schulen im Schuljahr 2022/23 wieder in den Präsenzunterricht zurück. Jedoch gibt es auch weiterhin Kinder, die krankheitsbedingt längerfristig nicht am Präsenzunterricht teilnehmen können. Mittlerweile bieten verschiedene Unternehmen sog. Telepräsenzroboter an. Die Geräte verfügen – ähnlich wie Videokonferenzsysteme – über Kameras und Mikrofone, mit denen der Unterricht aus dem Klassenraum nach Hause oder ins Krankenhaus übertragen („gestreamt“) werden kann. Gleichzeitig kann sich das Kind aktiv am Unterricht beteiligen und so Kontakt zu den Klassenkamerad:innen halten.

Im Berichtszeitraum beriet der LfDI sowohl Schulen als auch das Ministerium für Bildung des Landes Rheinland-Pfalz in rechtlichen und technischen Fragen, die beim Einsatz dieser Telepräsenzroboter zu beachten sind. Die neuen schulrechtlichen Regelungen (s. 28. Tb, Tz. 12.5) ermöglichen es glücklicherweise, diese digitalen Hilfsmittel relativ schnell und unbürokratisch nutzen zu können (§§ 1 Abs. 6 und 67 Abs. 1 SchulG). Hinsichtlich der weiteren Rahmenbedingungen, wie z.B. die erforderlichen Informationspflichten gegenüber den Klassenkamerad:innen und Lehrkräften, stellte der LfDI entsprechende Mustertexte auf seiner Homepage bereit:

https://www.datenschutz.rlp.de/de/themenfelder-themen/telepraesenzroboter/

12.3 Sicherheitscoach patzt bei Datensicherheit

Ein privater Coach für Sicherheitsberatung bot Grundschulklassen Trainings in seinen Räumlichkeiten an und forderte hierzu im Vorfeld der Veranstaltung eine Übermittlung der Klassenliste der teilnehmenden Schüler:innen per unverschlüsselter E-Mail. Eine Schule, die sich weigerte, die Liste zu übermitteln, verwies der Anbieter darauf, dass dies in seinen Allgemeinen Geschäftsbedingungen stünde.

Der LfDI erteilte dem Anbieter daraufhin den Hinweis, dass Allgemeine Geschäftsbedingungen keine tragfähige Rechtsgrundlage für die Weitergabe von Schülerdaten durch eine Schule an ein privates Unternehmen darstellen. Als eine solche rechtliche Grundlage kam vorliegend nur die Einwilligung der Eltern in Betracht. Auch hinsichtlich der zukünftigen Vermeidung des unverschlüsselten E-Mail-Versands, dem Erstellen entsprechender Mustereinwilligungserklärungen und der Einhaltung der Vorgaben der Art. 13 und 14 DS-GVO sah der LfDI ein Erfordernis, gegenüber dem Sicherheitscoach klarstellende Vorgaben zu machen, die dieser fortan beachtete.

12.4 Handbuch Schule.Medien.Recht

Schulen und Schulträgern wird mit dem Handbuch „Schule.Medien.Recht“ seitens des Landes ein umfangreiches Kompendium zu datenschutz- und medienrechtlichen Fragestellungen angeboten. Diese Sammlung an juristischen und technischen Fachartikeln, Mustervorlagen und Handreichungen wurde im Jahr 2022 unter Mitarbeit des LfDI vom Ministerium für Bildung und dem Pädagogischen Landesinstitut neu überarbeitet veröffentlicht. Auf der Seite **https://schulemedienrecht.bildung-rp.de/startseite/** finden sich nun die jeweils gültigen Vorgaben und Rechtsnormen sowie aktuelle datenschutzrechtliche Themen.

Begleitend zu der Neuauflage des Handbuchs führten Mitarbeitende des LfDI im Herbst Online-Grundlagenschulungen für neue schulische Datenschutzbeauftragte durch.

