33. Tätigkeitsbericht

der Landesbeauftragten für Datenschutz und Informationsfreiheit

Berichtszeitraum: 2024

Dem Landtag und der Landesregierung
vorgelegt am 25. Juni 2025
(Landtagsdrucksache 17/1440)

Im Interesse einer besseren Lesbarkeit wird im Text überwiegend darauf verzichtet, geschlechtsspezifische Formulierungen zu verwenden. Sämtliche Personenbezeichnungen richten sich in gleicher Weise an die Angehörigen aller Geschlechter.

Vorwort

Der vorliegende 33. Tätigkeitsbericht blickt auf ein Jahr zurück, in dem die Digitalisierung unseres Alltags gerade auch mit Anwendungen der künstlichen Intelligenz ihren Siegeszug unvermindert fortgesetzt hat. Individuell zugeschnittene Dienste oder intelligente Assistenzsysteme bringen zweifelsohne Komfortgewinne und eine Effektivierung von Arbeitsabläufen mit sich, bergen aber auch Risiken für Grundrechte, die es zu bewältigen gilt.

Auf europäischer Ebene wurde mit der am 1. August 2024 in Kraft getretenen Verordnung über die künstliche Intelligenz (KI-Verordnung) ein europaweit einheitlicher Rechtsrahmen geschaffen, der dieser rasanten technischen Entwicklung Rechnung tragen soll und nicht zuletzt auch datenschutzrechtliche Risiken adressiert. Die Regelungen der KI-Verordnung sind nun mit der Datenschutz-Grundverordnung in Einklang zu bringen, um einen innovativen, aber dennoch datenschutzkonformen Einsatz der KI zu gewährleisten. Dies stellt Entwickler und Betreiber von KI-Modellen durchaus vor erhebliche Hürden. Vor diesem Hintergrund und mit Blick auf den Vorsprung der KI-Entwicklung in den USA und China überrascht es nicht, dass in diesem Spannungsfeld zwischen technischer Innovation und Grundrechtsschutz Stimmen aus der Wirtschaft und zunehmend auch aus der Politik Datenschutz als Innovationshemmnis darstellen und sinnbildlich mit überbordender Bürokratie gleichsetzen. Doch diese Sichtweise greift zu kurz; Datenschutz ist kein Selbstzweck und keine bloße Verwaltungsaufgabe – Datenschutz ist ein Grundrecht, das in einer zunehmend digitalisierten Welt Würde und Freiheit jedes Einzelnen schützen soll. Wo Regeln individuelle Rechte garantieren und Transparenz schaffen, entsteht langfristig Vertrauen – die Grundlage für nachhaltige, menschenzentrierte Innovation.

Daher bleibt es die zentrale Aufgabe meiner Behörde, den Datenschutz als Grundrecht und als Voraussetzung für eine freiheitliche digitale Gesellschaft zu verteidigen und den Schutz der

Daten der Bürgerinnen und Bürger zu gewährleisten. Mit dieser Zielsetzung haben wir auch im Berichtsjahr die Kommunen und Behörden des Landes bei ihren Digitalisierungsanstrengungen intensiv und konstruktiv begleitet. In diesem Bereich wird auch weiterhin ein Schwerpunkt unserer Beratungstätigkeit liegen, da auch die saarländische Verwaltung nicht zuletzt aufgrund immer knapper werdender Ressourcen zur Entlastung ihrer Arbeitsprozesse künftig auf den Einsatz von KI-Anwendungen zurückgreifen wird. Soweit im Rahmen dieser Anwendungen personenbezogene Daten von Bürgerinnen und Bürgern verarbeitet werden, wird hier in besonderem Maße darauf zu achten sein, wie ein Kontrollverlust über diese Daten verhindert, transparente und nachvollziehbare Datenverarbeitungsprozesse garantiert sowie Betroffenenrechte gewährleistet werden können.

Ungeachtet der relativ neuen Aufgabenstellungen für die Datenschutzaufsichtsbehörden im Zusammenhang mit der KI-Verordnung und zahlreichen weiteren neuen Europäischen Digitalrechtsakten und deren Zusammenspiel mit der Datenschutz-Grundverordnung, war meine Behörde im Berichtsjahr mit einer wieder gestiegenen Zahl an gemeldeten Datenschutzverletzungen und Beschwerden betroffener Bürgerinnen und Bürger befasst. Unabhängig davon, ob es sich hierbei um versehentliche Datenlecks, gezielte Angriffe oder um bewusst oder nachlässig unzureichend gestaltete Datenverarbeitungsprozesse handelte, zeigen all diese Verfahren, wie wichtig ein verantwortungsvoller und datenschutzkonformer Umgang mit personenbezogenen Daten für das nötige Vertrauen in einer zunehmend digitalisierten Welt ist.

Wird dieses Vertrauen der Nutzerinnen und Nutzer durch vorwerfbares Handeln der Datenverarbeiter enttäuscht, ist in Einzelfällen auch eine Sanktionierung dieses Verhaltens durch Verhängung von Geldbußen geboten, um den verantwortlichen Stellen ein klares Signal zu senden und die Wahrung datenschutzrechtlicher Vorgaben künftig zu gewährleisten. Daher wurden auch im vergangenen Berichtszeitraum gegenüber Un-

ternehmen und auch gegen Einzelpersonen eine erneut gestiegene Anzahl an Geldbußen verhängt.

Anhand anschaulicher Beispiele soll der vorliegende Tätigkeitsbericht den Leserinnen und Lesern einen Einblick in unsere vielschichtige Arbeit gewähren. Die Bewältigung der umfangreichen und hier nur in einem Ausschnitt dargestellten Aufgaben einer Datenschutzbehörde wäre indes ohne das große Engagement der Mitarbeiterinnen und Mitarbeiter und ihrer persönlichen Identifikation mit den an sie gestellten Anforderungen nicht möglich. Dafür möchte ich mich an dieser Stelle ganz herzlich bei dem gesamten Team des Unabhängigen Datenschutzzentrums bedanken.

Saarbrücken, im Juni 2025

Monika Grethel

Landesbeauftragte für Datenschutz
und Informationsfreiheit

Inhaltsverzeichnis

Abbildungsverzeichnis

I.

Zahlen und Fakten

1 Zahlen & Fakten

Die Datenschutz-Grundverordnung (DSGVO) verpflichtet die Datenschutzaufsichtsbehörden zur jährlichen Erstellung eines Berichts über die Schwerpunkte ihrer Tätigkeit (Art. 59 DSGVO). Diese Tätigkeitsberichte stellen eine wesentliche Informationsquelle für die Öffentlichkeit und die Parlamente über aktuelle Entwicklungen im Datenschutzrecht dar. Um einen ersten und allgemeinen Überblick über die Anzahl der Sachverhalte zu geben, mit denen sich die deutschen Aufsichtsbehörden im Berichtszeitraum befasst haben und um die Transparenz und Vergleichbarkeit der Tätigkeit der Aufsichtsbehörden zu erhöhen, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) gemeinsame Kriterien zur statistischen Darstellung von Tätigkeitsschwerpunkten aufgestellt. Entsprechend dieser Vereinbarung werden im Folgenden die wesentlichen Kategorien von Verfahren, mit denen sich das Unabhängige Datenschutzzentrum Saarland (UDZ) im Berichtszeitraum zu befassen hatte, aufgeführt, wobei landesspezifische Aufgaben und Tätigkeiten nicht erfasst werden.

1.1 Beschwerden

Hier wird eine Übersicht über die Anzahl von im Berichtszeitraum eingegangenen Beschwerden gegeben. Als Beschwerden werden solche Vorgänge erfasst, die schriftlich eingehen und bei denen eine natürliche Person eine persönliche Betroffenheit darlegt. Die zahlreichen an die Behörde gerichteten Anregungen, einem als datenschutzwidrig angenommenen Sachverhalt aufsichtsbehördlich nachzugehen, fließen mithin nicht in die Statistik ein. Diese werden ebenso wie (fern-)mündliche Beschwerden nur dann statistisch erfasst, wenn sie verschriftlicht werden und zu weitergehenden Maßnahmen Veranlassung geben.

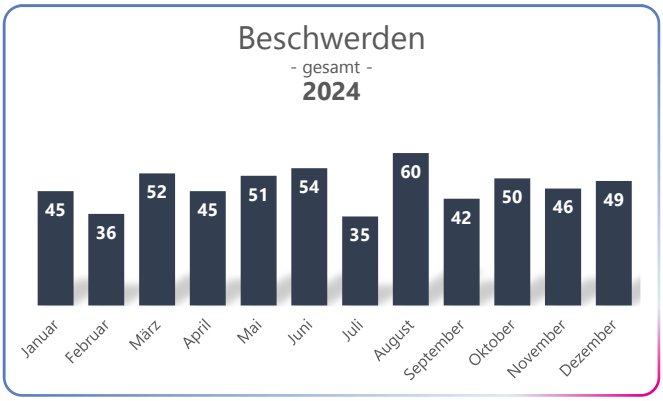

Abb. 1: Beschwerden (gesamt) 2024

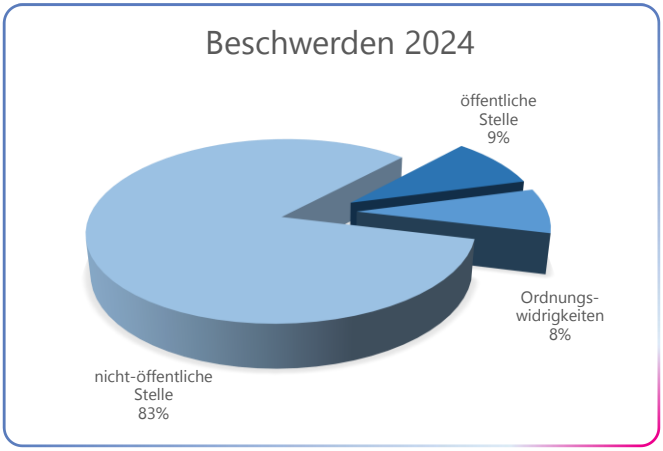

Abb. 2: Beschwerden (Aufteilung) 2024

1.2 Beratungen

Hier wird eine Übersicht über die Anzahl von schriftlichen Beratungen gegeben. Dies umfasst Beratungen von Verantwortlichen, betroffenen Personen und der Landesregierung. Aus-

schließlich (fern-)mündliche Beratungen werden statistisch nicht erfasst, obwohl diese einen sehr hohen Anteil der an unsere Behörde gerichteten Anfragen darstellen und einen hohen zeitlichen Aufwand erfordern.

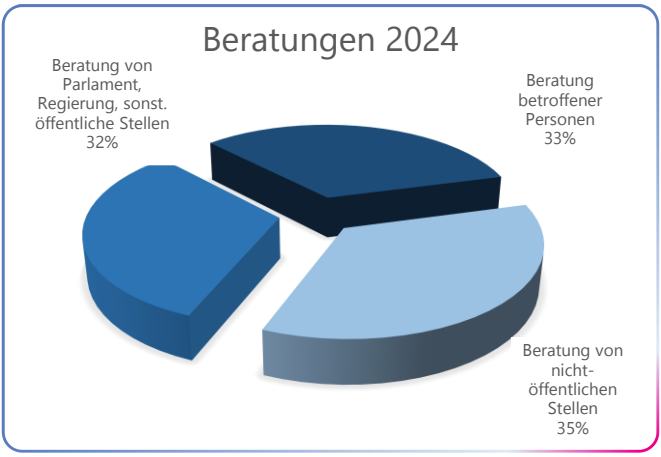

Abb. 3: Beratungen (gesamt) 2024

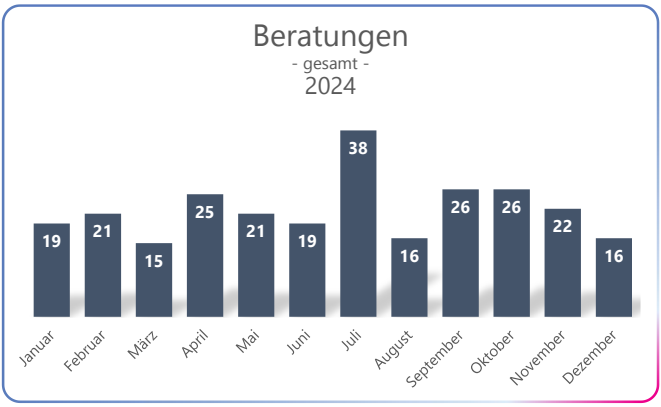

Abb. 4: Beratungen (Aufteilung) 2024

1.3 Meldungen von Datenschutzverletzungen

Hier wird eine Übersicht über die Anzahl schriftlich eingegangener Meldungen von Verantwortlichen über Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DSGVO gegeben.

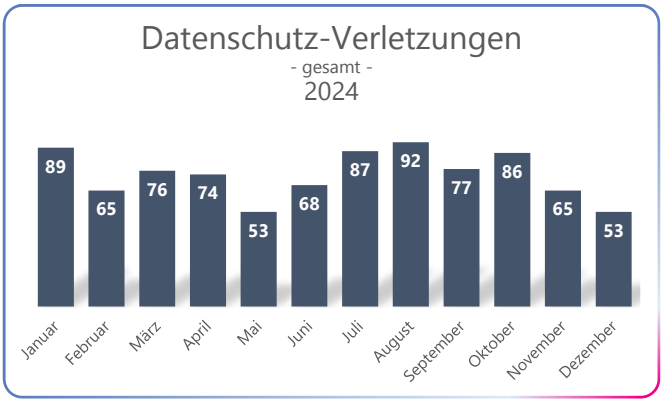

Abb. 5: Datenschutzverletzungen 2024

1.4 Abhilfemaßnahmen

Um drohende datenschutzrechtliche Verstöße zu verhindern oder festgestellte Verstöße zu sanktionieren, werden den Aufsichtsbehörden in Art. 58 Abs. 2 DSGVO verschiedene Abhilfemaßnahmen zur Verfügung gestellt, die sie – je nach Schwere der Verstöße – nach pflichtgemäßem Ermessen anwenden. Positiv hervorzuheben ist an dieser Stelle, dass sehr viele verantwortliche Stellen bereits im Laufe des Verwaltungsverfahrens reagieren und somit nur selten Anweisungen und Anordnungen getroffen werden müssen. Hier wird die Anzahl folgender Abhilfemaßnahmen der DSGVO aufgelistet, die im Berichtszeitraum getroffen wurden:

- Warnungen nach Art. 58 Abs. 2 lit. a DSGVO,
- Verwarnungen nach Art. 58 Abs. 2 lit. b DSGVO,
- Anweisungen und Anordnungen nach Art. 58 Abs. 2 lit. c – g und j DSGVO,
- Geldbußen nach Art. 58 Abs. 2 lit. i DSGVO sowie
- Widerruf von Zertifizierungen nach Art. 58 Abs. 2 lit. h DSGVO.

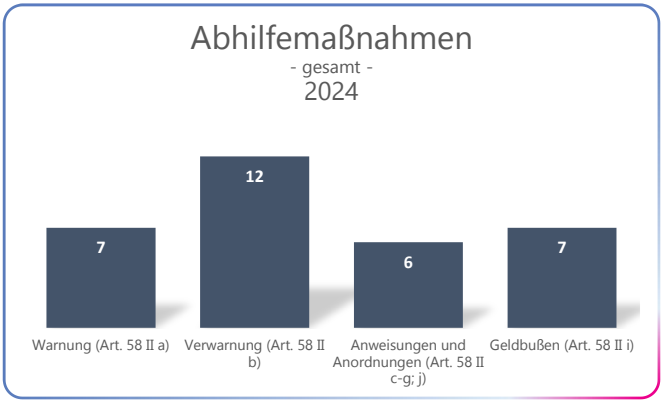

Abb. 6: Abhilfemaßnahmen (gesamt) 2024

1.5 Europäische Verfahren

Einen zunehmenden Stellenwert bei der Aufgabenwahrnehmung des UDZ kommt der Zusammenarbeit mit anderen europäischen Datenschutzaufsichtsbehörden zu.

Wie bereits im letzten Tätigkeitsbericht beschrieben, enthält die DSGVO in ihrem Kapitel VII für alle europäischen Datenschutzaufsichtsbehörden verbindliche Verfahrensvorgaben, die eine engere Zusammenarbeit und damit eine einheitliche Anwendung der DSGVO innerhalb der gesamten EU gewährleisten sollen. Obwohl der dadurch gestiegene Koordinierungsaufwand auch beim UDZ in zunehmendem Maße erhebliche personelle und zeitliche Ressourcen beansprucht, ist dieser Mehraufwand

wiederum durch den für alle Seiten gewinnbringenden europäischen Austausch gerechtfertigt.

Ein Teilaspekt dieser Verfahren besteht darin, dass nationale Datenschutzaufsichtsbehörden die Möglichkeit erhalten, auf Verfahren in anderen EU-Mitgliedstaaten Einfluss zu nehmen, sofern diese auch für die eigenen Bürger von Bedeutung sind. So kann jede Aufsichtsbehörde sicherstellen, dass die Rechte der Bürger im eigenen (Bundes-)Land gewahrt bleiben, selbst dann, wenn datenverarbeitende Stellen im innereuropäischen Ausland niedergelassen sind. Voraussetzung hierfür ist, dass die verantwortliche Stelle personenbezogene Daten „grenzüberschreitend" (Art. 4 Nr. 23 DSGVO) verarbeitet. Dies ist etwa dann der Fall, wenn Daten Betroffener durch Niederlassungen in mehreren EU-Mitgliedstaaten verarbeitet werden oder etwa wenn Personen in mehreren EU-Mitgliedstaaten von einer Verarbeitung erheblich betroffen sind.

	Bundesrepublik Deutschland	Saarland
Verfahren mit Betroffenheit Art. 56 Abs. 1	618	3
Verfahren mit Federführung Art. 56 Abs. 2	39	0
Verfahren gem. Kapitel VII DSGVO	3483	1276

Abb. 7: Europäische Verfahren (gesamt) 2024

Zu diesem Zweck hatte auch das UDZ im Jahr 2024 in insgesamt 618 Fällen zu beurteilen, inwieweit es als „betroffene Aufsichtsbehörde" im Sinne des Art. 4 Nr. 22 DSGVO gem. Art. 56 Abs. 1 DSGVO an diesen grenzüberschreitenden Verfahren zu beteiligen war, weil bspw. eine Niederlassung der verarbeitenden Stelle im Saarland existiert oder weil auch saarländische Bürger von einer konkreten Verarbeitung erheblich betroffen sein könnten.

In 3 Fällen wurde diese Betroffenheit für das UDZ bejaht.

Eine federführende Zuständigkeit i. S. v. Art. 56 Abs. 2 DSGVO lag im Berichtsjahr nicht beim UDZ.

Im gleichen Zeitraum hatte das UDZ zudem in insgesamt 3483 Fällen zu beurteilen, inwiefern eine Beteiligung an Verfahren gem. Kapitel VII (Zusammenarbeit und Kohärenz) vorlagen. In insgesamt 1276 Fällen traf dies zu. Hierzu zählen u.a. an das UDZ i. S. v. Art. 61 DSGVO gerichtete freiwillige Amtshilfeersuchen europäischer Aufsichtsbehörden, im Rahmen derer ein allgemeiner Austausch über diverse datenschutzrechtliche Fragestellungen erfolgte.

1.6 Förmliche Begleitung von Rechtsetzungsvorhaben

Hier werden die von dem Parlament und der Regierung angeforderten und durchgeführten Stellungnahmen zu Gesetzgebungsvorhaben genannt. Ein solches Vorhaben wird durch unsere Dienststelle einmal statistisch erfasst, selbst wenn die Stellungnahmen gegenüber unterschiedlichen Stellen in verschiedenen Verfahrensstadien erfolgen. Gerade bei Gesetzgebungsverfahren erfolgt unsere Beteiligung mitunter bereits im Rahmen der ressortinternen Entwurfserstellung, sodann bei der externen Anhörung und schließlich im Zusammenhang mit der parlamentarischen Anhörung im Landtag.

Im Berichtzeitraum wurde das Unabhängige Datenschutzzentrum Saarland (UDZ) hiernach in 16 Rechtsetzungsvorhaben verfahrensbegleitend tätig.

1.7 Gerichts- und gerichtliche Bußgeldverfahren

In 2024 führte das Unabhängige Datenschutzzentrum insgesamt 6 Gerichts- und 18 Bußgeldverfahren.

1.8 Presseanfragen

In 2024 wurden insgesamt 26 Presseanfragen an hiesige Dienststelle gerichtet.

II.

Rechtsetzungsverfahren

2 Rechtsetzungsverfahren

Gemäß § 19 Abs. 2 Satz 1 SDSG ist die Landesbeauftragte für Datenschutz vor dem Erlass von Rechts- und Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten betreffen, zu hören. Da der Landtag ausweislich des § 2 Abs. 1 Satz 4 SDSG grundsätzlich nicht Adressat der Bestimmungen des SDSG ist, betrifft die Verpflichtungen zur Anhörung vor allem Landes- und Kommunalbehörden bevor sie Rechtsvorschriften (bspw. Gesetze, Verordnungen, Satzungen) oder Verwaltungsvorschriften (bspw. Dienstanweisungen) erlassen oder – im Falle der Landesregierung – ins parlamentarische Gesetzgebungsverfahren einbringen. Im Berichtszeitraum wurden wir in den folgenden Angelegenheiten nach § 19 Abs. 2 Satz 1 SDSG im Rahmen der internen oder externen Anhörung durch die federführenden Ministerien beteiligt.

2.1 Schulwesen-Datenschutzgesetz

Zum 02.08.2024 trat das Schulwesen-Datenschutzgesetz (SchulwDSG) und zum 23.08.2024 die Schulwesen-Datenschutzverordnung (SchulwDSV) im Saarland in Kraft. Mit diesen Rechtsnormen hat das Ministerium für Bildung und Kultur einen eigenständigen Rechtsrahmen für die Datenverarbeitung im schulischen Bereich geschaffen und damit auf die Anforderungen des digitalen Wandels in der Schullandschaft reagiert und letztendlich auch die seit langem erforderlichen Änderungen und Anpassungen an die Datenschutz-Grundverordnung vorgenommen.

Schon frühzeitig wurden wir vom Ministerium bei der Gestaltung dieser Rechtsnormen eingebunden. In zahlreichen Sitzungen wurden Entwürfe diskutiert, Szenarien der Datenverarbeitung aus dem Schulalltag eruiert und gemeinsam versucht, einen möglichst umfassenden Rechtsrahmen zu schaffen, der den digitalen und analogen Schulalltag datenschutzrechtlich abbildet und legitimiert. Durch die konstruktive Zusammenarbeit unserer Behörden konnte ein Großteil unserer Anmerkungen und Anregungen in die Entwürfe des Gesetzes und der nach Verab-

schiedung des Gesetzes erlassenen Verordnung aufgenommen werden.

Einzig in zwei Punkten sahen wir im Rahmen der parlamentarischen Beratungen zum SchulwDSG noch Änderungsbedarf, welchem aber letztlich nicht entsprochen wurde. Zum einen ging es dabei um die Problematik des Einsatzes von sogenannten Telepräsenzavataren, den wir in diesem Tätigkeitsbericht ausführlich unter Punkt 7.1 beschreiben. Zum anderen sahen wir einen Konkretisierungsbedarf in § 10 SchulwDSG, der die Datensicherheit bei der Verarbeitung personenbezogener Daten in Schulen betrifft. Hier hielten wir es für erforderlich, den Schulen die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten präzise und von informationstechnisch professioneller Seite vorzugeben. Hiermit sollte vor allem erreicht werden, dass nicht die jeweilige Schulleitung in der Pflicht ist, entscheiden zu müssen, welche konkreten technischen Maßnahmen zum Schutz der personenbezogenen Daten ausreichend und angemessen sind. Das hierfür notwendige Fachwissen kann unseres Erachtens nicht vom zuständigen Lehrpersonal erwartet werden. Durch eine entsprechende Verordnung hätte man zudem saarlandweit einheitliche hohe Datensicherheitsstandards für die Schulen und Schulträger vorgeben können. Diese Möglichkeit wurde leider nicht ergriffen.

Nun gilt es, die neuen gesetzlichen Vorgaben im Schulalltag zu etablieren und praxisnah umzusetzen. Hierzu wurde vom Ministerium für Bildung und Kultur angekündigt, für alle saarländischen Schulen diverse Leitlinien für ein datenschutzkonformes Handeln in der Praxis zu entwickeln. Wir würden es beispielsweise sehr begrüßen, wenn den Schulen seitens des Ministeriums ein saarlandweit einheitliches Formular zur Art und Weise der Veröffentlichung von Schülerfotos auf einer schuleigenen Internetpräsenz oder in der lokalen Presse zur Verfügung gestellt würde.

Fazit

Durch die frühzeitige Einbindung unserer Behörde im Gesetzgebungsprozess und die gute und konstruktive Zusammenarbeit mit dem Ministerium für Bildung und Kultur sind nunmehr gesetzliche Regelungen geschaffen worden, die aus datenschutzrechtlicher Sicht Rechtssicherheit im Schulalltag herstellen können.

2.2 Maßregelvollzugsgesetz

Die frühzeitige Berücksichtigung datenschutzrechtlicher Implikationen bei Gesetzesvorhaben trägt wesentlich zu Rechtssicherheit und zur Vermeidung späterer Korrekturen bei. Wenn unsere Behörde, wie dies § 19 Abs. 2 des Saarländischen Datenschutzgesetzes (SDSG) vorsieht, von Beginn an in die Erarbeitung neuer Regelungen einbezogen wird, können datenschutzrechtliche Erfordernisse bereits in der Entwurfsphase identifiziert und berücksichtigt werden. Dies ermöglicht eine effiziente Gestaltung von Gesetzen und verhindert aufwändige nachträgliche Anpassungen.

Ein positives Beispiel stellt die frühzeitige Einbindung unserer Behörde bei der geplanten Novellierung des saarländischen Abfallwirtschaftsgesetzes (SAWG) dar[1], bei der wesentliche datenschutzrechtliche Aspekte bereits frühzeitig erörtert werden können. Im Gegensatz dazu erfolgte die Beteiligung des Unabhängigen Datenschutzzentrums Saarland an der Novellierung des Maßregelvollzugsgesetzes (MRVG) erst im Rahmen der finalen Entwurfsphase. Dennoch konnten wir vor Einbringung des Gesetzentwurfs in das parlamentarische Verfahren noch auf datenschutzrechtliche Bedarfe aufmerksam machen und auf notwendige Änderungen hinwirken.

[1] Siehe hierzu den Beitrag zur Videoüberwachung von Wertstoffcontainern in Kapitel 9 des vorliegenden Tätigkeitsberichts.

Die Notwendigkeit einer Anpassung des MRVG ergab sich dabei nicht nur aus der Tatsache, dass die darin enthaltenen Normen seit dem Jahr 1989 im Wesentlichen unverändert geblieben waren, sondern auch daraus, dass die Umsetzung der europäischen Richtlinie (EU) 2016/680 (JI-Richtlinie) seit fast sieben Jahren (Mai 2018) aussteht. Die genannte Richtlinie bestimmt den Rahmen der Verarbeitung personenbezogener Daten durch Behörden im Kontext der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

Da der Maßregelvollzug zum einen der medizinischen Versorgung und Heilung der untergebrachten Person, zum anderen aber vor allem auch der Gefahrenabwehr (Schutz der Allgemeinheit vor von der untergebrachten Person ausgehenden Gefahren) dient, unterliegt die Datenverarbeitung im Maßregelvollzug den Anforderungen der JI-Richtlinie. Die bislang existierenden datenschutzrechtlichen Vorgaben des MRVG genügen den dortigen Voraussetzungen jedoch nicht.

In unserer ersten Stellungnahme zu den geplanten Neuerungen des Gesetzentwurfs befassten wir uns deswegen mit der Umsetzung der JI-Richtlinie im Allgemeinen und der Ausgestaltung einzelner Rechtsgrundlagen im Speziellen. Problematisch war unserer Ansicht nach, dass der Gesetzentwurf weitgehend auf pauschale Verweisungen auf andere Fachgesetze setzte und sich auf generalklauselartige Regelungen beschränkte, anstatt aus Gründen der Bestimmtheit und Normenklarheit konkrete Bedingungen für die typischen Verarbeitungssituationen im Maßregelvollzug zusammen mit den spezifischen Voraussetzungen der JI-Richtlinie im MRVG selbst zu regeln.

Insbesondere, weil im Maßregelvollzug gerade auch besonders sensible Informationen der untergebrachten Personen verarbeitet werden, forderten wir eine eingehende Prüfung, ob für bestimmte Verarbeitungsvorgänge aufgrund ihres Eingriffsgewichts gesonderte Rechtsgrundlagen zu schaffen wären. Dies

betraf insbesondere die Möglichkeit der Datenübermittlung sowie die geplante Verwendung personenbezogener Daten von Patienten zu Forschungszwecken. In diesem Zusammenhang empfahlen wir eine strikte Begrenzung auf anonymisierte Datensätze.

Weiter forderten wir, im Gesetz angelegte Fristen mit konkreten Zeitvorgaben zu versehen und so etwa die zulässige Dauer von Eingriffsmaßnahmen sowie die Aufbewahrungszeit von personenbezogenen Daten (Aufbewahrungs- bzw. Löschfristen) konkret zu beziffern. Hinsichtlich der im Gesetzentwurf enthaltenen, speziellen Rechtsgrundlagen für die Durchführung von Videoüberwachungsmaßnahmen und zur Einschränkung der Telekommunikation machten wir ebenfalls Anmerkungen. So forderten wir teilweise redaktionelle Änderungen zur Verbesserung des Verständnisses und regten an, die Reichweite der vorgesehenen Eingriffe zu begrenzen.

In zeitlicher Nähe zum Redaktionsschluss des vorliegenden Tätigkeitsberichts wurde eine angepasste Version des Gesetzentwurfs an den Ministerrat zur Beschlussfassung über die Einbringung der Vorlage in den Landtag übersandt. Einige der von uns angemerkten Aspekte wurden in dieser Fassung bereits berücksichtigt. Es bleibt abzuwarten, ob und ggf. welche weiteren datenschutzrechtlichen Anpassungen im weiteren parlamentarischen Verfahren vorgenommen werden.

2.3 Kommunale Wärmeplanung

Die kommunale Wärmeplanung, welche das Ziel verfolgt, eine kostengünstige und effiziente Wärmeversorgung für die Zukunft zu sichern, erfordert eine umfangreiche Erhebung hierauf bezogener Informationen. Obzwar hierbei keine unmittelbaren Auskünfte zu den jeweiligen Eigentümern von Immobilien und sonstigen Hausbewohnern erforderlich sind, beinhaltet die Wärmeplanung gleichwohl Aussagen zu den jeweiligen Immobilien, die Art derer Wärmeversorgung sowie Angaben zum Wärmenergieverbrauch. Diese Informationen stellen, zumindest

mittelbar, personenbezogene Daten dar und unterfallen daher den datenschutzrechtlichen Bestimmungen.

Das im 1. Januar 2024 in Kraft getretene Gesetz für die Wärmeplanung und zur Dekarbonisierung der Wärmenetze (Wärmeplanungsgesetz – WPG) trägt diesem Umstand Rechnung und enthält in seinem 3. Abschnitt ausführliche Vorgaben für den Datenschutz. Den Dreh- und Angelpunkt bildet hierbei die „planungsverantwortliche Stelle". Selbige ist nach § 10 WPG befugt, zu Zwecken der wärmeplanungsrechtlichen Bestands- (§ 15 WPG) und/oder Potentialanalyse (§ 16 WPG) die erforderlichen Daten zu verarbeiten. Sie darf hierzu auf öffentliche Register zugreifen (§ 10 Abs. 3 WPG) und in weitem Umfang immobilienbezogene Auskünfte einholen, etwa bei Behörden, Energieversorgern sowie Bezirksschornsteinfegern (§ 11 Abs. 1 WPG).

§ 33 WPG ermöglicht es dem Land, als originär planungsverantwortlichen Stelle, die Pflicht zur Erstellung der Wärmepläne durch Rechtsverordnung auf die Kommunen oder sonstige Rechtsträger zu übertragen und diese damit als planungsverantwortliche Stellen zu bestimmen. Mit dem am 29. November 2024 in Kraft getretenen Wärmeplanungsumsetzungsgesetz (WPUG) hat das Saarland hiervon Gebrauch gemacht. Die saarländischen Städte und Gemeinden sind nach § 3 Abs. 1 WPUG nunmehr planungsverantwortliche Stellen und haben sicherzustellen, dass auf ihrem Stadt-/Gemeindegebiet Wärmepläne nach Maßgabe des Wärmeplanungsgesetzes rechtzeitig erstellt werden.

Flankiert wird das WPUG durch das zeitgleich in Kraft getretene Gesetz zur Umsetzung von Solarkatastern und landesweiter Datenbereitstellungen (Solarkataster- und Datenbereitstellungsumsetzungsgesetz (SDUG)).[2] Als Annex zu der vorgenannten Datenverarbeitungskompetenz der Städte und Gemeinden (planungsverantwortliche Stellen), enthält dieses Gesetz in § 3

[2] Siehe hierzu auch 5.1. „Bereitstellung onlinebasierter Solarkataster".

Abs. 1 zusätzlich folgende eigene Verarbeitungsbefugnis für das Land:

> *„Soweit eine planungsverantwortliche Stelle Daten, die für die Aufgabenerfüllung nach § 15 und § 16 des Wärmeplanungsgesetzes erforderlich sind, nicht oder nicht vollständig erhoben hat oder das Land ein berechtigtes Interesse hat, darf das für Energie zuständige Ministerium anstelle der planungsverantwortlichen Stelle diese Daten nach Maßgabe des Abschnitts 3 des Wärmeplanungsgesetzes erheben und verarbeiten, soweit dies zur Erfüllung im öffentlichen Interesse liegender Aufgaben erforderlich ist."*

Diese Norm ist nach hiesiger Auffassung sowohl europarechtswidrig als auch mit höherrangigem Bundesrecht nicht zu vereinbaren.

Seine dogmatischen Anleihen findet § 3 Abs. 1 (2. Alt.) SDUG in Art. 6 Abs. 1 lit. f DSGVO, wonach eine Verarbeitung personenbezogener Daten rechtmäßig ist, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die entgegenstehenden Interessen der betroffenen Person nicht überwiegen.

Nach der Rechtsprechung des EuGH sind nationalrechtliche Generalklauseln, welche eine mehr oder weniger bloße Wiederholung der Bestimmungen der DSGVO darstellen, in diesem Zusammenhang einer Wiederholung des Wortlauts von Art. 6 Abs. 1 lit. f DSGVO, nicht europarechtskonform.[3]

Will das Land im Rahmen der Wärmeplanung eine eigene Datenverarbeitung vornehmen, ist dies allenfalls im Rahmen einer öffentlichen Aufgabenwahrnehmung nach Art. 6 Abs. 1 lit. e DSGVO denkbar. Die gesetzlichen Aufgaben müssen durch den nationalen Normgeber sodann jedoch hinreichend bestimmt formuliert werden (Art. 6 Abs. 3 lit. b DSGVO).

Eine auf eine behördliche Aufgabenwahrnehmung gerichtete Generalklausel, welche, wie vorliegend, das Tatbestandsmerk-

[3] Urteil vom 30. März 2023 – C-34/21.

mal des vieldeutigen und daher in hohem Maße auslegungsbedürftigen Begriffs des „berechtigten Interesses“ bemüht, läuft dem Regelungszweck des Art. 6 Abs. 1 DSGVO zuwider. In eindeutiger Form geht dies aus Art. 6 UAbs. 2 DSGVO hervor, welcher bestimmt, dass sich Behörden in Erfüllung ihrer Aufgaben nicht auf Art. 6 Abs. 1 lit. f DSGVO, mithin nicht auf ein berechtigtes Interesse, berufen können. Seinen Grund findet dies darin, dass es nicht der handelnden Behörde obliegt, im Zuge einer Interessenabwägung tätig zu werden, sondern den Gesetzgeber die Pflicht trifft, den diesbezüglichen Rechtsrahmen und damit auch die Grenzen der Aufgabenerfüllung, eindeutig zu bestimmen.

§ 3 Abs. 1 SDUG ist darüber hinaus nicht mit den Bestimmungen des Wärmeplanungsgesetzes in Einklang zu bringen. In letzterem findet sich für die Länder gerade keine Befugnis, eine Doppelzuständigkeit im Bereich der Datenverarbeitung zu regeln. Die jeweiligen planungsverantwortlichen Stellen sind vielmehr alleinzuständig für die Datenverarbeitungen nach § 10 WPG, deren Zwecke darüber hinaus auch nicht durch Landesrecht erweiterbar sind.

2.4 Videoüberwachung an Wertstoffcontainern

Die Videoüberwachung von Wertstoffcontainern, vorwiegend für Glasflaschen, Kartonagen sowie Altpapier, aber auch von sonstigen öffentlichen Wertstoffsammeleinrichtungen beschäftigt unsere Behörde bereits seit längerer Zeit. Grund hierfür ist, dass sich die Problematik der illegalen Müllentsorgung an diesen Einrichtungen für viele Kommunen als immer belastender erweist. Auch die Kosten zur regelmäßigen Beseitigung der Vermüllung an den Standorten werden zunehmend als nicht mehr tragbar erachtet.

Die Idee einer punktuellen Videoüberwachung zu präventiven, abschreckenden Zwecken ist vor diesem Hintergrund nicht neu. Ihre Verwirklichung scheitert bislang jedoch vornehmlich an dogmatischen Grenzen. Bis dato besteht nämlich keine gesetz-

liche Grundlage, welche es den Kommunen ermöglicht, eine Videoüberwachung – in welcher Gestalt auch immer – in diesem Bereich einzusetzen.

