Die Landesbeauftragte für
Datenschutz und Informationsfreiheit

34. Tätigkeitsbericht Datenschutz

UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

2025

Unabhängiges Datenschutzzentrum Saarland
Die Landesbeauftragte für Datenschutz und Informationsfreiheit
Fritz-Dobisch-Straße 12
66111 Saarbrücken

Tel.: 0681.94781-0
Fax: 0681.94781-29
poststelle@datenschutz.saarland.de

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

34. Tätigkeitsbericht

der Landesbeauftragten
für Datenschutz
und Informationsfreiheit

Berichtszeitraum 2025

Dem Landtag und der Landesregierung
vorgelegt am 18. März 2026
(Landtagsdrucksache 17/1987)

ABBILDUNGSVERZEICHNIS

Vorwort

Der 34. Tätigkeitsbericht meiner Behörde blickt auf ein Jahr zurück, in dem auf dem Datenschutzrecht wie selten zuvor erheblicher Druck lastete. Unter dem Schlagwort „Bürokratieabbau" forderten Stimmen aus Wirtschaft und Politik den ihrer Ansicht nach überbordenden Datenschutz einzuhegen, um der (Digital-)Wirtschaft endlich Innovationen zu ermöglichen. Regulatorische Anpassungen, die die Pflichten für datenverarbeitende Stellen mit Blick auf Risiken bei der Verarbeitung skalieren und die Verfahren effizienter gestalten, ohne dabei jedoch das Grundrecht auf Schutz personenbezogener Daten einzugrenzen, sind zweifelsohne zu befürworten; ob dies mit dem am Ende des Berichtszeitraums von der EU-Kommission vorgeschlagenen Digitalomnibus und der damit geplanten Novellierung der Datenschutz-Grundverordnung gelingen wird, ist zum jetzigen Zeitpunkt jedoch zu bezweifeln.

Der erheblichen Kritik an dem datenschutzrechtlichen Regelungsrahmen und den sich für datenverarbeitende Stellen ergebenden Pflichten steht die seit Geltungseintritt der Datenschutz-Grundverordnung im Jahr 2018 bisher höchste Zahl von an meine Behörde adressierten Beschwerden und Meldungen von Datenschutzverletzungen gegenüber. Diese Entwicklung ist grundsätzlich sehr begrüßenswert, als sie ein zunehmendes Bewusstsein für Rechte und Bedingungen bei der Verarbeitung personenbezogener Daten deutlich werden lässt. Allerdings erhöht sich damit auch der auf meiner Behörde lastende Vollzugsdruck, den berechtigten Erwartungen nach einer sachgerechten Befassung mit Belangen einer immer größer werdenden Zahl von beschwerdeführenden Bürgerinnen und Bürgern sowie meldenden Unternehmen und Behörden gerecht zu werden. Unter Berücksichtigung nahezu unveränderter Ressourcen führen die steigenden Fallzahlen und eine Zunahme der Komplexität der Verfahren jedoch dazu, dass berechtigte Anliegen von Betroffenen und Ratsuchenden nur verzögert oder in reduziertem Umfang bearbeitet werden können, was letztlich die Gefahr eines Vertrauensverlustes in die Wirksamkeit der Aufsichtsstrukturen mit sich bringt.

Aufgrund der Fokussierung auf die zwingend gebotene Bearbeitung von Beschwerden und Meldungen von Datenschutzverletzungen sind proaktive Prüfungen, präventive Kontrollen oder strategische Schwerpunktsetzungen nicht oder allenfalls noch sehr eingeschränkt möglich. Angesichts einer immer weiter fortschreitenden Digitalisierung und dem zunehmenden Einsatz von Anwendungen der Künstlichen Intelligenz sind jedoch solche Untersuchungen ebenso wie eine frühzeitige beratende Begleitung bei der Umsetzung digitaler Prozesse essentiell; während durch die individuell vorgetragene Beschwerde strukturelle Fehlentwicklungen erst im Nachgang ersichtlich werden, können vorgelagerte Untersuchungs- und Prüfhandlungen dem Vorfeldschutz der Datenschutzrechte einer Vielzahl potenziell betroffener Personen dienen.