12.5 Datenschutz-Schülerworkshops

Nach Abklingen der Pandemie wurden die Datenschutz-Schülerworkshops wieder stark nachgefragt und übertrafen mit 508 Workshops an 110 Schulen sogar die letzten Vor-Corona-Zahlen. Hierbei machten die Gymnasien mit 46 Schulen den größten Anteil aus, gefolgt von 36 Grundschulen. Rund ein Viertel der Gymnasien führte die Workshops in gleich zwei Jahrgängen durch, da die Workshops dort mittlerweile zum festen Baustein des Medienkonzeptes gehören und durch einen Ausfall im Vorjahr keine Lücke einzelner Stufen entstehen sollte. Die Finanzierung der Veranstaltungen gelang dank der Übertragung von im Vorjahr nicht verausgabten Mitteln. Hierbei stellte, wie in den Vorjahren, das Ministerium für Familie, Frauen, Kultur und Integration einen Großteil über einen entsprechenden Titel zur Verbraucherbildung bereit.

13. MELDEWESEN UND WAHLEN

13.1 Landesrechtliche Umsetzung der Änderung pass-, ausweis- und melderechtlicher Vorschriften

Der LfDI wurde vom Ministerium des Innern des Landes Rheinland-Pfalz (MDI) um eine datenschutzrechtliche Einschätzung hinsichtlich der landesrechtlichen Regelungen zur Umsetzung des Pass- und Personalausweisgesetzes sowie des Bundesmeldegesetzes gebeten.

Vorausgegangen waren Änderungen der genannten Gesetze auf Bundesebene, bei der der BfDI beteiligt worden war. Dessen grundlegende Bedenken (abrufbar unter **https://s.rlp.de/bfdi-st1** und **https://s.rlp.de/bfdi-st2**) wurden im Gesetzgebungsverfahren des Bundes allerdings nur unzureichend berücksichtigt.

Zu den wesentlichen datenschutzrechtlichen Verschlechterungen, die die genannten bundes- und landesrechtlichen Regelungen für die Bürger:innen mit sich bringen, gehört u.a., dass

- auf Landesebene zentrale Lichtbildregister einzurichten sind, die Abrufe von Lichtbildern und Unterschriften für Sicherheitsbehörden künftig bundesweit „rund um die Uhr“ ermöglichen sollen;
- der melderechtliche Begriff der sog. einfachen Behördenauskunft abgeschafft und durch einen deutlich erweiterten Datenkranz an abruffähigen Informationen ersetzt wurde;
- eine Protokollierung nur bei den abrufberechtigten Stellen (und nicht bei den Meldeämtern) in einer nur sehr eingeschränkten Form ermöglicht wird und
- im Fall einer freien Suche für Sicherheitsbehörden die Trefferzahl auf 4.000 Treffer und bei sonstigen öffentlichen Stellen auf 1.000 „begrenzt“ wurde.

Der LfDI machte hinsichtlich der genannten Punkte gegenüber dem MDI auch seinerseits erhebliche Bedenken geltend und wies darauf hin, dass die Schaffung von zentralen Lichtbildregistern mit bundesweiten Abrufmöglichkeiten in höchstem Maße datenschutzrelevant ist und dass mit zentralen Datenbeständen stets hohe Risiken für die Betroffenen einhergehen.

Denn zentrale Datenbestände wecken regelmäßig Begehrlichkeiten, das Missbrauchsrisiko steigt mit der Zahl der Abrufberechtigten und bei automatisierten Abrufen ist die Beachtung der Grundsätze der Erforderlichkeit und der Verhältnismäßigkeit kaum sicherzustellen. Hinzu kommt, dass bei der Verarbeitung von Lichtbildern zumindest mittelbar „besondere Kategorien personenbezogener Daten“ im Sinne des Art. 9 DS-GVO betroffen sind und der Kreis der Zugriffsberechtigten durch die im Land Rheinland-Pfalz vorgesehenen Formen der Auftragsverarbeitungen durch öffentliche und private Auftragnehmer kaum noch zu überschauen ist.

In der Folge wurde der LfDI zwar bei der praktischen Umsetzung des Registers mit einbezogen; auch die erforderliche Datenschutz-Folgenabschätzung wurde nachgeholt. Im Ergebnis bleibt es aber dabei, dass sowohl auf Bundes- wie auch auf Landesebene erhebliche datenschutzrechtliche Verschlechterungen, wie insb. der Zugriff von Sicherheitsbehörden auf Fotos der Bundesbürger:innen, festzustellen sind.