Eine Videoüberwachung von Wertstoffcontainern durch die Kommunen, welche sich darauf richtet, an diesen Standorten illegale Müllablagerungen zu verhindern, ist weder im Rahmen der Wahrnehmung des Hausrechts noch im Zuge der sonstigen Aufgabenerfüllung nach § 25 des Saarländischen Datenschutzgesetzes (SDSG) möglich. Seinen Grund findet dies in einer gesetzlichen Sonderzuweisung nach dem Abfallwirtschaftsgesetz und dem hieraus resultierenden Vorrang des Polizeirechts. Nach § 36 Abs. 1 S. 1 des Saarländischen Abfallwirtschaftsgesetzes (SAWG) sind es die Ortspolizeibehörden, welche verpflichtet sind dafür Sorge zu tragen, dass Abfälle nicht ohne Genehmigung außerhalb der dafür zugelassenen Abfallentsorgungsanlagen beseitigt werden. Insbesondere sind die Ortspolizeibehörden dazu verpflichtet, die ordnungsgemäße Beseitigung anzuordnen und diese auch durchzusetzen. Ortspolizeibehörden sind gemäß § 76 Abs. 3 des Saarländischen Polizeigesetzes (SPolG) die Bürgermeisterinnen oder die Bürgermeister.

Rechtsfolge dieser Kompetenzzuweisung ist, dass für Videoüberwachungsmaßnahmen durch die Ortspolizeibehörden nicht die Bestimmungen des § 25 SDSG, sondern ausschließlich die spezialgesetzlichen Vorschriften des Saarländischen Gesetzes über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG) Anwendung finden. Letztere regeln jedoch ausschließlich die Videoüberwachung (Bild- und Tonaufzeichnungen) durch die Vollzugspolizei (§ 32 SPolDVG) und enthalten gerade keine diesbezüglichen Befugnisse für die Ortspolizeibehörden.

Man kann in dem Fehlen dieser Befugnis auch keine Art Regelungslücke des Gesetzes erblicken, da es sich tatsächlich um eine bewusste Entscheidung des Saarländischen Gesetzgebers handelte, die bis zum 18. Dezember 2014 bestandene Möglich-

keit einer Videoüberwachung durch die Ortspolizeibehörden[4] entfallen zu lassen.

Für den Bereich des Abfallwirtschaftsgesetzes bereitet nunmehr das federführende Ministerium für Umwelt, Klima, Mobilität, Agrar und Verbraucherschutz einen Gesetzentwurf vor, bei dem wir beratend hinzugezogen wurden und der im Rahmen eines auf fünf Jahre befristeten Pilotprojekts die Möglichkeit einer präventiven Videoüberwachung an besonders vermüllten Wertstoffsammeleinrichtungen gestatten soll.

[4] Vgl. § 27 Abs. 2 S. 2 SPolG, LT-Drs. 15/899, 5

III.

Datenschutzaufsicht

3 Datenschutzaufsicht

3.1 Beschwerdeverfahren

3.1.1 Bedingungen der aufsichtsbehördlichen Befassung mit Beschwerden

Die Datenschutzbehörde ist die „*Garantin der Einhaltung der Bestimmungen der DSGVO*";[5] diese aufsichtsbehördliche Rolle und der damit verbundene Schutz- und Überwachungsauftrag hat seine primärrechtliche Grundlage in Art. 8 Abs. 2 Grundrechtecharta der Europäischen Union (EU-GRCh) und wird hinsichtlich der Aufgaben in Art. 57 DSGVO konkretisiert.

Unter den in der Vorschrift aufgezählten Aufgaben sticht die in Art. 57 Abs. 1 lit. f DSGVO geregelte Befassung mit Beschwerden heraus. Die Vorschrift verpflichtet die Aufsichtsbehörden, sich mit Beschwerden zu befassen, den Gegenstand des Anliegens angemessen zu untersuchen und die beschwerdeführende Person oder Stelle binnen einer angemessenen Frist über den Fortgang und das Ergebnis der Befassung zu unterrichten. Spiegelbildlich dazu verleihen Art. 77 und 78 Abs. 1 DSGVO der von einer Datenverarbeitung betroffenen Person das Recht auf Beschwerde bei einer Aufsichtsbehörde und die Möglichkeit der gerichtlichen Überprüfung der aufsichtsrechtlichen Beschwerdeentscheidung.

Die Beschwerde ist damit nicht nur das zentrale Instrument, das Unionsbürgerinnen und -bürgern zur individuellen Durchsetzung ihres in Art. 8 EU-GRCh garantierten Grundrechts auf Schutz personenbezogener Daten dient, sondern auch „*wertvolle Informationsquelle fur die Aufsichtsbehörde* [...], *die es ihr ermoglicht, Verstoße aufzudecken*".[6] Eine, wenn nicht die aufsichtsbehördliche Kernaufgabe bildet damit letztlich die Befassung mit Beschwerden betroffener Personen.

[5] Schlussanträge des Generalanwalts Pikamäe vom 16. März 2023 – verbundene Rechtssachen C-26/22 und C-64/22, Rn. 41.

[6] Schlussanträge des Generalanwalts Pikamäe, a. a. O., Rn. 39.

3.1.2 Aufsichtsbehördliches Ermessen

Auch wenn der Verordnungsgeber den Aufsichtsbehörden bereits verfahrensbezogene Parameter zur Beschwerdebefassung unmittelbar in Art. 57 Abs. 1 lit. f DSGVO und Erwägungsgrund 141 vorgibt, hat der Europäische Gerichtshof die Rahmenbedingungen dieser aufsichtsbehördlichen Pflichtaufgabe in seiner Rechtsprechung fortwährend konkretisiert.

So gebietet die mit Blick auf Art. 57 Abs. 1 lit. f DSGVO und Erwägungsgrund 141 zu fordernde Angemessenheit der Untersuchung „*eine solche Beschwerde mit aller gebotenen Sorgfalt* [zu] *bearbeiten*."[7] Dieser gerichtlich statuierten Pflicht zur Sorgfalt liegt zugrunde, dass einem potenziellen Datenschutzverstoß grundsätzlich eine Verletzung des Grundrechts auf Schutz personenbezogener Daten innewohnt und damit ein Ermessen der Aufsichtsbehörde, ob sie sich überhaupt mit einer Beschwerde befasst, mit ihrem gesetzlichen Auftrag zur Wahrung eines gleichmäßigen und hohen Schutzniveaus für personenbezogene Daten nicht in Einklang gebracht werden kann.[8]

Sind somit bei Beschwerdeeinlegung Anhaltspunkte für das Vorliegen eines Datenschutzverstoßes erkennbar, ist die Aufsichtsbehörde grundsätzlich zum Tätigwerden angehalten. Hinsichtlich der Untersuchungs- und Abhilfebefugnisse nach Art. 58 Abs. 1 und 2 DSGVO kommt ihr jedoch mit Blick auf die verfahrensindividuell angemessenen und geeigneten Maßnahmen, um dem festgestellten Verstoß zu begegnen und damit der Beschwerde abzuhelfen, regelmäßig ein Auswahlermessen zu.[9] Auch wenn das Vorliegen eines Verstoßes somit grundsätzlich eine aufsichtsrechtliche Maßnahme bedingt, betont die Rechtsprechung, dass nach den Umständen des Einzelfalls jedoch auch die Entscheidung für einen vollständigen Verzicht auf

[7] EuGH, Urteil vom 16. Juli 2020 – C-311/18, Rn. 109.

[8] Schlussanträge des Generalanwalts Pikamäe, a. a. O., Rn. 39.

[9] Schlussanträge des Generalanwalts Saugmandsgaard Øe vom 19. Dezember 2019- C-311/18, Nr. 146 ff.; EuGH, Urteil vom 7. Dezember 2023 - C-26/22 und C-64/22, Rn. 68 und Urteil vom 26. September 2024 – C-768/21, Rn. 37 ff.

Abhilfebefugnisse nach Art. 58 Abs. 2 DSGVO ermessensfehlerfrei sein kann.[10] Insbesondere dann, wenn ein Datenschutzverstoß ein singuläres Ereignis darstellt, das somit gerade nicht auf strukturelle Missstände bei der Verarbeitung personenbezogener Daten zurückzuführen ist, und der Beschwerdegegner eigeninitiativ effektive Maßnahmen zur Vermeidung vergleichbarer Verstöße ergriffen hat, kann ein solcher Verzicht auf aufsichtsrechtliche Maßnahmen in Frage kommen.

Unter Berücksichtigung dieser mit dem Ziel der Gewährleistung eines effektiven Grundrechtsschutzes gesetzlich vorgegebenen und gerichtlich konturierten Aufgabenbeschreibung, kann letztlich für das Verfahren der aufsichtsbehördlichen Beschwerdebefassung, entgegen der in der Vergangenheit häufig vertretenen Auffassung,[11] keine petitionsähnliche Verfasstheit mehr angenommen werden.

3.1.3 Rechtsnatur und gerichtliche Kontrolle der Entscheidung über die Beschwerde

Den formellen Verfahrensabschluss bildet die an die beschwerdeführende Person adressierte Mitteilung über das Ergebnis der Beschwerdebefassung, die nach Art. 77 Abs. 2 in Verbindung mit Art. 78 Abs. 1 DSGVO als rechtsverbindlicher Beschluss ausgestaltet ist. Gegen diesen Beschluss der Aufsichtsbehörde muss die beschwerdeführende Person nach Art. 78 Abs. 1 und 2 DSGVO einen wirksamen gerichtlichen Rechtsbehelf bei einem nationalen Gericht geltend machen können. Mit Blick auf das für

[10] EuGH, Urteil vom 26. September 2024 – C-768/21, Rn. 41 ff.; VG Berlin, Urteil vom 12. Oktober 2023 - VG 1 K 561/21, Rn. 69, openjur mit Betonung, dass eine aufsichtsrechtliche Maßnahme als Verstoß gegen das Übermaßverbot qualifiziert werden kann; VG Düsseldorf, Urteil vom 11. November 2024 – 29 K 4853/22, Rn. 78 ff., juris.

[11] Schlussanträge des Generalanwalts Pikamäe, a. a. O., Rn. 42; EuGH, a. a. O., Rn. 58; noch für ein petitionsähnliches Verfahren eintretend: OVG Rheinland-Pfalz, Urteil vom 26. Oktober 2020 – 10 A 10613/20 Rn. 29, juris; VGH Baden-Württemberg, Urteil vom 22. Januar 2020 – 1 S 3001/19 Rn. 51, juris; SG Frankfurt (Oder), Urteil vom 8. Mai 2019 – S 49 SF 8/19; VG Berlin, Beschluss vom 28. Januar 2019 – 1 L 1.19; VG des Saarlandes, Gerichtsbescheid vom 30. Juni 2023 - 5 K 1191/21.

die deutschen Aufsichtsbehörden jeweils geltende Verwaltungsverfahrensrecht stellen diese unionsrechtlichen Beschlüsse daher klassische Verwaltungsakte[12] dar, die unmittelbar mittels Klage vor dem örtlich zuständigen Verwaltungsgericht angegriffen werden können.[13]

Unter Bezugnahme auf den flankierenden Erwägungsgrund 141 soll insbesondere für den Fall, dass die Aufsichtsbehörde auf eine Beschwerde hin nicht tätig wird, eine Beschwerde teilweise oder ganz abweist oder ablehnt oder nicht tätig wird, obwohl dies zum Schutz der Rechte der betroffenen Person notwendig ist, ein gerichtlicher Rechtsbehelf möglich sein. Allerdings beschränkt sich dieser unionsrechtliche Rechtsschutz nicht auf belastende aufsichtsbehördliche Beschlüsse; vielmehr hat die beschwerdeführende Person auch für den Fall, dass ihrer Beschwerde abgeholfen wurde, aber beispielsweise trotz eines festgestelltes Datenschutzverstoßes keine oder aus ihrer subjektiven Sicht „zu milde" Sanktionen ergriffen wurden, das Recht das gesamte aufsichtsrechtliche Handeln und die damit verbundenen Sach- und Rechtsfragen im Zusammenhang mit der Beschwerdebefassung einer vollumfänglichen gerichtlichen Nachkontrolle zuzuführen.[14]

Allerdings sehen – wie bereits ausgeführt – weder die Verordnung noch die Rechtsprechung einen subjektiven Rechtsanspruch auf das Ergreifen spezifischer aufsichtsbehördlicher Einzelmaßnahmen vor, so dass sich die nachgelagerte gerichtliche Überprüfung auf potenzielle Ermessensfehler bei der Auswahl der im Einzelfall adäquaten aufsichtsbehördlichen Maßnahmen beschränkt.[15]

[12] Boehm, in Simitis/Hornung/Spieker gen. Döhmann, Datenschutzrecht, 2. Auflage 2025, Art. 77 Rn. 21.

[13] § 20 Abs. 3 und 6 Bundesdatenschutzgesetz.

[14] EuGH, Urteil vom 7. Dezember 2023 - C-26/22 und C-64/22, Rn. 59.

[15] EuGH, a. a. O, Rn. 68 und 69 sowie Urteil vom 26. September 2024 - C-768/21, Rn. 41; VG des Saarlandes, Urteil vom 30. Oktober 2024 – 5 K 1176/21.

3.1.4 Unterrichtung über die Ergebnisse der Beschwerde

Im Lichte dieses unionsrechtlichen, durch die Rechtsprechung konturierten Rechtsschutzes ist auch die in Art. 77 Abs. 2 DSGVO geregelte Unterrichtungspflicht auszulegen. Die der beschwerdeführenden Person nach Verfahrensabschluss von der Aufsichtsbehörde zu gebende Pflichtinformation über die „*Ergebnisse der Beschwerde*" ist dabei notwendigerweise in Anlehnung an die Rechtsprechung nicht mit einem Ausschweigen über konkret ergriffene Aufsichtsmaßnahmen zu vereinbaren. Neben der Information über die Stattgabe einer Beschwerde und damit verbunden die Feststellung eines Verstoßes gegen die Verordnung, erfasst „Ergebnisse" somit gerade auch die Abhilfebefugnisse nach Art. 58 Abs. 2 DSGVO, von denen im jeweiligen Verfahren Gebrauch gemacht wurde;[16] ferner sind – mit Blick auf die Nachvollziehbarkeit der aufsichtsbehördlichen Ermessensentscheidung – notwendigerweise die Gründe, auf die sich die im beschwerdegegenständlichen Fall erfolgende Entscheidung über ergriffene aufsichtsrechtliche Maßnahmen stützt, darzustellen.[17]

3.1.5 Faktische Grenzen

Während die Beschwerde aus Sicht der Aufsichtsbehörden die vorrangige Erkenntnisquelle über potenzielle Datenschutzverstöße darstellt, ist sie für betroffene Personen ein Instrument, um ihrem Grundrecht auf Schutz personenbezogener Daten unmittelbar Geltung zu verschaffen. Diese wesentliche Funktion der Beschwerde und das damit verbundene Schutzziel stoßen allerdings schnell an die faktischen Grenzen der aufsichtsbehördlichen Ressourcenwirklichkeit.

Auch wenn nach dem Willen des Verordnungsgebers eine zügige Bearbeitung durch die mit dem Vollzug der DSGVO beauf-

[16] Schlussanträge des Generalanwalts Pikamäe vom 11. April 2024 in der Rechtssache C-768/21, Rn. 41 und 42.

[17] EuGH, Urteil vom 26. September 2024 - C-768/21, Rn. 49.

tragten mitgliedstaatlichen Behörden die Regel sein soll, sind angesichts der Vielzahl und Vielgestaltigkeit von Anliegen, die an die Aufsichtsbehörde adressiert werden, die Möglichkeiten zur zeitnahen, sachgerechten Beschwerdebefassung behördenindividuell begrenzt.

Da die unterschiedslose Gewährleistung subjektiver Rechte der beschwerdeführenden Personen bei der Beschwerdebefassung keine von der Behörde selbst gewählten Schranken – bspw. anhand von Erheblichkeitsschwellen eines Datenschutzverstoßes, hinsichtlich der Anzahl an Beschwerden oder potenziell betroffenen Personen – zulässt, führt dies unweigerlich zu den oftmals angeprangerten[18] langen Verfahrensdauern. Vor diesem Hintergrund schafft die Rechtsprechung des EuGH[19] mit Blick auf die Grenzen des einzelfallbezogenen Verzichts auf Abhilfebefugnisse weitere Klarheit hinsichtlich des aufsichtsbehördlichen Ermessensspielraums, bietet aber angesichts enger Grenzen beim Verzicht auf Abhilfebefugnisse in Bagatellfällen keine wesentlichen Erleichterungen bei der Beschwerdebefassung. Ungeachtet dessen gilt es, um dem grundrechtlichen Schutzauftrag und dem Gebot der „*guten Verwaltung*"[20] auch mit Blick auf die Verfahrensdauer gerecht zu werden, die aufsichtsrechtlichen Prozesse und Vorgehensweisen kontinuierlich auf Möglichkeiten der Effektivierung hin zu untersuchen.[21]

3.2 Datenschutzaufsicht über den Landtag

Das Verhältnis des Europäischen Datenschutzrechts zu den nationalen Rechtsordnungen, auch im legislativen Bereich, ist seit Inkrafttreten der DSGVO Gegenstand intensiver Diskussionen.

[18] Pressemitteilung noyb: noyb-Sieg: 4,75 Millionen Euro Strafe gegen Netflix; abrufbar unter https://noyb.eu/de/noyb-win-dutch-authority-fines-netflix-eu475-million

[19] Urteil vom 26. September 2024 – C-768/21.

[20] Schlussanträge des Generalanwalts Pikamäe vom 16. März 2023 – verbundene Rechtssachen C-26/22 und C-64/22, Rn. 40.

[21] Siehe in Bezug auf Beschwerden zu Videoüberwachungsmaßnahmen 32. Tätigkeitsbericht Datenschutz 2023, 9.1 Verwaltungsvorschrift zum Umgang mit Beschwerden.

Dies betrifft unter anderem die Frage der Anwendbarkeit der DSGVO auf Datenverarbeitungen der nationalen Parlamente (Landes-/Bundesparlamente) im Kontext ihrer legislativen Tätigkeit.

3.2.1 Bisherige Rechtsauffassung unserer Behörde

Das Unabhängige Datenschutzzentrum vertrat bislang die Rechtsauffassung, dass die Regelungen der DSGVO keine Anwendung auf die Verarbeitung personenbezogener Daten durch die nationalen Parlamente finden, soweit diese Datenverarbeitung im Zusammenhang mit dem legislativen Beratungs- und Entscheidungsprozess steht. Diese Sichtweise gründete auf folgenden rechtlichen Überlegungen.

Gemäß Art. 2 Abs. 2 lit. a findet die DSGVO keine Anwendung auf die Verarbeitung personenbezogener Daten, „(…) *im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt*". Die diesbezügliche Aussage ist als Klarstellung zu begreifen und nimmt Bezug auf den unionsrechtlichen Grundsatz der begrenzten Einzelermächtigung. Gemäß Art. 5 Abs. 1 S. 1, Abs. 2 EUV wird die EU hiernach nur innerhalb der Grenzen derjenigen Zuständigkeiten tätig, welche die Mitgliedstaaten ihr in den Verträgen zur Verwirklichung der darin niedergelegten Ziele zuvor übertragen haben. Alle der Union nicht in den Verträgen übertragenen Zuständigkeiten verbleiben bei den Mitgliedstaaten.

Aus diesem Grundsatz leiteten auch wir bis dato ab, dass neben den in Erwägungsgrund Nr. 16 der DSGVO genannten Tätigkeiten der nationalen Sicherheit, auch die parlamentarische Organisation innerhalb der Mitgliedstaaten sowie die nationalverfassungsrechtliche Ausgestaltung des Abgeordnetenmandats als vom Anwendungsbereich des europäischen Datenschutzregimes ausgenommen angesehen werden muss. Eine weitere rechtliche Stütze fand diese Ansicht unserer Auffassung nach in Art. 4 Abs. 2 S. 1 EUV, wonach die Union die jeweilige nationale Identität der Mitgliedstaaten achtet, „(…) *die in ihren grundle-*

genden politischen und verfassungsmäßigen Strukturen einschließlich der regionalen und lokalen Selbstverwaltung zum Ausdruck kommt".

Auch wenn sich die diesbezügliche Zuständigkeitsvermutung nicht auf sämtliche (Neben-) Bereiche der parlamentarischen Arbeit erstreckt (Bsp. Beschäftigtendatenschutz), erschien es uns als folgerichtig, dass jedenfalls die den parlamentarischen Beratungs- und Entscheidungsfindungsprozess unmittelbar betreffenden Verarbeitungstätigkeiten hiervon erfasst seien. Selbige kann man als wesentliche, den Aufbau und das Eigenverständnis des Staates prägende Entscheidungen ansehen, welche von unionsrechtlichen Vorgaben – auch solchen nur mittelbarer Natur – freigestellt sein sollten. Letzteres bezog sich dabei auf die in den nationalen Verfassungen unmittelbar geregelten Grundsätze der gesetzgebenden Gewalt sowie auf die diesbezüglich erlassenen förmlichen Gesetze und Geschäftsordnungen, welche den innerparlamentarischen Entscheidungsfindungsprozess nachvollziehen und näher ausgestalten.[22]

In seinem Urteil vom 21.1.2020 – Lv 15/19, vertritt auch der Saarländische Verfassungsgerichtshof die Auffassung, dass die parlamentarische Tätigkeit des saarländischen Landtages aufgrund von Art. 2 Abs. 2 lit. a DSGVO nicht in den Anwendungsbereich der DSGVO fällt.[23]

3.2.2 Neuere Judikatur des EuGH

Anfang des Jahres 2024 hat sich der Europäische Gerichtshof (EuGH) in einer Entscheidung zu der Frage der Anwendbarkeit der Datenschutz-Grundverordnung (DSGVO) im parlamentarischen Bereich geäußert und hierbei weitgehende und bedeutende Feststellungen getroffen.[24]

[22] Vgl. etwa Art. 70 Abs. 1 SVerf.
[23] Rn. 70 f., juris.
[24] Urteil vom 16. Januar 2024-C-33/22.

In dem Urteil gelangt der EuGH zu der Einschätzung, aus Art. 16 Abs. 2 S. 1 AEUV und Art. 2 Abs. 2 lit. a DSGVO könne nicht geschlossen werden, dass eine Datenverarbeitung allein deshalb außerhalb des Anwendungsbereichs des Unionsrechts liege und damit dem Anwendungsbereich der DSGVO entzogen sei, weil sie von einem vom Parlament eines Mitgliedstaats eingesetzten Untersuchungsausschuss ausgeübt werde.[25] Ein parlamentarischer Untersuchungsauschuss unterfällt hiernach grundsätzlich den Vorschriften der DSGVO und unterliegt demnach auch einer diesbezüglichen Datenschutzaufsicht.

In einer ähnlich gelagerten Entscheidung aus dem Jahr 2020 hatte der EuGH bereits entschieden, dass parlamentarische Petitionsausschüsse dem Anwendungsbereich der DSGVO unterfallen. Selbige seien insoweit als "Verantwortliche" im Sinne des Art. 4 Nr. 7 DSGVO einzustufen, inwieweit sie allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheiden.[26]

Nach dieser Rechtsprechung des EuGH, welche von einem weiten Anwendungsbereich der DSGVO ausgeht, ist fraglich, ob die eingangs erwähnte Rechtsauffassung aufrecht erhalten werden kann. Die Beantwortung dieser Frage hängt vor allem davon ab, ob man die Rechtsprechung des EuGH isoliert auf Petitions- und Untersuchungsausschüsse bezieht, oder ihr eine allgemeine Aussage zum Anwendungsbereich des Europäischen Datenschutzrechts entnimmt, welche für die gesamte parlamentarische Tätigkeit Gültigkeit beansprucht.

Wie auch immer man diese Frage beantworten mag, eindeutig ist die Rechtsprechung des EuGH jedenfalls in dem Punkt der Datenschutzaufsicht im parlamentarischen Bereich. Das Gericht führt hier aus, dass es gemäß Art. 51 Abs. 1 DSGVO im Ermessen der Mitgliedstaaten stehe, so viele Datenschutzaufsichtsbehörden in ihrem Hoheitsgebiet einzurichten, wie es sich insbesondere aufgrund ihrer verfassungsmäßigen Struktur als erforder-

[25] Urteil vom 16. Januar 2024 – C-33/22, Rn. 43, curia.
[26] Urteil vom 9. Juli 2000 – C-272/19, Rn. 73, curia.

lich erweist. In Fällen, in welchen sich ein Mitgliedstaat für die Einrichtung nur einer einzigen Aufsichtsbehörde entscheide, sei diese Behörde zwangsläufig auch für den parlamentarischen Bereich mit allen Zuständigkeiten ausgestattet, die die DSGVO den Aufsichtsbehörden überträgt[27].

3.2.3 Konsequenzen für die Datenschutzaufsicht im Saarland

Für das Saarland ist die Landesbeauftragte für Datenschutz gemäß § 16 SDSG bis zu einer Neuregelung durch den Landtag die derzeit einzige allgemeine Datenschutzaufsichtsbehörde. Nach der Judikatur des EuGH obliegt dem Unabhängigen Datenschutzzentrum Saarland daher auch die Kontrolle der Rechtmäßigkeit der Verarbeitung personenbezogener Daten im gesamten Tätigkeitsbereich des Saarländischen Landtages, d. h. auch hinsichtlich von Verarbeitungen, welche über den Bereich der bloßen Landtagsverwaltung hinausgehen und den parlamentarischen Bereich (die parlamentarische Kerntätigkeit) betreffen.

3.3 KI-Verordnung: Datenschutz und Künstliche Intelligenz

3.3.1 Allgemeines

Nachdem sich unsere Behörde im Jahr 2023 bereits aus konkretem Anlass mit den datenschutzrechtlichen Implikationen beim Einsatz von Künstlicher Intelligenz beschäftigt hatte,[28] standen auch im aktuellen Berichtszeitraum die Entwicklungen in diesem Bereich weiterhin im Fokus der datenschutzrechtlichen Diskussionen, sowohl in unserem Haus als auch innerhalb der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK). Insbesondere der Umstand, dass die Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter

[27] Urteil vom 16. Januar – C-33/22, Rn. 64, 69, curia.
[28] 32. Tätigkeitsbericht 2023, Bericht 10, S. 151 ff.

Vorschriften für künstliche Intelligenz (Verordnung über künstliche Intelligenz, KI-VO) am 1. August 2024 in Kraft getreten ist, hat der Diskussion im Jahr 2024 eine neue Dynamik gegeben.

Die KI-VO soll einen einheitlichen Rechtsrahmen für KI-Systeme festlegen, der im Einklang mit den Werten und Grundrechten der Europäischen Union steht und so auch einen Schutz vor schädlichen Auswirkungen von KI-Systemen gewährleisten, ohne Innovationen übermäßig zu behindern.[29] Dies will der Verordnungsgeber erreichen, indem er besondere Anforderungen an sog. Hochrisiko-KI-Systeme und KI-Modelle mit allgemeinem Verwendungszweck stellt, besondere Transparenzpflichten normiert und Rahmenbedingungen für aufsichtsbehördliche Strukturen in den Mitgliedstaaten der EU zur Kontrolle dieser Vorschriften schafft. Der Schwerpunkt der KI-VO liegt damit zwar nicht im Bereich des Datenschutzes, soweit aber KI-Systeme bei der Verarbeitung personenbezogener Daten eingesetzt werden, haben die von ihr aufgestellten Rahmenbedingungen jedoch mittelbar erhebliche Auswirkungen auf die Auslegung und Anwendung der datenschutzrechtlichen Vorgaben.

Die DSK hat die Entwicklungen rund um die KI-VO intensiv begleitet und sich dabei auch mit den zu etablierenden aufsichtsbehördlichen Strukturen auf nationaler Ebene befasst. Die KI-VO sieht vor, dass diese spätestens bis zum 2. August 2025 zu schaffen sind, da zu diesem Zeitpunkt weite Teile der KI-VO unmittelbar in den Mitgliedstaaten der EU gelten.[30] Unmittelbar in der KI-VO sind die Datenschutzaufsichtsbehörden bereits als zuständige Marktüberwachungsbehörden für die Bereiche Strafverfolgung, Wahlen, Grenzkontrolle und Justizverwaltung vorgesehen.[31] In einem Positionspapier hat sich die DSK für klare und einheitliche behördliche Zuständigkeiten eingesetzt und insoweit die Bereitschaft der Datenschutzaufsichtsbehörden erklärt, die Aufgaben der nationalen Marktüberwachungs-

[29] ErwG 1 KI-VO.
[30] Art. 113, 70 Abs. 2 KI-VO.
[31] Art. 74 Abs. 8 i. V. m. Anhang III Nr. 1, 6, 7, 8.

behörden für KI-Systeme zu übernehmen; dem liegt zugrunde, dass sie bereits über umfassende Erfahrung im digitalen Grundrechtsschutz und etablierte, kooperative Aufsichts- und Abstimmungsmechanismen verfügen und so eine enge Verzahnung der KI-Verordnung mit der DSGVO sicherstellen können.[32] Auch der Europäische Datenschutzausschuss (EDSA) hatte den Mitgliedstaaten der EU empfohlen, entsprechende Erwägungen anzustellen.[33]

Im Berichtszeitraum wurde von der DSK zudem zur Unterstützung von Unternehmen und Behörden die Orientierungshilfe „Künstliche Intelligenz und Datenschutz" veröffentlicht,[34] die einen Überblick über die Kriterien für eine datenschutzkonforme Nutzung von KI-Anwendungen gibt. Im Mittelpunkt stehen dabei Rechtmäßigkeit, Zweckbindung, Transparenzpflichten und der Schutz von Betroffenenrechten.

Mit Beschluss vom 15. November 2024 hat die DSK zur Bündelung der technischen und rechtlichen Expertise der deutschen Datenschutzaufsichtsbehörden einen eigenen Arbeitskreis Künstliche Intelligenz eingerichtet.[35] Zu seinen Schwerpunktthemen gehören unter anderem die datenschutzrechtlichen Anforderungen an die Verarbeitung personenbezogener Daten im Rahmen des KI-Trainings sowie die Prüfung der Auswirkungen von KI-Systemen auf die Rechte betroffener Personen. Die Arbeit des Arbeitskreises wird gerade auch von der schwierigen Aufgabe geprägt sein, einen Ausgleich zu finden, der einerseits auf die Einhaltung der datenschutzrechtlichen Vorgaben drängt und so einen Beitrag zur Wahrung der Interessen und Grundrechte der BürgerInnen leistet, andererseits aber nicht aus den

[32] https://www.datenschutzkonferenz-online.de/media/dskb/20240503_DSK_Positionspapier_Zustaendigkeiten_KI_VO.pdf
[33] https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_de
[34] https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf
[35] https://www.datenschutzkonferenz-online.de/media/pm/2024-11-15_PM_108_DSK.pdf

Augen verliert, dass im Interesse des Allgemeinwohls auch innovationsfreundliche Rahmenbedingungen im Bereich KI erforderlich sind.

Auch auf der Ebene des EDSA setzen sich die Datenschutzaufsichtsbehörden eingehend mit dem Thema KI auseinander. So wurde beispielsweise auf Antrag der irischen Datenschutzbehörde eine Stellungnahme des Ausschusses zu bestimmten Datenschutzaspekten im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen von KI-Modellen erarbeitet und am 17. Dezember 2024 angenommen.[36]

3.3.2 Wechselwirkungen zwischen KI-Verordnung und Datenschutzrecht

Das Inkrafttreten der Verordnung (EU) 2024/1689 über künstliche Intelligenz (KI-VO) am 1. August 2024 hat auch Konsequenzen für das Datenschutzrecht, da beide Rechtsgebiete sich wechselseitig ergänzen. So definiert etwa Art. 5 KI-VO diverse Praktiken im KI-Bereich, die verboten sind, da mit ihnen nach Wertung des EU-Gesetzgebers ein zu hohes Risiko für die Grundrechte von Betroffenen einhergeht. Die in Art. 5 KI-VO abschließend aufgezählten Praktiken sind dabei solche, bei denen zwangsläufig auch personenbezogene Daten verarbeitet würden.

So ist es nach Art. 5 Abs. 1 lit b KI-VO beispielsweise verboten, mittels KI die Vulnerabilität einer Person aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation auszunutzen, um deren Verhalten in einer sie erheblich schädigenden Weise zu beeinflussen. Denklogisch setzt diese verbotene Praktik also die Nutzung von Informationen über die betroffene Person voraus, weshalb hier zugleich eine automatisierte Verarbeitung personenbezogener Daten i. S. v. Art. 2 Abs. 1 DSGVO vorliegt und damit neben der KI-VO auch das Datenschutzrecht nach der DSGVO anwendbar ist. Als weiteres Beispiel sei Art. 5 Abs. 1 lit. f KI-VO genannt, wonach

[36] https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_de

die Verwendung von KI-Systemen zur Ableitung von Emotionen einer natürlichen Person am Arbeitsplatz und in Bildungseinrichtungen grundsätzlich verboten ist. Auch zu diesem verbotenen Zweck wäre eine Verarbeitung von personenbezogenen Daten etwa in Gestalt von Gesichtsausdruck, Stimmklang oder Körpersprache erforderlich.

Die Verbote aus Art. 5 KI-VO haben damit unmittelbare Auswirkungen auf die datenschutzrechtliche Zulässigkeit der Verarbeitung personenbezogener Daten, da einer nach Art. 5 KI-VO verbotenen Handlung kein legitimer Verarbeitungszweck im Sinne des Art. 5 Abs. 1 lit. b DSGVO innewohnen kann; die Vorgaben des Art. 5 KI-VO haben verantwortliche Stellen i. S. d. Art. 4 Nr. 7 DSGVO bereits ab dem 2. Februar 2025 zu beachten.

Aber nicht nur Verantwortliche sind hiervon betroffen, sondern auch Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO, da sie nach Art. 28 Abs. 3 Unterabsatz 2 DSGVO dazu verpflichtet sind, Verantwortlichen – und damit ihren Kunden – mitzuteilen, soweit Weisungen gegen die Vorgaben der DSGVO verstoßen. Dies gilt insbesondere dann, wenn der Verantwortliche dem Auftragsverarbeiter offensichtliche Rechtsverstöße abverlangt, indem er eine Verarbeitungstätigkeit beauftragt, die offensichtlich gegen die KI-VO verstößt.[37] Zumindest mittelbar kann die KI-VO also auch Auswirkungen auf datenschutzrechtliche Pflichten von Auftragsverarbeitern haben. Ungeachtet dessen wird der Auftragsverarbeiter in vielen Fällen gleichzeitig als „Anbieter" i. S. d. Art. 3 Nr. 3 KI-VO unmittelbar Adressat von Pflichten nach der KI-VO sein, sofern Gegenstand der Beauftragung gerade der Einsatz eines KI-Systems ist.

Auch hier wird die enge Verzahnung der KI-VO mit den Vorgaben der DS-GVO deutlich. Die KI-VO setzt damit nicht nur allgemeine Standards, sondern stärkt zudem die datenschutzrechtliche Position von Betroffenen im Umgang mit KI-Systemen.

[37] Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 28 Rn. 83.

IV.

Grundsatzfragen

4 Grundsatzfragen

4.1 Anforderungen an das Vorliegen eines Personenbezugs

4.1.1 Umgang mit Daten juristischer Personen

Die Vorschriften der Datenschutz-Grundverordnung (DSGVO) dienen nach ihrem Art. 1 Abs. 1 und 2 ausschließlich dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Während somit der individuelle Mensch als Träger von Rechten und Pflichten von diesem gesetzlichen Schutzauftrag ausdrücklich erfasst ist, gilt dies nicht zwangsläufig für Vereinigungen von natürlichen Personen und Personenmehrheiten, die mit eigener Rechtsfähigkeit ausgestattet sind; denn unter Berücksichtigung von Satz 2 des Erwägungsgrunds 14 der DSGVO

> *"Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person."*

sollen datenschutzrechtliche Vorgaben für rein unternehmensbezogene Kontaktinformationen regelmäßig keine Anwendung finden.

Oftmals lässt sich allerdings die Linie zwischen unternehmens- und personenbezogenen Daten nicht trennscharf ziehen: So sind bei Klein- oder Einzelunternehmen die Daten der juristischen Person und die der dahinterstehenden natürlichen Person häufig deckungsgleich (beispielsweise „Erika Mustermann GmbH"); auch können Kontaktdaten einer die juristische Person nach außen vertretenden natürlichen Person (Organwalter wie GmbH-Geschäftsführer oder Vorstand einer Aktiengesellschaft) oder von Mitarbeitenden als nach außen auftretenden Ansprechper-

sonen (E-Mail-Adresse: max.mustermann@firma.com) als personenbezogene Daten qualifiziert werden.

In der dahingehenden Literatur und Rechtsprechung werden zur Frage des Schutzumfangs des Unionsrechts unterschiedliche Ansichten vertreten: Während eine nah am Wortlaut des Erwägungsgrunds 14 der DSGVO orientierte Auslegung eine Verarbeitung von Kontaktinformationen von juristischen Personen vom Schutzbereich der DSGVO ausnimmt,[38] ist nach einer vermittelnden Position eine differenzierende Betrachtung erforderlich; eine Erstreckung des sachlichen Anwendungsbereichs der Verordnung auf die juristische Person hänge demnach davon ab, ob und inwieweit zwischen juristischer und dahinter stehender natürlicher Person eine hinreichend nahe Beziehung bestehe.[39] Eine enge finanzielle, personelle oder wirtschaftliche Verflechtung, wie sie typischerweise bei einer Einpersonen-GmbH vorkomme,[40] spreche für eine umfassende Anwendung des Datenschutzrechts auch auf diese Unternehmensdaten. Das in Art. 1 Abs. 2 DSGVO genannte Schutzziel der Verordnung und der Wortlaut von Erwägungsgrund 14 bedingen auch hiesigen Erachtens letztlich eine differenzierende Betrachtung des jeweiligen Verarbeitungshandelns unter Berücksichtigung von Verarbeitungsziel und -kontext.