Die rasanten technologischen Entwicklungen, bei denen immer größere Datenmengen verarbeitet werden, lassen die Anforderungen an den Datenschutz auch in Zukunft nicht geringer werden. Werden notwendige Schutzmaßnahmen für die verarbeiteten personenbezogenen Daten nicht ergriffen, kann dies sehr schnell Datenschutzverletzungen zur Folge haben. Damit können nicht nur unmittelbare finanzielle Risiken, sondern auch Reputationsverluste für die verantwortlichen Stellen und auch gravierende Gefahren und Schäden für die Betroffenen verbunden sein. Eine „Entbürokratisierung", die die Pflichten der Datenverarbeiter pauschal reduziert und dadurch das Datenschutzniveau absenkt, gefährdet die Grundrechte der Bürgerinnen und Bürger und untergräbt letztlich das Vertrauen in die Digitalisierung. Der laufende Reformprozess muss daher verantwortungsvoll fortgeführt werden und darf nicht unter dem falsch verstandenen Leitbild „Bürokratieabbau" zu einer Aushöhlung des Datenschutzes führen.

Dies gilt auch mit Blick auf die Bestrebungen auf nationaler Ebene, wesentliche Zuständigkeiten und Kompetenzen im Bereich der Datenschutzaufsicht künftig bei der Bundesbeauftragten für den Datenschutz zu bündeln. An der steigenden Zahl von an meine Behörde adressierten Belangen und

der Vielzahl an Kontakten mit ratsuchenden Personen und Stellen aus dem Saarland, die außerhalb einer statistischen Erfassung das Alltagsgeschäft maßgeblich prägen, lässt sich nicht nur eine gestiegene Sensibilität für datenschutzrechtliche Themen, sondern auch die Wertschätzung einer ortsnahen Kontaktmöglichkeit ablesen. Während die Gewährleistung einer niedrigschwelligen Erreichbarkeit den Dialog zwischen Bürgerinnen und Bürgern, Rechtsanwendern und Aufsicht im Saarland entscheidend stärkt, dürften von einer Zentralisierung gegenteilige Effekte ausgehen.

Mit dem vorliegenden Bericht soll dem Landtag, der Landesregierung und der Öffentlichkeit ein Überblick über die vielfältigen an unsere Behörde gerichteten Datenschutzthemen des vergangenen Jahres gegeben werden – von Alltagsfragen bis hin zu komplexen Digitalisierungsprojekten.

Mein besonderer Dank gilt meinen Mitarbeiterinnen und Mitarbeitern, die trotz deutlich gestiegener Arbeitsbelastung mit großem Engagement und hoher fachlicher Expertise zur Erfüllung unserer gesetzlichen Aufgaben beitragen.

Saarbrücken, im März 2026

Monika Grethel

Landesbeauftragte für Datenschutz
und Informationsfreiheit

ZAHLEN UND FAKTEN

1. ZAHLEN UND 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, die Parlamente und die Regierungen 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

Diese Darstellung bietet einen Überblick über die Anzahl der eingegangenen Beschwerden im Berichtszeitraum. Als Beschwerden gelten ausschließlich schriftliche Eingaben, in denen eine natürliche Person ihre persönliche Betroffenheit schildert. Hinweise oder Anregungen zu möglichen datenschutzrechtlichen Verstößen, die an die Behörde herangetragen werden, werden nicht in die Statistik aufgenommen, sofern sie nicht in schriftlicher Form vorliegen und zu weiteren Maßnahmen führen. Gleiches gilt für (fern) mündlich vorgetragene Beschwerden – diese finden nur dann Eingang in die Statistik, wenn sie dokumentiert werden und Anlass zu weitergehenden behördlichen Schritten geben.

Im Berichtsjahr 2025 lag die Zahl der Beschwerdeverfahren mit insgesamt 783 deutlich über dem Niveau des Vorjahres (2024: 565).

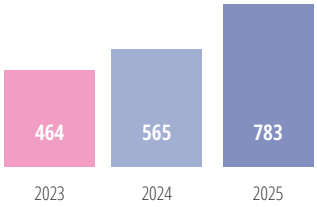


Abbildung 1: Entwicklung der Beschwerdezahlen 2023–2025

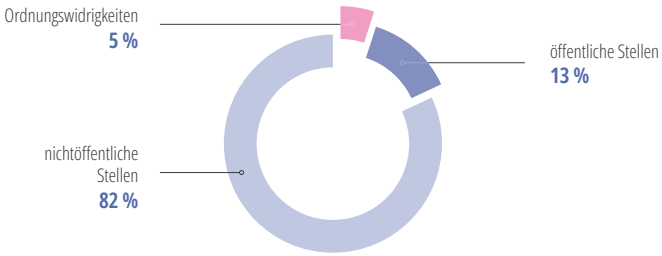


Abbildung 2: Beschwerden (Aufteilung) 2025

1.2 Beratungen

Diese Übersicht zeigt die Anzahl der schriftlichen Beratungen. Erfasst werden Beratungen von Verantwortlichen, betroffenen Personen sowie der Landesregierung. (Fern-)mündliche Beratungen werden statistisch nicht berücksichtigt, obwohl sie einen erheblichen Anteil der an unsere Behörde gerichteten Anfragen ausmachen und mit einem hohen zeitlichen Aufwand verbunden sind.