13.2 Datenschutzverstöße im Rahmen der Impfkampagne

Im Rahmen der Impfkampagne der Landesregierung wurden bestimmte Altersgruppen von Bürger:innen über einen längeren Zeitraum in insgesamt vier Impfaufrufen per Brief über die Möglichkeiten der Inanspruchnahme einer Corona-Schutzimpfung informiert. Die Adressdaten wurden im Wege einer sog. Gruppenauskunft aus dem rheinland-pfälzischen Melderegister gewonnen, welche durch die Gesellschaft für Kommunikation und Wissenstransfer (KommWis) vorgenommen wurde. Mit der Verarbeitung und Zustellung der Briefe wurde die Deutsche Post E-POST Solutions GmbH beauftragt.

Den Anschreiben war eine „Datenschutzrechtliche Information" beigegefügt, in der das Gesundheitsministerium als „Verantwortlicher" genannt wurde. Das Schreiben enthielt keine Informationen dazu, dass vorliegend Meldedaten für die individuelle Adressierung verwendet wurden und sowohl die KommWis als auch die Deutsche Post E-POST Solutions als Dienstleister beteiligt waren.

Die „Datenschutzrechtliche Information" enthielt aber den Hinweis, dass die verarbeiteten personenbezogenen Daten „und Gesundheitsdaten" in der Zentralabteilung des Gesundheitsministeriums vorgehalten würden. In diesem Zusammenhang wurde auch Art. 9 DS-GVO als Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten ausdrücklich genannt.

Beim LfDI gingen nach dem letzten Impfaufruf, bei dem rund 1.250.000 Bürger:innen angeschrieben wurden, zahlreiche Beschwerden ein, in denen u.a. die Verwendung der Adressdaten sowie der angebliche heimliche Aufbau eines Impfregisters problematisiert wurden.

Der LfDI bewertete den Vorgang wie folgt:

Nach Art. 14 Abs. 2 lit. f DS-GVO sind Betroffene darüber zu informieren, aus welcher Quelle die personenbezogenen Daten stammen, wenn die Daten nicht bei ihnen selbst erhoben wurden. Vorliegend enthielten die Datenschutzhinweise des Ministeriums jedoch keine Hinweise auf die Herkunft der Daten.

Auch wurden entgegen Art. 14 Abs. 1 lit. c DS-GVO die hier einschlägigen melderechtlichen Rechtsgrundlagen für die Datenverarbeitung nicht genannt.

Weiterhin wurden die Betroffenen entgegen Art. 14 Abs. 1 lit. e DS-GVO nicht über die Einschaltung von externen Dienstleistern, wie hier der KommWis und der Deutschen Post E-POST Solutions GmbH, informiert. Die Information, dass eine Verarbeitung von Gesundheitsdaten stattfand, war objektiv falsch und führte bei zahlreichen Bürger:innen zu der irrigen Annahme, dass sie gezielt als ungeimpfte Person angesprochen wurden.

Zusammenfassend stellte dies einen Verstoß gegen Art. 14 Abs. 1 lit. c, lit. e, Abs. 2 lit. e und f DS-GVO dar und wurde gem. Art. 58 Abs. 6 DS-GVO i.V.m. § 17 Abs. 1 LDSG beanstandet.

Angesichts der großen Datenbestände, die sowohl beim Ministerium als auch bei der KommWis und der Deutschen Post E-POST Solutions GmbH verarbeitet wurden, kam der vollständigen Löschung der verarbeiteten Meldedaten eine erhebliche Bedeutung zu. Um verlässlich auszuschließen, dass bei den beteiligten Stellen ein „Schattenregister" aus Meldedaten von Bürger:innen aufgebaut wurde, forderte der LfDI entsprechende Löschbestätigungen der beteiligten Stellen, die auch zeitnah vorgelegt wurden.

13.3 Wahlwerbung für Minderjährige

Im Berichtszeitraum erreichten den LfDI mehrere Beschwerden von Bürger:innen, weil ihre Kinder Wahlwerbung von einer politischen Partei erhielten.