Im Berichtszeitraum adressierten Beratungsanfragen und Beschwerden die Verarbeitung personenbezogener Daten juristischer Personen in einer großen Bandbreite: Neben den häufig thematisierten Wirtschaftsinformationsdiensten, lagen den Anliegen auch Referenzlisten bei öffentlichen Ausschreibungen und sonstige Einzelfälle der Verarbeitung von Unternehmensdaten als Gegenstand zugrunde.

[38] Karg, in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 1. Auflage 2019, Art. 4, Rn. 45, beck-online; Bundesfinanzhof, Beschluss vom 8. Februar 2024 – IX B 113/22, Rn .12 ff., juris.

[39] Gola, in Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz 3. Aufl. 2022, Art. 4 Rn. 28, beck-online.

[40] Klabunde/Horváth, in Ehmann/Selmayr, Datenschutz-Grundverordnung 3. Aufl. 2024, Art. 4 Rn. 14, beck-online.

- **Wirtschaftsinformationsdienste**

  Für registerrechtlich geregelte Informationsdienste wie dem gemeinsamen Registerportal der Bundesländer (Handelsregister)[41] erfolgt eine Veröffentlichung personenbezogener Daten von GmbH-Geschäftsführern nach Art. 6 Abs. 1 lit. c DSGVO zur Erfüllung einer gesetzlichen Publizitätspflicht aus § 9 Abs. 1 Satz 2, § 10 Abs. 1 Handelsgesetzbuch, § 52 Verordnung über die Einrichtung und Führung des Handelsregisters.[42] Dahingegen können sich Anbieter privater Wirtschaftsinformationsdienste nicht auf eine gesetzliche Verarbeitungspflicht berufen; diese können personenbezogene Daten im Kontext von juristischen Personen zur Verfolgung wirtschaftlicher Interessen gestützt auf die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO regelmäßig in zulässiger Weise verarbeiten:

  Soweit im Hinblick auf die Art der Geschäftstätigkeit ausschließlich öffentlich zugängliche Unternehmensinformationen, mithin aber auch Angaben im Zusammenhang mit der beruflichen Betätigung einer natürlichen Person, mit dem Ziel der Bereitstellung eines branchen- und unternehmensbezogenen Such- und Informationsdienstes verarbeitet werden, stellt diese kommerzielle Tätigkeit grundsätzlich ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit. f DSGVO dar. Auch sind in diesem Kontext die Informationsinteressen von potenziellen Nutzenden dieser Dienste als Drittinteresse berücksichtigungsfähig und als berechtigt anzusehen. Maßgeblich für die Abwägungsentscheidung im Sinne der Vorschrift ist ferner, inwiefern schutzwürdige Interessen, Grundrechte und Grundfreiheiten der betroffe-

[41] https://www.handelsregister.de/rp_web/welcome.xhtml
[42] BGH, a. a. O., Rn. 13 und 14, juris.

nen Person(en) das Verarbeitungsinteresse gegebenenfalls überwiegen.

Zunächst ist die Art und Herkunft der Daten maßgeblich: Hier kann statuiert werden, dass für Wirtschaftsdaten, die mit der unternehmerischen oder beruflichen Betätigung einer natürlichen Person konnotiert sind und die öffentlich zugänglich sind, zunächst eine geringere Schutzwürdigkeit unterstellt werden kann.[43] Auch die Verarbeitung als solche und die beteiligten Akteure sind zu berücksichtigen; die beabsichtigte Veröffentlichung von Informationen im Internet und der damit verbunden potenziell unbeschränkte Kreis von Empfängern ist zwar grundsätzlich mit einer erheblichen Eingriffstiefe verbunden, allerdings handelt es sich bei den veröffentlichten Daten um solche, die ohnehin bereits aus öffentlich zugänglichen Informationsregistern entnommen werden können. Die über den Informationsdienst abrufbaren Daten, wären auch für potenzielle Nutzende des Dienstes als Datenempfänger voraussetzungslos durch eine Recherche im Handelsregister und ergänzenden Quellen auffindbar.

- **Referenzlisten**

  In Ausschreibungsverfahren öffentlicher Auftraggeber können Bieter dazu angehalten sein, Informationen über erledigte Aufträge bspw. in Form schriftlicher Referenzen von früheren Auftraggebern vorzulegen. Diese sollen nach § 122 Abs. 2 Nr. 3 Gesetz gegen Wettbewerbsbeschränkungen und § 46 Abs. 3 Nr. 1 Vergabeverordnung dem öffentlichen Auftraggeber im Vergabeverfahren die Prüfung der Eignung und Leistungsfähigkeit des bietenden Unternehmens ermöglichen. Stellt ein Unternehmen keine Referenzliste zur Verfü-

[43] Landgericht Hamburg, Urteil vom 3. September 2021 - 324 O 86/20, Rn. 67 ff., juris; Kühling/Buchner/Buchner/Petri, 3. Aufl. 2020, DS-GVO Art. 6 Rn. 150 ff.

gung, kann dies den Ausschluss im Ausschreibungsverfahren bedeuten.

Regelmäßig werden im Zusammenhang mit der Zurverfügungstellung von Referenzen von früheren Auftraggebern auch personenbezogene Daten im Kontext juristischer Personen – insbesondere auch in Form von Angaben zu Ansprechpersonen – im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO in zulässiger Weise verarbeitet. Mit dieser Weitergabe von Unternehmens- oder beruflichen Kontaktinformationen eines früheren Auftraggebers verfolgt das an dem Vergabeverfahren teilnehmende Unternehmen ein berechtigtes kommerzielles Interesse im Sinne der Vorschrift; denn nur hierdurch wird eine Teilnahme am Ausschreibungsverfahren überhaupt erst ermöglicht. Ferner kann auch das Interesse der datenempfangenden öffentlichen Auftraggeber an der Ermöglichung einer Eignungsprüfung als berechtigtes Drittinteresse anerkannt werden. Schließlich gilt zu berücksichtigen, dass das den vergaberechtlichen Regelungen zugrundeliegende Unionsrecht[44] eine Offenlegung der privaten oder öffentlichen Empfänger von Lieferungen/Dienstleistungen im Vergabeprozess vorsieht.

Wie bei den Wirtschaftsinformationsdiensten spricht auch hier grundsätzlich für eine Zulässigkeit der Datenweitergabe, dass eine geringere Schutzwürdigkeit für Daten zur unternehmerischen oder beruflichen Betätigung einer natürlichen Person unterstellt werden kann; ferner lässt eine Zurverfügungstellung von Informationen gegenüber einem öffentlichen Auftraggeber, für den im Übrigen eine besondere Bindung an Recht und Gesetz besteht, nicht auf eine erhebliche Eingriffstiefe in Rechte der betroffenen Personen schließen.

[44] Art. 58 Abs. 4 und Art. 60 Abs. 1 und 4 Richtlinie 2014/24/EU in Verbindung mit Anhang XII Teil II RL 2014/24/EU.

Allerdings kann jedoch abhängig von spezifischen Besonderheiten der Tätigkeit des bietenden Unternehmens die Einholung einer Einwilligung nach Art. 4 Nr. 11 in Verbindung mit Art. 6 Abs. 1 lit. a DSGVO der von der Datenweitergabe betroffenen Personen erforderlich sein. So kann es für Rechtsanwälte als Bieter unter Berücksichtigung berufsspezifischer Verschwiegenheitspflichten zumutbar sein, Einwilligungen der von der Datenweitergabe in Referenzlisten betroffenen Mandanten einzuholen.[45]

- **Gesellschaftssitz am Wohnort**

  Gerade bei Einpersonengesellschaften kann der Unternehmenssitz mit dem Wohnsitz des Alleingesellschafters zusammenfallen, allerdings kann allein die Übereinstimmung von Privat- und Geschäftsanschrift mit Blick auf Erwägungsgrund 14 nicht dazu führen, dass für die Verarbeitung personenbezogener Daten der juristischen Person datenschutzrechtliche Vorgaben zwangsläufig Berücksichtigung finden müssen. Wie eingangs erwähnt, gebietet sich jedoch eine differenzierende Betrachtung mit Blick auf das spezifische Ziel und den Zusammenhang einer Datenverarbeitung.

  Wird in der Einzelfallbefassung ersichtlich, dass der Verarbeitung der personenbezogenen Daten der juristischen Person vorrangig oder ausschließlich auf die dahinterstehende natürliche Person abzielt, müssen mit Blick auf deren Schutzziel hierfür die Verarbeitungsbedingungen der DSGVO gelten. Werden bspw. Werbebotschaften an die juristische Person adressiert, aber richtet sich die beworbene Ware oder Dienstleistung erkennbar ausschließlich an die hinter der Gesellschaft stehende natürliche Person, kann für diese Datenver-

[45] Bundeskartellamt, 1. Vergabekammer des Bundes, Beschluss vom 1. Juni 2023 – VK 1 – 37/23, Rn. 57, juris.

wendung nicht der Ausschlussgrund nach Erwägungsgrund 14 gelten.

Gleiches kann auch bei der Verarbeitung personenbezogener Daten einer juristischen Person angenommen werden, wenn die Gesellschaft bereits aufgelöst wurde; teilt bspw. ein Betriebsnachfolger Kundinnen und Kunden Name („Max Mustermann GmbH“) und Adresse der veräußernden Gesellschaft mit, damit diese dort Ersatz für durch den Veräußerer ausgestellte Wertgutscheine geltend machen können, ist diese Weitergabe von Kontaktdaten nach den Vorgaben der DSGVO zu beurteilen, wenn der Betriebsnachfolger nachweislich Kenntnis von der bereits erfolgten Liquidation der Gesellschaft haben kann.

4.1.2 Korrektur eines Schadensberichts: Sach- vs personenbezogene Daten

Im 30. Tätigkeitsbericht für das Berichtsjahr 2021[46] wurde das Beschwerdeverfahren einer Wohnungseigentümerin, die versuchte, gegen einen Schadensbericht hinsichtlich der Feststellung eines Wasserschadens im Gemeinschaftskeller durch Geltendmachung datenschutzrechtlicher Betroffenenrechte vorzugehen, dargestellt.

Mit dem Ziel, die Angaben im Schadensbericht hinsichtlich des Schadensorts und der Schadensursache in ihrem Sinne zu korrigieren, machte die Beschwerdeführerin gegenüber dem Schadensermittler zunächst einen Auskunftsanspruch nach Art. 15 DSGVO und anschließend einen Berichtigungsanspruch nach Art. 16 DSGVO geltend und forderte diesen sodann zur Löschung der sie betreffenden personenbezogenen Daten nach Art. 17 DSGVO aus dem ihres Erachtens fehlerhaft erstellten Schadensbericht auf. Nach Weigerung des Schadensermittlers, den geltend gemachten Betroffenenrechten zu entsprechen und nach Abweisung ihrer Beschwerde nach Art. 77 DSGVO

[46] Bericht 4.23.3.

klagte die Beschwerdeführerin gegen die Einstellung des Verfahrens.

Mit Urteil vom 30. Oktober 2024[47] hat das Verwaltungsgericht des Saarlandes diese Klage abgewiesen und im Weiteren entschieden, dass die Beschwerdeabweisung keinen Verstoß gegen aufsichtsbehördliche Pflichten nach Art. 57 Abs. 1 lit. f DSGVO darstellt. Das Gericht bestätigte damit unsere Auffassung, dass es sich bei den isolierten Angaben zu Schadensort und -ursache im Schadensbericht um reine Sachdaten und nicht um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO handelte; demzufolge konnte seitens der Aufsichtsbehörde keine Unrichtigkeit im Sinne des Art. 16 DSGVO festgestellt werden und es wurden damit – ermessensfehlerfrei – keine Maßnahmen nach Art. 58 Abs. 2 DSGVO ergriffen. Die von der Klägerin begehrte Überprüfung der inhaltlichen Richtigkeit eines Schadensberichts konnte somit im Rahmen eines datenschutzrechtlichen Beschwerdeverfahrens gerade nicht erreicht werden. Auch im Übrigen lag aus Sicht der Kammer eine berechtigte Datenverarbeitung vor, so dass auch eine Löschung der personenbezogenen Daten der Klägerin im Schadensbericht ausgeschlossen war.

Wenn auch das Verwaltungsgericht die aufsichtsbehördliche Beschwerdeabweisung und damit die dieser zugrundeliegende Differenzierung zwischen Sach- und personenbezogenen Daten bestätigt hat, wirft diese Abgrenzung in vergleichbaren Fällen nach wie vor erhebliche Schwierigkeiten auf.

So wird in der Rechtsprechung teilweise ein Personenbezug von gebäudespezifischen Sachangaben bei der Geltendmachung von Auskunftsrechten nach Art. 15 DSGVO bejaht und in diesem Zusammenhang auch ein Schadensgutachten als solches als personenbezogenes Datum qualifiziert.[48] Aber auch mit dieser Rechtsprechung zu gebäudespezifischen Sachangaben lässt sich – unter Berücksichtigung der auch der aufsichtsbehördli-

[47] Geschäftszeichen 5 K 1176/21.

[48] OVG für das Land Mecklenburg-Vorpommern, Beschluss vom 14. Dezember 2023 – 1 LZ 413/21 OVG, Rn. 14 und 15, juris.

chen Beschwerdeabweisung zugrundeliegenden Rechtsprechung des Europäischen Gerichtshofs (EuGH)[49] – eine Binnendifferenzierung zwischen personenbezogenen Daten und Sachdaten im Schadensbericht in Einklang bringen; während somit für den Fall der Geltendmachung eines Auskunftsrechts für einen Schadensbericht ein Personenbezug angenommen werden kann, kann für die verfolgte Berichtigung oder Löschung von Schadensdaten in einem Schadensbericht etwas anderes gelten.

Da in zunehmendem Maße über Beschwerden bei der Aufsichtsbehörde versucht wird, subjektiv unvorteilhafte Gutachten, Bewertungen oder behördliche Entscheidungen durch Geltendmachung datenschutzrechtlicher Berichtigungs- und Löschrechte anzugreifen, wäre eine weitere Konturierung dieser Fragestellung in der Rechtsprechung wünschenswert. In dem entschiedenen Sachverhalt hat die Klägerin allerdings von einer Berufung abgesehen.

4.2 Benennung eines stellvertretenden Datenschutzbeauftragten

Immer wieder erreichen uns Beratungsanfragen aus dem öffentlichen und nicht-öffentlichen Sektor, ob neben dem betrieblichen bzw. behördlichen Datenschutzbeauftragten auch ein stellvertretender Datenschutzbeauftragter zu benennen sei. Gerade im Fall einer längeren Abwesenheit des originär benannten Datenschutzbeauftragten, beispielsweise wegen Urlaub, Unfall oder Erkrankung, stellt sich die Frage, wer dessen Aufgaben zu übernehmen hat und wie das weitere Prozedere betriebs- oder behördenintern geregelt werden muss, um den Datenschutz und die damit zusammenhängenden Vorgaben umsetzen und

[49] Urteile vom 17. Juli 2014 – verbundene Rechtssachen C-141/12 und C-372/12; obwohl diese Entscheidung noch die Rechtslage vor Geltungseintritt der DSGVO betrifft, ist diese nach wie vor relevant, siehe BGH, Urteil vom 15. Juni 2021 – VI ZR 576/19 Rn. 22 ff., juris.

die Aufgaben des Datenschutzbeauftragten nahtlos weiterführen zu können.

Weder Art. 7 DSGVO noch das Bundesdatenschutzgesetz kennen eine Pflicht zur Benennung eines stellvertretenden Datenschutzbeauftragten. Auch im Saarländischen Datenschutzgesetz existiert im Gegensatz zu einigen Landesdatenschutzgesetzen, beispielsweise in Hessen, Nordrhein-Westfalen und Thüringen, keine Regelung, die die Benennung eines Vertreters des Datenschutzbeauftragten explizit vorsieht.

Auch ohne eine solche ausdrückliche gesetzliche Obliegenheit, erscheint unserer Behörde die Benennung eines stellvertretenden Datenschutzbeauftragten jedoch geboten. Dies vor allem aus zwei Gründen. Zum einen entbindet die längere Abwesenheit eines Datenschutzbeauftragten den Verantwortlichen weder von seinen Pflichten aus der DSGVO noch reduziert sie deren Umfang. Der Verantwortliche kann sich in diesen Fällen, etwa bei der Erfüllung von Betroffenenrechten nach den Art. 12 ff. DSGVO, folglich nicht mit dem Argument exkulpieren, durch den Wegfall seines Datenschutzbeauftragten fehle es (vorübergehend) an der nötigen Expertise. Auch in diesen Situationen hat der Verantwortliche den datenschutzrechtlichen Ansprüchen und Fragestellungen umfassend zeitnah Rechnung zu tragen und muss sich die nötige Fachexpertise notfalls schnellstmöglich über externe Dienstleister verschaffen. Zum anderen nimmt die Person des Datenschutzbeauftragten in gewissen Konstellationen eine besondere Vertrauensstellung zwischen Verantwortlichen und Betroffenem ein. Gerade im Rahmen von Beschäftigungsverhältnissen kommt es nicht selten vor, dass Arbeitnehmerinnen und Arbeitnehmer den Beschwerdeweg zunächst über den Datenschutzbeauftragten suchen, sei es, dass sie den Weg über die Geschäftsleitung oder die Personalvertretung noch nicht für opportun halten oder gar persönliche berufliche Konsequenzen bei einer direkten Konfrontation mit der Chefebene fürchten. Hieraus erklärt sich sodann auch das Erfordernis eines exklusiven Kommunikationszugangs zu der Person des Datenschutzbeauftragten, etwa in Form einer

nur diesem zugänglichen Funktions-E-Mail-Adresse. Nur durch die Bereitstellung eines Stellvertreters kann der Verantwortliche vorgenannten Problemen effektiv begegnen und eine permanente, zeitlich lückenlose Umsetzung des in Art. 39 DSGVO genannten Aufgabenspektrums eines Datenschutzbeauftragten sicherstellen.

Diese Überlegungen können dogmatisch in Art. 38 Abs. 2 DSGVO verortet werden, wonach der Verantwortliche seinem Datenschutzbeauftragten die zur Aufgabenerfüllung erforderlichen, auch personellen, Ressourcen zur Verfügung stellen muss.

Klar ist bei einer Benennung eines Stellvertreters des Datenschutzbeauftragten jedoch, dass er nicht die in Art. 38 Abs. 3 DSGVO vorgesehenen Privilegien des eigentlich benannten Datenschutzbeauftragten für sich beanspruchen kann, da diese eindeutig und exklusiv dem originär benannten Datenschutzbeauftragten zustehen.

Fazit

Eine Pflicht zur Benennung eines Stellvertreters des Datenschutzbeauftragten existiert im Saarland nicht, jedoch ist eine solche interne Aufgabenzuweisung gerade für den Fall einer längerfristigen Abwesenheit des benannten Datenschutzbeauftragten empfehlenswert.

V.

Digitalisierung der Verwaltung

5 Digitalisierung der Verwaltung

5.1 Bereitstellung onlinebasierter Solarkataster

Im Berichtszeitraum führte das Unabhängige Datenschutzzentrum Saarland ein aufsichtsbehördliches Verfahren gegen eine kommunale Gebietskörperschaft, den Regionalverband Saarbrücken, durch. Anlass war die Einführung und der Betrieb eines digitalen Solarkatasters, das seit Juli 2024 öffentlich zugänglich war. Ziel der Plattform war es, Eigentümerinnen und Eigentümern über das Sonneneinstrahlungspotential ihrer Dachflächen zu informieren und eine Wirtschaftlichkeitsbetrachtung für Solaranlagen zu ermöglichen.

Das Solarkataster ermöglichte es jeder beliebigen Person, durch einfache Eingabe einer Adresse oder Auswahl eines Gebäudes auf einer interaktiven Karte umfassende Informationen zu erhalten, darunter solche zur Ausrichtung, Neigung und Verschattung der Dachfläche, zur Größe der potentiellen Modul- oder Kollektorfläche sowie zum maximalen Energieertrag. Zudem konnte auf Grundlage dieser Daten eine Wirtschaftlichkeitsberechnung einer möglichen Solaranlage durchgeführt werden.

Diese Informationen wurden für sämtliche Gebäude im Gebiet des Regionalverbands bereitgestellt, unabhängig davon, ob es sich um öffentliche oder private Immobilien handelte. Die Plattform sah dabei keinerlei Authentifizierungs- oder Berechtigungsprüfung vor. Es war demnach weder erforderlich, sich als Eigentümerin oder Eigentümer des betreffenden Grundstücks auszuweisen noch ein sonstiges berechtigtes Interesse am Zugriff darzulegen. Auch ein technischer Zugriffsschutz, etwa durch ein Login-Verfahren, existierte nicht.

Faktisch bedeutete dies, dass die wirtschaftlich relevanten Daten zu sämtlichen Wohngebäuden im Regionalverband für jedermann – ohne jede Zugangshürde – abrufbar waren. Die bloße technische Möglichkeit, durch Auswahl auf einer Karte oder Eingabe einer Adresse an die Daten zu gelangen, war für jeden In-

ternetnutzenden gegeben. Die Nutzung des Solarkatasters war damit nicht auf die Zielgruppe der Gebäudeeigentümerinnen und -eigentümer beschränkt, sondern stand auch institutionellen Akteuren wie Solartechnikunternehmen, Immobilienmaklern, Datenvermittlern oder auch beliebigen Dritten offen.

Diese gebäudebezogenen Informationen sind – entgegen laienhafter Vermutung – nicht per se anonym. Vielmehr handelt es sich um personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO, da sie sich auf identifizierbare natürliche Personen – hier die Eigentümerinnen und Eigentümer der betroffenen Gebäude – beziehen. Der Personenbezug kann sich entweder unmittelbar durch die Kenntnis der Eigentumsverhältnisse oder mittelbar durch die Verknüpfung mit anderen Datenquellen herstellen lassen. Besonders bei Einfamilienhäusern ist regelmäßig ein unmittelbarer Bezug zwischen Immobilie und Eigentümerin oder Eigentümer gegeben. Institutionelle Nutzende wie Immobilienmakler oder Datenhandelsunternehmen können durch Kombination mit öffentlich zugänglichen Informationen (z. B. Online-Verzeichnissen oder Kartendiensten) systematisch Personenbezüge rekonstruieren. Auch sind diese Informationen alles andere als trivial, lassen sich aus ihnen doch Wirtschaftlichkeitserwägungen hinsichtlich der Nutzung des Gebäudes ableiten, was im Falle einer Veräußerungsabsicht als wertbildender Faktor durchaus in die Preisverhandlung und Preisfindung Eingang finden kann.

5.1.1 Fehlende datenschutzrechtliche Grundlage / Verarbeitungsbefugnis

Der Betrieb des Solarkatasters in der beschriebenen Form war mit den Vorgaben der Datenschutz-Grundverordnung (DSGVO) nicht vereinbar. Art. 6 Abs. 1 DSGVO verlangt eine geeignete Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch öffentliche Stellen. Diese war hier nicht gegeben.

Eine vom Regionalverband selbst erlassene Solarkataster-Satzung, die die Befugnis zur Veröffentlichung gebäudebezogener

Daten vorsah, stützte sich auf § 5 Abs. 2 und § 197 KSVG. Diese Vorschriften erlauben zwar den Erlass kommunaler Satzungen zur Erfüllung öffentlicher Aufgaben, stellen jedoch keine hinreichende Ermächtigungsgrundlage für grundrechtsrelevante Datenverarbeitungen dar. Nach der ständigen Rechtsprechung des Bundesverfassungsgerichts sowie des Verfassungsgerichtshofs des Saarlandes[50] sind für derartige Eingriffe vielmehr formell-gesetzliche Regelungen mit normenklarer Bestimmung des Zwecks, der Datenarten, der betroffenen Personen und der Zugriffsmodalitäten erforderlich.

Andere gesetzliche Erlaubnistatbestände, etwa aus dem Saarländischen Datenschutzgesetz (SDSG), konnten ebenfalls nicht als Rechtsgrundlage für solche institutionalisierten Verarbeitungen herangezogen werden.

Schließlich stellte auch die vom Regionalverband eingeräumte Möglichkeit zum Widerspruch gegen die Darstellung des eigenen Gebäudes im Solarkataster keinen Ersatz für eine gesetzliche Grundlage dar. Der Grundrechtsschutz besteht unabhängig davon, ob betroffene Personen ihr Recht aktiv geltend machen.

Trotz frühzeitig geäußerter Bedenken im Rahmen der Beteiligung nach § 19 Abs. 2 SDSG wurde das Solarkataster durch den Regionalverband in der beanstandeten Form in Betrieb genommen. Um die Rechte der betroffenen Personen zu wahren, erließen wir daher eine aufsichtsbehördliche Anordnung gemäß Art. 58 Abs. 2 lit. d und f DSGVO. Sie verpflichtete den Regionalverband unter anderem dazu, den Zugriff auf die sensiblen Gebäudedaten künftig durch ein Antrags- und Prüfverfahren abzusichern, das nur berechtigten Personen (z. B. Eigentümerinnen und Eigentümern) den Zugang erlaubt. Bis zur Umsetzung eines solchen Verfahrens wurde die öffentliche Zugänglichmachung untersagt. Gegen die Anordnung wurde Klage beim Verwaltungsgericht des Saarlandes erhoben.

[50] Lv 15/20, Rn. 127 ff.

5.1.2 Gesetzliche Grundlage für den Betrieb von Solarkatastern im Saarland

Der Landesgesetzgeber hat unsere rechtlichen Bedenken am Fehlen einer datenschutzrechtlichen Verarbeitungsbefugnis zur Veröffentlichung personenbezogener Daten im Kontext von Solarkatastern geteilt. Im Rahmen des am 29. November 2024 in Kraft getretenen Wärmeplanungsumsetzungsgesetzes (WPUG)[51] hat der saarländische Landtag mit § 2 des Solarkataster- und Datenbereitstellungsumsetzungsgesetzes (SDUG) nunmehr eine formell-gesetzliche Grundlage geschaffen, die den oben skizzierten Anforderungen an Bestimmtheit und Normenklarheit genügt.

Die Vorschrift gestattet dem Land, den Gemeinden und Landkreisen sowie dem Regionalverband Saarbrücken nunmehr die Einrichtung und den Betrieb von Solarkatastern unter Verarbeitung der dort konkret bezeichneten gebäudebezogenen Datenkategorien. Zugleich sieht die Regelung vor, dass diese gebäudebezogenen Daten mit Geobasisdaten und mit Gebäudedaten der Vermessungsämter derart verknüpft werden dürfen, dass die Eignung von Gebäudedächern zur Nutzung solarer Strahlungsenergie qualitativ klassifiziert, analysiert und visualisiert werden kann. Das Ergebnis und die Grundlage dieser Auswertung darf jedermann öffentlich zugänglich gemacht werden, wenn nicht der Eigentümer des betroffenen Gebäudes der Bereithaltung im Internet widerspricht.

> ***§ 2 Solarkataster***
>
> *(1) Das Land, die Gemeinden, die Landkreise und der Regionalverband Saarbrücken können Solarkataster einrichten, in denen die Eignung von Dachflächen und Flächen des ruhenden Verkehrs sowie sonstiger Flächen innerhalb der im Zusammenhang bebauten Ortsteile für die Nutzung solarer Strahlungsenergie zur Wärmegewinnung und zur Stromerzeugung erfasst wird. Zu diesem Zweck dürfen Daten*

[51] Siehe oben 2.4. „Kommunale Wärmeplanung".

1. zur Lage des Gebäudes (Anschrift, Flurstücksbezeichnung),

2. zu Größe, Ausrichtung, Neigung und Verschattung der Dachfläche und Flächen des ruhenden Verkehrs,

3. zur maximalen Größe der Installationsfläche,

4. zur maximalen Größe der Kollektor- oder Modulfläche,

5. zum maximalen Energieertrag sowie

6. zur maximalen CO_2-Reduzierung

verarbeitet werden.

(2) Die in § 2 Absatz 1 Satz 2 genannten Daten dürfen insbesondere durch die Anfertigung und Nutzung von Luftaufnahmen gleich welcher Art sowie durch deren Auswertung gewonnen werden. Die in § 2 Absatz 1 Satz 2 genannten Daten dürfen mit Geobasisdaten und mit Gebäudedaten der Vermessungsämter verknüpft sowie in Bezug auf die Nutzung solarer Strahlungsenergie qualitativ klassifiziert, analysiert und visualisiert werden.

(3) Die Daten nach § 2 Absatz 1 Satz 2 dürfen für die folgenden Zwecke erhoben, erfasst, geordnet, gespeichert, verwendet, offengelegt und übermittelt werden:

1. Bereitstellung der Daten „Neigung", „maximale PV-Fläche", „Einstrahlung" und „Verschattung" eines Daches beziehungsweise einer Fläche im Internet zum Abruf für jedermann.

2. Bereitstellung der Ergebnisse bezüglich der Eignung eines Daches oder einer Fläche für die Nutzung von Strahlungsenergie im Internet zum Abruf für jedermann.

3. Bereitstellung einer Anwendung im Internet zum Abruf für jedermann zur Berechnung der Wirtschaftlichkeit der Nutzung eines Daches für solare Strahlungsenergie anhand von vom Nutzer einzugebenden Verbrauchsdaten und damit einhergehende Übermittlung der Daten an den jeweiligen Anwender.

Wenn es ermöglicht wird, dass Verbrauchsdaten von Nutzern der Internetanwendung selbst eingegeben werden, so sind diese unmittelbar nach Erstellung des Ergebnisses der Berechnung automatisiert zu löschen.

(4) Soweit die Eigentümer der erfassten Gebäude oder Flächen der Bereitstellung im Internet zum Abruf durch jedermann nach § 2 Absatz 3 widersprechen, ist der Abruf im Internet vom Verantwortlichen umgehend zu sperren. Auf das unbefristete Widerspruchsrecht ist mindestens vier Wochen vor der beabsichtigten Veröffentlichung im Internet durch öffentliche Bekanntmachung sowie dauerhaft im Internet hinzuweisen.

Auf Grund der geänderten Rechtslage haben wir unsere ursprünglich gegenüber dem Regionalverband Saarbrücken erlassene Anordnung widerrufen. Der Verwaltungsrechtsstreit dürfte sich damit erledigt haben. Zum Zeitpunkt des Redaktionsschlusses war das Verfahren allerdings noch anhängig.

5.2 Übertragung der Beihilfebearbeitung

Im April 2024 wurde die Bearbeitung von Beihilfeanträgen der Saarländischen Beamtinnen und Beamten von der Zentralen Beihilfestelle (ZBS) auf die Postbeamtenkrankenkasse (PBeaKK), einer bundesunmittelbaren Körperschaft des öffentlichen Rechts, übertragen. Dieser Übertragung vorausgegangen war ein langer Prozess, in welchen unsere Behörde bereits frühzeitig seit März 2022 involviert war.

Gemäß Art. 6 Abs. 1 lit. e Datenschutz-Grundverordnung (DSGVO) ist eine Datenverarbeitung rechtmäßig, soweit sie zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Die Gewährung der Beihilfe für Beamte stellt eine solche Aufgabe dar. Nach Abs. 2 der Norm können die Mitgliedstaaten spezifische Bestimmungen für die Verarbeitung zur Erfüllung einer Aufgabe gem. lit. e einführen. Die saarländische Landesregierung hat von dieser Regelung Gebrauch gemacht und mit § 67a Saarländi-

sches Beamtengesetz (SBG) eine Rechtsnorm eingeführt, die die Übertragung der Gewährung von Beihilfen im Landesbereich im Rahmen der Organleihe auf andere Einrichtungen des öffentlichen Rechts legitimiert. Dabei sieht § 67a Abs. 2 SBG ausdrücklich vor, dass personenbezogene Daten aus der Beihilfeakte für die Übernahme der Aufgabe an die Einrichtung des öffentlichen Rechts im erforderlichen Umfang – auch schon vorab – übermittelt werden dürfen. Die aufgrund der Verordnungsermächtigung in § 67a Abs. 3 SBG erlassene Verordnung zur Übertragung der Gewährung von Beihilfen im Landesbereich auf die PBeaKK (PBeaKKBhLÜbV SL) konkretisiert die Regelungen aus § 67a SBG und bestimmt in § 1 Abs. 1 der Verordnung die PBeaKK als Einrichtung des öffentlichen Rechts im Sinne des § 67a SBG.

Nach der landesweiten Bekanntgabe der unmittelbar bevorstehenden Übertragung der Beihilfebearbeitung von der Beihilfestelle der ZBS an die PBeaKK erreichten uns hierzu mehrere Anfragen betroffener Beamter. Eine Anfrage bezog sich dabei insbesondere auf die Frage, welche personenbezogenen Daten konkret im Rahmen der Aufgabenübertragung an die PBeaKK übertragen worden seien.

Dies zum Anlass genommen fand im April 2024 ein erneuter gemeinsamer Austausch zwischen unserer Behörde, Vertretern der PBeaKK, der ZBS sowie dem Ministerium der Finanzen und für Wissenschaft (MFW) statt. Geklärt werden sollte die Frage, welche Daten nach Abschluss der Aufgabenübertragung und erfolgter Migration tatsächlich bei der PBeaKK vorliegen und ob die Absprachen aus dem vorhergehenden Projektverlauf mit dem UDZ diesbezüglich eingehalten wurden. Ebenso wurde die Einhaltung von Löschfristen bei der PBeaKK und der ZBS erörtert.

Die ursprüngliche Absprache mit unserer Behörde hinsichtlich des Umfangs der Übermittlung vorhandener Daten bzw. Dokumente an die PBeaKK orientierte sich entsprechend der Vorgabe des § 67a Abs. 2 SBG am Erforderlichkeitsgrundsatz. Insoweit

war insbesondere festgehalten worden, dass Beihilfebescheide einschließlich der jeweiligen Belege aus dem vorangegangenen Jahr ausreichend sein sollten, um eine ausreichende Grundlage für die weitere Bearbeitung durch die PBeaKK sicherstellen zu können. Es stellte sich jedoch heraus, dass entgegen dieser Festlegung tatsächlich Beihilfebescheide der vergangenen drei Jahre übertragen worden waren, diese jedoch ohne die jeweils zugehörigen Abrechnungsbelege. Diese Vorgehensweise wurde damit begründet, dass sich im Laufe der Entwicklung des Projekts Änderungen in der Planung ergeben hatten, aufgrund derer nunmehr die Migration weiter zurückliegender Beihilfebescheide für erforderlich gehalten worden war. Die Begründung hierfür liege insbesondere in der im Saarland vorgesehenen Löschfrist von 3 Jahren, die sich aus § 101 Abs. 2 SBG ergibt. Die Verpflichtung zur Einhaltung der Löschfristen sei bei der Übertragung der Beihilfebearbeitung mit auf die PBeaKK übergegangen. Ein weiterer Grund seien absehbare Anfragen von Beihilfeempfängern, in welchen auf gewährte Leistungen aus vergangenen Beihilfebescheiden verwiesen werde, um eine erneute Leistungsgewährung zu erhalten. Diese Begründung konnte unsere Behörde von der Erforderlichkeit der Datenübertragung insgesamt überzeugen.

Zu der Frage der Einhaltung der Löschfristen wurde von unserer Seite bestätigt, dass diese den gleichen Löschroutinen unterfallen wie zuvor bei der ZBS.

VI.

Gesundheit & Soziales

6 Gesundheit & Soziales

6.1 Kopie der Patientenakte

In unserem letzten Tätigkeitsbericht[52] wurde das Verhältnis zwischen dem Auskunftsanspruch nach Art. 15 DSGVO und dem Recht auf Einsicht in und Kopie der Patientenakte nach § 630g Bürgerliches Gesetzbuch (BGB) vor dem Hintergrund des Urteils des Europäischen Gerichtshofs aus Oktober 2023[53] thematisiert.

Mit diesem Urteil hat der EuGH unter anderem festgestellt, dass die erste Kopie dieser Akte den Patienten kostenfrei zur Verfügung zu stellen ist.

Die Datenschutzkonferenz (DSK) hat das Urteil in einer Entschließung vom 11. September 2024[54] aufgegriffen und darauf hingewiesen, dass das Urteil eine Änderung des § 630g BGB erforderlich macht, da diese Vorschrift eine Erstattung von Kosten für die Überlassung elektronischer Abschriften der Patientenakte vorsieht.

Der Bundesgesetzgeber hat diesen Änderungsbedarf in § 630g Abs. 2 Satz 2 BGB zwar erkannt und in einem Referentenentwurf des Bundesministeriums für Justiz[55] eine entsprechende Anpassung des BGB vorgesehen, allerdings ist diese Gesetzesänderung bislang noch nicht erfolgt.

Mit ihrer Entschließung hat die DSK darüber hinaus die Heilberufekammern aufgefordert, ihre Berufsordnungen entsprechend anzupassen. In vielen Berufsordnungen existieren näm-

[52] 32. Tätigkeitsbericht 2023, Kapitel 6.3, S. 103.

[53] EuGH, Urteil vom 26.10.2023, C-307/22, Celex-Nr. 62022CJ0307.

[54] Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. September 2024: Recht auf kostenlose Erstkopie der Patientenakte kann durch eine nationale Regelung nicht eingeschränkt werden! Datenschutzaufsichtsbehörden sehen konkreten Handlungsbedarf auf Seiten der Heilberufskammern; abrufbar unter https://www.datenschutzkonferenz-online.de/index.html

[55] https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/2024_Einsichtnahme_Patientenakte.html

lich nach wie vor Regelungen, welche die Möglichkeit eröffnen, bereits für die erste Kopie der Behandlungsdokumentation Kosten zu erheben. Derartige Normen stehen nunmehr ebenfalls im Widerspruch zur Rechtsprechung des EuGH, so dass sie nicht mehr anzuwenden sind.