Die Anzahl an Beratungsverfahren im Jahr 2025 beträgt 272 (2024: 264).

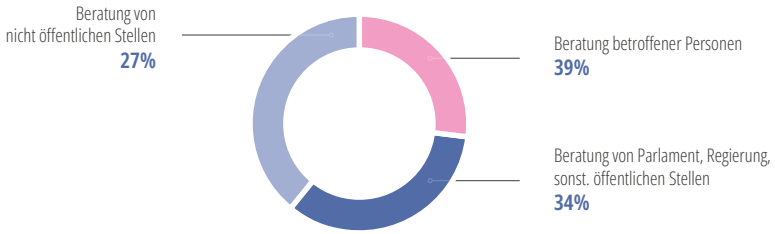


Abbildung 3: Beratungen (Aufteilung) 2025

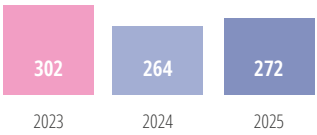


Abbildung 4: Entwicklung der Beratungsverfahren 2023–2025

1.3 Meldungen von Datenschutzverletzungen

Diese Übersicht zeigt, wie viele schriftliche Mitteilungen Verantwortlicher zu Datenschutzverletzungen gemäß Artikel 33 DSGVO eingegangen sind.

Hier ist im Berichtsjahr ein Zuwachs von 885 Meldungen im Jahr 2024 auf 913 Meldungen im Jahr 2025 festzustellen.

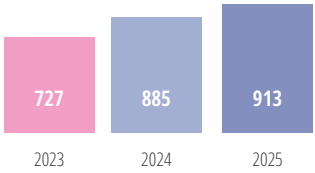


Abbildung 5: Meldungen von Datenschutzverletzungen 2023–2025

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 auf unsere Hinweise 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.

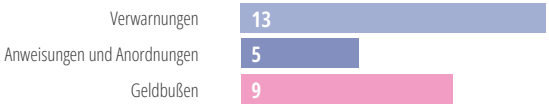


Abbildung 6: Abhilfemaßnahmen 2025

1.5 Europäische Verfahren

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

Die DSGVO enthält 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.

Zu diesem Zweck hatte auch das UDZ im Jahr 2025 in insgesamt 854 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 7 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 war das UDZ zudem in insgesamt 1579 Fällen an Verfahren gem. Kapitel VII (Zusammenarbeit und Kohärenz) beteiligt. 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

In diesem Bereich werden die Stellungnahmen aufgeführt, die von Parlament und Regierung zu Gesetzgebungsvorhaben angefordert und durch unsere Dienststelle erstellt wurden. Jedes Vorhaben wird einmalig statistisch erfasst, unabhängig davon, ob die Stellungnahmen gegenüber unterschiedlichen Instanzen in verschiedenen Stadien des Verfahrens abgegeben werden. Bei Gesetzgebungsverfahren erfolgt unsere Beteiligung häufig bereits während der ressortinternen Entwurfsphase, anschließend im Zuge

externer Anhörungen sowie abschließend im Rahmen der parlamentarischen Anhörung im Landtag.

Im Berichtzeitraum wurde das Unabhängige Datenschutzzentrum Saarland hiernach in neun Rechtsetzungsvorhaben verfahrensbegleitend tätig.

1.7 Gerichts- und Bußgeldverfahren

Im Jahr 2025 führte das Unabhängige Datenschutzzentrum insgesamt sechs Gerichts- und 63 Bußgeldverfahren.

1.8 Presseanfragen

Im Jahr 2025 wurden insgesamt 31 Presseanfragen an hiesige Dienststelle gerichtet.