Gemäß § 50 Abs. 1 BMG darf die Meldebehörde innerhalb von sechs Monaten vor einer Wahl oder Abstimmung Parteien Auskunft aus dem Melderegister über Familienname, Vornamen, Doktorgrad und Anschriften bestimmter Gruppen von Wahlberechtigten erteilen, soweit für deren Zusammensetzung das Lebensalter bestimmend ist.

Eine Partei kann also beispielsweise Namen und Anschriften aller 18- bis 25-Jährigen innerhalb eines Wahlkreises erfragen, nicht aber die genauen Geburtsdaten der Wahlberechtigten. Die Partei darf diese Auskunft nur für die Werbung bei einer Wahl oder Abstimmung verwenden und hat sie spätestens einen Monat nach der Wahl oder Abstimmung zu löschen oder zu vernichten. Grund für dieses Privileg ist die in der Verfassung verankerte Aufgabe der Parteien, an der politischen Willensbildung mitzuwirken.

Im vorliegenden Fall erfolgte jedoch bei der Eingabe der zu übermittelnden Daten eine Fehleingabe, sodass es neben der Übermittlung der korrekten Daten der volljährigen Wähler:innen auch zu einer Übermittlung von Adressdaten von nicht wahlberechtigten Minderjährigen kam.

Dadurch, dass die Geburtsdaten nicht übermittelt wurden, war es für die Partei nicht möglich, diesen Fehler zu erkennen. Die Daten wurden nach Bekanntwerden des Vorfalls umgehend gelöscht.

Die für die Datenschutzverletzung verantwortliche Verbandsgemeindeverwaltung hatte eine ordnungsgemäße Datenpannenmeldung an den LfDI übersandt und in der Lokalpresse auf das Versehen hingewiesen. Die Beschwerdeführer wurden entsprechend unterrichtet.

13.4 Zensus 2022

13.4.1 Durchführung des Zensus

Die EU-Verordnung 763/2008 legt fest, dass seit 2011 in den EU-Mitgliedstaaten alle zehn Jahre eine Bevölkerungszählung durchzuführen ist. Dieser „Zensus“ hätte nach 2011 eigentlich schon 2021 stattfinden sollen, wurde jedoch aufgrund der Corona-Pandemie um ein Jahr verschoben. Als Zensus-Stichtag wurde der 15.05.2022 festgelegt. Zwar wurden einige wichtige Schritte des Zensus auch schon vor diesem Termin erledigt, ab dem Stichtag besuchten aber Erhebungsbeauftragte einen Teil der Bevölkerung zu Hause, so dass der Zensus in den Fokus der Öffentlichkeit rückte.

Der Zensus soll Informationen darüber liefern, wie viele Menschen in Deutschland leben, wie sie wohnen, welchen Beruf sie ausüben und welchen Bildungsgang sie beschritten haben. Diese Informationen dienen wiederum als Grundlage für zukünftige staatliche Entscheidungen und Planungen in Bund, Ländern und Kommunen, wie etwa die Ausstattung mit staatlicher Infrastruktur (z.B. Schulen, Sportstätten, Straßen, öffentlicher Nahverkehr) oder Landesplanung und -entwicklung.

Der Zensus wurde von den Statistischen Ämtern des Bundes und der Länder und den Erhebungsstellen in den Kreisverwaltungen und kreisfreien Städten durchgeführt. Wie bereits beim Zensus 2011 wurde auch der Zensus 2022 nicht als vollständige Erhebung durch Befragungen durchgeführt. Der Großteil des Zensus lief vielmehr registergestützt ab. Dies bedeutet, dass bestehende Datenbestände der staatlichen Verwaltung (insbesondere aus den Melderegistern) zur statistischen Aufbereitung an das Bundesamt für Statistik übermittelt wurden. Im Rahmen der Haushaltebefragung wurde nur ein geringer Anteil der Bevölkerung direkt befragt, nämlich bundesweit eine Stichprobe von ca. 10-12%. Vom 15.05.2022 bis in den August fand eine Befragung von Bürger:innen an nach

dem Zufallsprinzip ausgewählten Anschriften statt. Diese Haushaltebefragung diente zum einen der Ermittlung realitätsgerechter Einwohnerzahlen. Zum anderen wurden Informationen erhoben, die nicht in Verwaltungsregistern verfügbar sind (z. B. Bildungsstand und Erwerbsbeteiligung).