Das Unabhängige Datenschutzzentrum Saarland hat daher die im Saarland betroffenen Heilberufekammern kontaktiert und auf die notwendige Anpassung ihres Berufsrechts hingewiesen. Alle Kammern haben uns mitgeteilt, dass sie im Rahmen ihrer berufsständischen Beratung die geänderte Rechtslage bereits berücksichtigen. Gleichzeitig wurden entsprechende Änderungen der Berufsordnungen in Aussicht gestellt. Im Falle der Psychotherapeutenkammer des Saarlandes ist die Umsetzung zwischenzeitlich erfolgt.

6.2 Vermieterbescheinigungen in Sozialleistungsverfahren

Durch die Beschwerde eines Betroffenen sowie eine Kontrollanregung wurden wir im Berichtszeitraum auf die Problematik der Anforderung von sogenannten Vermieterbescheinigungen durch Sozialleistungsträger aufmerksam gemacht.

Sowohl Jobcenter als auch Sozialämter benötigen für die Ermittlung des Bedarfs eines Leistungsempfängers unter anderem Informationen über die Kosten für Unterkunft und Heizung. Hierfür sind detaillierte Angaben zu Miete und Nebenkosten erforderlich.

Auch in diesem Zusammenhang gilt der Grundsatz aus dem Bereich des Sozialdatenschutzes, wonach Daten vorrangig bei der betroffenen Person zu erheben sind (Ersterhebungsgrundsatz, § 67a Abs. 2 SGB X). Leistungsempfängern liegen die benötigten Informationen in aller Regel in Form von Mietverträgen und Nebenkostenabrechnungen oder Verträgen mit Versorgungsunternehmen vor.

Um die Antragsbearbeitung zu vereinfachen bzw. zu beschleunigen, fordern viele Sozialleistungsbehörden Antragsteller dazu auf, gesonderte Formulare zu nutzen, mit denen die benötigten Angaben abgefragt werden. Diese sollen dann vom Vermieter unterschrieben und der Behörde vorgelegt werden.

Legen Leistungsempfänger ihrem Vermieter eine solche Bescheinigung vor, kommt dies einer Offenlegung des Sozialleistungsbezuges gegenüber dem Vermieter gleich. Hierzu kann der Leistungsberechtigte jedoch nicht gezwungen werden, wenn die erforderlichen Nachweise auch auf anderem, weniger eingriffsintensivem Weg erbracht werden können.

Hinzu kommt, dass für Vermieter grundsätzlich keine Auskunfts- oder Mitwirkungspflichten gegenüber dem Sozialleistungsträger bestehen. Weder die Behörde noch der Antragsteller können also Vermieter verpflichten, die Bescheinigung auszufüllen oder zu unterschreiben.

Vermieterbescheinigungen dürfen daher nur auf freiwilliger Basis verwendet werden. Auf die Freiwilligkeit ist durch die Behörde deutlich hinzuweisen.

Wir haben die Beschwerde und die Kontrollanregung zum Anlass genommen, die Jobcenter sowie ein Sozialamt in unserem Zuständigkeitsbereich auf diese Rechtslage hinzuweisen. Die Behörden haben unseren Hinweis zum Anlass genommen, die verwendeten Formulare – soweit nicht bereits enthalten – um einen Hinweis auf die Freiwilligkeit der Vorlage zu ergänzen. Ebenfalls baten wir darum, die Beschäftigten der Behörden diesbezüglich zu sensibilisieren, was uns auch zugesagt wurde.

6.3 Digitale Bereitstellung von Notfalldaten

Im Berichtszeitraum trat der Zweckverband für Rettungsdienst und Feuerwehralarmierung Saar (ZRF) an unsere Behörde heran und bat um datenschutzrechtliche Einschätzung zu einem Vorhaben im Bereich des Rettungswesens.

Die Fahrzeuge des ZRF sind mit dem System NIDA (Notfall-, Informations- und Dokumentationsassistent) zur digitalen Dokumentation der rettungsdienstlichen Einsätze ausgestattet. In dem System werden die Notfalleinsätze protokolliert, die Stammdaten und medizinischen Daten der transportierten Patienten dokumentiert und zwecks Übergabe an das aufnehmende Krankenhaus vorgehalten.

Der Einsatz von NIDA und die damit verbundene Datenverarbeitung erfolgt dabei (noch) nicht in ausschließlich digitaler Form, denn bis dato müssen die softwareseitig erfassten Protokolle durch den Rettungsdienst ausgedruckt und bei Einlieferung ins Krankenhaus den dortigen Mitarbeitern in Papierform übergeben werden.

Um diesen Übergabeprozess zwischen Rettungsdienst und weiterbehandelnder Stelle effizienter zu gestalten, bietet das eingesetzte System speziell für Krankenhäuser und Kliniken die Komponente „NIDAklinik" an. Die Implementierung dieser Komponente ermöglicht es, über eine Schnittstelle die Datenübertragung vom Rettungswagen an die aufnehmende Klinik in digitaler Form durchzuführen, was naturgemäß mit einer Beschleunigung der Patientenübergabe verbunden ist.

Der ZRF plant, den saarländischen Krankenhäusern die Nutzung von NIDAklinik vorzuschlagen. Testweise sollten zunächst zwei Kliniken angebunden werden.

Nach unserer Rechtsauffassung kann die Datenübermittlung vom Rettungswagen an das Krankenhaus auf § 27 Abs. 3 Nr. 1 Saarländisches Rettungsdienstgesetz (SRettG) gestützt werden. Danach ist eine Verarbeitung einschließlich der Übermittlung personenbezogener Daten zulässig, wenn es zur Versorgung des Patienten erforderlich ist. Dies ist vorliegend der Fall, da das aufnehmende Klinikum Informationen über den Gesundheitszustand des Patienten und die bislang ergriffenen Maßnahmen benötigt, um über das weitere Vorgehen bei der Behandlung zu entscheiden.

Auf welchem Weg diese Datenübermittlung erfolgt – wie bisher in Papierform oder elektronisch – ist für die grundsätzliche datenschutzrechtliche Zulässigkeit nicht entscheidend. Bei beiden Varianten sind jeweils technische und organisatorische Maßnahmen zu ergreifen, um die sensiblen Daten der Patienten hinreichend vor unbefugten Zugriffen zu schützen.

Zum Datenschutzkonzept des Anbieters, welches uns durch den ZRF vorgelegt wurde, ergaben sich Fragen hinsichtlich der Verschlüsselung der Daten sowie der Übertragungswege zwischen den einzelnen System-Komponenten.

So waren die Ausführungen zur technischen Absicherung des Übertragungsvorgangs zwischen den einzelnen Komponenten des NIDA-Systems nicht eindeutig. Maßnahmen der Verschlüsselung verfolgen hauptsächlich den Zweck der Sicherung der Vertraulichkeit gegen unberechtigte Kenntnisnahme personenbezogener Daten. Das Risiko unberechtigter Zugriffe von außen kann dabei durch einen providerseitigen VPN und eine Transportverschlüsselung minimiert werden, zudem ist aber auch das Risiko von Datenschutzverletzungen zu minimieren, die von unberechtigten Dritten mit privilegiertem internen Zugang ausgehen können. Die im Datenschutzkonzept von NIDAklinik vorgesehene Form der Verschlüsselung trug dem Szenario eines internen Angreifers nach hiesiger Auffassung noch nicht hinreichend Rechnung, so dass wir mit Blick auf die Sensibilität der betroffenen personenbezogenen Daten eine Überarbeitung der technischen Absicherung des Übertragungsvorgangs für geboten hielten.

Weiter stellten sich Fragen zum Umfang der zu übermittelnden Daten und zur Aufbewahrungsdauer, wo wir auf kürzere, vor allem auch konkrete und differenzierte Speicherfristen hingewirkt haben.

Auch haben wir eine Überprüfung des Rollen- und Berechtigungskonzepts angeregt, da wir es bspw. nicht für erforderlich hielten, dass ein Administrator unbegrenzt auch auf medizinische Daten zugreifen kann. Der ZRF hat unsere Hinweise aufge-

griffen und umgesetzt, so dass NIDAklinik nunmehr datenschutzkonform eingesetzt werden kann.

6.4 Beratung zum Impf-Informations-System (IISAAR)

Zu Beginn des Berichtszeitraums ist das Universitätsklinikum des Saarlandes (UKS) mit der Bitte um datenschutzrechtliche Begleitung eines Forschungsprojekts an uns herangetreten.

Bei dem Projekt „Aufbau eines Impf-Informations-Systems Saarland (IISAAR)" handelt es sich um ein durch das Bundesministerium für Gesundheit gefördertes Vorhaben, das als ELFA-Maßnahme („Ein Land Für Alle") konzipiert ist. Das Saarland hat hierbei die Federführung übernommen, kooperierende Bundesländer sind Baden-Württemberg, Bayern und Brandenburg. Ziel ist die bundesweit erstmalige, modellhafte Umsetzung eines Impf-Informations-Systems im Saarland (und in den kooperierenden Bundesländern) sowie die Schaffung einer gesetzlichen Grundlage zur datenschutzkonformen Nutzung und Verknüpfung von Impfdaten.

Unter einem Impf-Informations-System (IIS) wird international eine zugangsgesicherte, computergestützte Datenbank verstanden, mit deren Hilfe sowohl individuelle als auch bevölkerungsbezogene Informationen über durchgeführte Schutzimpfungen in einer vorbestehenden geopolitischen Region gesammelt, gespeichert und zur Vervollständigung des Impfstatus genutzt werden können. Darüber hinaus soll ein modernes IIS die Verbindung zu anderen elektronischen Datenbanken (z.B. Krebsregister, Infektionsmeldungen gemäß Infektionsschutzgesetz, Impfnebenwirkungen) ermöglichen und die Verfügbarmachung von zusätzlichen Management-Instrumenten zur Verbesserung der Impfleistungen bzw. der Immunisierungslage in der Bevölkerung (z. B. durch Recall-Systeme und elektronische Impfdokumentation).

Ziel des Forschungsprojekts ist es, zu untersuchen, unter welchen rechtlichen und technischen Rahmenbedingungen der

Aufbau eines IIS möglich ist. Da hierbei Gesundheitsdaten in großem Umfang verarbeitet werden, spielen datenschutzrechtliche Aspekte eine entscheidende Rolle.

Der Projektplan für IISAAR sieht eine zweistufige Umsetzung vor, bei der ein bereits vorhandenes IT-Basissystem in Stufe 1 als Prototyp im Sinne eines Impfregisters etabliert und auf dieser Basis dann in Stufe 2 das Impf-Informations-System mit der Möglichkeit z.B. von Verknüpfungen verschiedener Datenelemente aus unterschiedlichen Quellen vorbereitet werden soll.

Zu den datenschutzrechtlichen Herausforderungen gehörte zunächst vor allem die Frage nach der Rechtsgrundlage, auf die eine „Erstbefüllung" des Impfregisters mit Daten gestützt werden könnte.

Ursprünglich war beabsichtigt, die für das System notwendigen Daten auf Grundlage der im Forschungsbereich vorhandenen Rechtsgrundlagen zu erheben. Hiervon wurde aber im Laufe der Beratung Abstand genommen, da zweifelhaft war, ob die jeweiligen Voraussetzungen erfüllt sind. Die Ersterhebung der Daten soll nunmehr auf eine informierte Einwilligung der Betroffenen nach Art. 9 Abs. 2 lit. a DSGVO gestützt werden.

In mehreren Terminen wurden wir über den Stand des Projekts informiert und haben auf die Berücksichtigung datenschutzrechtlicher Regelungen sowie die Erstellung der erforderlichen Dokumente (Datenschutzkonzept, Einwilligungserklärung, Patienteninformation) hingewirkt.

Wir werden das Projekt weiterhin datenschutzrechtlich begleiten.

6.5 Beratung zum saarländischen Patientenportal

Mit der Bitte um Beratung und datenschutzrechtliche Begleitung eines Projekts hat sich die Saarländische Krankenhausgesellschaft e.V. (SKG), der Verband der Krankenhausträger im Saarland, im Berichtszeitraum an uns gewandt.

Die SKG bat um Unterstützung bei dem Digitalisierungsprojekt „Patientenportal" der saarländischen Krankenhäuser. Dabei handelt es sich um eine Maßnahme, die nach dem Krankenhauszukunftsgesetz (KHZG) förderungsfähig ist (§ 19 Abs. 1 Nr. 2 Krankenhausstrukturfonds-Verordnung – KHSFV i. V. m. § 14a Abs. 2 S. 1 Krankenhausfinanzierungsgesetz – KHG) und im Saarland umgesetzt werden soll.

Das landesweite Projekt sieht den Aufbau einer Portallösung (interoperable Plattform) vor, deren Zielsetzung es nach Aussage der SKG ist, dass „*die Patienten nicht weiter den Daten hinterherlaufen müssen, sondern die Daten den Patienten folgen und dort zur Verfügung stehen, wo sie gerade benötigt werden*".

Das Portal soll bis spätestens Ende 2025 von den derzeit zwölf am Projekt beteiligten Krankenhäusern in Betrieb genommen werden. Perspektivisch sollen alle saarländischen Kliniken an das Portal angebunden werden; dessen Nutzung soll für die Patienten aber freiwillig sein und demnach auf Einwilligungsbasis erfolgen.

Vorgesehen ist, dass sich Patienten bereits im Vorfeld einer Behandlung selbst in dem Portal registrieren und hierüber z.B. Termine vereinbaren können. Patienten, die sich noch nicht registriert haben, sollen bei Aufnahme in der Klinik gefragt werden, ob sie eine Nutzung wünschen.

In dem Portal sollen klinisch relevante Daten der Patienten in strukturierter Form eingestellt werden und so für die weitere Behandlung durch andere Kliniken sowie für die Patienten selbst abrufbar sein. Die Speicherung der Daten soll auf einen relativ kurzen Zeitraum (wenige Wochen nach Abschluss der Behandlung) begrenzt werden.

Bei der Beratung standen zunächst die technischen Aspekte des als Cloud-Lösung geplanten Portals im Vordergrund (Verschlüsselung, Mandatententrennung u.ä.). So waren die Vorgaben, die die SKG im Rahmen der Ausschreibung für das Portal vorsah, im Hinblick auf den Umfang und die Sensibilität der Daten, die ver-

arbeitet werden sollen, nach unserer Auffassung noch nicht ausreichend.

Nutzen mehrere datenschutzrechtlich Verantwortliche eine gemeinsame IT-Infrastruktur, muss durch eine datenschutzkonforme Mandantentrennung systemseitig sichergestellt werden, dass die Grundsätze der Zweckbindung und Vertraulichkeit der Datenverarbeitung gewahrt werden. Vereinfacht gesagt ist bezogen auf das Patientenportal zu gewährleisten, dass jedes Krankenhaus nur auf „seine" Patientendaten zugreifen kann. In diesem Zusammenhang haben wir insbesondere auf die Berücksichtigung der Maßnahmen in dem Dokument Baustein 50 „Trennen" des von den Datenschutzaufsichtsbehörden entwickelten Standard-Datenschutzmodells (SDM), das eine Hilfestellung bei der Umsetzung der rechtlichen Anforderungen der DSGVO bieten soll, hingewiesen.[56]

Hinsichtlich der Verschlüsselung ist nach unserer Auffassung beim Aufbau des Patientenportals die Technische Richtlinie TR-03161: „Anforderungen an Anwendungen im Gesundheitswesen – Teil 3. Hintergrundsysteme"[57] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu berücksichtigen. Darin wird als Anforderung an die Datensicherheit unter anderem verlangt, dass sensible Daten zwingend verschlüsselt gespeichert werden müssen. Für das geplante System liegt es nahe, diese technische Richtlinie als Maßstab für die Gewährleistung der Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität zu Grunde zu legen.

Im Zuge der Gespräche wurde seitens der SKG zugesagt, im Rahmen der weiteren Konzeptionierung unsere Anmerkungen zu berücksichtigen.

[56] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V30a.pdf

[57] Abrufbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema- sortiert/tr03161/tr03161_node.html

Herausfordernd für die praktische Umsetzung des Patientenportals dürfte sein, dass sich die Abläufe in den Kliniken unterscheiden und verschiedene Krankenhausinformationssysteme (KIS) genutzt werden, so dass jedes Haus für sich prüfen muss, wie die Nutzung des Portals eingebunden werden kann. Zum Teil soll es Schnittstellen für die Übertragung von Daten aus dem KIS in das Portal geben, oft werden Daten – zumindest vorerst – aber auch händisch erfasst werden müssen.

VII.

Schule & Bildung

7 Schule & Bildung

7.1 Telepräsenz-Avatare

Telepräsenz-Avatare ermöglichen es Schülerinnen und Schülern, deren regelmäßige Teilnahme am Unterricht beispielsweise wegen einer Langzeiterkrankung für eine längere Zeit nicht zu erwarten ist, per Tablet und App von zu Hause aus oder aus dem Krankenhaus live am Schulunterricht teilzunehmen. Der Avatar, der im Unterrichtsraum der zugehörigen Schulklasse platziert wird, fungiert dabei als Stellvertreter des Kindes im Unterricht. Dieses hat so die Möglichkeit, dem Unterricht zu folgen, sich aktiv daran zu beteiligen und mit seinen Mitschülern zu kommunizieren. Dadurch besteht die Möglichkeit, den Kontakt zur Klassengemeinschaft zu erhalten, Lernlücken zu vermeiden und die Teilnahme am Unterricht trotz längerer Abwesenheit zu ermöglichen.

Mit dem Einsatz solcher Telepräsenz-Avatare sind jedoch auch Datenverarbeitungsprozesse verbunden, die datenschutzrechtlich begleitet werden müssen. Es werden Bild- und Tonaufnahmen aus dem Unterrichtsraum über den Anbieter des Telepräsenz-Avatars an das Tablet des Kindes oder Jugendlichen übermittelt und umgekehrt von dem Kind in den Unterrichtsraum an Lehrkräfte und Mitschüler gesendet. Diese Daten müssen gem. Art. 25 und 32 DSGVO mittels technischer und organisatorischer Maßnahmen vor unbefugten Zugriffen geschützt werden.

Schon in der Vergangenheit kam als Legitimationsgrundlage für diese Datenverarbeitung lediglich eine Einwilligung aller Schüler bzw. deren Erziehungsberechtigten und der in der Klasse unterrichtenden Lehrkräfte in Frage. Für den Einsatz des Avatars bedarf es daher einer Vielzahl von Einwilligungserklärungen; sofern nur eine der betroffenen Personen diese Einwilligung nicht erklärt oder im Nachhinein von ihrem Widerrufsrecht Gebrauch macht, besteht für das Kind keine Möglichkeit mehr, auf diesem Weg am Unterricht teilzunehmen.

Im Rahmen der umfassenden Neuregelung der rechtlichen Grundlagen für die Verarbeitung personenbezogener Daten in den Schulen durch das Schulwesen-Datenschutzgesetz (Schulw-DSG) und die dazugehörige Schulwesen-Datenschutzverordnung (Schulw-DSV) hatte unsere Behörde angeregt, eine rechtssichere Grundlage für den Einsatz des Telepräsenz-Avatars zu schaffen. Bei der Abwägung zwischen den Eingriffen in das informationelle Selbstbestimmungsrecht der Betroffenen und dem Recht des langfristig erkrankten Kindes, am Erziehungs- und Bildungsauftrag der Schule teilnehmen zu können, sahen wir es als verhältnismäßig an, eine gesetzliche Regelung zu schaffen, die die Einwilligung der Betroffenen entbehrlich macht und die mit dem Einsatz des Telepräsenz-Avatars einhergehende Datenverarbeitung legitimiert.

Der Gesetzgeber hat sich letztendlich dafür entschieden, zunächst weiterhin an der Erforderlichkeit einer Einwilligung aller Betroffenen in die Maßnahme als Legitimationsgrundlage festzuhalten. Jedoch hat er gesetzlich festgelegt, dass die praktische Umsetzung in drei Jahren evaluiert werden soll. Aufgrund der dann vorliegenden Erfahrungen soll erneut über eine gesetzliche Rechtsgrundlage diskutiert werden.

7.2 Datenschutzverletzung in Kindergarten-App

Für Aufsehen sorgte im Berichtszeitraum die Veröffentlichung einer Sicherheitslücke in einer Kindergarten-App, die deutschlandweit im Einsatz ist.[58] Die App wird unter anderem dazu genutzt, Eltern und Angehörige über Termine im Kindergarten zu informieren, Kinder vom Kindergartenbesuch abzumelden oder sie zum Mittagessen in der Kita anzumelden. Der Betreiber der App informierte die betroffenen Einrichtungen darüber, dass durch einen Konfigurationsfehler auf einem Webserver persönliche Daten der Nutzer wie Namen, Geburtsdaten, Anschriften, Notfallkontakte, Avatarbilder etc. ungeschützt und öffentlich

[58] https://www.heise.de/news/Datenleck-bei-beliebter-KiTa-App-Stay-Informed-9662578.html

abrufbar waren. Die unbeschränkte Zugriffsmöglichkeit Unbefugter auf diese Informationen stellt eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 33 DSGVO dar. Datenschutzrechtlich verantwortlich im Sinne von Art. 4 Nr. 7 DSGVO ist dabei der Träger der Kindergärten, der sich entscheidet, die App seinen Einrichtungen zur Nutzung zur Verfügung zu stellen. Der Entwickler und technische Betreiber der App fungiert hierbei als sogenannter Auftragsverarbeiter im Sinne von Art. 28 DSGVO, der die technische Infrastruktur zur Datenverarbeitung per App zur Verfügung stellt.

Viele im Saarland ansässigen Träger der Kindergärten, bei denen die betroffene App im Einsatz war, kamen zeitnah ihrer gesetzlichen Pflicht zur Meldung einer Verletzung des Schutzes personenbezogener Daten innerhalb der in Art. 33 DSGVO vorgesehenen 72-Stunden-Frist gegenüber uns als zuständiger Datenschutz-Aufsichtsbehörde nach. Die meldenden Einrichtungen wurden durch uns daraufhin informiert, dass die von dieser Datenschutzverletzung betroffenen Personen, deren Daten zugänglich waren, gem. Art. 34 DSGVO zu informieren seien und auf eine erhöhte Achtsamkeit beim Umgang beispielsweise mit E-Mails und Telefonanrufen hingewiesen werden müssen.

Durch eine nachgehende Recherche konnten wir darüber hinaus acht weitere hiervon betroffene Kindergärten und Kommunen ausfindig machen, welche die App ebenfalls im Einsatz hatten, jedoch der gesetzlichen Pflicht zur Information unserer Behörde nach Art. 33 DSGVO nicht nachgekommen waren. Als Folge nahmen wir Kontakt zu diesen Verantwortlichen auf und baten um Stellungnahme, unter anderem warum vorliegend auf eine Meldung gem. Art. 33 DSGVO verzichtet wurde und ob und ggf. welche weiteren Maßnahmen durch die Verantwortlichen ergriffen wurden. Einige Verantwortliche wiesen uns dabei darauf hin, dass sie im Rahmen der Prüfung des Vorfalls von dem Entwickler der App die Information erhalten hätten, von der Datenschutzverletzung nicht betroffen gewesen zu sein, da sie bestimmte Funktionalitäten der App nicht nutzten. Einige Träger gaben an, von der Datenschutzverletzung zu spät erfahren zu

haben, was letztlich auf eine unzureichende Kommunikation zwischen Kindergarten und Träger zurückzuführen war. Hierbei ist anzumerken, dass es ungeachtet dessen dem Träger als Verantwortlichem obliegt, die Kommunikation mit seinen Kindergärten derart zu organisieren, dass ihm Datenschutzverletzungen zeitnah gemeldet werden. Er kann sich nicht darauf berufen, dass eine solche Tatsache nur dem Kindergarten bekannt war und nicht weitergeleitet wurde. Die Pflicht zur Weiterleitung einer bekannt gewordenen Datenschutzverletzung an den Träger ist bestenfalls durch schriftliche Anweisung zu regeln.

Durch unsere nachgehende Recherche zu diesem Datenschutzvorfall konnten wir letztlich sicherstellen, dass alle im Saarland von der Datenschutzverletzung betroffenen Personen informiert und sensibilisiert wurden.

Fazit

Verantwortliche sind gemäß Art. 33 Abs. 1 DSGVO im Falle des Bekanntwerdens einer Datenschutzverletzung zum unmittelbaren Tätigwerden verpflichtet. Dies gilt unabhängig von der Frage, welcher internen Organisationseinheit des Verantwortlichen die Verletzung bekannt wurde. Eine unverzügliche Information der für den Datenschutz zuständigen Stelle hat der Verantwortliche daher organisatorisch sicherzustellen.

7.3 Schullaufmeisterschaften

Die Saarländischen Schullaufmeisterschaften sind eine seit dem Jahr 1999 stattfindende alljährliche Sportveranstaltung, bei welcher Schülerinnen und Schüler der teilnehmenden saarländischen Schulen gemeinsam im sportlichen Wettstreit ihre Talente in diesem Bereich unter Beweis stellen. Die Schullaufmeisterschaften unterstehen dabei der Regie eines Landkreises als Veranstalter.

Im Rahmen einer Eingabe von Eltern eines Schülers/einer Schülerin wurden wir darauf hingewiesen, dass sowohl Ergebnisse als

auch Fotografien beispielsweise der Zieleinläufe von Kindern und Jugendlichen, die an den Saarländischen Schullaufmeisterschaften teilgenommen hatten, offen und für jedermann im Internet abrufbar veröffentlicht wurden.

Diese Verfahrensweise, welche in der Vergangenheit nicht näher hinterfragt wurde, muss in datenschutzrechtlicher Hinsicht gleichwohl die gesetzlichen Anforderungen erfüllen. Dies nicht aufgrund formaler Selbstzwecke, sondern aus ganz naheliegenden Gründen. Denn obgleich die meisten Schülerinnen und Schüler bzw. deren Erziehungsberechtigte einer derartigen Veröffentlichung wohl unkritisch gegenüber stehen dürften, ist das Anliegen, nicht mit einer Fotografie der eigenen Person öffentlich im Internet in Erscheinung zu treten, nachvollziehbar und zu respektieren; dies umso mehr, als es sich vorliegend um minderjährige Teilnehmerinnen und Teilnehmer handelt, die auch und gerade vor der omnipräsenten und unkontrollierbaren Öffentlichkeit des Internets zu schützen sind.

Ausgehend davon, dass die Teilnahme an der Veranstaltung für die Schülerinnen und Schüler freiwillig ist, sie also nicht angehalten sind, die Sportwettkämpfe in ihrer Freizeit zu bestreiten, sondern eigens hierfür vom regulären Schulunterricht befreit werden, können die Schulmeisterschaften als eine freiwillige schulische Veranstaltung eingeordnet werden.

Dieser schulische Charakter der Veranstaltung bedeutet indes nicht, dass es die teilnehmenden Schülerinnen und Schüler bzw. ihre Eltern hinnehmen müssten, dass die Teilnahme zwangsläufig mit einer Veröffentlichung von personenbezogenen Daten im Internet verbunden ist. Insbesondere ist diese Datenverarbeitung nicht gemäß Art. 6 Abs. 1 lit. e DSGVO für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe, hier dem Bildungsauftrag der Schule, erforderlich.

Daher bedarf es für die Veröffentlichung grundsätzlich einer Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO. Nach Art. 4 Nr. 11 DSGVO ist eine Einwilligung jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene

Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Der Veranstalter der Schullaufmeisterschaft hat daher bereits in der Anmeldung zu der Veranstaltung sowie auf der betreffenden Internetseite die Schülerinnen und Schüler bzw. ihre Erziehungsberechtigten umfassend darüber zu informieren, welche Daten in welcher Form verarbeitet werden. Auch über den jeweiligen Ort der Veröffentlichung ist zu informieren; im Falle einer Veröffentlichung im Internet beinhaltet dies grundsätzlich die Nennung der jeweiligen Website. Ebenso sind die Teilnehmerinnen und Teilnehmer bzw. deren Erziehungsberechtigte eindeutig darauf hinzuweisen, dass ihnen ein jederzeitiges voraussetzungsloses Widerrufsrecht gegen diese Datenverarbeitung zusteht, welches sie auch schon im Vorfeld der Teilnahme geltend machen können.

Von Seiten des Veranstalters ist für den Fall des Widerrufs einer Einwilligung zu gewährleisten, dass dieser Widerruf zur Kenntnis genommen und umfassend berücksichtigt wird.

In unseren Augen wird hierdurch eine Situation geschaffen, bei welcher auf der einen Seite die bisher gelebte und bewahrenswerte Praxis des Anfertigens von Erinnerungsfotos für die Teilnehmerinnen und Teilnehmer beibehalten werden kann und zugleich der nachvollziehbare Wunsch nach einer Nichtveröffentlichung im Rahmen einer sportlichen Veranstaltung in leichter Form geäußert werden kann. Für den Veranstalter bedeutet dies nicht zuletzt auch ein größeres Maß an Rechts- und Planungssicherheit, da er die Widersprüche im Rahmen der Anmeldung in dokumentierter schriftlicher Form erhält und die Fotografen der Veranstaltung hiernach genau anweisen kann.

Nachdem wir den Verantwortlichen auf die Rechtslage hingewiesen haben, räumte dieser ein, dass das bisherige Verfahren dem besonderen Schutzinteresse der Kinder und Jugendlichen nicht gerecht wurde und man im nächsten Jahr für alle Teilneh-

merinnen und Teilnehmer eine Einwilligungserklärung einholen werde, welche bei Kindern durch die Sorgeberechtigten unterschrieben werden muss. Eine entsprechend umfassende Information zur Datenverarbeitung werde den Eltern im Rahmen einer Datenschutzerklärung im Sinne von Art. 13 DSGVO im Vorfeld der Veranstaltung zur Verfügung gestellt. Darüber hinaus werde ausführlich im Infoflyer und auf der entsprechenden Website auf die Thematik hingewiesen.

VIII.

Inneres & Kommunen

8 Inneres & Kommunen

8.1 Turnusmäßige Kontrollen von ATD/RED und EURODAC

Auch im Berichtsjahr initiierte das Unabhängige Datenschutzzentrum Saarland wieder die gesetzlich vorgegebenen turnusmäßigen Kontrollen zur Antiterrordatei (ATD) und zur Rechtsextremismus-Datei (RED) sowie zum europäischen Fingerabdruck-Identifizierungssystem Eurodac.

8.1.1 Kontrolle von ATD und RED

ATD und RED sind gem. § 10 Abs. 2 Antiterrordateigesetz (ATDG) bzw. § 11 Abs. 2 Rechtsextremismusdatei-Gesetz (RED-G) mindestens alle zwei Jahre in datenschutzrechtlicher Hinsicht zu kontrollieren. In den Zuständigkeitsbereich der saarländischen Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) fallen hierbei die „Abteilung V – Verfassungsschutz" des Ministeriums für Inneres, Bauen und Sport sowie das saarländische Landespolizeipräsidium (LPP). Aufgrund der hohen Prüfdichte – gerade im Sicherheitsbereich – und der geringen Personalkapazität unserer Behörde wurden in den vergangen Jahren die ATD und die RED jährlich und hierbei alternierend zwischen der Abteilung V und dem LPP (somit bei beiden Behörden immer im Turnus von zwei Jahren) kontrolliert.

Die vergangenen Prüfungen zeigten jedoch auf, dass die Anzahl der von saarländischen Sicherheitsbehörden in den Vorsorgedateien gespeicherten Personen gering war. Eine Evaluierung des Arbeitsaufwands zeigte deswegen auf, dass das alternierende Vorgehen eher mehr als weniger Aufwand mit sich brachte. Aus diesem Grund entschied sich das Unabhängige Datenschutzzentrum Saarland dazu, die Datenverarbeitung im Kontext von ATD und RED ab dem Berichtsjahr wieder (unter Aufgabe der Alternierung) bei beiden Behörden gleichzeitig durchzuführen.

Um einen Gleichlauf der Kontrollen zu gewährleisten wurde ein gemeinsamer Stichtag gewählt (01.09.2024) zu dem der aktuelle, von der jeweiligen Behörde eingespeicherte Datenbestand in ATD und RED zu ermitteln war. Gleichzeitig sollten die Neueinspeicherungen in die Vorsorgedateien für den Zeitraum vom 01.01.2024 bis zum Stichtag mitgeteilt werden. Nach Auswertung der übersandten Protokolldaten („Standardreports") erfolgte zunächst bei der Abteilung V ein Vor-Ort-Termin zur Klärung von Detailfragen und zur Einsicht in die Systeme. Datenschutzrechtliche Verstöße wurden hierbei nicht festgestellt.

Der Besuch beim LPP, der vorwiegend der Klärung technischer und organisatorischer Detailfragen dient, steht zum Zeitpunkt des Redaktionsschlusses noch aus. Aufgrund erster Erkenntnisse aus den vorab schriftlich zugelieferten Informationen wird derzeit nicht davon ausgegangen, dass die Einsicht ins System größere datenschutzrechtliche Mängel aufzeigen wird.

8.1.2 Kontrolle von Eurodac

Auch die Datenverarbeitung im Zusammenhang mit dem Fingerabdruck-Identifizierungssystem Eurodac ist von unserer Behörde regelmäßig zu kontrollieren. Eine jährliche Überprüfung ist für solche Abfragen des Systems vorgesehen, die zum Zwecke der Gefahrenabwehr und Strafverfolgung vorgenommen werden.

Wie bereits im vergangenen Jahr, zeigte die diesjährige Kontrolle erneut auf, dass Eurodac-Daten in Gefahrenabwehr- und Ermittlungsverfahren der saarländischen Polizei keine wirkliche Rolle spielen. Während in der letzten Prüfung für die Jahre 2018 bis April 2023 lediglich ein Zugriff ausgewiesen wurde, bescheinigte uns das LPP für den dieses Mal relevanten Zeitraum von April 2023 bis September 2024 keine einzige Recherche im System.

Da sich eine weitere Untersuchung der Datenverarbeitung zu präventiven und repressiven Zwecken somit erübrigte, wurde der Fokus der Prüfung stattdessen auf den ausländerrechtlichen Kontext gelegt. Bereits im Jahr 2022 hatte sich unsere Behörde

die Verfahren mit Bezug zu Eurodac bei der saarländischen Ausländerbehörde und der Landesaufnahmestelle in Lebach vorstellen lassen: Dort werden Fingerabdruckdaten im Zuge der Erstregistrierung bei asylsuchenden Personen erhoben und zur Durchführung des Dublin-Verfahrens an Eurodac übermittelt.[59]

Da bei der Polizei aber ebenfalls die Äußerung eines Asylgesuchs möglich ist und von den Sicherheitsbehörden auch im Falle des Aufgreifens einer Person bei unerlaubter Einreise oder bei illegalem Aufenthalt in Deutschland Daten an Eurodac übermittelt werden, wurde im Berichtsjahr das entsprechende Vorgehen bei der Datenverarbeitung beim LPP überprüft.

So stellte das LPP das Standard-Vorgehen der operativen Dienststellen bei der erkennungsdienstlichen Behandlung dar. Hierbei wurde auf die verschiedenen Anlässe im ausländerrechtlichen Kontext und die hierfür einschlägigen Rechtsgrundlagen (§ 14 AsylG; § 49 Abs. 8, Abs. 9 AufenthG) hingewiesen. Auch wurde anhand eines Falles im Echtsystem das Vorgehen im Detail präsentiert.

Die vorgestellte Datenverarbeitung begegnete dabei keinen grundlegenden datenschutzrechtlichen Bedenken.

Neben einer geringen Anpassungsbedürftigkeit einzelner Formulare, erschien aus datenschutzrechtlicher Sicht jedoch die Bereitstellung von Informationen über die Datenverarbeitung verbesserungswürdig. So teilte das LPP in einem Vor-Ort-Termin mit, dass standardmäßig nur eine Belehrung über die Möglichkeit eines verwaltungsrechtlichen Widerspruchs (§§ 68 ff. VwGO) erfolge. Datenschutzhinweise würden bei der erkennungsdienstlichen Behandlung dagegen nicht erteilt. Gemäß Art. 29 Eurodac-VO sind der betroffenen Person diese Informationen jedoch zum Zeitpunkt der Fingerabdruckabnahme zur Verfügung zu stellen.

Das Unabhängige Datenschutzzentrum Saarland wird auf eine diesbezügliche Verbesserung hinwirken. Hierbei wird insbeson-

[59] Siehe hierzu ausführlicher der Beitrag im 32. Tätigkeitsbericht (Kapitel 4.4.1).

dere zu beachten sein, dass die verpflichtend zu erteilenden Informationen zukünftig noch präziser und ausführlicher gestaltet werden müssen. Hierbei wird auch die vom europäischen Verordnungsgeber im Mai dieses Jahres beschlossene Novellierung des Eurodac-Systems Berücksichtigung finden. Die neue Verordnung (EU) 2024/1358 wird die bisherige Verordnung (EU) 603/2013 mit Geltung zum 12. Juni 2026 ablösen.

Ob mit den neuen Vorgaben (insbesondere mit der Ausweitung der in Eurodac zu hinterlegenden Daten) auch eine Änderung im Zugriffsverhalten der Polizei einhergehen wird, kann derzeit noch nicht abgeschätzt werden. Der weiterhin vorgesehenen, jährlichen Kontrollverpflichtung werden wir jedenfalls auch im Jahr 2025 und den Folgejahren umfänglich nachkommen.