RECHTSETZUNGSVERFAHREN

2. RECHTSETZUNGS-VERFAHREN

2.1 Elektronische Aufenthaltsüberwachung

Im Berichtszeitraum konnten wir zu einem Gesetzgebungsvorhaben Stellung nehmen, das die elektronische Aufenthaltsüberwachung auf Fälle häuslicher Gewalt ausweiten sollte (LT-Drs. 17/1282). Ziel des Vorhabens war es nach der Gesetzesbegründung, den Schutz gefährdeter Personen auf Landesebene zu stärken und damit – zeitlich vorgelagert gegenüber einer möglichen Reform des Gewaltschutzrechts auf Bundesebene – zusätzliche Instrumente der Gefahrenabwehr bereitzustellen. Gerade im Kontext häuslicher Gewalt besteht ein erhebliches Schutzbedürfnis: Gefährdungslagen können sich dynamisch entwickeln, Annäherungs- und Kontaktverbote werden nicht immer eingehalten, und eine effektive Durchsetzung von Schutzmaßnahmen ist für die Betroffenen von zentraler Bedeutung. Gleichzeitig handelt es sich bei der elektronischen Aufenthaltsüberwachung um eine Maßnahme, die aufgrund ihrer technischen Funktionsweise zu einer dauerhaften, hochintensiven Verarbeitung personenbezogener Daten führt und damit datenschutz- und grundrechtlich besonders sorgfältig zu begründen und auszugestalten ist.

Bei der elektronischen Aufenthaltsüberwachung wird eine Person verpflichtet, ein technisches Gerät zur Aufenthaltsbestimmung dauerhaft und in betriebsbereitem Zustand am Körper zu führen. Die umgangssprachlich als „elektronische Fußfessel" bezeichnete Technik erhebt fortlaufend Positionsdaten und übermittelt diese an die für die Überwachung zuständige Stelle. Je nach Ausgestaltung der Systeme können zusätzlich Ereignis- und Statusdaten anfallen (z. B. Manipulations- oder Ausfallmeldungen). In der Praxis erlaubt die Maßnahme damit nicht nur punktuelle Kontrollen, sondern die kontinuierliche Feststellung, wo sich eine Person aufhält und – bei entsprechenden Auswertefunktionen – auch, wie sie sich über die Zeit bewegt. Diese Eingriffsqualität unterscheidet die elektronische Aufenthaltsüberwachung deutlich von weniger invasiven Kontrollinstrumenten.

Im Regelfall wird ausschließlich die zu überwachende Person mit einem Überwachungsgerät ausgestattet. Technisch können geografisch definierte Bereiche festgelegt werden, die nicht betreten oder nicht verlassen werden dürfen („Geofencing"), etwa zum Schutz der gefährdeten Person oder zur Durchsetzung behördlicher Auflagen. Bei Zuwiderhandlungen (z. B. Überschreiten einer festgelegten Grenze) kann ein Alarm ausgelöst und die Polizei informiert werden. Die Maßnahme ist damit auf den Primärzweck ausgerichtet, Aufenthaltsweisungen effektiv kontrollierbar zu machen und Verstöße frühzeitig zu erkennen. Datenschutzrechtlich ist hierbei hervorzuheben, dass bereits die Datenerhebung selbst – unabhängig davon, ob es zu einem konkreten Alarm kommt – eine fortlaufende Erfassung von Standortdaten bedeutet.

Eine Sonderkonstellation stellt das sogenannte „spanische Modell" dar. Dabei wird nicht nur die mutmaßlich gewaltausübende Person verpflichtet, ein entsprechendes Gerät zu führen; auch die gefährdete Person kann auf eigenen Wunsch hin mit einem Sender bzw. Endgerät ausgestattet werden. Durch einen Abgleich der jeweiligen Gerätepositionen lassen sich Annäherungen ortsunabhängig erkennen. Dies kann in Konstellationen Vorteile bieten, in denen starre geografische Verbotszonen weder praktikabel noch hinreichend wirksam sind, etwa wenn die gefährdete Person ihren Aufenthaltsort wechseln muss oder bestimmte Orte nicht dauerhaft meiden

kann. Gleichwohl wirft dieses Modell zusätzliche datenschutzrechtliche Fragen auf: Es betrifft eine weitere Person, die zwar nicht Adressatin der Anordnung ist, aber deren Datenverarbeitung – je nach Systemarchitektur – ebenfalls laufend ausgelöst wird. Besonders wichtig ist daher, dass Freiwilligkeit, informierte Entscheidung sowie der Schutz vor sekundären Risiken (z. B. unbeabsichtigte Offenlegung von Aufenthaltsorten) hinreichend berücksichtigt werden.