Die Befragungen wurden in Rheinland-Pfalz von 36 regionalen Erhebungsstellen in den Landkreisen und kreisfreien Städten organisiert. Dabei kamen besonders geschulte und auf den Datenschutz verpflichtete Erhebungsbeauftragte zum Einsatz. Die Erhebung erfolgte bei rund 390.000 in Rheinland-Pfalz in die Stichprobe einbezogenen Personen im Direktinterview. Fragen zum Bildungsstand, zur Erwerbstätigkeit und zu einer ggf. vorhandenen Migrationserfahrung konnten per Online-Fragebogen beantwortet werden. Soweit dies nicht möglich oder nicht gewünscht war, konnte alternativ auch ein Papierfragebogen ausgefüllt werden. Für diese Erhebung bestand Auskunftspflicht.

Neben der Haushaltebefragung wurden in der Gebäude- und Wohnungserhebung sämtliche Eigentümer:innen sowie sonstige Verfügungs- und Nutzungsberechtigte befragt. Diese Befragung wurde online oder schriftlich durchgeführt.

13.4.2 Kontrollen durch den LfDI

Der LfDI begleitete als datenschutzrechtliche Aufsichtsbehörde bereits die Vorbereitungen für den Zensus und stimmte konkrete Anforderungen zur Sicherstellung von Datenschutz und Datensicherheit mit dem Statistischen Landesamt ab. Wie beim Zensus 2011 führte der LfDI zusätzlich stichprobenweise Vor-Ort-Kontrollen bei Erhebungsstellen durch. Der überwiegende Teil der Kontrollen erfolgte bereits vor dem Stichtag am 15.05.2022, ein kleinerer Teil fand nach dem Stichtag statt.

Insgesamt konnte aus datenschutzrechtlicher Sicht ein positives Fazit der Vor-Ort-Kontrollen gezogen werden. Die überwiegende Zahl der Erhebungsstellen hatte die Anforderungen an Datenschutz und Datensicherheit technisch und organisatorisch insgesamt gut umgesetzt. Festgestellte Mängel wurden unter Mitwirkung des LfDI unverzüglich beseitigt.

13.4.3 Berichterstattung über das Verfahren zur Erinnerung an die Zensus-Teilnahme

Anfang August 2022 wurde in den Medien berichtet, eine hohe Zahl rheinland-pfälzischer Bürger:innen habe Mahnschreiben mit der Androhung eines Zwangsgeldes wegen nicht beantworteter Zensus-Befragungen erhalten, obwohl diese ihre Antworten schon eingereicht oder gar keine Aufforderung zur Abgabe der Informationen erhalten hätten. Presseanfragen hierzu erreichten auch den LfDI und warfen die Frage auf, ob datenschutzrechtlich relevante Fehler bei der Verarbeitung der personenbezogenen Daten der von den Mahnschreiben betroffenen Personen vorgelegen hätten.

Der LfDI leitete daraufhin ein formales Verfahren ein. Nach Auskunft des Statistischen Landesamtes war in einer großen Zahl der Fälle die Abgabe der Zensus-Fragebögen tatsächlich trotz zugegangener Aufforderung nicht fristgemäß. In einer Reihe von Fällen hätten aber Fehler bei den Zustelldiensten dazu geführt, dass Personen die Aufforderung zur Teilnahme am Zensus tatsächlich nicht erhalten hätten. Anhaltspunkte für Datenschutzverstöße durch das Statistische Landesamt konnten seitens des LfDI aber nicht festgestellt werden. Weitere Informationen des Statistischen Landesamtes zur Aufklärung des Sachverhalts finden sich hier:

https://s.rlp.de/statnews1

https://s.rlp.de/statnews2

13.4.4 Hinweise, Beschwerden und Nachfragen zum Zensus

Hinweise, Beschwerden und Nachfragen den Zensus betreffend wurden insbesondere um den Zensus-Stichtag herum und noch eine Weile danach eingereicht. Die Menge der Eingaben war gemessen an der Menge der Auskunftspflichtigen (s.o.) gering. Sie lag unter zwanzig. Zum einen handelte es sich um die (üblichen) allgemein skeptischen Nachfragen zur Rechtmäßigkeit der Datenabfragen im Rahmen des Zensus.