8.2 AK Sicherheit: Entschließung zu Gesichtserkennungssystemen

Zur Gewährleistung eines einheitlichen, europäischen Datenschutzniveaus ist nicht nur die Festlegung klarer Regeln für die Verarbeitung personenbezogener Daten, sondern auch die größtmögliche Harmonisierung auf Ebene der Aufsicht und Durchsetzung erforderlich. Um letztere im föderalen Deutschland zu gewährleisten, haben sich die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Datenschutzkonferenz (DSK) zusammengeschlossen. Die DSK fördert den Datenschutz und verständigt sich auf gemeinsame Positionen. Hierbei wird sie von zahlreichen Untergremien in Form von Arbeitskreisen unterstützt. Diese arbeiten der DSK zu und bereiten deren Entscheidungen vor.

Obgleich das Saarland derzeit keinen Vorsitz eines Arbeitskreises innehat, nahmen wir gerne die Aufgabe wahr, im Berichtsjahr die Herbstsitzung des „Arbeitskreises Sicherheit" (Vorsitz: Schleswig-Holstein) als Gastgeber in Saarbrücken auszurichten. Die diesbezügliche Tagung fand am 18. und 19. September 2024 in den Räumlichkeiten des Landtags des Saarlandes statt.

Unter anderem befasste sich der Arbeitskreis mit der Erstellung eines Entschließungsentwurfs zu automatisierten Gesichtserkennungssystemen. Hintergrund waren konkrete Bestrebungen der Politik, das Instrument der automatisierten biometrischen Gesichtserkennung in unterschiedlichen rechtlichen Zusammenhängen zu erlauben. So gedachte etwa die Ampelkoalition im September 2024 als Reaktion auf die Anschläge in Solingen durch ein „Sicherheitspaket" weitreichende neue Eingriffsmöglichkeiten für die Sicherheitsbehörden zu schaffen. Zu diesen gehörte auch die Ermächtigung, einen biometrischen Abgleich mit Daten (insbesondere Bildern) aus dem Internet vornehmen zu dürfen. Da bereits im Frühjahr 2024 die Nutzung eines Gesichtserkennungssystems durch die sächsische Polizeidirektion ohne ausreichende rechtliche Grundlage bekannt geworden war und die Europäische Union mit der im Juni 2024 verabschiedeten Verordnung über künstliche Intelligenz (KI-Verordnung) weitreichende Vorgaben, unter anderem auch für die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme, erlassen hatte, bereitete der AK Sicherheit eine Entschließung der DSK vor, in der die Position der deutschen Datenschutzaufsichtsbehörden zum polizeilichen Einsatz von Gesichtserkennungssystemen dargelegt wurde.

Aufgrund der unmittelbar bevorstehenden Beratungen des Gesetzentwurfs im Bundestag wurde die Entschließung „Vorsicht bei dem Einsatz von Gesichtserkennungssystemen durch die Sicherheitsbehörden" bereits am 20. September von der DSK einstimmig verabschiedet.

Die DSK macht darin gezielt auf die rechtlichen Grenzen und Voraussetzungen automatisierter Gesichtserkennung aufmerksam. Sie appelliert an den Gesetzgeber, die unbedingte Erforderlichkeit einer Legitimation solcher Eingriffe zunächst sorgfältig zu prüfen und sich im Falle einer Entscheidung für diese Option intensiv mit den zu beachtenden rechtlichen Vorgaben auseinanderzusetzen.

Die Entschließung und die diesbezügliche Pressemitteilung sind auf der Website der Datenschutzkonferenz abrufbar.[60]

8.3 Auskunftsrecht gegenüber der Vollzugspolizei

8.3.1 Rechtsgrundlage des Auskunftsrechts

Das Auskunftsrecht betroffener Personen ist im Geltungsbereich der Datenschutz-Grundverordnung (DSGVO) durch Art. 15 DSGVO zentral und abschließend harmonisiert worden. Die Existenz dieses Rechts und seine ungefähre Reichweite sind mittlerweile weitgehend bekannt. Weniger geläufig ist hingegen, dass datenschutzrechtliche Auskunftsersuchen an Sicherheitsbehörden, wie die Polizei, die im Rahmen der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten tätig werden, nicht unter die DSGVO[61], sondern unter die Richtlinie (EU) 2016/680 (JI-Richtlinie) fallen.

Das in den Art. 14 und 15 JI-Richtlinie geregelte Auskunftsrecht weist zwar Parallelen zu Art. 15 DSGVO auf, unterscheidet sich jedoch in mehreren wesentlichen Aspekten. Da die JI-Richtlinie lediglich Mindeststandards vorgibt und keine unmittelbare Rechtswirkung in den Mitgliedstaaten entfaltet, war und ist ihre Umsetzung in nationales Recht erforderlich. In Deutschland fällt die Regelungsmaterie im Kontext der polizeilichen Datenverarbeitung (jedenfalls für den Bereich der allgemeinen Gefahrenabwehr) zudem in die Gesetzgebungskompetenz der Länder, wodurch die spezifischen Ausgestaltungsgesetze in einzelnen Punkten voneinander abweichen können. Im Saarland ist so beispielsweise gegenüber der Vollzugspolizei eine Auskunft auf Grundlage von § 11 des Saarländischen Gesetzes über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG) möglich.

[60] Die Entschließung ist abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/2024-09-20_Entschliessung_DSK_Gesichtserkennung.pdf; die diesbezügliche Pressemitteilung vom 20.09.2024 ist abrufbar unter: https://www.datenschutzkkonferenz-online.de/media/pm/2024-90-20_PM%Entschliessung_DSK_Gesichtserkennung.pdf

[61] Vgl. Art. 2 Abs. 2 lit. d DSGVO.

Föderal bedingte, unterschiedliche gesetzliche Rahmenbedingungen wirken sich dabei erheblich auf die praktische Handhabung datenschutzrechtlicher Auskunftsersuchen durch die Vollzugspolizei aus. Mit Blick auf die Mindestanforderungen der JI-Richtlinie lassen sich zwar gemeinsame Grundmuster erkennen, die divergierenden Umsetzungen in den Landesgesetzen erschweren jedoch die Formulierung einheitlicher und verbindlicher Aussagen zu datenschutzrechtlichen Problematiken im Kontext solcher Auskunftsersuchen.

Im vergangenen Jahr beschäftigte sich unsere Dienststelle daher vertieft mit in der Praxis häufig gestellter Fragen rund um das datenschutzrechtliche Auskunftsrecht speziell bei der Polizei. Neben den Inhalten des § 11 SPolDVG setzten wir uns insbesondere auch mit der Auslegung der Vorschriften der JI-Richtlinie auseinander.

Im Folgenden werden zwei zentrale Themenbereiche der Antragstellung und der Auskunftsgewährung durch die Polizei betrachtet.

8.3.2 Rahmenbedingungen der Antragstellung

Schon vor der Geltendmachung des Anspruchs auf Auskunft über die Verarbeitung personenbezogener Daten stellen sich für betroffene Personen zahlreiche praktische Fragen: Ist für den Antrag eine bestimmte Form vorgeschrieben? Gibt es zu beachtende Fristen? Fallen hierbei Kosten an? Die Antwort auf alle diese Fragen lautet grundsätzlich „nein“.

So schreibt die JI-Richtlinie beispielsweise keine spezifische Form für die Stellung eines Auskunftsanspruchs vor. Anträge können daher mündlich (vor Ort), schriftlich per Post, E-Mail oder Fax eingereicht werden. Es empfiehlt sich jedoch, ein Ersuchen auf schriftlichem Wege zu stellen, das Name, Anschrift und Geburtsdatum der anfragenden Person enthält, da hierdurch eine eindeutige Zuordnung der bei der Polizei gespeicherten Daten ermöglicht wird und der Vorgang eindeutig dokumentiert ist. Auch müssen so seltener, Rückfragen durch die Polizei

erfolgen. Eine Begründung für das Auskunftsersuchen ist grundsätzlich nicht erforderlich.

Da das Auskunftsrecht als höchstpersönliches Recht zu qualifizieren ist, kann es grundsätzlich nur von der betroffenen Person selbst geltend gemacht werden. Daneben können ausnahmsweise aber auch bevollmächtigte Dritte, wie beispielsweise Rechtsanwälte, ein Auskunftsersuchen stellen, sofern sie eine entsprechende Vollmacht vorlegen. Gesetzliche Vertreter, etwa Eltern minderjähriger Kinder, sind ebenfalls berechtigt, einen Antrag zu stellen, solange die Kinder nicht selbst bereits die erforderliche Einsichtsfähigkeit besitzen, wovon in der Regel ab dem vollendeten 14. Lebensjahr auszugehen ist. Erfolgt die Antragstellung in solchen Fällen dennoch nur durch die Eltern, so wird die Polizei die minderjährige Person vor Gewährung der Auskunft zu beteiligen haben, um zu ermitteln, ob sie die Auskunft auch tatsächlich wünscht.[62]

Da polizeiliche Informationen darüber hinaus häufig sensibler Natur sind und unbefugte Ausforschungsanfragen vermieden werden sollen, ist die Polizei verpflichtet, die Identität der anfragenden Person zweifelsfrei zu verifizieren und die Auskunftsberechtigung zu überprüfen / festzustellen. Bei begründeten Zweifeln ist die Polizei deswegen befugt, klärende Identitätsnachweise anzufordern (Art. 12 Abs. 5 JI-Richtlinie; § 15 Abs. 4 SPolDVG). Unverhältnismäßige Hürden für die Antragsteller dürfen dabei aber nicht geschaffen werden.

Ist die antragstellende Person der Polizei etwa bereits aus anderen Verfahren persönlich bekannt oder äußert sie das Auskunftsersuchen sogar als direkte Reaktion auf ein Anschreiben der Polizei, so dürfte es nicht erforderlich sein, nochmals zusätzlich einen Nachweis über die Identität zu fordern. Gleiches gilt, wenn sich die in der Anfrage angegebenen personenbezogenen Daten (insbesondere die Adresse) mit den vorhandenen Infor-

[62] Etwaige eigene Informationsansprüche der Eltern gegenüber der Polizei hinsichtlich der Daten des minderjährigen Kindes, die aus ihrer Personensorge erwachsen, bleiben hiervon unberührt.

mationen aus den polizeilichen Informationssystemen decken oder eine Auskunft von einem zugelassenen Rechtsanwalt im Namen seines Mandanten gefordert wird.

In Fällen, in denen die vorgenannten Wege der Authentifizierung nicht zum Erfolg führen und andere verlässliche Authentifizierungsverfahren nicht zur Verfügung stehen, können Zweifel letztlich durch Übersendung einer Kopie eines Ausweisdokuments ausgeräumt werden. Ein solches Vorgehen kann zwar in bestimmten Konstellationen unverhältnismäßig erscheinen,[63] allerdings ist die polizeiliche Datenverarbeitung häufig mit einem erhöhten Risiko für die Rechte der betroffenen Person verbunden, sodass entsprechende Anforderungen zur letztverbindlichen Klärung der Identität im Einzelfall erforderlich sein können. Zu beachten ist hierbei, dass nicht relevante Informationen wie Lichtbild, Seriennummer, Körpergröße oder Augenfarbe geschwärzt werden dürfen. Wird der Antrag außerdem *persönlich* auf einer Polizeidienststelle gestellt, genügt es in der Regel bereits, wenn die Identität der antragstellenden Person *vor Ort* durch Polizeibedienstete festgestellt und vermerkt wird, ohne dass eine Kopie eines Ausweises angefertigt werden muss.

Antragstellern steht es aber letztlich auch frei, einen entsprechenden Identitätsnachweis zur Beschleunigung des Verfahrens bereits zusammen mit dem Antrag einzureichen.

Kosten oder Gebühren fallen bei Geltendmachung eines datenschutzrechtlichen Auskunftsanspruchs im Regelfall nicht an. Nur bei offenkundig unbegründeten oder exzessiven Anträgen kann eine angemessene Gebühr verlangt oder von einer Beantwortung vollständig abgesehen werden (Art. 12 Abs. 4 lit. a JI-Richtlinie; § 15 Abs. 3 S. 2 SPolDVG).

Zu beachten ist zudem, dass - anders als in der DSGVO - im Bereich der JI-Richtlinie keine bestimmte Frist (DSGVO: 1 Monat) zur Bearbeitung der Anfrage vorgeschrieben ist. Im Regel-

[63] Siehe hierzu der Beitrag zum CEF in Kapitel 8.8 und die Ausführungen in den Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht, Rn. 73 ff. jeweils zum Auskunftsanspruch unter der DSGVO.

fall dürfte eine finale Beantwortung jedoch auch bei der Polizei innerhalb weniger Wochen möglich sein. Eine Eingangsbestätigung ist zudem unverzüglich zu versenden (Art. 12 Abs. 3 JI-Richtlinie; § 15 Abs. 2 SPolDVG).

8.3.3 Reichweite der Auskunft

Hinsichtlich Art und Umfang der Auskunftserteilung entsprechen die Rechtsfolgen im Geltungsbereich der JI-Richtlinie weitgehend denen der DSGVO. Zunächst ist der antragstellenden Person mitzuteilen, ob sie betreffende personenbezogene Daten von der Polizei verarbeitet werden (Art. 14 Halbsatz 1 JI-Richtlinie; § 11 Abs. 1 S. 1 SPolDVG). Im Falle einer Verarbeitung sind zusätzliche Informationen bereitzustellen (Art. 14 Halbsatz 2 JI-Richtlinie; § 11 Abs. 1 S. 2 SPolDVG). Dazu gehören insbesondere der Zweck der Verarbeitung, die einschlägigen Rechtsgrundlagen sowie die Speicherdauer der personenbezogenen Daten.

Im Saarland wird zur Beantwortung eines Auskunftsersuchens durch die Vollzugspolizei in der Regel ein Übersichtsbogen erstellt und versandt. Dieser gibt insbesondere Aufschluss über das betroffene polizeiliche Datenverarbeitungssystem (z. B. das Vorgangsbearbeitungssystem POLADIS oder das polizeiliche Informationssystem POLIS/INPOL) und den Anlass der Speicherung, etwa das konkrete Verfahren.

Die Bereitstellung einer solchen Übersicht genügte bisher in der Regel, um den Informationsbedarf der betroffenen Personen zu decken. Fordert eine antragstellende Person nach Erhalt jedoch ergänzend detaillierte Informationen zu einzelnen Vorgängen oder explizit eine vollständige Auskunft über sämtliche personenbezogene Daten, ist die Polizei verpflichtet, diese umfassend zu gewähren.

Angesichts der besonderen Anforderungen des Sicherheitsrechts kann der Auskunftsanspruch mit sicherheitsbehördlichen Geheimhaltungsinteressen kollidieren. Die JI-Richtlinie und entsprechend auch das SPolDVG sehen deswegen die Möglichkeit

vor, eine Auskunft in bestimmten Situationen und in gewissem Umfang zu beschränken (Art. 15 JI-Richtlinie; § 11 Abs. 3 i. V. m. § 10 Abs. 2, 5 oder 6 SPolDVG). Die betroffene Person ist hierüber unverzüglich mit einer entsprechenden Begründung zu benachrichtigen. Ein zeitlicher Aufschub der Mitteilung (bis keine Gefährdung der polizeilichen Maßnahme mehr besteht) ist jedoch ebenfalls möglich.

In Fällen, in denen der betroffenen Person seitens der Polizei mit Verweis auf Sicherheitsinteressen keine Informationen zur Verfügung gestellt werden oder auf eine entsprechende Anfrage überhaupt nicht reagiert wird, kann das Auskunftsrecht auch alternativ über unsere Behörde geltend gemacht werden (sog. „indirekte Auskunft"; Art. 17 JI-Richtlinie; § 15 Abs. 6 SPolDVG). In einer solchen Situation nehmen wir in die betroffenen Datensätze Einsicht, überprüfen, ob die damit einhergehende Datenverarbeitung in zulässiger Weise erfolgt, und werden gegebenenfalls die erforderlichen datenschutzrechtlichen Maßnahmen ergreifen, um eine unzulässige Handhabung zu unterbinden.

8.3.4 Anpassung des Musterformulars zu Auskunftsersuchen gem. § 11 SPolDVG

Aufgrund der oben beschriebenen Feststellungen zu den Rahmenbedingungen für die Geltendmachung des Auskunftsrechts und für die Identifizierung des Absenders durch die Polizei, wurde von unserer Behörde im Berichtsjahr das bisher als Hilfestellung veröffentlichte Muster für die Formulierung eines Auskunftsersuchens bei der Saarländischen Polizei überarbeitet.[64] Auch der dazugehörige Begleittext auf unserer Website wurde entsprechend angepasst.

Bislang wies das Formular darauf hin, dass eine Kopie eines amtlichen Ausweisdokuments beizufügen ist. Vor dem Hintergrund,

[64] Das Muster kann auf unserer Website unter dem Menüpunkt „Themen > Polizei > Auskunftsersuchen" abgerufen werden (https://www.datenschutz.saarland.de/themen/polizei#c2672).

dass eine Identitätsprüfung auch auf andere Weise erfolgen kann, bietet der neue Vordruck nun folgende Optionen:

- Kopie eines Identitätsnachweises: Personalausweis / Reisepass
- Ich bin Ihrer Behörde bereits aus folgendem Verfahren bekannt (Aktenzeichen):
- Sonstige Anmerkung:
  Nach wie vor steht es der Polizei weiter frei, bei begründeten Zweifeln über die Identität der anfragenden Person auch gezielt weitere oder andere Informationen einzufordern. Über das Freitextfeld „Sonstige Anmerkung" kann nunmehr auch von Vornherein auf besondere Aspekte des Einzelfalls (z.B. Möglichkeit der Identifizierung auf sonstigem Wege, Existenz einer Bevollmächtigung oder Stellung des Antrags im Namen eines minderjährigen Kindes) hingewiesen werden.

Auch künftig werden wir das von uns bereitgestellte Musterformular an aktuelle Entwicklungen anpassen. So sind insbesondere weitere Konkretisierungen auf europäischer Ebene zu erwarten, etwa in Form der derzeit in Erarbeitung befindlichen Leitlinien zum Auskunftsrecht im Geltungsbereich der JI-Richtlinie durch den Europäischen Datenschutzausschuss.

8.4 Waffenrechtliche Erlaubnisverfahren

Bereits in den vergangenen Tätigkeitsberichten wurde die Notwendigkeit betont, die im Saarland verwendeten Antragsformulare zum „kleinen Waffenschein" datenschutzkonform zu gestalten. Diese Arbeiten erfolgten in Zusammenarbeit mit dem Ministerium für Inneres, Bauen und Sport (MIBS) und führten zu einem überarbeiteten Musterformular sowie angepassten Datenschutzhinweisen.[65]

[65] Siehe hierzu die Beiträge im 32. Tätigkeitsbericht (Kapitel 2.4) und im 31. Tätigkeitsbericht (Kapitel 4.2).

Auch im Berichtsjahr wurden diese Bemühungen fortgeführt und in einer Besprechung im Juni 2024 die noch offenen Fragestellungen erörtert und das weitere Vorgehen abgestimmt.

8.4.1 Musterformular „kleiner Waffenschein"

Ein zentrales Thema war das bereits mit unserer Behörde abgestimmte und finalisierte Musterformular zur Beantragung des kleinen Waffenscheins. Obwohl es den saarländischen Waffenbehörden bereits durch das MIBS hätte zur Verfügung gestellt werden können, ist dies bislang noch nicht geschehen. Zwischenzeitlich wurde im Rahmen eines IT-Projekts zur Umsetzung des Online-Zugangsgesetzes auch die Möglichkeit für eine digitale Antragstellung für den kleinen Waffenschein geschaffen, die bereits von mehreren saarländischen Kommunen genutzt wird.

Da das bisherige Beantragungsverfahren weiterhin als analoge Alternative zu der digitalen Antragstellung bestehen bleiben soll, wurde gemeinsam mit dem MIBS entschieden, einen inhaltlichen Gleichklang von Online- und Papierformularen anzustreben. Das MIBS bat deswegen im Rahmen der besagten Unterredung um einen angemessenen Zeitraum für eine Machbarkeitsprüfung.

8.4.2 Datenschutzhinweise im Kontext waffenrechtlicher Erlaubnisse

Ein weiterer Fokus lag auf der Überarbeitung der Datenschutzinformationen, die insbesondere den Antragstellern in waffenrechtlichen Erlaubnis- und Genehmigungsverfahren zur Verfügung gestellt werden. Bisher bestand das Ziel des MIBS darin, ein allgemeingültiges Dokument zu erstellen, das für alle waffenrechtlichen Erlaubnisse verwendet werden konnte. Da Datenschutzhinweise so konkret wie möglich sein sollen, um der betroffenen Person die in ihrem Fall relevanten Informationen zur Verfügung zu stellen, die rechtlichen Rahmenbedingungen der Datenverarbeitung (z.B. Umfang der Datenerhebung oder

Löschfristen) bei den unterschiedlichen waffenrechtlichen Erlaubnisformen aber teils stark variieren können, stellte sich dieses Vorhaben als schwierig dar.

Um den Anforderungen an konkrete und transparente Datenschutzhinweise gerecht zu werden, wurde die Möglichkeit geprüft, separate Datenschutzhinweise für verschiedene Erlaubnisformen zu entwickeln. Das MIBS erklärte sich bereit, zu prüfen, inwieweit Anpassungen vorgenommen werden sollen. Eine Rückmeldung hierzu ist bis zum Redaktionsschluss jedoch noch nicht erfolgt.

8.4.3 Zeitliche Grenzen der Aktenaufbewahrung

Die komplexeste Fragestellung betraf die Festlegung konkreter Löschfristen. Grundsätzlich orientiert sich die zulässige Speicherdauer personenbezogener Daten am Kriterium der Erforderlichkeit (Art. 5 Abs. 1 lit. e, Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO und § 4 Abs. 1 SDSG). Fehlt eine spezialgesetzliche Regelung, die eine weitere Nutzung und Aufbewahrung gestattet, sind Daten zu löschen, sobald sie für die Zwecke, für die sie erhoben und verarbeitet wurden, nicht mehr benötigt werden.

Vorgaben für die Aufbewahrung von „Unterlagen" (also nicht speziell nur für personenbezogene Daten) finden sich etwa in § 44a des Waffengesetzes (WaffG). Allerdings knüpft diese Vorschrift lediglich an zwei bestimmte Konstellationen an: Während § 44a S. 1 WaffG solche Daten betrifft, die zur Nachverfolgung von Besitzverhältnissen und Verkaufswegen erforderlich sind, lässt § 44a S. 2 WaffG eine Aufbewahrung von Informationen zu, „aus denen sich die Versagung einer waffenrechtlichen Erlaubnis […], einschließlich der Gründe hierfür, ergibt".

Aufbewahrungsfristen finden sich auch an anderer Stelle, wie zum Beispiel dem Waffenregistergesetz (WaffRG). § 27 Abs. 4 Nr. 2 lit. a WaffRG betrifft jedoch nur die Speicherung von Daten im nationalen Waffenregister als zentrale / übergreifende Datenbank – die Speicherung von Informationen in lokalen behördlichen Aktenbeständen wird hiermit gerade nicht reguliert.

Für alle anderen personenbezogenen Daten im waffenrechtlichen Kontext, die gerade nicht unter die vorbeschriebenen Fälle fallen, sind keine spezialgesetzlichen Vorgaben getroffen worden. Folglich sind sie allein am Maßstab der Erforderlichkeit zu bemessen (siehe oben). Bei der Bemessung von Aufbewahrungsfristen ist insbesondere das nachvollziehbare Bedürfnis einer effektiven waffenrechtlichen Aufsicht / Kontrolle zu berücksichtigen, gleichzeitig aber auch die Gefahr einer überschießenden Aufbewahrung von personenbezogenen Informationen (etwa als umfassender und lückenloser Lebenslauf einer Person) zu verhindern.

In Ermanglung spezifischer gesetzlicher Vorgaben zur Aufbewahrung waffenrechtlicher Vorgänge haben wir vorgeschlagen, sich bei der Bewertung von Löschfristen an der regelmäßigen Überprüfung waffenrechtlicher Erlaubnisse gemäß § 4 Abs. 3 WaffG zu orientieren Demnach könnte eine dreijährige Aufbewahrungsfrist für entsprechende Vorgangsakten angemessen sein, sofern keine Gründe für eine Versagung der Erlaubnis vorliegen.

Das MIBS sagte zu, sich nochmals vertieft mit der Fragestellung intern (gegebenenfalls auch unter Einbeziehung der kommunalen Stellen / Waffenbehörden) befassen zu wollen.

8.4.4 Sachstand

Trotz des erfolgten Austauschs wurde unserer Behörde seit der Besprechung im Juni 2024 kein aktualisierter Sachstand mitgeteilt. Auch eine Nachfrage im September 2024 führte lediglich zu einem ein Verweis auf andauernden Klärungsbedarf. Angesichts der datenschutzrechtlichen Defizite halten wir es für dringend geboten, dass das MIBS zeitnah zu einer abschließenden Klärung gelangt. Insbesondere das Verfahren zur Angleichung des analogen Musterformulars zum „kleinen Waffenschein“ im Saarland sollte im Jahr 2025 endgültig zum Abschluss gebracht werden.

8.5 Einsatz polizeilicher Drohnen bei Fußballspielen

Der Einsatz von Drohnen, auch bekannt als ULS (Unbemanntes Luftfahrtsystem) oder UAV (Unmanned Aerial Verhicles), ist heutzutage keine Seltenheit mehr. Dank der zunehmend vereinfachten Betriebsbedingungen finden sie nicht mehr nur im Freizeitbereich Anwendung, sondern sind auch im professionellen Umfeld immer weiter verbreitet (etwa im Mess- und Katasterwesen, in der Solarbranche, in der Landwirtschaft oder im Baugewerbe). Auch öffentliche Stellen nutzen Drohnen in zunehmendem Maße für ihre Zwecke.

Im Berichtszeitraum erreichte uns eine Beschwerde, die den polizeilichen Einsatz eines ULS im Vorfeld eines Fußballspiels im Ludwigsparkstadion in Saarbrücken betraf. Der Beschwerdeführer (ein Anhänger der Gastmannschaft) bemängelte, dass beim Einlass zu der Drittligabegegnung die Polizei mittels einer Drohne den Eingang zum Gästeblock überwacht habe, ohne dass die Besucher darüber informiert wurden. Weder vorab noch während des Spiels sei über den Einsatz der Drohne aufgeklärt worden. Selbst direkte Nachfragen bei den vor Ort eingesetzten Polizisten wären erfolglos geblieben.

Die Beschwerde warf zwei wesentliche Fragestellungen auf: Zum einen, ob sich der Einsatz der Kameradrohne durch die saarländische Polizei auf eine rechtliche Befugnis zur Videoüberwachung stützen konnte. Zum anderen, ob die Polizei den Einsatz der Drohne hinreichend bekannt (öffentlich) gemacht hat und der Einsatz damit „offen" erfolgte.

8.5.1 Rechtliche Grundlage für den polizeilichen Einsatz von Kameradrohnen

Das Saarländische Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG) sieht in § 32 SPolDVG eine Regelung vor, die „offene Bild- und Tonaufzeichnungen" durch die Vollzugspolizei gestattet. Da die Formulierung bewusst technikoffen gestaltet ist, kann auch der polizeiliche Ein-

satz von Kameradrohnen darunter subsumiert werden. Eine spezielle Ermächtigungsgrundlage für die Nutzung von ULS existiert im Saarland nicht.

Gemäß § 32 Abs. 1 S. 2 SPolDVG dürfen Bild- und Tonaufzeichnungen insbesondere bei Veranstaltungen und Ansammlungen durchgeführt werden, die ein besonderes Gefährdungsrisiko aufweisen. Das Gesetz geht in drei Fallkonstellationen von einem solchen Gefährdungsrisiko aus:

1. Wenn eine aktuelle Gefährdungsanalyse für Veranstaltungen / Ansammlungen gleicher Art und Größe die Gefahr terroristischer Anschläge ausweist.
2. Wenn aufgrund der Art und Größe der Veranstaltung / Ansammlung erfahrungsgemäß mit Gefahren für die öffentliche Sicherheit zu rechnen ist.
3. Wenn konkrete Anhaltspunkte die Begehung erheblicher Ordnungswidrigkeiten oder Straftaten nahelegen.

Insbesondere bei größeren Veranstaltungen können alle drei Tatbestandsalternativen einschlägig sein. Bei Fußballspielen dürften jedoch die unter Variante 2 zu fassenden „Gelb- und Rotspiele" im Fokus stehen, deren Risikopotential allgemein bekannt ist.

Bei Vorliegen der vorbeschriebenen Voraussetzungen darf die Vollzugspolizei „Bild- und Tonaufzeichnungen" offen anfertigen. Zwar legt der Begriff „Aufzeichnung" nahe, dass stets nur eine Kombination aus Erhebung von Bilddaten und anschließender, dauerhafter Speicherung zulässig wäre. Nach unserem Verständnis umfasst die Vorschrift jedoch auch das reine Live-Monitoring, also die Beobachtung eines Geschehens ohne Speicherung der Daten.

Im Fall der Beschwerde war das betroffene Fußballspiel von der Polizei im Vorfeld mit einer „gelben" Gefährdungseinstufung versehen worden. Die Polizei nutzte deswegen die Kameradrohne zur Fertigung von Übersichtsaufnahmen, die per Live-Bild (ohne Speicherung) in die Einsatzzentrale übertragen wurden.

Diese dienten der besseren Koordination des Einsatzes. Durch die Beobachtung der Verkehrssituation, der Fanbewegungen, des Personenaufkommens und möglicher Störer sollte ein frühzeitiges Reagieren auf Gefahren für die öffentliche Sicherheit ermöglicht werden. Unter diesen Umständen war der Einsatz der Drohne grundsätzlich rechtmäßig.

8.5.2 Videobeobachtung als „offene Maßnahme" und Transparenzpflichten

Trotzdem war die datenschutzrechtliche Zulässigkeit der polizeilichen Maßnahme im konkreten Fall in Frage zu stellen, da § 32 SPolDVG ausdrücklich nur die „offene Erhebung von Bild- und Tonaufzeichnungen" erlaubt. Offen ist eine Maßnahme jedoch nur dann, wenn sie von den betroffenen Personen auch als solche wahrgenommen werden kann. Werden Drohnen eingesetzt, so sind diese – abhängig von ihrer Flughöhe – mit bloßem Auge nur schwer erkennbar und auch akustisch nicht immer wahrnehmbar. Außerdem kann deren Zugehörigkeit zur Polizei meist nicht ohne Weiteres festgestellt werden.

Die Polizei hat bei entsprechenden Einsätzen deswegen besonderes Augenmerk auf die in § 32 Abs. 5 SPolDVG normierten Hinweispflichten zu legen, die hier nicht nur die formale Nebenpflicht zur Transparenz betreffen, sondern auch unmittelbaren Einfluss auf die materielle Rechtmäßigkeit der Maßnahme nehmen. Die Vorschrift gibt vor, dass „durch Schilder oder in sonstiger geeigneter Form" auf die Maßnahme hingewiesen werden muss. Im Beschwerdefall waren die polizeilichen Bemühungen jedoch als unzureichend zu bewerten.

So finden sich zwar am Ludwigsparkstadion bereits Hinweistafeln, die über eine polizeiliche Videoüberwachung aufklären. Sowohl das verwendete Piktogramm als auch der Hinweistext beziehen sich allerdings ausschließlich auf die im Stadion angebrachten, fest installierten Kamerasysteme. Ein Einsatz mobiler Kameradrohnen ist aus diesen Informationen für betroffene Personen nicht ersichtlich.

Zwar sind die für den Drohneneinsatz verantwortlichen Polizeibediensteten stets besonders gekennzeichnet und das eingesetzte Fahrzeug als auch die Polizeivollzugsbeamtinnen und -beamten, durch die das ULS gesteuert wird, verfügen über eine besondere Beschriftung bzw. Dienstkleidung. Zudem werden am Start- und Landepunkt der Drohne entsprechende Durchsagen getätigt. Dies ändert allerdings nichts an der Tatsache, dass für einen Großteil der betroffenen Stadionbesucher diese Datenverarbeitung meist nicht wahrnehmbar und damit nicht transparent ist. Denn Drohnen sollen aus Sicherheitsgründen nicht direkt über Personenansammlungen geflogen werden, sodass sich die eingesetzten Kräfte häufig nicht in unmittelbarer Hör- oder Sichtweite der Betroffenen befinden. So auch im Beschwerdefall, bei dem sich der Start- und Landepunkt in einer vom Stadion mehrere hundert Meter entfernten, nicht einsehbaren Seitenstraße befand.

Wegen der unzureichenden Transparenzmaßnahmen war der Drohneneinsatz nicht als „offen" im Sinne der gesetzlichen Vorschrift zu qualifizieren. Damit lag ein wichtiges Tatbestandsmerkmal der Ermächtigungsgrundlage nicht vor, weswegen die polizeiliche Maßnahme insgesamt als datenschutzrechtlich unzulässig zu bewerten war. Sowohl der Beschwerdeführer als auch das Landespolizeipräsidium wurden über diese Einschätzung in Kenntnis gesetzt.

8.5.3 Zugesicherte Verbesserungen der Transparenz seitens der Polizei

Weitere aufsichtsbehördliche Maßnahmen waren in diesem Fall nicht erforderlich. Da die Drohne ausschließlich zur Live-Beobachtung genutzt wurde, existierten keine gespeicherten Aufnahmen des betreffenden Tages, deren Löschung hätte angeordnet werden müssen. Zudem hatte die Polizei in ihrer Stellungnahme frühzeitig Bereitschaft signalisiert, den datenschutzrechtlichen Bedenken künftig durch verbesserte Transparenzmaßnahmen Rechnung zu tragen.

Hierzu zählen unter anderem neue Hinweisschilder, die im Umfeld von Veranstaltungen, insbesondere an Zu- und Abgangsbereichen, angebracht werden sollen. Die uns vorgelegten Muster weisen unter Ausweisung des voraussichtlichen Einsatzgebiets ein Drohnenpiktogramm auf und machen damit ausdrücklich auf den Einsatz mobiler ULS aufmerksam. Zusätzlich sollen die eingesetzten Kameradrohnen künftig mit einer gut sichtbaren Polizei-Folierung versehen werden.

Bei sicherheitsrelevanten Fußballbegegnungen ist außerdem geplant, digitale Leuchttafeln auf Lautsprecherfahrzeugen einzusetzen, um die Überwachungsmaßnahmen auch in größeren Menschenmengen besser erkennbar zu machen. Darüber hinaus wurde ein verbessertes Informationsmanagement im Vorfeld von Veranstaltungen angekündigt. Künftig sollen planbare Drohneneinsätze zuvor durch Pressemitteilungen und Beiträge in sozialen Medien kommuniziert werden.

8.6 Kommunale Hundebestandsaufnahme

Bereits in zurückliegenden Tätigkeitsberichten befasste sich unsere Behörde ausführlich mit der datenschutzrechtlichen Bewertung von flächendeckenden kommunalen Hundebestandsaufnahmen (Hundebestandsermittlungen).[66]

Eine solche Form der Datenerhebung, bei welcher Mitarbeiter eines externen privaten Dienstleisters die Einwohnerinnen und Einwohner in der Regel im häuslichen Umfeld aufsuchen und um Auskunft bitten, ob in dem Haushalt ein Hund gehalten wird, erachteten wir zum damaligen Zeitpunkt als datenschutzrechtlich unzulässig. Dies war insbesondere auf eine fehlende kommunale Satzungskompetenz für diese Art der Vor-Ort-Befragung sowie die fehlende Befugnis der Überantwortung einer steuerrechtlichen (abgabenrechtlichen) Aufgabe auf den privatrechtlichen Bereich zurückzuführen.[67]

[66] Vgl. 18. Tätigkeitsbericht 1999/2000, S. 102; 27. Tätigkeitsbericht 2017/2018, S. 54 ff.
[67] 27. Tätigkeitsbericht, S. 55 f.

Das Kommunalabgabengesetz hat zwischenzeitlich Änderungen erfahren, durch welche die Möglichkeit der Durchführung einer Hundebestandsaufnahme den Städten und Gemeinde erstmals explizit eröffnet wird und zwar auch und gerade in Form einer Beauftragung privater Dienstleister.

Auch nach dieser Gesetzesnovellierung besteht indes weiterhin keine Befugnis einer Vor-Ort-Befragung an der Haustür bzw. im näheren häuslichen Umfeld. Dies vor allem, wenn hierfür kein konkreter Anlass besteht, etwa in Form des Verdachts einer nicht gemeldeten Hundehaltung.

8.6.1 Möglichkeit der Beauftragung privater Dritter mit der Durchführung der Hundebestandsaufnahme (§ 2 Abs. 3 KAG)

Der im Jahr 2018 in das Kommunalabgabengesetz neu eingefügte § 2 Abs. 3 S. 1 KAG ermöglicht nunmehr grundsätzlich eine Beauftragung privater Dritter mit Aufgaben des kommunalabgabenrechtlichen Ermittlungsverfahrens. Dessen Vorgängernorm (§ 2 Abs. 3 S. 1 KAG (a.F.)) stellte hierfür noch ein rechtliches Hindernis dar. Hiernach konnte in den kommunalen Abgabensatzungen zwar bestimmt werden, „(...) *dass die Festsetzung und die Erhebung von Abgaben von einer damit beauftragten Stelle außerhalb der Verwaltung vorgenommen* (wird)". Eine Beauftragung privater Stellen im Rahmen des vorgelagerten steuerlichen Ermittungsverfahrens, genauer der Ermittlung von Steuersachverhalten und deren Grundlagen, schied jedoch von vornherein aus.