In diesem Zusammenhang ist eine Entscheidung des Verwaltungsgerichts Neustadt a.d.W. zur Rechtsmäßigkeit des Zensus von Interesse. Das Gericht stellte in einem Beschluss vom 27.10.2022 fest, dass das Statistische Landesamt Rheinland-Pfalz berechtigt ist, im Zuge der Gebäude- und Wohnungszählung (GWZ) im Rahmen des Zensus 2022 die im Gesetz zur Durchführung des Zensus im Jahr 2022 (ZensG 2022) näher bezeichneten, strukturellen Angaben einschließlich sogenannter statistischer Hilfsmerkmale zu erheben. Die Antragsteller hatten sich im Eilverfahren gegen die Aufforderung des Statistischen Landesamtes zur Teilnahme an der Gebäude- und Wohnungszählung gewehrt und eine Verletzung ihres Rechts auf informationelle Selbstbestimmung durch die Durchführung des Zensus geltend gemacht. Das Gericht lehnte den Antrag ab und stellte fest, dass der Zensus in seiner gesetzlich ausgestalteten Form das Recht auf informationelle Selbstbestimmung nicht verletze.

Zum anderen lagen die Schwerpunkte der Beschwerden auf der im Einzelfall nicht immer mangelfreien Verarbeitung personenbezogener Daten durch die Erhebungsbeauftragten und auf Nachfragen zur Berichterstattung über die o.g. Erinnerungen an die Zensus-Teilnahme.

14. RECHTSDURCHSETZUNG

Im Jahr 2022 konnte der LfDI nach der Corona-Zeit wieder zu einer weitgehend normalen Verfahrensgestaltung zurückkehren.

Verantwortliche und Auftragsverarbeiter sind grundsätzlich verpflichtet, auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten. Informationsersuchen sind unabdingbar, um die Sachverhalte zu ermitteln und dem Anliegen der Beschwerdeführer gerecht zu werden. Da jedoch nicht alle Verantwortlichen sofort ihren Mitwirkungspflichten nachkamen, wurde in 50 Fällen ein Zwangsgeld (überwiegend Verfahren wegen Videoüberwachung) von durchschnittlich 500,00 € angedroht. In 13 Fällen mussten die Zwangsgelder auch bereits festgesetzt werden. In 63 (größtenteils Art. 15, 17 DS-GVO) Fällen wurde gegenüber Verantwortlichen eine Anweisung erlassen und in 46 Fällen eine Verwarnung ausgesprochen. Ein besonderes Augenmerk wurde weiterhin auf die datenschutzkonforme Beauskunftung nach Art. 15 DS-GVO gelegt. Dabei konnte im Vergleich zum Vorjahr eine stärkere Sensibilisierung der Verantwortlichen festgestellt werden. Im öffentlichen Sektor kam es in fünf Fällen zu einer Beanstandung. Dabei ging es um unberechtigte Weitergabe personenbezogener Daten. Zwei Verfahren betrafen die Nutzung von Daten aus der Luca-App durch die Sicherheitsbehörden.

Im Jahr 2022 wurden vier Bußgeldbescheide erlassen. In Verfahren zu Dashcams ließ sich feststellen, dass zunehmend Modelle mit Beschleunigungssensoren verwendet werden. Verfahren gegen Beamte wegen unzulässiger Datenbankabrufe gab es nur sehr wenige. Die Bußgeldverfahren wurden im Mai 2022 mit der „Guideline on the calculation of administrative fines under the GDPR“ auf eine europäische Grundlage gestellt.