Problematisch erweist sich an der Neuregelung der Satz 2 des § 2 Abs. 3 KAG (n.F.), welcher in seinem Aussagegehalt nicht ganz verständlich ist. Er bestimmt, dass,

> *„Die Stelle (außerhalb der Verwaltung) nur beauftragt werden (darf), wenn die ordnungsgemäße Erledigung und Prüfung nach den für die Gemeinden und Gemeindeverbände geltenden Vorschriften gewährleistet ist und diese Stelle in engen rechtlichen oder wirtschaftlichen Beziehungen zum*

Gegenstand der Abgabenerhebung oder zu einem Sachverhalt steht, an den der Abgabengegenstand oder die Abgabenpflicht anknüpft."

Auf den ersten Blick scheint die Vorschrift als Einschränkung recht ausdifferenziert und, zumindest vordergründig, präzise formuliert. Bei näherer Befassung bleibt jedoch weitgehend unklar, welche Stellen – insbesondere in Bezug auf die örtlichen Verbrauch- und Aufwandsteuern – der Gesetzgeber hier genau im Blick hatte. Die Gesetzesmaterialien schweigen hierzu leider. Eine formale Einschränkung, etwa auf die rechtsdienstleistenden oder steuerberatenden Berufe ist unseres Erachtens hiermit jedenfalls nicht gewollt. Wir sehen in § 2 Abs. 3 S. 2 KAG (n.F.) letztlich daher die Kodifizierung eines allgemeinen gesteigerten Sorgfalts- und Zuverlässigkeitsmaßstabes. Es soll hiernach nicht jedes beliebige Dienstleistungsunternehmen als Verwaltungshelfer von der Kommune mit einer (steuer-) abgabenrelevanten Hilfstätigkeit betraut werden, sondern nur solche, welche die notwendigen Fach- und Rechtsexpertise in diesem Bereich aufweisen. Hier kommt der Kommune ein Beurteilungsspielraum zu, im Rahmen dessen es ihr obliegt, die Eignung und Zuverlässigkeit des ins Auge gefassten Dienstleisters zu eruieren und im Lichte von § 2 Abs. 3 S. 2 KAG (n.F.) rechtlich zu bewerten.

8.6.2 § 2 Abs. 3 KAG als Datenverarbeitung i.S.e. Auftragsverarbeitung

Wird eine externe Stelle mit einer Ermittlungshandlung in Form einer Hundebestandsaufnahme beauftragt, so stellt dies aus datenschutzrechtlicher Sicht eine Auftragsverarbeitung i. S. d. Art. 4 Nr. 8, 28 DSGVO dar. Die Frage, ob dem Auftragnehmer eine Verarbeitungstätigkeit hierbei womöglich nur im Umfange einer Hilfs- und Unterstützungsfunktion zugewiesen ist, oder selbige aufgrund eines eigenen Entscheidungsspielraums darüber hinausgeht, ist nicht entscheidend.

Die Abgrenzung zwischen Verantwortlichkeit und Auftragsverarbeitung erfolgt anhand der Legaldefinition des Art. 4 Nr. 7 DSGVO. Hiernach ist Verantwortlicher, wer „(...) *über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet*". Ein Verantwortlicher legt die Zwecke und Mittel der Verarbeitung fest, wenn er über das „Warum" und das „Wie" der Verarbeitung bestimmt. Er muss sowohl über die Zwecke als auch über die Mittel der Verarbeitung entscheiden. Nicht maßgeblich ist demgegenüber der tatsächliche, faktische Zugang zu den verarbeiteten Daten oder der Umfang der Datenverarbeitung. Die Kommune determiniert in ihrer jeweiligen Abgabensatzung den Zweck der Datenverarbeitung, welcher in einer Erfassung von Hundehaltungen im Gemeindegebiet liegt. Sie gibt auch die wesentlichen Mittel dieser Verarbeitung vor, indem sie den Auftragnehmer anweist, die nötigen Informationen in Form einer persönlichen Befragung vor Ort an sämtlichen Privathaushalten zu erheben und in entsprechender Form aufzubereiten. Sie ist es demnach, mit deren Wissen und Wollen die Verarbeitung steht und fällt.[68]

8.6.3 Freiwilligkeit einer Vor-Ort-Befragung

Besteht demnach grundsätzlich die Möglichkeit einer Hundebestandsaufnahme (Hundebestandsermittlung) durch einen behördenexternen privaten Verwaltungshelfer in Gestalt einer Auftragsverarbeitung, so müssen in diesem Rahmen gleichwohl die Anforderungen des § 12 Abs. 5 KAG erfüllt sein.

Die Vorschrift des § 12 Abs. 5 KAG spricht hier zunächst in allgemeiner Form von „Befragungen". Gestattet sind demnach Befragungen sämtlicher Art, d. h. in mündlicher, schriftlicher oder elektronischer Form. Entscheidend ist nach dem Wortlaut des Gesetzes jedoch die „*freiwillige Teilnahme*" an einer solchen Befragung.

[68] Zu den weiteren Einzelheiten der diesbezüglichen Abgrenzung siehe EDPB, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, Version 2.0).

Aufgrund des Umstands, dass eine derartige Befragung mit einer u. U. weitreichenden Erhebung personenbezogener Daten verbunden ist, muss das Tatbestandsmerkmal der Freiwilligkeit in europarechtskonformer Art und Weise, d. h. im Lichte der Bestimmungen der DSGVO ausgelegt werden. Aus hiesiger Sicht unterscheidet es sich dabei in keiner Weise von der Freiwilligkeit, wie sie die Einwilligung nach den Art. 4 Nr. 11, 7 DSGVO voraussetzt. Die betroffene Person muss demnach in hinreichender Form im Vorhinein über die Datenverarbeitung und deren Umstände informiert werden (vgl. Art. 13 DSGVO) und diese sodann aus freien Stücken befürworten, d. h. nicht bloß erdulden oder über sich ergehen lassen.

Dass diese Freiwilligkeit bei einer Befragung im häuslichen Umfeld der Betroffenen in der Regel nicht gegeben sein dürfte, wurde von uns in unserem 27. Tätigkeitsbericht der Jahre 2017/2018 bereits umfassend dargelegt (vgl. Seite 54 ff.). Das Instrument einer freiwilligen Befragung ist dem deutschen Steuerrecht auch grundsätzlich fremd. Erfüllt eine Person einen steuerlichen bzw. einen sonstigen Abgabentatbestand, hat sie sich in aller Regel von sich aus mit allen zur Festsetzung notwendigen Informationen entsprechend zu erklären. Zur effektiven Rechtsdurchsetzung bzw. der Gewährleistung einer gleichmäßigen Steuererhebung stehen der Steuerbehörde nach § 93 AO weitreichende Ermittlungs- und Auskunftsrechte zu. Diese Rechtsgrundlagen beinhalten sodann auch die hierfür erforderlichen Datenverarbeitungen, u. U. in Form einer persönlichen Auskunftsheranziehung des Steuerpflichtigen oder Dritter. Bestehen hinreichend konkrete Verdachtsmomente, dass steuerpflichtige Personen der Meldung eines Hundes nicht nachgekommen sind, so können die erforderlichen Informationen auf Grundlage von § 93 AO demnach unproblematisch erlangt werden. Wann dessen tatbestandliche Voraussetzungen vorliegen, scheint wiederum durch die Rechtsprechung des Bundesfinanzhofs hinreichend geklärt.[69]

[69] So etwa BFH, Urt. v. 23.10.1990 – VIII R 1/86.

Außerhalb des § 93 AO erscheint uns eine freiwillige Befragung vor Ort aufgrund der den Einzelnen möglicherweise überrumpelnden „Haustürsituation“ sowie generell aufgrund des gerade in Steuerangelegenheiten bestehenden Subordinationsverhältnisses zwischen Bürger und Behörde indes ausgeschlossen. § 12 Abs. 5 KAG ist aus hiesiger Sicht demnach als Annex zu § 93 AO zu begreifen, welcher es der Kommune zwar gestattet, die Bürgerinnen und Bürger daran zu erinnern – wenn man so will auch zu ermahnen – eine Hundehaltung auch tatsächlich zu melden. Es zeigt sich hierbei jedoch nicht als erforderlich, selbiges persönlich am Wohnort der betroffenen Personen zu tun. Dies kann ebenso gut in Form eines elektronischen Meldeformulars oder mittels Briefeinwurf in den Haushalten geschehen.

8.7 Datenschutz bei Wahlen

Regelmäßig treten in der Vorbereitungs- und Durchführungsphase von Wahlen auf europäischer, nationaler, landes- oder kommunaler Ebene spezifische datenschutzrechtliche Fragestellungen auf. Diese betreffen sowohl die Verarbeitung personenbezogener Daten der Wahlberechtigten als auch der Wahlhelferinnen und Wahlhelfer. Da diesbezügliche Fragen zum Datenschutz auch im Rahmen der zurückliegenden Bundestagswahl wieder thematisiert wurden, wollen wir aus unserer Sicht wichtige Aspekte des Datenschutzes in diesem Bereich nochmals ins Gedächtnis rufen:

8.7.1 Datenverarbeitung auf Wahlbenachrichtigungskarten

Die amtlichen Wahlbenachrichtigungskarten informieren die Wählerinnen und Wähler über den Wahltermin, den Wahlbezirk und das zuständige Wahllokal. Dabei enthalten die Karten in der Regel Name und Anschrift der Wahlberechtigten. Für den Fall einer offenen Versendung der Wahlbenachrichtigungskarten (in Form einer unverschlossenen Postkarte) gelten besondere Anforderungen an die Minimierung der mitgeteilten Daten.

Aus datenschutzrechtlicher Sicht ist das Aufdrucken des Geburtsdatums auf Wahlbenachrichtigungskarten unzulässig. Dies ergibt sich aus den Regelungen der jeweiligen Wahlordnungen. Für die Kommunalwahl findet sich in § 7 Kommunalwahlordnung (KWO) eine explizite Regelung, was Bestandteil einer diesbezüglichen Wahlbenachrichtigung (Wahlbenachrichtigungskarte) ist (vgl. Muster der Anlage 2 zur KWO). Für die Europa-, die Bundestags- sowie die Landtagswahl finden sich die betreffenden Regelungen in § 19 Abs. 1 der Bundeswahlordnung (BWO) i. V. m. § 4 Europawahlgesetz (EuWG) sowie § 13 Abs. 1 S. 2 Landeswahlordnung (LWO). Selbige Regelungen erwähnen das Geburtsdatum nicht. Zwar handelt es sich bei den Normen um „Soll-Vorschriften", welche in erster Linie den Mindestinhalt einer diesbezüglichen Wahlbenachrichtigung regeln. Dies bedeutet jedoch nicht, dass die Wahlbenachrichtigungskarte ohne Weiteres mit zusätzlichen Daten – wie dem Geburtsdatum – angereichert werden dürfte; dies erst recht, da es sich um eine offene Versendung ohne Briefumschlag handelt.

Die Informationen auf den Wahlbenachrichtigungskarten müssen sich auf das Notwendige beschränken. In diesem Zusammenhang liegt kein hinreichender Zweck vor, welchen das Aufdrucken des Geburtsdatums zusätzlich erfüllt. Vor- und Zuname sowie die Anschrift des Wahlberechtigten genügen vielmehr für sich genommen bereits, die erforderlichen Informationen hinreichend sicher zu adressieren.

8.7.2 Bekanntgabe von Wahlvorschlägen

Als Wahlvorschläge bezeichnet man die zu einer Wahl aufgestellten Bewerberinnen und Bewerber.

Bei der Wahl zum Deutschen Bundestag sind dies die Kreiswahlvorschläge nach den §§ 20 ff. BWG, mit welchen sich die Bewerberinnen und Bewerber in den jeweiligen Wahlkreisen zur Wahl stellen. Inhalt und Form der Kreiswahlvorschläge regelt § 34 BWO, woraus sich zugleich der Umfang der Verarbeitung von Bewerberdaten ergibt. Nach dessen Absatz 1, Satz 2, Nummer 2

muss der Kreiswahlvorschlag „*den Familiennamen, den Vornamen, den Beruf oder Stand, das Geburtsdatum, den Geburtsort und die Anschrift* (Hauptwohnung) *des Bewerbers*" enthalten. Es handelt sich folglich um eine sehr weitreichende Offenlegung von Identitätsmerkmalen einer Person, welche mit der Angabe der Wohnanschrift zudem durchaus sensiblen Inhalt aufweist.

Im Rahmen der gesetzlich angeordneten öffentlichen Bekanntmachung der Kreiswahlvorschläge finden sich indes datenschutzrechtliche Schutzbestimmungen, welche die mit der Veröffentlichung verbundenen Eingriffe in die datenschutzrechtlichen Positionen der Bewerberinnen und Bewerber abmildern. So enthält die durch den Kreiswahlleiter vorzunehmende Veröffentlichung der Wahlvorschläge gemäß § 38 S. 3 BWO zwar grundsätzlich die vorgenannten Angaben, „*statt des Geburtsdatums ist jedoch jeweils nur das Geburtsjahr und statt der Anschrift nur der Wohnort* (Ort der Hauptwohnung) *des Bewerbers anzugeben*". Für die Wahl zum Saarländischen Landtag findet sich die entsprechende Parallelnorm in § 29 Abs. 1 S. 1 LWO.

Zu beachten ist, dass im Jahr 2023 nunmehr auch für die Kommunalwahlen eine inhaltsgleiche datenschutzrechtliche Änderung eingeführt wurde, welche die öffentliche Bekanntmachung der Wahlvorschläge betrifft und die eine Balance zwischen demokratischer Transparenz und individuellem Datenschutz gewährleisten soll.

Auch die Wahlvorschläge im Rahmen einer Kommunalwahl sind nach § 30 Abs. 4 S. 2 KWG öffentlich bekannt zu geben. Gemäß § 24 Abs. 5 KWG beinhalten sie grundsätzlich auch „*den Familiennamen, den Vornamen, den Beruf, das Geburtsdatum, den Wohnort und Wohnung*" der Bewerberin/des Bewerbers. Gemäß § 25 Abs. 1 Kommunalwahlordnung (KWO) dürfen nunmehr indes auch in diesem Bereich nur das Geburtsjahr (statt des Geburtsdatums) und lediglich der Wohnort (statt der vollständigen Anschrift) veröffentlicht werden.

8.7.3 Datenschutz für Wahlhelferinnen und Wahlhelfer

Ehrenamtlich tätige Wahlhelferinnen und Wahlhelfer spielen eine unverzichtbare Rolle bei der Organisation und Durchführung von Wahlen. Personenbezogene Daten von Wahlhelferinnen und Wahlhelfern werden dabei insbesondere für administrative Zwecke verarbeitet.

Im Berichtszeitraum wurden wir mit der Frage befasst, unter welchen Umständen die Weitergabe von Namen und Anschriften von Landesbeamten durch die Zentrale Besoldungs- und Versorgungsstelle des Landesamtes für Zentrale Dienste an die Kommunen zulässig sei, um bei Vorliegen eines entsprechenden Bedarfs diese als Wahlhelfer verpflichten zu können.

Spezielle Regelungen hierzu in den einzelnen Wahlgesetzen finden sich in § 9 Abs. 5 BWG, § 5 Abs. 8 LWG sowie § 5 Abs. 6 KWG. Hiernach sind zur Bildung von Wahlorganen auf Ersuchen der Gemeindebehörden (Gemeindewahlleitung) und zur Sicherstellung der Wahldurchführung die Behörden des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, der Länder, der Gemeinden der Gemeindeverbände sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts verpflichtet, aus dem Kreis ihrer Bediensteten unter Angabe von Name, Vorname, Geburtsdatum und Anschrift zum Zweck der Berufung als Mitglieder der Wahlvorstände Personen zu benennen, die im Gebiet der ersuchenden Gemeinde wohnen. Die ersuchte Stelle hat den Betroffenen dabei über die übermittelten Daten und den Empfänger zu benachrichtigen.

Ein Widerspruchsrecht gegen die Datenverarbeitung (Datenübermittlung) steht den betroffenen Bediensteten, im Gegensatz zu allgemein wahlberechtigten Personen im Falle einer Datenverarbeitung zwecks Bildung von Wahlorganen, nicht zu (vgl. § 9 Abs. 4 BWG, § 5 Abs. 7 LWG, § 5 Abs. 5 KWG).

8.8 Koordinierte Prüfung zur Umsetzung des Auskunftsrechts (CEF 2024)

Im Jahr 2024 beteiligte sich das Unabhängige Datenschutzzentrum Saarland zusammen mit 27 weiteren europäischen Datenschutzaufsichtsbehörden an der europaweiten Initiative des Europäischen Datenschutzausschusses (EDSA) zur Überprüfung des Rechts auf Auskunft nach Artikel 15 DSGVO. Diese Maßnahme, die im Rahmen des sog. Coordinated Enforcement Framework (CEF) erfolgte, dient dazu, die Umsetzung zentraler Regelungen der DSGVO in verschiedenen Organisationen innerhalb der Europäischen Union zu analysieren und zu verbessern.[70] Ziel der letztjährigen Maßnahme war es, einen umfassenden Einblick in die Bearbeitung von an Unternehmen gerichteten Auskunftsersuchen zu gewinnen, die Qualität der Antworten zu bewerten und etwaige systemische Schwächen in der Umsetzung des Rechts auf Auskunft zu identifizieren.

Das Auskunftsrecht ist ein wesentlicher Bestandteil des Datenschutzes und gibt Bürgerinnen und Bürgern die Möglichkeit nachzuvollziehen, wie ihre personenbezogenen Daten von Unternehmen und Behörden verarbeitet werden. Es dient außerdem oft als Grundlage, um weitere Betroffenenrechte der DSGVO, wie das Recht auf Löschung oder Berichtigung, geltend zu machen.

Eine wichtige Quelle, um einen Überblick über die Anforderungen des Auskunftsrechts nach Art. 15 DSGVO zu bekommen, sind die vom EDSA hierzu veröffentlichten Leitlinien[71]. In den Leitlinien finden sich zu den einzelnen Anforderungen des Auskunftsrechts detaillierte Ausführungen mit Praxisbeispielen. Insbesondere der Umfang dessen, was unter den Begriff der zu

[70] https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-coordinated-enforcement-framework-under-regulation_de
[71] https://www.edpb.europa.eu/system/files/2024-04/edpb_guidelines_202201_data_subject_rights_access_v2_de.pdf

beauskunftenden personenbezogenen Daten fällt, wird dort sehr ausführlich erläutert.

8.8.1 Untersuchungsschwerpunkt im Saarland

Im Saarland konzentrierte sich die Prüfung auf Energieversorgungsunternehmen, die wegen ihrer zentralen Rolle bei der Verarbeitung von Verbraucherdaten im öffentlichen Bereich ausgewählt wurden. Insgesamt haben wir im Rahmen unserer Prüfung 22 Energieversorger angeschrieben und den Verantwortlichen konkrete Fragen zur Kenntnis und Umsetzung der Leitlinie des EDSA gestellt.

Den zur Prüfung ausgewählten Unternehmen wurde ein Fragebogen übersandt, der die prozesshafte Umsetzung des Rechts auf Auskunft in der Praxis zum Gegenstand hatte.

Hierbei wurden folgende Feststellungen getroffen:

- **Dokumentation und prozessbezogene Fragen**

  Der Fokus der Fragen lag hier auf zwei wesentlichen Punkten. Zunächst wurde geprüft, wie die Verantwortlichen sicherstellen, dass die Daten, die zur Beauskunftung der Anfragen notwendig sind, mit Blick auf die Grundsätze des Art. 5 DSGVO nur zum festgelegten Zweck und nur von bestimmten Personenkreisen eingesehen werden können. Die Verantwortlichen sollten hier, beispielsweise durch Darstellung eines Rechte- und Rollenkonzepts und einer Dokumentation des Auskunftsprozesses darlegen, dass sie sich der Grundsätze der Datenverarbeitung bewusst sind und diese umsetzen. Weiterhin sollte dargelegt werden, nach welchen Grundsätzen Prozesse eingeführt und umgesetzt werden, insbesondere in Bezug auf Löschfristen.

  Nahezu alle Befragten konnten umfängliche Angaben zu ihrem Dokumentationsprozess und dem Umgang mit Anträgen machen. Entsprechende Vorkehrungen

fehlten insbesondere dort, wo bisher kaum Anträge eingegangen sind. Auch die Rückmeldung zu Löschfristen erfolgte in den überwiegenden Fälle unter Nennung einer gesetzlichen Grundlage und unter Angabe einer konkreten Frist. Nur in zwei Fällen erfolgte lediglich ein allgemeiner Verweis auf gesetzliche Fristen, ohne diese auch zu benennen. Eine lediglich abstrakte Angabe von Lösch- bzw. Aufbewahrungsfristen ist hingegen nicht ausreichend, da für die Betroffenen aufgrund der Angabe erkennbar sein muss, wie lange die sie betreffenden Daten noch gespeichert werden.[72]

- **Umsetzung allgemeiner Anforderungen aus Art. 12 DSGVO**

  In diesem Teil wurden unterschiedliche Themen behandelt. Zunächst sollte dargelegt werden, ob spezielle Kommunikationskanäle für Auskunftsersuchen bereitgestellt werden und wie das Vorgehen der Verantwortlichen ist, wenn Anfragen über andere Kanäle eingehen. Zudem wurde abgefragt, ob bestimmte Anforderungen an die Form des Antrags gestellt werden und die Beantwortung von der Einhaltung der Form abhängig gemacht wird. Auch wie die Einhaltung der Monatsfrist gemäß Art. 12 Abs. 3 DSGVO sichergestellt wird und welche Vorkehrungen zur Identifizierung und Authentifizierung des Antragstellers getroffen wurden, sollte dargestellt werden.

  Die Rückmeldungen der Verantwortlichen lassen hier zum Großteil eine gute Umsetzung der Anforderungen in der Praxis erkennen. In der Regel stellen die Verantwortlichen geeignete Kanäle zum Eingang von Anfragen zur Verfügung, machen die Nutzung dieser Eingangskanäle aber nicht zur Bedingung einer Bearbei-

[72] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn. 118.

tung. Der EDSA betont hierzu, dass es Aufgabe der Verantwortlichen ist, den Eingang und die Weiterleitung sicherzustellen.[73] Ein anderes Bild ergab sich bei der Frage, ob die Bearbeitung von der Einhaltung einer bestimmten Form abhängig gemacht wird. Hier gaben sechs der befragten Unternehmen an, dass sie Anträge nur unter Einhaltung der von ihnen vorgesehenen Formvorgaben behandeln. So erfolgte bei diesen beispielsweise keine Beauskunftung, wenn der Antrag über einen anderen als den vorgegebenen Kanal gestellt wurde (z.B. E-Mail statt Formular), der Antrag nicht schriftlich gestellt wurde oder wenn der Antrag ohne vorgegebene Identifikationsmittel (z.B. Kopie des Personalausweises, Kundenummer etc.) gestellt wurde.

Die Leitlinie des EDSA hebt hervor, dass die DSGVO keine Anforderungen an die Form des Antrags stellt und daher in der Regel auch eine E-Mail ausreichend ist. Insofern ist insbesondere mit Blick auf die Berücksichtigung besonderer Bedürfnisse (wie etwa einer Sehbeeinträchtigung) klarzustellen, dass auch mündliche Anfragen grundsätzlich zulässig sind.

Etwas anderes kann sich dort ergeben, wo aufgrund der gewählten Form Zweifel an der Identität der Betroffenen bestehen. Bei Zweifeln an der Identität des Betroffenen ist es grundsätzlich die Aufgabe der Verantwortlichen im Einzelfall abzuwägen, welche weiteren Informationen zur Identifikation oder Authentifikation erforderlich sind, ohne gleichzeitig zu hohe Hürden für die Ausübung des Auskunftsrechts aufzustellen. Welche Maßnahmen hier im Einzelnen ergriffen werden, hängt stark von der Beziehung zwischen dem Verantwortlichen und dem Betroffenen ab und muss sich zudem am Grundsatz der Verhältnismäßigkeit und der Datenmini-

[73] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn. 52 ff.

mierung orientieren. Zu betonen ist dabei, dass die Kopie eines Ausweisdokuments *in der Regel* kein geeignetes Mittel zur Authentifizierung darstellt, weil sie ein Risiko für die Sicherheit personenbezogener Daten darstellt und zu einer unbefugten oder unrechtmäßigen Verarbeitung führen kann und daher als unangemessen betrachtet werden sollte. Etwas anderes kann dort gelten, wo verantwortliche Stellen besondere Kategorien personenbezogener Daten verarbeiten oder eine Datenverarbeitung vornehmen, die ein Risiko für die betroffene Person darstellen kann. Weniger invasive Maßnahmen zur Identitätsfeststellung stellen z.B. Textnachricht mit Bestätigungslinks, Sicherheitsfragen oder Bestätigungscodes an zuvor im ursprünglichen Authentifizierungsprozess hinterlegte E-Mail-Adressen oder Telefonnummern dar. Auch wenn das Auskunftsrecht durch Dritte ausgeübt wird, sollten die bereits aufgeführten Erwägungen zu Identifikation/Authentifikation und entsprechende Verhältnismäßigkeitsprüfungen angestellt werden.[74]

Letztlich konnten bei den befragten Unternehmen auch keine gravierenden Mängel bei der Umsetzung und Einhaltung der Bearbeitungsfrist nach Art. 12 Abs. 3 DSGVO festgestellt werden. Die Verantwortlichen haben in aller Regel Prozesse etabliert, um die Anfragen zügig an die intern zuständige Stelle weiterzuleiten und somit fristgerecht zu beantworten. Keiner der Befragten musste nach eigenen Angaben im relevanten Zeitraum 2023 die Bearbeitungsfrist verlängern. Eine solche Verlängerung ist eingeschränkt unter den Voraussetzungen des Art. 12 Abs. 3 DSGVO möglich, sollte aber nur in seltenen Fällen genutzt werden. Verantwortliche, die häufig auf eine Fristverlängerung zurückgreifen müssen, sollten

[74] Zur Identifizierung, Authentifizierung der Verhältnismäßigkeitsprüfung siehe Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn 58-79.

die internen Prozesse optimieren. Insbesondere betont der EDSA in seiner Leitlinie, dass weder ein großer Aufwand bei der Beantwortung, noch eine Vielzahl von Anträgen bei großen Unternehmen das Merkmal der „Komplexität" in Art. 12 Abs. 3 DSGVO erfüllen.[75]

- **Inhalt von Auskunftsanträgen und deren Beantwortung**

  Weiterhin wurde der Inhalt und die Beantwortung der Anträge, insbesondere die Art der Bereitstellung der zu beauskunftenden Daten und das Recht auf Kopie behandelt. Die Fragen befassten sich beispielsweise damit, wie die Verantwortlichen den Umfang der zu betrachtenden Daten bestimmen und ob die Bereitstellung von Daten in einem mehrstufigen Konzept („layered approach") bekannt ist. Zudem wurden Fragen zur Bereitstellung der Informationen gemäß Art. 15 Abs. 1 lit.a – h), Art. 15 Abs. 2 DSGVO und Sonderformen der Verarbeitung, wie Bilder oder Videos und der Bereitstellung von Kopien gestellt.

  Der Umfang dessen was zu beauskunften ist, ergibt sich aus Art. 4 Nr. 1 DSGVO. Die Verantwortlichen können sich hier mithilfe des Verzeichnisses der Verarbeitungstätigkeiten einen besseren Überblick über mögliche relevante Verarbeitungsvorgänge verschaffen. Sofern pseudonymisierte Daten verarbeitet werden, müssen auch diese beauskunftet werden, da es sich dabei, im Gegensatz zu anonymisierten Daten, ebenfalls um personenbezogene Daten handelt.[76] Nur wenige der Verantwortlichen gaben an, pseudonymisierte Daten zu verarbeiten, diejenigen waren sich allerdings bewusst,

[75] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn 164.
[76] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn 45.

dass diese ebenfalls Teil der Auskunft sein müssen. Probleme hatten die Verantwortlichen allerdings bei der Bestimmung des Referenzzeitpunkts für die Beauskunftung. Entscheidend ist hier der Zeitpunkt, zu dem der Verantwortliche die Anfrage erhält. Dies ist besonders dort von Bedeutung, wo aufgrund kurzer Löschfristen Daten möglicherweise nicht mehr zur Verfügung stehen, wenn die Beantwortung z.B. die volle Frist in Anspruch nimmt. Es ist daher Aufgabe der Verantwortlichen für diese Fälle Vorsorge zu treffen und entsprechende Prozesse bereitzuhalten, die den Verlust der Daten, welche Teil des Auskunftsantrags sind, verhindern.[77] Hier gab mehr als die Hälfte der Befragten an, dass sie für diese Fälle keine Maßnahmen getroffen haben. Das gleiche Bild ergab sich bezüglich des Referenzzeitpunkts. Auch hier gab mehr als die Hälfte der Verantwortlichen an, nicht den Zeitpunkt der Antragstellung zu beauskunften.

Art. 12 DSGVO betont in Absatz 2, dass es Aufgabe der Verantwortlichen ist, die Ausübung des Auskunftsrechts zu erleichtern. Eine Möglichkeit kann sein, die Betroffenen um Präzisierung ihrer Angaben zu bitten, wenn große Mengen von personenbezogenen Daten verarbeitet werden, die schnell unübersichtlich für den Betroffenen werden können. Es ist dabei allerdings unerlässlich, dass der Verantwortliche im Rahmen einer Vorprüfung festgestellt hat, dass tatsächlich große Datenmengen verarbeitet werden, denn die Bitte um Präzisierung darf in keinem Fall zu einer faktischen Einschränkung der Rechteausübung führen. Ein weiterer Ansatz kann die Bereitstellung der Daten in einem mehrstufigen Konzept („layered approach") sein. Hierbei übermittelt der Verantwortliche die Daten unter bestimmten Voraussetzungen in mehreren Ebenen. Die Modalitäten

[77] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn. 37 ff.

und Voraussetzungen eines solchen Ansatzes erläutert der EDSA im Detail in seiner Leitlinie.[78]

Weiterhin ist zu betonen, dass bei der Bereitstellung der Informationen gemäß Art. 15 Abs. 1 lit. a – h), Art. 15 Abs. 2 DSGVO, diese konkret auf die betroffene Person und den spezifischen Auskunftsantrag zugeschnittene sind. Ein Verweis auf allgemeine Datenschutzrichtlinien ist insofern in aller Regel nicht ausreichend.[79] Auch in Bezug auf die Darlegung der Speicherdauer nach Art. 5 Abs. 1 lit. d DSGVO sind die Verantwortlichen verpflichtet, die Angaben möglichst konkret zu machen indem z.B. entweder das Löschdatum oder das Ereignis, das die Löschfrist auslöst mitgeteilt wird. Die Betroffenen müssen anhand der Angaben in der Lage sein, die Speicherdauer zu ermitteln. Wie bereits oben erläutert, sind Angaben wie „Entsprechend der gesetzlichen Aufbewahrungsfrist" nicht ausreichend.[80]

Das Recht, eine Kopie zu erhalten, beinhaltet nicht notwendigerweise auch ein Recht auf Originaldokumente, es sei denn, diese Dokumente sind erforderlich, um die Verarbeitung zu verstehen und deren Rechtmäßigkeit zu überprüfen.[81] Verantwortliche können aufgrund der Umstände entscheiden, ob die Kopie z.B. per E-Mail oder auf dem Postweg zur Verfügung stellt. Wurde der Antrag elektronisch gestellt, sind die Informationen gem. Art. 15 Abs. 3 DSGVO in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern die betroffene Person keine andere Art der Zurverfügungstel-

[78] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn. 143 ff.
[79] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn. 113.
[80] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn. 118.
[81] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn. 23 und 152; EuGH, Urteil vom 4. Mai 2023, C-487/21.

lung wünscht. Die Auswertung der Antworten der Energieversorger ließ hier ein sehr gemischtes Bild erkennen. Während ein großer Teil der Verantwortlichen die Modalitäten kennt und entsprechend handelt, auch in Bezug auf die Ansprüche an die Verständlichkeit der überlassenen Dokumente und besondere Anforderungen der Betroffenen, lassen einige Verantwortliche ein nur moderates Verständnis für die Ausgestaltung des Anspruchs erkennen. So gaben einige der Verantwortlich an, neben der Überlassung einer Kopie nach Art. 15 Abs. 3 DSGVO grundsätzlich keine weitere Möglichkeit des Zugangs zur Verfügung zu stellen. Der EDSA weist in diesem Zusammenhang darauf hin, dass etwa die Einsichtnahme vor Ort, z.B. bei der Verarbeitung großer Mengen nicht digitalisierter Daten, eine anfängliche Maßnahme sein kann, um weitergehend zu entscheiden, welche Daten wirklich relevant sind für die Erfüllung des Auskunftsersuchens.[82] Letztlich bleibt festzuhalten, dass nach Ansicht des EDSA auch nicht-textuelle personenbezogene Daten, wie etwa Sprachaufzeichnungen unter das Auskunftsrecht fallen können.[83]

- **Einschränkung von Auskunftsanträgen**

  Die Möglichkeit Auskunftsanfragen nur eingeschränkt zu beantworten oder vollständig abzulehnen, ist nur in engen Grenzen möglich. Ein offenkundig unbegründeter Antrag oder die exzessive Rechteausübung im Sinne des Art. 12 Abs. 5 DSGVO und die Beeinträchtigung von Rechten und Freiheiten anderer Personen entsprechend Art. 15 Abs. 4 DSGVO stellen hier die häufigsten Ausnahmetatbestände dar. Daneben können auch Rechtsvorschriften der Union oder der Mitgliedstaaten gemäß

[82] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn. 132 ff.
[83] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn. 106.

Artikel 23 DSGVO das Auskunftsrecht beschränken. Das bedeutet im Umkehrschluss, dass eine Einschränkung des Auskunftsrechts aufgrund von Verhältnismäßigkeitserwägungen nicht zulässig ist.

Die Befragung ergab, dass der überwiegende Teil der Verantwortlichen noch nie einen Antrag abgelehnt hat.

Wird ein Antrag entsprechend Art. 12 Abs. 5 DSGVO als offenkundig unbegründet oder exzessiv bewertet, kann der Verantwortliche entweder ein angemessenes Entgelt verlangen, um dennoch eine Beauskunftung vorzunehmen oder sich weigern aufgrund des Antrags tätig zu werden. Hier sind die Verantwortlichen allerdings nicht völlig frei in ihrer Wahl, sondern müssen unter Berücksichtigung der besonderen Umstände eine angemessene Entscheidung im Einzelfall treffen.[84] Auch in Bezug auf die Rechte Dritter konnten nahezu alle Verantwortlichen ihr entsprechendes Vorgehen darlegen. Der EDSA empfiehlt insofern eine dreistufige Prüfung bei der Einschätzung, ob die Rechte Dritter einer Auskunft entgegenstehen. Sollte dies bejaht werden, ist für den Fall, dass die Informationen über andere Personen nicht unkenntlich gemacht werden können, zu entscheiden, welche der kollidierenden Rechte und Freiheiten Vorrang haben[85].

Um einen reibungslosen Ablauf in der Bearbeitung von Auskunftsersuchen zu gewährleisten, sollten Verantwortliche frühzeitig Prozesse für den Umgang mit den Anfragen nach Art. 15 DSGVO etablieren. Gerade dort, wo wenige Anfragen eingehen, kann eine fehlende Operationalisierung schnell dazu führen, dass Rollenverteilungen unklar sind und Fristen übersehen werden. Der EDSA empfiehlt das Versenden einer Eingangsbestäti-

[84] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn. 191 ff.
[85] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn. 173.

gung als „good practice“.[86] Am Markt erhältliche Datenschutztools bieten hier gute Hilfestellungen. Auch die Benennung eines internen Verantwortlichen für die Bearbeitung datenschutzrechtlicher Eingänge ist ein geeignetes Mittel, um Anfragen nach Art. 15 DSGVO überhaupt als solche zu erkennen. Zudem sollten Mitarbeiter regelmäßig im Umgang mit datenschutzrechtlichen Belangen geschult werden. Dort, wo im Rahmen von Digitalisierungsvorhaben neue System beschafft werden, sollte im Sinne des Ansatzes „Data Protection by Design“ auf entsprechende Möglichkeiten der Einbindung und Nutzung im datenschutzrechtlichen Kontext geachtet werden. Hier kann z.B. bereits die Zusammenstellung der personenbezogenen Daten im Fall eines Auskunftsersuchens durch den Verantwortlichen oder die Betroffenen selbst, mitgedacht werden. Ebenfalls sollte auf eine ausreichende Dokumentation geachtet werden. Verantwortliche müssen in der Lage sein, ihren Entscheidungsprozess, etwa in Bezug auf die Ablehnung oder Einschränkung eines Ersuchens, nachweisen zu können.

Die Untersuchung im Saarland zeigte ein insgesamt positives Ergebnis. Die befragten Verantwortlichen zeigten im Durchschnitt eine hohe Qualität in der Bearbeitung der Anfragen bzw. in den etablierten Prozessen. Es wurden keine gravierenden Verstöße gegen die datenschutzrechtlichen Vorgaben des Art. 15 DSGVO festgestellt. Die in die Prüfung einbezogenen Energieversorger im Saarland erfüllen die diesbezüglichen Anforderungen der DSGVO insgesamt gut. Lediglich in einzelnen Fällen wurden kleinere Unstimmigkeiten erkannt, etwa bei der Annahme von Anträgen oder der Prozessorganisation. Daher waren keine weitergehenden Maßnahmen, wie ergänzende Kontrollen oder die Einleitung von Bußgeldverfahren gegenüber den Verantwortlichen erforderlich.

Die aus der Untersuchung im Saarland und den anderen teilnehmenden deutschen Behörden gewonnenen Erkenntnisse

[86] Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht; Rn. 57.

sind in einen konsolidierten Bericht eingeflossen, den die deutschen Datenschutzbehörden gemeinsam für den EDSA unter Federführung des Bundesbeauftragten für den Datenschutz erstellt haben. Dieser Abschlussbericht wird vom EDSA Anfang 2025 veröffentlicht und soll einen umfassenden Überblick über die Umsetzung des Rechts auf Auskunft in Deutschland und anderen EU-Mitgliedsstaaten geben. Ziel der koordinierten Prüfung ist es, auf europäischer Ebene gemeinsame Maßnahmen zu fördern, die neben dem Ziel der Sensibilisierung und Informationsbeschaffung auch den Anstoß für Ermittlungen und Durchsetzungsmaßnahmen geben können. Die Ergebnisse werden auf europäischer Ebene zudem genutzt, um Leitlinien und Empfehlungen für die Praxis weiterzuentwickeln.

IX.

Wirtschaft

9 Wirtschaft

9.1 Smart-Data-Verfahren in der Kreditwirtschaft

Im Berichtszeitraum wurde unsere Dienststelle von der niedersächsischen Aufsichtsbehörde darüber informiert, dass sich in dortigen Prüfverfahren im Bankenbereich Hinweise auf den Einsatz von sog. Smart-Data-Verfahren durch saarländische Banken ergeben hätten.[87]

Smart-Data-Verfahren dienen Banken dazu, mittels einer statistisch-algorithmischen Auswertung diverser Informationen über ihre Kundinnen und Kunden, die Wahrscheinlichkeit eines potenziellen Interesses an einem konkreten Produkt der Bank zu bestimmen. Auf Basis des abgeschätzten Interesses, das sich in einem sog. Affinitäts- bzw. Scorewert niederschlägt, haben die Banken so die Möglichkeit, diese zusätzlichen Erkenntnisse für werbliche Maßnahmen zu verwenden.

Unsere Dienststelle hat aufgrund des Hinweises aus Niedersachsen in einem ersten Schritt Prüfverfahren bei allen genossenschaftlichen Banken in unserer Zuständigkeit eingeleitet, um zu ermitteln, ob und in welchem Umfang derartige Verfahren im Saarland zum Einsatz kommen. Unter Hinweis auf ihre Rechenschaftspflicht aus Art. 5 Abs. 2 Datenschutz-Grundverordnung (DSGVO) wurden die Banken daher aufgefordert, den eventuellen Einsatz eines solchen Verfahrens sowie dessen Umfang und datenschutzrechtliche Rahmenbedingungen näher darzulegen.

In der Regel dürfen derartige Verfahren nur mit ausdrücklicher Einwilligung der Bankkundinnen und -kunden nach Art. 6 Abs. 1 lit. a DSGVO durchgeführt werden. Im Einzelfall hängt dies jedoch von den durch die Bank verwendeten Datenkategorien und deren Sensibilität ab. Eine Einwilligung ist aber dann erforderlich, wenn beispielsweise Zahlungsverkehrsdaten für die Bil-

[87] Vgl. Tätigkeitsbericht der Landesbeauftragten für Datenschutz Niedersachsen, 2022, J.5.1, S. 143 f., Tätigkeitsbericht des Landesbeauftragten für Datenschutz Niedersachsen, 2023, G.3.3, S. 73 f.

dung der Affinitätswerte verwendet werden, denn Zahlungsverkehrsdaten ermöglichen regelmäßig einen sehr tiefgehenden Einblick in die persönlichen Lebensumstände der Betroffenen. Zwar haben Banken ein berechtigtes Interesse an der Vermarktung ihrer Produkte, dieses Interesse muss jedoch in einem angemessenen Verhältnis zum schutzwürdigen Interesse ihrer Kundinnen und Kunden stehen, dass derart private und sensible Informationen nicht vorbehaltlos für Marketingzwecke ausgewertet werden. In diesen Fällen kann daher weder die Bildung von Affinitätswerten mittels sensibler Kundendaten noch die sich hieran anschließende Werbemaßnahme nach Art. 6 Abs. 1 lit. f DSGVO legitimiert werden.

Diese Einordnung steht auch im Einklang mit der Rechtsprechung des Europäischen Gerichtshofs, der bereits für ein soziales Netzwerk entschieden hat, dass Nutzende vernünftigerweise nicht damit rechnen können, dass der Betreiber ihre Daten ohne Einwilligung für personalisierte Werbung verwendet.[88] Für ein soziales Netzwerk können sich, wie für Kreditinstitute, durch die jeweils verarbeiteten Daten erhebliche Einblicke in die private Lebensgestaltung des Einzelnen ergeben; werden unter Auswertung und Zusammenführung umfangreicher Datensätze, wie etwa Zahlungsverkehrsdaten, Wahrscheinlichkeitsprognosen zu einer Produktaffinität erstellt, ergibt sich daher eine vergleichbare Eingriffsintensität.

Von nahezu allen saarländischen Banken wurde der Einsatz eines derartigen Verfahrens verneint. Lediglich eine Bank bestätigte den Einsatz von Smart-Data-Verfahren. Insoweit erfolgt eine weitergehende Prüfung durch unsere Dienststelle, welche zum Ende des diesjährigen Berichtszeitraumes indes noch nicht abgeschlossen war.

[88] EuGH, Urteil vom 4.7.2023 - C-252/21, Rn. 117.

9.2 Datenaustausch in der Versicherungswirtschaft

9.2.1 Hinweis- und Informationssystem der Versicherungswirtschaft

Das Hinweis- und Informationssystem der deutschen Versicherungswirtschaft (HIS) dient der Aufdeckung und Verhinderung von Fällen des Versicherungsbetrugs und -missbrauchs. Versicherungsunternehmen können in das HIS Daten zu Versicherungsfällen einmelden, die Anhaltspunkte für ein möglicherweise missbräuchliches Verhalten von Versicherungsnehmern gegeben haben. Das HIS ist als Auskunfteiunternehmen ausgestaltet und wird von der informa HIS GmbH mit Sitz in Wiesbaden betrieben. Es ist für sämtliche Versicherungssparten außer der privaten Krankenversicherung konzipiert und wird getrennt nach Versicherungssparten geführt; Meldungen und Datenübermittlungen erfolgen grundsätzlich für jede Sparte getrennt.

Da der Versicherungswirtschaft durch Versicherungsbetrug jährlich ein Schaden von mehreren Milliarden Euro entsteht, haben die Versicherungsunternehmen, aber auch die Versichertengemeinschaft, ein legitimes Interesse daran, dass der finanzielle Nachteil, bedingt durch missbräuchliche, fehlerhafte, unwahre oder unvollständige Angaben, möglichst gering gehalten wird.

Reichen versicherte Personen Anträge auf Schadensregulierung ein, kann das Versicherungsunternehmen durch eine Abfrage im HIS in Erfahrung bringen, ob über die Person oder das Versicherungsobjekt Angaben vorliegen, die auf einen Versicherungsbetrug oder -missbrauch hindeuten könnten.

Da sowohl bei der Einmeldung von Informationen über Personen und Versicherungsobjekte als auch bei der Abfrage durch Versicherungsunternehmen personenbezogene Daten im Sinne des Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO) verarbeitet werden, ist stets zu prüfen, ob eine Rechtsgrundlage herangezogen werden kann, auf die die Datenverarbeitung zulässigerweise gestützt werden kann. Als eine solche Rechtsgrundlage kommt insbesondere die Interessenabwägung nach Art. 6

Abs. 1 lit. f DSGVO in Betracht. Danach ist die Datenverarbeitung zulässig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und keine schutzwürdigen Interessen der betroffenen Personen überwiegen.

Um den datenschutzrechtlichen Grundprinzipien der Datensparsamkeit, dem Gebot der Erforderlichkeit und auch den schutzwürdigen Interessen der betroffenen Personen gerecht zu werden, enthalten die zwischen den Aufsichtsbehörden des Bundes und der Länder und dem Gesamtverband der deutschen Versicherungswirtschaft e.V. (GDV) vereinbarten Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft konkrete, standardisierte Kriterien, unter denen Einmeldungen von Daten in das HIS möglich sind. Die hierdurch gewährleistete einheitliche Vorgehensweise bei der Dateneinmeldung dient einerseits dem Interesse an einem effektiven Schutz vor Versicherungsbetrug und soll andererseits gewährleisten, dass der durch die Datenverarbeitung bedingte Grundrechtseingriff nicht unverhältnismäßig zum angestrebten Verarbeitungszweck ist.

Versicherungsunternehmen, die Informationen in das HIS einmelden oder eine Abfrage in der Datenbank durchführen, sind verpflichtet, die betroffene Person transparent über Art und Umfang der Datenverarbeitung nach Maßgabe der Art. 12 ff. zu informieren. Die Informationspflicht richtet sich bei einmeldenden Unternehmen nach Art. 13 DSGVO, wohingegen abfragende Unternehmen die Daten nicht bei der betroffenen Person selbst erheben und somit ein Fall der Dritterhebung vorliegt mit der Folge, dass die betroffene Person gemäß Art. 4 DSGVO zu informieren ist.

Im Berichtszeitraum erreichten uns mehrere Beschwerden von Personen, die von Versicherungsunternehmen darüber in Kenntnis gesetzt wurden, dass Informationen über das eigene Fahrzeug, im Einzelnen die Fahrzeugidentifikationsnummer (FIN) und das Kfz-Kennzeichen, an das HIS übermittelt wurden.

In den von den Betroffenen geschilderten Sachverhalten ging es um Fälle, in denen die jeweiligen Versicherungen Lackschäden in Höhe zwischen 500,-- EUR und 1000,-- EUR reguliert hatten, ohne dass die Schäden im Nachgang durch eine Werkstatt repariert wurden. Die versicherten Personen machten bei den Versicherungsunternehmen Widersprüche im Sinne des Art. 21 Abs. 1 DSGVO gegen die Datenweitergabe in das HIS geltend oder verlangten nach Art. 17 DSGVO von dem das HIS betreibende Unternehmen die Löschung ihrer personenbezogenen Daten aus der Datenbank.

Die adressierten Unternehmen wiesen die geltend gemachten Betroffenenrechte unter Verweis darauf ab, dass die Datenverarbeitung unter Berücksichtigung der für die Versicherungswirtschaft geltenden Verhaltensregeln in Bezug auf die Einmeldekriterien erfolgt sei und demnach die Voraussetzungen nach Art. 6 Abs. 1 lit. f DSGVO erfüllt seien. Dem liege zugrunde, dass das HIS dem Informationsaustausch zwischen den Versicherungsunternehmen und damit gerade auch dem Erkenntnisgewinn im Zusammenhang mit Versicherungsfällen unter Berücksichtigung früherer Schadensfälle dienen soll. Daten zu dem Fahrzeug könnten so zu einem späteren Zeitpunkt, wenn für dieses Fahrzeug ein Versicherungsantrag gestellt oder einem Versicherer gemeldet werde, von dem jeweiligen Versicherer abgefragt und genutzt werden; für den Fall des Fahrzeugverkaufs könne aufgrund der HIS-Meldung rechtswidrigen Handlungen eines Dritten vorgebeugt werden und somit das Risiko, dass der Schaden bei mehreren Versicherungsgesellschaften abgerechnet oder bei einem späteren Unfall erneut geltend gemacht werde, entscheidend minimiert werden.

Die Ausführungen der adressierten Unternehmen waren aus datenschutzrechtlicher Sicht nicht zu beanstanden. So sieht das HIS als möglichen Einmeldegrund Fälle vor, in denen Schäden über einem Wert von 500,-- EUR reguliert werden, jedoch kein Nachweis über die Reparatur erbracht wird. Über diesen Einmeldegrund kann insoweit Schadenshandlungen zu Lasten der Versicherungsunternehmen sowie der Versicherungsgemeinschaft

vorgebeugt werden, als missbräuchliche Doppelabrechnungen deutlich erschwert werden. Demgegenüber sind die entgegenstehenden schutzwürdigen Interessen der betroffenen Personen allenfalls als marginal einzustufen, da lediglich Fahrzeugdaten im HIS eingemeldet wurden und allein durch diese Einmeldung zunächst keine nachteiligen Auswirkungen für die betroffenen Personen zu befürchten sind; weder hat dies Auswirkungen auf den Abschluss künftiger Versicherungsverträge noch tangiert dies einen potenziellen Verkaufswert eines Fahrzeugs. Im Übrigen kann die Einmeldung in HIS nach erfolgter Reparatur und Vorlage eines entsprechenden Nachweises verhindert bzw. rückgängig gemacht werden.

Anhand des vorliegenden Sachverhalts wird deutlich, dass die Einmeldung und Speicherung personenbezogener Daten im HIS – entgegen der subjektiven Wahrnehmung im jeweiligen Fall – nicht dazu dient, den betroffenen Personen eine Betrugsabsicht zu unterstellen; vielmehr dient der Informationsaustausch der Versicherungsunternehmen dazu, das Risiko betrügerischer oder missbräuchlicher Handlungen zu Lasten der Versicherer und der Versichertengemeinschaft zu minimieren.

9.2.2 Gemeinsame Prüfaktion: Betrugsprävention im Bereich der Auslandskrankenversicherung

Der standardisierte Informationsaustausch zwischen Versicherungsunternehmen zum Zwecke der Betrugsprävention kann – wie bei dem bereits dargestellten HIS – dem Grunde nach ein legitimes Interesse darstellen. Da nicht alle Versicherungssparten, wie beispielsweise private Krankenversicherungen, dem HIS angeschlossen sind und für diese Sparten kein vergleichbares institutionalisiertes Instrument existiert, ist in diesen Fällen die datenschutzrechtliche Zulässigkeit eines Informationsaustausches zu Versichertendaten im Einzelfall zu betrachten.

Im Berichtszeitraum wurden wir von der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen darüber in Kenntnis gesetzt, dass zwischen diversen Versiche-

rungsunternehmen unter Beteiligung eines in unserem Zuständigkeitsbereich ansässigen Unternehmens ein inoffizieller E-Mail-Verteiler für den Austausch personenbezogener Daten zu Betrugsverdachtsfällen von Versicherten im Bereich der Auslandskrankenversicherung etabliert wurde.

Über den Verteiler wurden personenbezogene Daten der Versicherten sowie mitversicherter – auch minderjähriger – Personen ausgetauscht.

Im Unterschied zum HIS war vorliegend davon auszugehen, dass die Nutzung des Verteilers weder auf einer systematisch beschriebenen Vorgabe noch einem standardisierten Prozess basierte, sondern vielmehr im Einzelfall dann erfolgte, wenn es dem jeweiligen Sachbearbeiter eines Versicherungsfalles sinnvoll erschien.

Auf unsere aufsichtsbehördliche Nachfrage teilte das Unternehmen mit, dass die weitere Teilnahme an dem Verteiler umgehend eingestellt worden sei, da die Ausgestaltung des Verteilers den datenschutzrechtlichen Ansprüchen des Unternehmens nicht entspräche. Allerdings gehe man davon aus, dass der Verteiler durchaus auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden könne, da in betrügerischer Absicht handelnde Versicherte kein schutzwürdiges Interesse für sich in Anspruch nehmen könnten, welches das berechtigte Interesse an der Datenverarbeitung zur Eindämmung von Versicherungsbetrug überwiegen würde.

Betrugsprävention und -bekämpfung stellen zweifelsohne ein berechtigtes Interesse der Versicherungsunternehmen dar, allerdings waren vorliegend keine verbindlich festgelegten Prozesse für den Austausch feststellbar; vielmehr erfolgten die Abfragen und die damit verbundene Datenverarbeitung ad hoc nach subjektiver Intuition der am Verteiler beteiligten Mitarbeitenden diverser Unternehmen. Es konnte nicht festgestellt werden, dass schutzwürdigen Interessen und Grundrechten/-freiheiten der betroffenen versicherten Personen überhaupt bei der einzelfallbezogenen Verarbeitung Rechnung getragen wurde; da zudem für die betroffenen Personen mangels Information

nach Art. 13 oder 14 DSGVO die dem Informationsaustausch zugrundeliegende Datenverarbeitung vollkommen intransparent geblieben ist, war eine Befugnis zur Datenverarbeitung gestützt auf Art. 6 Abs. 1 lit. f DSGVO und somit die Voraussetzungen für einen datenschutzrechtlich zulässigen Informationsaustausch nicht ersichtlich.

Zum Zeitpunkt des Redaktionsschlusses war die Sachbefassung mit Blick auf potenzielle aufsichtsrechtliche Maßnahmen nach Art. 58 Abs. 2 DSGVO nicht abgeschlossen.

9.3 Videoüberwachung

9.3.1 Anfertigung von Bildaufnahmen durch Privatpersonen

Da Smartphones und Kameras mittlerweile allgegenwärtig sind, erreichen die Aufsichtsbehörde regelmäßig eine Vielzahl an Fragestellungen zur Rechtmäßigkeit von kameragestützten Datenverarbeitungen. In diesem Berichtszeitraum kam es wiederum zu einer beträchtlichen Anzahl an Beschwerden, die eine Anfertigung von Bildaufnahmen durch Privatpersonen zum Gegenstand hatten. Den Verfahren lag dabei zumeist zugrunde, dass Bilder von privaten Grundstücken, der betroffenen Person selbst oder des eigenen Fahrzeugs aufgenommen und diese vermeintlich an Dritte übermittelt worden seien.

Bildaufnahmen von Personen, die im Rahmen persönlicher oder familiärer Tätigkeiten im Sinne des Art. 2 Abs. 1 lit. c Datenschutz-Grundverordnung (DSGVO), beispielsweise zur Freizeitgestaltung bei Ausübung eines Hobbys oder anlässlich eines Urlaubs, angefertigt werden, sind grundsätzlich nicht Regelungsgegenstand der DSGVO. Keine ausschließlich persönliche oder familiäre Tätigkeit im Sinne der Vorschrift liegt beispielsweise dann vor, wenn Bildaufnahmen, die auf eine identifizierbare Person zurückschließen lassen können, insbesondere zu dem Zweck der Dokumentation und Ahndung eines Fehlverhaltens angefertigt, mit dem Ziel der Ahndung oder Bloßstellung

weitergegeben bzw. – bspw. auf Social-Media-Kanälen – veröffentlicht werden[89] oder wenn fremde Personen im öffentlichen Raum gezielt und heimlich fotografiert werden.[90] Für derartige Verarbeitungen von Bildaufnahmen durch Privatpersonen entfalten die Vorgaben der DSGVO uneingeschränkt Wirkung.

Die Weitergabe von Bildaufnahmen von vermeintlichen Falschparkern an ein Inkassounternehmen führte im Berichtszeitraum zu einer erheblichen Zahl von Beschwerden. Ein Anwohner einer stark frequentierten Straße fühlte sich von im öffentlichen Verkehrsraum vor seinem Wohnhaus abgestellten Fahrzeugen derart beeinträchtigt, dass er diese unabhängig davon, ob sie tatsächlich ein Hindernis für die Nutzung seines Grundstücks darstellten, ablichtete und die Aufnahmen an ein Inkassounternehmen weiterleitete. Dieses Inkassounternehmen nimmt dabei in Anspruch als Rechtsdienstleister aufzutreten und bietet eine App an, mit der Nutzende Bildaufnahmen von vermeintlich widerrechtlich auf privaten Parkplätzen abgestellten oder den Zugang zu privaten Parkplätzen blockierenden Fahrzeugen übermitteln können. Gegenüber dem ermittelten Halter werden dann – exemplarisch – erhöhte Parkentgelte, Halterermittlungskosten, eine Einigungsgebühr analog zu Nr. 1000 VV RVG und diverse Kommunikationspauschalen als eine „Vertragsstrafe" geltend gemacht.

Auch wenn das Verwaltungsgericht Ansbach[91] die durch Privatpersonen vorgenommene Anfertigung von Bildaufnahmen von im öffentlichen Raum abgestellten Fahrzeugen und die anschließende Übermittlung an Ortspolizeibehörden zur Ahndung von Parkverstößen grundsätzlich als datenschutzrechtlich zulässig qualifiziert, ohne dass es auf eine persönliche Betroffenheit des Anzeigenerstatters ankommt, konnte dies für die in der datenschutzrechtlichen Verantwortlichkeit des Anwohners erfolgte Anfertigung von Bildaufnahmen nicht gelten. In den be-

[89] Europäischer Gerichtshof, Urteil vom 11.Dezember 2014 – C-212/13, Rn. 35, juris.
[90] Amtsgericht Hamburg, Beschluss vom 3. Juli 2020 – 163 Gs 656/20.
[91] Urteil vom 2. November 2022 - AN 14 K 22.00468 und AN 14 K 21.01431.

schwerdegegenständlichen Fällen waren, soweit die aufgenommenen Fahrzeuge in dafür vorgesehenen, am Fahrbahnrand liegenden Parkbuchten abgestellt waren, gerade keine Verkehrsordnungswidrigkeit und ferner auch keine Beeinträchtigung bei der Nutzung des eigenen Grundstücks erkennbar. Dies bestätigte auch die Kommune, die nach hiesiger Bitte um Darlegung der verkehrsrechtlichen Situationen mitteilte, dass die aufgenommenen Fahrzeuge weder widerrechtlich abgestellt waren noch für Anlieger eine Beeinträchtigung dargestellt hätten. Dementsprechend erfolgte durch den Anwohner auch keine Datenweitergabe an eine zur Verfolgung von Verkehrsverstößen zuständige Stelle, sondern an einen von ihm für seine eigenen Zwecke ausgewählten „Rechtsdienstleister".

Angesichts der unzulässigen Datenerhebung durch den Anwohner und der daher auch fehlenden rechtlichen Grundlage für eine geltend gemachte „Vertragsstrafe", konnte auch die Datenweitergabe an diesen Dienstleister nicht auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden.

Zwischenzeitlich wurde die hiesige Bußgeldstelle mit dem Sachverhalt befasst.

9.3.2 Trainieren unter Aufsicht – Videoüberwachung im Fitnessstudio

Auch Betreiber von Fitnessstudios setzen zunehmend auf Videoüberwachungsmaßnahmen. Die vorgetragenen Gründe für den Betrieb von Videokameras sind vielfältig und reichen vom Schutz vor unsachgemäßem Gebrauch der Trainingsgeräte, Diebstählen zulasten der Betreiber oder Trainierenden über Einlasskontrollen bis hin zur Verhinderung oder Aufklärung von sexuellen Übergriffen. Allerdings stoßen Videoüberwachungsmaßnahmen im Fitnessstudio häufig an datenschutzrechtliche Grenzen.

Vor dem Hintergrund eines Beschwerdeverfahrens, in dessen Zusammenhang sich eine betroffene Kundin durch eine in einem Kursraum eines Fitnessstudios installierte Kamera unzulä-

sigerweise überwacht und nicht transparent über die mit der Videoüberwachung erfolgende Datenverarbeitung unterrichtet fühlte, setzte sich die Aufsichtsbehörde mit einem nahezu lückenlosen Kameraeinsatz im Innenraum eines Fitnessstudios auseinander.

Der Betreiber des Studios teilte mit, dass die Überwachung der Trainingsbereiche der Sicherheit der Mitarbeitenden und Trainierenden vor sexuellen Übergriffen und Handgreiflichkeiten diene. Darüber hinaus werde die Videoüberwachung zum Zwecke des Schutzes des Eigentums vor Sachbeschädigung und – im Falle ungesicherten Equipments – vor Diebstahl betrieben. Letztlich solle im Falle von Einbrüchen eine nachträgliche Identifizierung von Tätern ermöglicht werden. Die kameragestützte Überwachung werde auf die datenschutzrechtliche Einwilligung der Trainierenden gestützt, die in der Datenschutzerklärung, in den Allgemeinen Geschäftsbedingungen zum Trainingsvertrag und über angebrachte Hinweisschilder über die Videoüberwachung informiert werden.

Eine wirksame Einwilligung erfordert nach Art. 4 Nr. 11 DSGVO eine freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden Daten einverstanden ist. Eine solche eindeutige bestätigende Handlung der Trainierenden kann allerdings nicht in der bloßen Kenntnisnahme der Hinweise auf die Videoüberwachung in den Datenschutzhinweisen und der Hinweisbeschilderung gesehen werden, da Stillschweigen oder Untätigkeit gerade keine Einwilligung darstellen.[92]

Soweit der Studiobetreiber ergänzend auf die Allgemeinen Geschäftsbedingungen des Trainingsvertrags verwiesen hat, wonach die Videoüberwachung Vertragsbestandteil geworden sei,

[92] Erwägungsgrund 32 zur DSGVO.

konnte auch dies rechtlich nicht überzeugen. Nach Art. 6 Abs. 1 lit. b DSGVO ist eine Datenverarbeitung rechtmäßig, wenn sie zur Erfüllung eines Vertrags, dessen Vertragspartner die betroffene Partei ist, erforderlich ist. Der zwischen dem Betreiber und den Trainierenden geschlossene Vertrag regelte die vertragliche Pflicht, dass die Trainierenden einen monatlichen Beitrag leisten und als Gegenleistung im Fitnessstudio trainieren können. Für die Erfüllung dieses Vertrags war die Anfertigung von Bildaufzeichnungen gerade nicht erforderlich. Zwar sind vertragliche Nebenpflichten wie Rücksichtnahme- und Schutzpflichten auch von dieser Vorschrift erfasst, jedoch ging die Videoüberwachung über diese Pflichten hinaus.[93]

Die Überwachung der Trainingsflächen konnte auch nicht zulässigerweise auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden. Nach dieser Vorschrift ist die Videoüberwachung zulässig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die schutzwürdigen Interessen der betroffenen Person das Verarbeitungsinteresse nicht überwiegen. Neben Eigeninteressen des Betreibers einer Videoüberwachungsanlage sind demnach auch Drittinteressen grundsätzlich schützenswert.

Die vom Fitnessstudiobetreiber kommunizierten Überwachungszwecke waren als grundsätzlich berechtigte Interessen im Sinne der Vorschrift anerkennenswert, da sie dem Schutz des Betreibers selbst, aber auch der Mitarbeitenden und Trainierenden vor Schadenshandlungen diverser Art dienen sollten. Neben dem Schutz der Mitarbeitenden und Trainierenden vor sexuellen Übergriffen und Handgreiflichkeiten sollte mit der Videoüberwachung überdies dem Schutz vor Beschädigung und Diebstahl des studioeigenen Equipments Rechnung getragen werden. Allerdings ist es nicht ausreichend, dass lediglich die

[93] Europäischer Datenschutzausschuss, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO in Zusammenhang mit der Erbringung von Online- Diensten, Version 2.0, Rn. 28 ff.; EuGH, Urteil vom 4. Juli 2023 in der Rechtssache C-252/21, Rn. 98; Schlussanträge des Generalanwalts Rantos vom 20. September 2022, Rn. 54.

Überwachungsinteressen abstrakt genannt werden; vielmehr muss eine Gefährdungslage hinreichend durch Tatsachen (konkrete Gefahr) oder die allgemeine Lebenserfahrung (abstrakte Gefahr) belegt werden, die über das allgemeine Lebensrisiko hinausgeht. Subjektive Befürchtungen oder ein allgemeines Gefühl der Unsicherheit reichen hierfür nicht aus.

Von Seiten des Anlagenbetreibers wurde allerdings keine ausreichend belastbaren Anhaltspunkte vorgetragen oder Dokumentationen vorgelegt, die das geltend gemachte Überwachungsinteresse objektiv gestützt hätten. Selbst für den Fall einer hinreichend konkreten Gefährdungslage ist die Videoüberwachung nur zulässig, wenn die Videoüberwachung geeignet ist, die Verarbeitungszwecke zu erreichen bzw. zu fördern und diesen nicht ebenso gut durch eine andere gleich wirksame, aber schonendere Maßnahme Rechnung getragen werden kann.

Dem Schutz des Eigentums der Trainierenden hätte bspw. dadurch Rechnung getragen werden können, dass Wertgegenstände und Kleidung in absperrbaren Spinden untergebracht werden. Eine Videoüberwachung zum Zweck des Einbruchsschutzes wäre während der Öffnungszeiten gerade nicht erforderlich, da sich entsprechende Schadenshandlungen außerhalb des Trainingsbetriebs unter Abwesenheit jeglicher sozialer Kontrolle ereignen.

Darüber hinaus ist auch eine erforderliche Videoüberwachung unzulässig, wenn die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, überwiegen. Bei einer durchgehenden Videoüberwachung im Fitnessstudio während der gesamten Öffnungszeiten auf allen Trainingsflächen handelte es sich um einen erheblichen Eingriff in die Grundrechte sämtlicher Trainierenden, also einer erheblichen Anzahl von Personen, die überwiegend keinen Anlass für die Überwachung gegeben haben. Die betroffenen Personen wurden gerade auch im Rahmen von Freizeitaktivitäten und damit besonders schützenswerten

Bereichen der allgemeinen Persönlichkeitsentfaltung überwacht und hatten keine Möglichkeit, sich der Videoüberwachung innerhalb des Fitnessstudios in räumlicher oder zeitlicher Hinsicht zu entziehen.

Da die Videoüberwachung folglich auf keine Rechtsgrundlage gestützt werden konnte, stellte der Betreiber die Videoüberwachung der Trainingsflächen während der Trainingszeiten im Laufe des Verfahrens ein.

X.

Wahlwerbung

10 Wahlwerbung

10.1 Personenbezug bei Wahlwerbung

Im Kontext der Kommunalwahl wurde die Aufsichtsbehörde durch eine Kontrollanregung um Prüfung eines Falls von Wahlwerbung gebeten. So hatte der Lokalverband einer Partei in einem Werbeflyer unter anderem den potenziellen Erwerb sogenannter Schrottimmobilien durch die Kommune aufgegriffen, die einen negativen Einfluss auf das Ortsbild und damit die Lebensqualität der Bevölkerung haben können. Datenschutzrechtliche Relevanz erfuhr der Sachverhalt schließlich dadurch, dass in diesem Flyer eine Bildaufnahme eines augenscheinlich im Verfall befindlichen Gebäudes in exponierter Ortslage mit Angabe des Familiennamens der zwischenzeitlich verstorbenen Eigentümer sowie der Erbengemeinschaft verbunden mit der wertenden Konnotation als „Schrottimmobilie“ abgedruckt war.

Die Angabe eines Familiennamens stellt unzweifelhaft ein personenbezogenes Datum im Sinne des Art. 4 Abs. 1 DSGVO dar. Danach sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Zwar findet die DSGVO entsprechend dem Erwägungsgrund 27 keine Anwendung auf die Daten verstorbener Personen, allerdings trugen auch einzelne Erben der Erbengemeinschaft den Familiennamen der verstorbenen Eigentümer. Insofern konnte durch die konkrete Benennung des in der Wahlwerbung abgebildeten Hauses ein Bezug zu den hinter der Erbengemeinschaft stehenden Personen hergestellt werden.

Nach Art. 5 Abs. 1 lit. a DSGVO ist Voraussetzung für die datenschutzrechtliche Zulässigkeit einer Verarbeitung personenbezogener Daten, dass diese auf eine Legitimationsgrundlage im Sinne des Art. 6 Abs. 1 DSGVO gestützt werden kann. Beruht die Verarbeitung personenbezogener Daten in der vorliegenden Konstellation nicht auf einer Einwilligung der betroffenen Per-

sonen im Sinne des Art. 6 Abs. 1 lit. a, Art. 4 Nr. 11 und Art. 7 DSGVO, kann auf die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO abgestellt werden. Nach dieser Vorschrift ist die Verarbeitung nur 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.

Der Begriff des berechtigten Interesses umfasst jedes rechtliche, wirtschaftliche und ideelle Interesse, soweit es rechtmäßig ist. Der Kommunalverband weist in dem Flyer auf die Notwendigkeit zur Erstellung eines Leerstandskatasters hin. Um dieser Forderung Nachdruck zu verleihen, wurde stellvertretend für den optischen Verfall eine Bildaufnahme des ortsbildprägenden Anwesens nebst Familiennamen der vormaligen Eigentümer sowie einiger Erben veröffentlicht. Dies dient der plakativen Darstellung der politischen Zielsetzung des Kreisverbands, um hiermit im Rahmen des Wahlkampfes um Stimmen der Bürgerinnen und Bürger zu werben, worin zweifelsfrei ein berechtigtes Interesse des Ortsverbandes zu sehen war.

Weiter müsste die Veröffentlichung des personenbezogenen Datums in Form des Familiennamens zur Wahrung des berechtigten Interesses erforderlich sein. So ist die Erforderlichkeit nur dann zu bejahen, wenn sie zur Zweckerreichung geeignet und auch verhältnismäßig ist. Sofern im Vergleich zur Verbreitung des Familiennamens weniger eingriffsintensive Mittel naheliegend sind, wäre auf diese auszuweichen. Es spricht aus hiesiger Sicht einiges dafür, dass die Abbildung der Gebäudefront zwecks Darstellung des Verfalles ortsbildprägender Anwesen bereits ausreichend gewesen wäre. Schließlich verdeutlicht bereits die Optik des Gebäudes den äußerlichen Verfall, ohne dass es einer kontextualisierenden Nennung des Familiennamens bedurfte.

Schließlich verlangt die Vorschrift in einem letzten Schritt die Vornahme einer Abwägung zwischen dem berechtigten Veröf-

fentlichungsinteresse des Kommunalverbands mit den schutzwürdigen Interessen der betroffenen Mitglieder der Erbengemeinschaft, dass eine solche Veröffentlichung unter namentlicher Nennung unterbleibt. Bei dieser Abwägung sind auch die vernünftigen Erwartungen der betroffenen Personen zu berücksichtigen. Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, können die Interessen und Grundrechte der betroffenen Person(en) das Interesse des Verantwortlichen überwiegen. Dass Mitglieder einer Erbengemeinschaft davon ausgehen können bzw. müssen, dass Informationen zu einer ihrem (Mit-)Eigentum stehenden Immobilie durch eine lokale Partei in einer bestimmten Form von Wahlwerbung verbreitet werden, liegt nach allgemeiner Lebenserfahrung nicht auf der Hand. Zwar konnte in dem zugrundeliegenden Sachverhalt die Bezeichnung des Anwesens mitsamt des Familiennamens in der Vergangenheit sowohl Presse- als auch Gemeindeveröffentlichungen entnommen werden und war umgangssprachlich verbreitet; allerdings ist zu berücksichtigen, dass mit dem Zusatz „Schrottimmobilie" eine abwertende Konnotation verbunden ist und die Bezeichnung der Immobilie als solche in Kombination mit der Namensnennung von den betroffenen und ortsbekannten Erben durchaus nicht gutgeheißen würde.

Unter Berücksichtigung dieser Erwägungen gab es nach hiesigem Dafürhalten Argumente dafür, dass die Namensnennung für die Zweckerreichung des Kommunalverbandes nicht erforderlich gewesen ist. Da der Sachverhalt nicht als Beschwerde einer betroffenen Person, sondern als eine Anregung zur datenschutzrechtlichen Prüfung des Sachverhalts, an die Aufsichtsbehörde herangetragen wurde, wurde die lokale Parteigliederung lediglich durch Hinweis nach Art. 58 Abs. 1 lit. d DSGVO darauf aufmerksam gemacht, dass im Zusammenhang mit dem Flyer personenbezogene Daten verarbeitet wurden und welche Parameter bei einer solchen Verarbeitung eine Rolle spielen können.

10.2 Postalische Wahlwerbung

Parteien sowie ihre Kandidatinnen und Kandidaten richten vor allem im zeitlichen Zusammenhang mit Wahlterminen postalische Werbebotschaften an Bürgerinnen und Bürger und adressieren dabei häufig gezielt bestimmte Wählergruppen – wie bspw. Erstwähler. Da die Adressaten in eine Datenverarbeitung für Zwecke der Wahlwerbung nicht eingewilligt hatten oder die Herkunft der so verwendeten Daten für sie nicht nachvollziehbar war, wurden auch im Vorfeld der Kommunal- und Europawahl eine Anzahl gleichgelagerter Beschwerden an die Aufsichtsbehörde gerichtet. Zwar war in diesen Fällen die persönliche Ansprache der Wahlberechtigten datenschutzrechtlich nicht zu beanstanden, jedoch enthielten sämtliche den Beschwerden zugrundeliegenden wahlwerblichen Botschaften keine Angaben zur Datenherkunft und ließen damit die für die Adressaten der Wahlwerbung erforderliche Transparenz vermissen.

Zunächst gilt, dass die Meldebehörden gestützt auf § 50 Abs. 1 S. 1 Bundesmeldegesetz (BMG) Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen binnen eines Zeitraums von sechs Monaten vor einer Wahl oder Abstimmung auf staatlicher oder kommunaler Ebene Auskunft aus dem Melderegister über die in § 44 Abs. 1 S. 1 BMG genannten Daten von Gruppen von Wahlberechtigten erteilen dürfen. Diese Auskunft umfasst den Vor- und Nachnamen, ggf. Doktorgrad sowie die derzeitige Wohnanschrift der wahlberechtigten Personen; das Geburtsdatum gehört nach § 50 Abs. 1 S. 2 BMG ausdrücklich nicht zu den zu beauskunftenden Daten. Allerdings sieht § 50 Abs. 1 S. 1 BMG vor, dass eine Auskunft nur über Personengruppen erteilt werden darf, wobei stets das Lebensalter für die Zusammensetzung der Gruppen maßgeblich ist. Dadurch kann die Wahlwerbung gezielt auf eine entsprechende Altersgruppe, wie beispielsweise Erstwähler oder Senioren, angepasst werden.

Mit dieser Übermittlungsbefugnis der Meldebehörde korrespondiert eine ausschließlich auf wahlwerbliche Zwecke be-

schränkte Nutzungsbefugnis der übermittelten personenbezogenen Daten durch die datenempfangenden Parteien oder kandidierenden Einzelpersonen. Die Person oder Stelle, der die Daten übermittelt werden, hat diese spätestens einen Monat nach der Wahl oder Abstimmung zu löschen oder zu vernichten. Eine Übermittlung von Daten in diesem Zulässigkeitskorridor ist nur dann ausgeschlossen, wenn bei der Meldebehörde ein Widerspruch oder eine Auskunftssperre im Sinne des § 50 Abs. 5 oder 6 BMG dokumentiert ist.