Im Jahr 2022 wurde gegen den LfDI in 21 Fällen Klage erhoben. In zehn Fällen wendete sich ein Beschwerdeführer gegen die Beendigung seines Verfahrens. Der LfDI hat diese Klagen für sich entschieden, da das VG Mainz hier konsequent der Entscheidung des OVG Koblenz vom 26. Oktober 2020 (Az. 10 A 10613/20.OVG) folgte. In drei Verfahren wurde Antrag auf Zulassung der Berufung gestellt. Fünf Bußgeldverfahren wurden abschließend durch das AG Mainz entschieden.

15. ZERTIFIZIERUNG UND AKKREDITIERUNG

Das Papier „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme – Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6)“, welches im Frühjahr 2021 durch die DSK angenommen wurde, liegt nun in der Version 2.0 vor.

Das Dokument beschreibt die Mindestanforderungen an die Zertifizierungskriterien, die ergänzend zu den Vorgaben der DIN EN ISO/IEC 17067 von allen Zertifizierungsprogrammen erfüllt sein müssen. Es soll den deutschen Aufsichtsbehörden bei der Bewertung von Zertifizierungsprogrammen als einheitliche Bewertungsgrundlage dienen und Programmeignern sowie Zertifizierungsstellen bei der Erstellung ihrer Dokumente als Orientierung helfen.

Das Papier wurde im Unterarbeitskreis Prüfkriterien des AK Zertifizierung weiterentwickelt. Die Struktur wurde hierbei beibehalten und es wurden Inhalte ergänzt, u.a. zur gemeinsamen Verantwortlichkeit nach Artikel 26 DS-GVO und zur Datenübermittlung in Drittstaaten gemäß Artikel 46 DS-GVO. Zudem enthält das Papier in der neueren Version Darstellungen zum Verfahrensablauf bei der Prüfung sowohl von nationalen als auch europäischen Zertifizierungskriterien. Der Unterarbeitskreis hat bei der Überarbeitung des Papiers konkrete Erfahrungen mit dessen Anwendung sowie Entwicklungen auf europäischer Ebene im Bereich der datenschutzrechtlichen Akkreditierung und Zertifizierung berücksichtigt. Um eine größere Sichtbarkeit auch u.a. auf europäischer Ebene zu erreichen, liegt das Papier mittlerweile auch in einer englischsprachigen Version vor. Der Unterarbeitskreis Prüfkriterien wird die Anwendung sowie die Handhabbarkeit des Papiers bei der Prüfung eingereichter Zertifizierungsprogramme auch weiter beobachten und – sofern erforderlich – auch weitere Anpassungen und Überarbeitungen des Papiers vornehmen.

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

ABKÜRZUNGSVERZEICHNIS

Arbeitskreis	AK
Berufsbildende Schule	BBS
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	BfDI
Bürgerliches Gesetzbuch	BGB
Ministerium für Bildung des Landes Rheinland-Pfalz	BM
Bundesmeldegesetz	BMG
Bundesnotarordnung	BNotO
Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff	BoBD
Datenschutz-Grundverordnung	DS-GVO
Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder	DSK
Der Europäische Datenschutzausschuss	EDSA
Europäischer Datenschutzbeauftragter	EDSB
Landesgesetz zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz	eGovG
Europäische Union	EU
Gemeindeordnung	GemO
Internal Market Information System	IMI
Infektionsschutzgesetz	InfSG
Justizvollzugsanstalt	JVA
Gesellschaft für Kommunikation und Wissenstransfer	KommWis

Landesbibliotheksgesetz Rheinland-Pfalz	LBibG
Landesdatenschutzgesetz Rheinland-Pfalz	LDSG
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz	LfDI
Landeswahlordnung Rheinland-Pfalz	LWO
Ministerium des Innern und für Sport Rheinland-Pfalz	MdI
Mietspiegelreformgesetz	MsRG
Mietspiegelverordnung	MsV
Oberlandesgericht Rheinland-Pfalz	OLG
Onlinezugangsgesetz	OZG
Sozialgesetzbuch	SGB
Strafgesetzbuch	StGB
Strafprozessordnung	StPO
Telekommunikation-Telemedien-Datenschutz-Gesetz	TTDSG
Verwaltungszustellungsgesetz	VwZG
Gesetz zur Durchführung des Zensus	ZensG

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