Vor diesem Hintergrund war für die beschwerdegegenständlichen Sachverhalte eine datenschutzwidrige Verwendung personenbezogener Daten nicht erkennbar. Die ausschließlich für Wahlwerbung erfolgende Nutzung der auf Grundlage des BMG seitens der Meldebehörde zur Verfügung gestellten Daten durch die Parteien sowie ihre Kandidatinnen und Kandidaten war dabei grundsätzlich als nach Art. 6 Abs. 1 lit. e Datenschutz-Grundverordnung (DSGVO) legitimiert anzusehen und setzte somit nicht das Vorliegen einer Einwilligung im Sinne des Art. 4 Nr. 11 in Verbindung mit Art. 6 Abs. 1 lit. a DSGVO voraus. Diese Wahlwerbung stellte letztlich einen Beitrag zum politischen Willensbildungsprozess dar, der im Sinne des Art. 6 Abs. 1 lit. e DSGVO als Aufgabe im öffentlichen Interesse qualifiziert werden kann. Wären allerdings weitere Datenkategorien – bspw. Kontaktinformationen wie E-Mail-Adressen[94] und Telefonnummern oder individuelle politische Präferenzen – verarbeitet worden, hätte diese Verarbeitung nicht auf Art. 6 Abs. 1 lit. e DSGVO gestützt werden können und hätte das Vorliegen einer wirksamen Einwilligung der wahlwerblich adressierten Personen vorausgesetzt.

Soweit die beschwerdegegenständlichen wahlwerblichen Botschaften jedoch keinen transparenten Hinweis zur Datenherkunft und den Umständen ihrer Verarbeitung im Sinne des Art. 14 DSGVO enthielten, wurden die Versender im Wege des

[94] 31. Tätigkeitsbericht Datenschutz 2022, 11.1.1 Wahlwerbung per E-Mail, S. 128.

Hinweises nach Art. 58 Abs. 1 lit. d DSGVO zur Gewährleistung ausreichender Transparenz angehalten; denn nur so kann ein hinreichendes Vertrauen der Bürgerinnen und Bürger in das Verarbeitungshandeln der Parteien und Parteiakteure garantiert werden.

10.3 EU-Verordnung über die Transparenz und das Targeting politischer Werbung

Am 13. März 2024 ist mit Verabschiedung der Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates über die Transparenz und das Targeting politischer Werbung (TTPW-VO) ein neues Thema in den Fokus der Datenschutzaufsichtsbehörden getreten. Ziel der Verordnung ist es im weitesten Sinne, die demokratischen Prozesse in der EU und deren Mitgliedstaaten zu stärken und die Integrität von Wahlen zu schützen. Da mittlerweile für die Wahlentscheidung Informationen aus dem Internet und insbesondere auch aus den sozialen Netzwerken von erheblicher Relevanz sind, ist es von hervorgehobener Bedeutung, dass Bürgerinnen und Bürger nachvollziehen können, von wem etwaige politische Werbung stammt und auf welche Weise diese ausgespielt wird. Denn Voraussetzung für einen demokratischen Wahlprozess ist es, dass Bürgerinnen und Bürger ihre demokratischen Rechte informiert ausüben können, indem beispielsweise Desinformation im Zusammenhang mit Wahlen eingedämmt wird.[95] Auch gilt es zu verhindern, dass Wahlentscheidungen unterschwellig beeinflusst werden, etwa indem spezifische Merkmale und mögliche Präferenzen von Wählerinnen und Wählern identifiziert und verwendet werden, um Anzeigen an bestimmten Orten und zu bestimmten Gelegenheiten auszuspielen, bei denen diese für die Botschaft potenziell besonders empfänglich sind.[96]

Um dem entgegenzuwirken, stellt die Verordnung neue Regeln bei der Nutzung personenbezogener Daten für Zwecke der po-

[95] ErwG 4 ff. TTPW-VO.
[96] ErwG 74 TPW-VO.

litischen Werbung auf. Die für die Kontrolltätigkeit der Datenschutzaufsichtsbehörden maßgebliche Regelungen finden sich neben der Zuweisung der Aufsichtszuständigkeit in Art. 22 TTPW-VO in Art. 18 und 19 TTPW-VO.

Art. 8 TTPW-VO bestimmt, in welchen Fällen die Nutzung personenbezogener Daten für Zwecke politischer Werbung mittels Targeting- und Anzeigenschaltverfahren zulässig ist; Targeting- und Anzeigenschaltverfahren zeichnen sich dadurch aus, dass personenbezogene Daten von Wählerinnen und Wählern verwendet werden, um eine politische Anzeige nur an eine bestimmte Person oder eine Personengruppe zu richten.[97] Die Vorschrift betrifft zwar nicht nur, aber insbesondere auch politische Werbung im Internet. Das Kernelement der Regelung besteht darin, dass Targeting- und Anzeigenschaltverfahren für Zwecke der politischen Werbung nur mit ausdrücklicher Einwilligung der betroffenen Person erfolgen dürfen (Art. 18 Abs. 1 lit. b TTPW-VO). Sie normiert damit einen umfassenden Einwilligungsvorbehalt. Es obliegt also allein den Wählerinnen und Wählern zu entscheiden, ob deren personenbezogene Daten verwendet werden dürfen, um ihnen personalisierte, politische Werbung auszuspielen. Art. 6 Abs. 1 lit. f DSGVO, der eine Verarbeitung personenbezogener Daten nach Abwägung der widerstreitenden Interessen ggf. auch ohne Einwilligung ermöglicht, scheidet daher mit Geltung der TTPW-VO in deren Anwendungsbereich als Legitimationsgrundlage aus.

Soll eine Einwilligung für Zwecke der politischen Werbung bei Betroffenen eingeholt werden, muss diese Einwilligung zunächst den allgemeinen Anforderungen der DSGVO aus Art. 4 Nr. 11 und Art. 7 DSGVO entsprechen. Sie muss daher insbesondere freiwillig und informiert erfolgen. Bereits aus der DSGVO folgt, dass eine Einwilligung immer nur für einen bestimmten Fall erfolgen kann und es daher nicht möglich ist, Generaleinwilligungen für allgemeine Zwecke mit hohem Abstrak-

[97] Art. 3 Nr. 11, 12 TPW-VO.

tionsgrad einzuholen.[98] Art. 18 Abs. 1 lit. b und Erwägungsgrund 80 Satz 3 TTPW-VO stellen dennoch ergänzend hierzu klar, dass eine Einwilligung für Zwecke der politischen Werbung gesondert erteilt werden muss. Wird beispielsweise eine Einwilligung in die Verarbeitung personenbezogener Daten für Zwecke personalisierter Werbung im Rahmen eines Einwilligungsbanners auf einer Webseite erteilt, umfasst dies demnach niemals automatisch auch die Verarbeitung der Daten für Zwecke der politischen Werbung.

Aufgrund der besonderen Bedeutung demokratischer Wahlen sind notwendigerweise im Bereich des Targetings zu Zwecken der politischen Werbung hohe Anforderungen an Transparenz und die Informiertheit zu stellen. So sieht Art. 19 TTPW-VO für Verantwortliche beim Einsatz von Targeting- und Anzeigenschaltverfahren weitreichende Rechenschaftsobliegenheiten, unter anderem in Form von Informationspflichten gegenüber konkret betroffenen Personen, Offenlegungspflichten von Verhaltensregeln und organisatorischer Vorgaben vor.

[98] Vgl auch Datenschutzkonferenz, OH Digitale Dienste, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf, Rn. 51 ff.

XI.

Ordnungswidrigkeiten & Bußgeldverfahren

11 Ordnungswidrigkeiten & Bußgeldverfahren

11.1 Unterlassene Mitwirkung im Verwaltungsverfahren

Gemäß Art. 31 DSGVO arbeiten der Verantwortliche, der Auftragsverarbeiter und gegebenenfalls deren Vertreter auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Diese Mitwirkungspflicht stellt eine zentrale Voraussetzung für die Aufgabenerfüllung der Aufsichtsbehörden dar, da sie die Grundlage dafür schafft, dass datenschutzrechtlich relevante Sachverhalte und die damit einhergehenden Verarbeitungen umfassend und effektiv aufgeklärt und bewertet werden können. Gleichzeitig dient sie der Gleichbehandlung aller Verantwortlichen, da sie sicherstellt, dass sich niemand seiner Verantwortung durch mangelnde Kooperation entziehen kann.

Verletzt eine der in Art. 31 DSGVO genannten Personen oder Stellen ihre Mitwirkungspflicht, so kann die Aufsichtsbehörde gemäß Art. 83 Abs. 4 lit. a DSGVO in Verbindung mit Art. 31 DSGVO ein Bußgeld in Höhe von bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängen.

Wegen der zentralen Bedeutung der Mitwirkungspflicht für unsere Aufgabenerfüllung werden Verstöße von uns konsequent geahndet und als Bußgeldverfahren wegen der Verletzung der Mitwirkungspflicht geführt. Ein solches Bußgeld wurde durch die hiesige Behörde im Berichtszeitraum u.a. auch gegenüber der Inhaberin eines Immobilienmaklerbüros festgesetzt. Dem Bußgeldverfahren lag ein Verwaltungsverfahren zu Grunde, das wegen des Verdachts der unzulässigen Erhebung personenbezogener Daten von Wohnungsinteressentinnen und Wohnungsinteressenten gegen die Betroffene geführt wurde. Konk-

ret wurde vermutet, dass Wohnungsbesichtigungstermine lediglich unter der Voraussetzung angeboten wurden, dass die Interessentinnen und Interessenten vorab personenbezogene Unterlagen und Nachweise übersendeten, obwohl diese für die Durchführung der Wohnungsbesichtigung nicht erforderlich waren.

Die verantwortliche Stelle wurde zunächst aufgefordert, die zur Aufklärung des Sachverhalts notwendigen Auskünfte zu erteilen, wobei sie auf ihre Mitwirkungspflicht nach Art. 31 DSGVO hingewiesen wurde. Nachdem diese Aufforderung gänzlich unbeantwortet blieb, wurde nach ordnungsgemäßer Anhörung schließlich eine Anordnung gemäß Art. 58 Abs. 1 lit. a DSGVO erlassen, mittels derer die verantwortliche Stelle zur Sachverhaltsermittlung zur Erteilung der erforderlichen und in der Anordnung näher bezeichneten Auskünfte verpflichtet wurde. Trotz dieser Anordnung verweigerte die verantwortliche Stelle weiterhin jede Mitwirkung und erteilte keine Auskünfte.

Die verantwortliche Stelle hat durch die Verweigerung der Auskunftserteilung ihre Verpflichtung aus Art. 31 DSGVO verletzt. Diese Verpflichtung entsteht für die in Art. 31 DSGVO genannten Stellen sobald eine Anfrage der Aufsichtsbehörde vorliegt, die mit der Erfüllung ihrer gesetzlichen Aufgaben verbunden ist.[99] Die Landesbeauftragte für Datenschutz und Informationsfreiheit kontrolliert als zuständige Landesaufsichtsbehörde für den Bereich des Datenschutzes im nicht öffentlichen Bereich gemäß § 16 Abs. 1 Nr. 2 SDSG in Verbindung mit § 40 BDSG und Art. 57 ff. DSGVO die Ausführung der Vorschriften des BDSG und der DSGVO sowie anderer Vorschriften über den Datenschutz. Somit oblag es ihr auch im vorliegenden Fall die notwendigen Ermittlungen durchzuführen, ob und in welcher Art und Weise eine Datenverarbeitung durch die Betroffene bezüglich ihrer Mietinteressentinnen und -interessenten vorgenommen wird. Bereits das erste Schreiben der Behörde stellte eine

[99] Ehmann/Selmayr/Raum DS-GVO Art. 31 Rn. 6.

rechtsverbindliche Anfrage dar, die die Mitwirkungspflicht nach Art. 31 DSGVO auslöste.

Da die hiesige Behörde keine Hinderungsgründe feststellen konnte, die der Erfüllung der Mitwirkungspflicht durch die Betroffene entgegenstanden, wurde nach Durchführung eines Ordnungswidrigkeitsverfahrens ein Bußgeld wegen der Verletzung dieser Pflicht gegen die verantwortliche Stelle verhängt.

Fazit

Gemäß Art. 31 DSGVO besteht für Verantwortliche, Auftragsverarbeiter und gegebenenfalls deren Vertreter eine Mitwirkungspflicht, die für die Aufgabenerfüllung der Datenschutzaufsichtsbehörden zentral ist. Verletzt daher eine der genannten Personen oder Stellen diese Pflicht, so kann es zur Verhängung eines Bußgelds kommen.

Die Pflicht zur Mitwirkung aus Art. 31 DSGVO erlischt allerdings weder durch die Verhängung noch durch die Zahlung eines Bußgelds, sodass die Betroffene weiterhin zur Erteilung erforderlicher Auskünfte verpflichtet blieb.

11.2 Veröffentlichungen in sozialen Medien

Im Berichtszeitraum führten mehrere Fälle unbefugter Veröffentlichungen von Foto- und Videomaterial durch Privatpersonen in sozialen Netzwerken wie Facebook, Snapchat und TikTok zu datenschutzrechtlichen Verfahren. Die veröffentlichten Inhalte waren dabei jeweils in dienstlichen oder beruflichen Kontexten mit privaten mobilen Endgeräten aufgezeichnet worden.

In einem Fall fertigte die Mitarbeiterin einer Gemeinde mit ihrem Mobiltelefon Fotos eines neu beantragten Personalausweises einer Bürgerin an und veröffentlichte diese anschließend auf Facebook. Auf den Aufnahmen waren sämtliche personenbezogenen Ausweisdaten, darunter das Lichtbild, der Name, das Geburtsdatum und die Anschrift der Antragsstellerin erkennbar.

Ein weiteres Verfahren betraf eine Pflegekraft, die während einer Nachtschicht in einer Pflegeeinrichtung einen öffentlichen Livestream über TikTok mit einer Kollegin außerhalb der Einrichtung übertrug. Während des Livestreams wurden die Namen von Heimbewohnern, die der Angehörigen und weiteren Mitarbeitenden genannt sowie medizinische Diagnosen und Indikationen einzelner Bewohner offengelegt.

Diese Vorfälle in Form der unbefugten Weitergabe personenbezogener Daten an einen unbegrenzten Empfängerkreis verstießen gegen die Datenschutz-Grundverordnung (DSGVO). Die Datenverarbeitung erfolgte ohne eine Rechtsgrundlage und stellte zudem einen Verstoß gegen das Verarbeitungsverbot aus Art. 9 Abs. 1 DSGVO dar. Gemäß Art. 9 DSGVO ist die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie die Verarbeitung genetischer und biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person, von Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung nur unter sehr engen Voraussetzungen zulässig. Dies liegt darin begründet, dass durch die Verarbeitung derart sensibler Daten erhebliche Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen auftreten können.[100]

Hinsichtlich der Veröffentlichung der Fotoaufnahme des Personalausweises handelte es sich insbesondere um die Preisgabe biometrischer Daten nach Art. 9 Abs. 1 DSGVO. Die in dem zweiten Fall geschilderte Preisgabe von medizinischen Diagnosen und Indikation der einzelnen Heimbewohner wog auf Grund der Tatsache, dass diese Gesundheitsdaten i. S. v. Art. 9 Abs. 1 DSGVO darstellen, ebenfalls besonders schwer.

In beiden Fällen war daher bei der Entscheidung über die Verhängung der Geldbußen und deren Höhe nach Art 83. Abs. 2

[100] Albers/Veit, in: BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg (49. Ed. 01.08.2024), DSGVO Art. 9 Rn. 1-4.

lit. g DSGVO zu berücksichtigen, dass jeweils personenbezogene Daten besonderer Kategorien betroffen waren und es sich im Ergebnis somit um besonders schwerwiegende Verstöße handelte.

11.3 Datenerhebung im Rahmen eines Bargeschäftes

Beispielhaft für immer wieder vorkommende Datenschutzverstöße im Versand- und Einzelhandel ist folgende Sachverhaltskonstellation:

Im Rahmen eines Bargeschäfts erwarb eine Kundin in einem Elektronikfachmarkt ein Mobiltelefon.

Dabei wurde die Kundin beim Bezahlvorgang seitens eines Mitarbeiters aufgefordert, ihren Namen sowie Anschrift, Geburtsdatum, E-Mail-Adresse und Mobilfunknummer anzugeben. Diese Daten wurden von dem Mitarbeiter sodann in das Datenverarbeitungssystem des Fachmarkts eingegeben und dort gespeichert, wobei sich der Verkäufer gegenüber der Kundin hinsichtlich des Erfordernisses der Datenerhebung auf gesetzliche Vorgaben berief.

Eine Rechtsgrundlage für diese Datenverarbeitung war vorliegend jedoch nicht gegeben. Der Erhebung personenbezogener Daten im Rahmen eines Kaufvertrages bedarf es nach Art. 6 Abs. 1 lit. b DSGVO nur dann, wenn die Datenverarbeitung für die Erfüllung des Vertrages erforderlich ist. Dies ist jedoch bei einem Barverkauf, in dessen Rahmen die gegenseitigen vertraglichen Verpflichtungen (Übereignung des Telefons und Zahlung des Kaufpreises) unmittelbar erfüllt werden, nicht der Fall. Erforderlich gewesen wäre die Erhebung der o. g. personenbezogenen Daten beispielsweise nur bei gleichzeitigem Abschluss eines Mobilfunkvertrags oder einer Ratenzahlungsvereinbarung.

Nach Aussage der Unternehmensleitung im Rahmen des eingeleiteten Bußgeldverfahrens war die unrechtmäßige Erhebung der Daten darauf zurückzuführen, dass der Mitarbeiter in dem

Datenverarbeitungssystem versehentlich die Maske für Finanzierungsgeschäfte geöffnet hatte und davon ausging, das Ausfüllen der dort hinterlegten Felder sei erforderlich.

Dies konnte letztlich jedoch nicht verfangen, da dem Mitarbeiter die fehlende Erforderlichkeit der Datenerhebung hätte bewusst sein müssen und er im Zweifelsfall Rücksprache mit einem Vorgesetzten oder dem Datenschutzbeauftragten hätte halten müssen.

Es wurde daher gegen das Unternehmen ein Bußgeld verhängt.

Fazit

Mitarbeiter sollten sowohl bei der Übertragung rechtlich komplexer Aufgaben als auch im Rahmen von Alltagsgeschäften hinsichtlich datenschutzrechtlicher Belange sorgfältig und umfassend geschult sowie angewiesen werden, in Zweifelsfällen Rücksprache mit dem Vorgesetzten oder dem Datenschutzbeauftragten zu halten.

11.4 Melderegisterabfragen

Auch in diesem Berichtsjahr war unsere Dienststelle wieder mit unzulässigen Abfragen des Melderegisters durch Mitarbeiter des öffentlichen Dienstes befasst. Dabei erlangten wir in den meisten Fällen durch Datenpannenmeldungen der öffentlichen Stellen Kenntnis von den jeweiligen Datenschutzverstößen.

Ergeben sich aus einer solchen Datenpannenmeldung Anhaltspunkte, dass ein konkreter Mitarbeiter für die Datenschutzverletzung verantwortlich ist, weil dieser beispielsweise aus privaten Gründen in ihm zu dienstlichen Zwecken zur Verfügung stehenden Informationssystemen personenbezogene Daten abgerufen hat, wird unsererseits die Einleitung eines Bußgeldverfahrens gegen die verantwortliche Person geprüft.

In einem konkreten Fall hatte eine Person gemäß Art. 15 DSGVO i. V. m. §§ 10, 11 Bundesmeldegesetz (BMG) von ihrem Aus-

kunftsrecht zu den zu ihrer Person im Melderegister gespeicherten personenbezogenen Daten sowie auch zu den Empfängern dieser Daten Gebrauch gemacht. Nach Auskunfterteilung wunderte sich die auskunftssuchende Person über eine Datenabfrage ihrer Melderegisterdaten durch ein Jugendamt und bat dieses daher um Mitteilung, aus welchem Grund ihre Daten abgefragt worden seien.

Eine sich anschließende Datenschutzkontrolle des behördlichen Datenschutz-beauftragten des Jugendamtes ergab nach Auswertung der Protokolldaten, dass ein Mitarbeiter in einem Zeitraum von 21 Monaten zu 27 Personen im saarländischen Meldebestand und drei Personen bundesweit unbefugte Melderegisterabfragen ohne Angabe eines Aktenzeichens, ohne dienstlichen Anlass und demnach mutmaßlich aus rein persönlichem Interesse getätigt hatte.

§ 40 Abs. 1 Bundesmeldegesetz (BMG) regelt die Protokollierungspflichten beim automatisierten Abruf von Daten einer einzelnen Person zum Zweck der Datenschutzkontrolle als auch hieraus folgender Ordnungswidrigkeitenverfahren oder gar Strafverfahren. So hat der Gesetzgeber in § 40 Abs. 1 BMG konkret festgelegt, dass die Meldebehörde bei einer Personensuche im automatisierten Abruf und bei einer Datenbestätigung die abrufberechtigte Stelle, die abgerufenen Daten, den Zeitpunkt des Abrufs, das Aktenzeichen der abrufenden Behörde, den Anlass des Abrufs, die Kennung der abrufenden Person oder bei einem maschinellen Abruf die Bezeichnung des Verfahrens und schließlich die nach den Auswahldaten als abrufbar gekennzeichneten Datensätze der gefundenen Personen (Treffer) zu protokollieren hat.

Die zur Verfügung stehenden Protokolldaten belegten, dass der Betroffene mit seiner Benutzerkennung im Meldeportal von einem dienstlichen Computer zu 30 Personen Abfragen getätigt und dabei jeweils erfolgreiche Treffermeldungen erhalten hatte. Hierdurch erlangte er aufgrund der ihm für dienstliche Zwecke zugewiesenen Zugriffsberechtigungen weitere personenbezo-

gene Daten wie Doktorgrad, Name, Rufname, weitere Vornamen, Geburtsname, Geschlecht, Geburtsdatum, Geburtsort, Familienstand, Religion und die aktuelle Wohnanschrift mit Einzugs- und Anmeldedatum zu diesen Personen. Darüber hinaus hatte der Betroffene keine korrekten Angaben zum Abfrageanlass gemacht und kein nachvollziehbares Aktenzeichen angegeben.

Nach § 27 Abs. 1 Nr. 2 Saarländisches Datenschutzgesetz (SDSG) handelt ordnungswidrig, wer entgegen der Verordnung (EU) 2016/679, dem SDSG oder einer anderen Rechtsvorschrift zum Schutz personenbezogener Daten geschützte personenbezogene Daten, die nicht offenkundig sind, unbefugt abruft, sich oder einem anderen verschafft oder durch unrichtige oder unvollständige Angaben ihre Übermittlung an sich oder andere veranlasst.

Die Abfragen erfolgten unbefugt, da sie ohne Rechtsgrundlage, nicht für dienstliche Zwecke und aus rein privaten Gründen durchgeführt wurden. Durch die Recherchen im Melderegister war auch der Tatbestand des § 27 Abs. 1 Nr. 2 Alt. 1 (Abruf) erfüllt. Insbesondere handelt es sich bei den im Melderegister verpflichtend zu den Einwohnern gespeicherten personenbezogenen Daten nicht um offenkundige Daten, da der Zugriff auf diese Daten nach den gesetzlichen Regelungen des Bundesmeldegesetzes in Verbindung mit den Meldegesetzen der Länder nur bestimmten Stellen vorbehalten ist. Hinsichtlich des jeweils nicht korrekt eingegebenen Abfrageanlasses sowie auch der fehlenden Angabe eines nachvollziehbaren Aktenzeichens war ebenso der Tatbestand des § 27 Abs. 1 Nr. 2 Alt. 3 SDSG erfüllt, da die Übermittlungen der Daten durch unrichtige oder unvollständige Angaben veranlasst wurden.

Die dem Betroffenen zur Last gelegten Verstöße waren als nicht nur geringfügige Ordnungswidrigkeiten einzustufen, was auch bei der Bemessung der Geldbuße zu bewerten war.

11.5 Fehlversand von ärztlichen Rezepten

In regelmäßigen Abständen ist unsere Dienststelle Adressat unerwarteter Übermittlungen personenbezogener Daten – und das ausgerechnet per Fax. Besonders kurios gestalteten sich dabei Fälle, in denen ärztliche Rezepte, mitunter mehrfach, in unserem Faxgerät landeten. Der Grund? Die tückischen Täuschungen der Online-Suchmaschinen.

Wer heute im Internet nach der Faxnummer einer bestimmten Praxis oder Apotheke sucht, kann leicht auf unsere Kontaktdaten stoßen. Dies liegt daran, dass zahlreiche Unternehmen und medizinische Einrichtungen in ihren Datenschutzerklärungen pflichtbewusst auf uns als zuständige Aufsichtsbehörde verweisen. Unsere dort veröffentlichten Kontaktdaten werden von den Suchmaschinen dann oftmals fälschlicherweise als Kontaktinformationen des betroffenen Unternehmens interpretiert und dargestellt. Eine oberflächliche Recherche kann so fatale Folgen haben: Ein Rezept wird nicht an die richtige Apotheke, sondern an das Unabhängige Datenschutzzentrum gesandt – ein Fall von Datenschutzironie in Reinform.

Besondere Brisanz erhält das Geschehen, wenn Gesundheitsdaten im Sinne des Art. 9 DSGVO betroffen sind. Während unsere Dienststelle sonst eher mit den Regelungen der Datenschutz-Grundverordnung und weniger mit konkreten Medikationsplänen zu tun hat, wuchs hier unfreiwillig unser Wissen über gängige Arzneimittelverordnungen.

In den meisten Fällen bleibt es bei einem wohlwollenden Hinweis an die absendende Stelle – immerhin kann ein einmaliger Irrtum jedem passieren. Doch im Jahr 2024 sah sich unsere Dienststelle gezwungen, ein Bußgeldverfahren einzuleiten. Der Grund: Hartnäckige Wiederholungstäter.

Nach dem Eingang eines fehlversandten Rezepts nahm unsere Dienststelle pflichtbewusst Kontakt mit der betroffenen Arztpraxis auf und wies freundlich auf den Fehler hin – auch, um sicherzustellen, dass der Patient sein Medikament zeitnah er-

hält. Die Reaktion am nächsten Tag? Das gleiche Rezept trudelte erneut per Fax bei uns ein. Ein weiteres Telefonat folgte – mit der klaren Bitte um Korrektur. Noch am selben Tag erreichte uns ein weiteres Rezept dieser Praxis, diesmal für einen anderen Patienten.

Die Faxübermittlung der Rezepte umfasste nicht nur Namen, Anschrift und Geburtsdatum der Patienten, sondern auch die Bezeichnung des verordneten Medikaments – mithin eine Offenlegung besonderer Kategorien personenbezogener Daten gemäß Art. 4 Nr. 2 i. V. m. Art. 9 Abs. 1 DSGVO. Eine Rechtsgrundlage für diese Form der Übermittlung war nicht ersichtlich – insbesondere lag keine Einwilligung der betroffenen Patienten zur Versendung an unsere Dienststelle vor.

Während sich viele ähnlich gelagerte Datenschutzverstöße oft mit Unkenntnis oder Nachlässigkeit erklären lassen, war in diesem Fall zumindest in den zwei Wiederholungsfällen grobe Fahrlässigkeit gegeben. Die Folge: Ein Bußgeld wurde verhängt – und wir können nur hoffen, dass sich die künftige Rezeptverteilung wieder auf den medizinisch vorgesehenen Weg begibt.

Für die Zukunft empfehlen wir medizinischen Einrichtungen neben der sorgfältigen Überprüfung der Faxnummer vor dem Versand auch eine grundsätzliche Überlegung: Ist Fax im Jahr 2024 noch das Mittel der Wahl für die Übermittlung sensibler Gesundheitsdaten? Mit der Einführung des E-Rezepts steht jedenfalls seit Januar 2024 in vielen Fällen eine sichere und effiziente Alternative zur Verfügung, die solche Fehlübermittlungen von vornherein ausschließt.

11.6 Akteneinsichtsrecht des Geschädigten

Gemäß § 406e StPO i. V. m. § 46 Abs. 1 OWiG kann der durch eine Ordnungswidrigkeit Verletzte selbst oder durch einen beauftragten Rechtsanwalt unter bestimmten Voraussetzungen Einsicht in Akten eines Bußgeldverfahrens beantragen. Dies schließt auch die Möglichkeit ein, amtlich verwahrte Beweisstücke zu besichtigen.

Im Berichtszeitraum erhielt die hiesige Behörde einen entsprechenden Antrag auf Akteneinsicht in einem Bußgeldverfahren, das zuvor nach § 46 Abs. 1 OWiG i. V. m. § 170 Abs. 2 StPO aus tatsächlichen Gründen wegen fehlenden Tatverdachts eingestellt worden war. Der Antragsteller hatte sich ursprünglich mit der Behauptung an unsere Behörde gewandt, durch die Verarbeitung seines ehemaligen Arbeitgebers in seinen Rechten verletzt zu sein. Die Ermittlungen mündeten später in ein Bußgeldverfahren.

Nach den Voraussetzungen des § 406 e StPO i. V. m. § 46 Abs. 1 OWiG kann dem Verletzten einer Ordnungswidrigkeit lediglich dann Einsicht in die Akten gewährt werden, wenn dieser ein schutzwürdiges rechtliches, wirtschaftliches oder ideelles Interesse schlüssig vorträgt und keine Versagungsgründe, wie beispielsweise ein überwiegendes schutzwürdiges Interesse des Betroffenen oder anderer Personen entgegenstehen.

Zwar trug der Antragsteller im Rahmen der Antragstellung vor, ein berechtigtes Interesse zu haben, da er die Akteneinsicht zur Überprüfung und gegebenenfalls zur Geltendmachung eines zivilrechtlichen Anspruchs gegen den Betroffenen benötige, allerdings standen dem Interesse des Antragstellers überwiegende schutzwürdige Interessen des Betroffenen entgegen. Der Antrag auf Akteneinsicht in die verfahrensgegenständliche Bußgeldakte war daher durch die hiesige Behörde abzulehnen.

Insbesondere stand dem Akteneinsichtsrecht vorliegend das grundrechtlich geschützte Recht des Betroffenen auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. Abs. 1 GG[101] entgegen. Dieses war nach vorgenommener Interessenabwägung gegenüber dem Anliegen des Antragstellers auf Einsichtnahme der Akten zur Überprüfung und Geltendmachung schadenersatzrechtlicher Ansprüche, als überwiegendes Interesse zu qualifizieren.

[101] BVerfG, Beschluss vom 26.10.2006 – 2 BvR 67/06.

Ein wichtiges Kriterium bei der Abwägung der widerstreitenden Interessen des Antragstellers und des Betroffenen ist dabei die Stärke des Tatverdachts hinsichtlich der verfahrensgegenständlichen Ordnungswidrigkeit.[102] In dem vorliegenden Fall wurde das Verfahren gegen den Betroffenen gerade deswegen eingestellt, weil ein hinreichender Tatverdacht nach dem Abschluss der Ermittlungen nicht bestand. Demgegenüber handelt es sich bei der Einsichtnahme in die Ermittlungsakte um einen erheblichen Eingriff in die Rechte des Betroffenen, insbesondere in dessen Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG. Weiterhin war zu beachten, dass dem Antragsteller die zur Überprüfung und gegebenenfalls zur Geltendmachung eines zivilrechtlichen Anspruchs erforderlichen Unterlagen im Wesentlichen bereits vorlagen und im Übrigen in einer für die Rechte des Betroffenen weniger eingriffsintensiven Art und Weise hätten beschafft werden können.

Dem Antragsteller wurde daher mitgeteilt, dass ihm ein Zugang zu der verfahrensgegenständlichen Bußgeldakte wegen überwiegender schutzwürdiger Interessen des Betroffenen nicht gewährt werden kann.

[102] LG Saarbrücken, Beschluss vom 2. 7. 2009 - 2 Qs 11/09, KK-StPO/Zabeck, 9. Aufl. 2023, StPO § 406e Rn. 5-8.

Anlagenverzeichnis

AsylG – Asylgesetz in der Fassung der Bekanntmachung vom 2. September 2008 (BGBl. I S. 1798), zuletzt geändert durch Artikel 2 des Gesetzes vom 25. Oktober 2024 (BGBl. 2024 I Nr. 332).

ATDG – Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz) vom 22. Dezember 2006 (BGBl. I S. 3409), zuletzt geändert durch Artikel 2 Absatz 1 des Gesetzes vom 30. März 2021 (BGBl. I S. 402).

AufenthG – Aufenthaltsgesetz in der Fassung der Bekanntmachung vom 25. Februar 2008 (BGBl. I S. 162), zuletzt geändert durch Artikel 3 des Gesetzes vom 25. Oktober 2024 (BGBl. 2024 I Nr. 332).

BGB – Bürgerliches Gesetzbuch: in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Art. 14 Viertes BürokratieentlastungsG vom 23.Oktober 2024 (BGBl. 2024 I Nr. 323)

DSGVO – Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 04.05.2016, S. 1 - 88).

Eurodac-VO – Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (Neufassung) (ABl. L 180 vom 29.06.2013, S. 1 - 30).

JI-Richtlinie – Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABs. L 119 vom 04.05.2016, S. 89 - 131).

KHG – Gesetz zur wirtschaftlichen Sicherung der Krankenhäuser und zur Regelung der Krankenhauspflegesätze (Krankenhausfinanzierungsgesetz) in der Fassung der Bekanntmachung vom 10. April 1991 (BGBl. I S. 886)

KHSFV – Verordnung zur Verwaltung des Strukturfonds im Krankenhausbereich (Krankenhausstrukturfonds-Verordnung): Vom 17. Dezember 2015 (BGBl. I S. 2350), zuletzt geändert durch Art. 4a KrankenhausversorgungsverbesserungsG vom 5.Dezember 2024 (BGBl. 2024 I Nr. 400)

KHZG – Gesetz für ein Zukunftsprogramm Krankenhäuser (Krankenhauszukunftsgesetz): Vom 23. Oktober 2020 (BGBl.I S. 2208), zuletzt geändert durch Art. 3d G zur Stärkung des Schutzes der Bevölkerung und insbesondere vulnerabler Personengruppen vor COVID-19 vom 16. September 2022 (BGBl. I S. 1454)

KI-VO – Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz)

MRVG – Gesetz Nr. 1257 über den Vollzug von Maßregeln der Besserung und Sicherung in einem psychiatrischen Krankenhaus und einer Entziehungsanstalt (Maßregelvollzugsgesetz) vom 29. November 1989 (Amtsbl. I S. 81), zuletzt geändert durch Gesetz vom 16. Mai 2007 (Amtsbl. S. 1226).

PBeaKKBhLÜbV SL – Verordnung zur Übertragung der Gewährung von Beihilfen im Landesbereich auf die Postbeamtenkrankenkasse: Vom 10. Oktober 2023 (Amtsbl. I S. 993)

RED-G – Gesetz zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus (Rechtsextremismus-Datei-Gesetz) vom 20. August 2012 (BGBl. I S. 1798), zuletzt geändert durch Artikel 2 Absatz 2 des Gesetzes vom 30. März 2021 (BGBl. I S. 402).

SAWG – Saarländisches Abfallwirtschaftsgesetz vom 26. November 1997 (Amtsbl. I S. 1352), zuletzt geändert durch Artikel 170 des Gesetzes vom 8. Dezember 2021 (Amtsbl. I S. 2629).

SBG – Saarländisches Beamtengesetz: Vom 11. März 2009 (Amtsbl. S. 514), zuletzt geändert durch Art. 2 G Nr. 2135 vom 24. April 2024 (Amsbl. I S. 354)

Schulw-DSG SL – Gesetz über den Schutz personenbezogener Daten im Schulwesen (Schulwesen-Datenschutzgesetz) vom 10. Juli 2024 (Amtsbl. I S 570)

Schulw-DSV SL – Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Schulwesen(Schulwesen-Datenschutzverordnung) vom 19. August 2024 (Amtsbl. I S. 624)

SDSG – Saarländisches Datenschutzgesetz vom 16. Mai 2018 (Amtsbl. I S. 254), zuletzt geändert durch Artikel 85 des Gesetzes vom 8. Dezember 2021 (Amtsbl. I S. 2629).

SGB X – Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130)

SKRG – Saarländisches Krebsregistergesetz: Vom 11. Februar 2015; letzte berücksichtigte Änderung: mehrfach geändert, § 13e neu eingefügt durch Artikel 1 des Gesetzes vom 12. Dezember 2023 (Amtsbl. I S. 88)

SPolDVG – Saarländisches Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei vom 6. Oktober 2020 (Amtsbl. I S. 1133), zuletzt geändert durch Artikel 1 des Gesetzes vom 19. Februar 2025 (Amtsbl. I S. 332).

SRettG – Saarländisches Rettungsdienstgesetz: Vom 11. November 2020 in der Fassung der Bekanntmachung vom 10. Dezember 2020 (Amtsbl. S. 1250)

TTPW-VO – Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates vom 13. März 2024 über die Transparenz und das Targeting politischer Werbung

VwGO – Verwaltungsgerichtsordnung in der Fassung der Bekanntmachung vom 19. März 1991 (BGBl. I S. 686), zuletzt geändert durch Artikel 5 des Gesetzes vom 24. Oktober 2024 (BGBl. 2024 I Nr. 328).

WaffG – Waffengesetz vom 11. Oktober 2002 (BGBl. I S. 3970, 4592; 2003 I S. 1957), zuletzt geändert durch Artikel 5 des Gesetzes vom 25. Oktober 2024 (BGBl. 2024 I Nr. 332).

WaffRG – Gesetz über das Nationale Waffenregister (Waffenregistergesetz) vom 17. Februar 2020 (BGBl. I S. 166, 184).