Seit Inkrafttreten des Saarländischen Gesetzes über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG) im Jahr 2020 verfügt die saarländische Polizei nach § 38 SPolDVG bereits über die Befugnis, Maßnahmen zur elektronischen Aufenthaltsüberwachung anzuordnen. Dies ist grundsätzlich auch unabhängig von einer gerichtlichen Anordnung nach dem Gewaltschutzgesetz möglich. Die im Jahr 2024 eingebrachte und im Berichtsjahr im Ausschuss diskutierte Überarbeitung des § 38 SPolDVG sollte die Anwendungsmöglichkeiten ausweiten und zugleich einzelne Regelungsaspekte präzisieren. Vorgesehen war, die Anordnung einer elektronischen Aufenthaltsüberwachung bereits bei sich konkretisierenden Gefährdungslagen zu ermöglichen. Als Beispiel nannte der Entwurf insbesondere Konstellationen, in denen Straftaten gegen die sexuelle Selbstbestimmung zu erwarten sind. Zudem sollte die Maßnahme nicht nur bei Aufenthaltsverboten, sondern auch bei Wohnungsverweisungen, Rückkehrverboten, Kontaktverboten und Aufenthaltsgeboten in Betracht kommen. Eine ausdrückliche Rechtsgrundlage für das „spanische Modell" war – entgegen der Gesetzesbegründung – zunächst nicht vorgesehen.

Im Rahmen der Ausschussanhörung haben wir zu dem Entwurf Stellung genommen. Ausgangspunkt unserer Bewertung war, dass der Einsatz einer elektronischen Aufenthaltsüberwachung, die eine dauerhafte Erfassung des Aufenthaltsortes ermöglicht, einen gewichtigen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt.

Standortdaten sind besonders aussagekräftig: Sie können Rückschlüsse auf Lebensgewohnheiten, soziale Kontakte, Bewegungsprofile, religiöse oder gesundheitliche Bezüge (etwa bei Besuchen bestimmter Einrichtungen)

zulassen und damit weit über den unmittelbaren Zweck einer Aufenthaltskontrolle hinausgehen. Vor dem Hintergrund der verfassungsgerichtlichen Rechtsprechung zu vergleichbaren Maßnahmen im repressiven Bereich (insbesondere im Kontext der Führungsaufsicht)[1] war die Existenz einer solchen Maßnahme als solche jedoch grundsätzlich nicht zu beanstanden. Entscheidend ist, dass der Gesetzgeber die Voraussetzungen, Zwecke, Grenzen und Sicherungen so bestimmt regelt, dass die Maßnahme verhältnismäßig bleibt, die Eingriffsschwelle hinreichend hoch ist und eine missbräuchliche oder ausufernde Nutzung verhindert wird. Die konkrete Ausgestaltung des Entwurfs gab insoweit an mehreren Stellen Anlass zu Kritik.

Anordnungsvoraussetzungen und Normenklarheit

Wir hielten die vorgeschlagene Formulierung der Voraussetzungen des neuen § 38 Abs. 1 Satz 1 Nr. 3 SPolDVG für überarbeitungsbedürftig. Zwar schienen die vorgesehenen Eingriffsschwellen den Vorgaben der einschlägigen Rechtsprechung des Bundesverfassungsgerichts im Grundsatz zu genügen, gleichwohl fehlte es aus unserer Sicht an einer hinreichenden Abgrenzung der neuen Tatbestandsvarianten von den bereits bestehenden Eingriffsbefugnissen. Der neue § 38 Abs. 1 Satz 1 Nr. 3 SPolDVG sah vor, dass in sich konkretisierenden Gefährdungslagen für Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung eine Aufenthaltsüberwachung möglich sein soll. Viele der davon erfassten Fälle können nach unserer Auffassung jedoch bereits über die bestehende Regelung in § 38 Abs. 1 Satz 1 Nr. 1 SPolDVG abgebildet werden, die in der Vorgängerfassung noch auf den Straftatenkatalog in § 100a StPO verwies und mittlerweile § 129a StGB referenziert. Aus rechtsstaatlicher Sicht ist eine trennscharfe, systematisch nachvollziehbare Abgrenzung der Eingriffsnormen besonders wichtig: Überschneidungen erschweren die Anwendungspraxis, erhöhen das Risiko uneinheitlicher Auslegung und können dazu führen, dass die eigentliche Eingriffsschwelle faktisch verwässert wird. Unsere Änderungsvorschläge zur Schaffung einer normenklaren und rechtssicher abgrenzbaren Regelung

1) BVerfG, Beschluss vom 01.12.2020 - 2 BvR 916/11, 2 BvR 636/12, BVerfGE 156, 63 - 182.

wurden nur teilweise übernommen; unsere diesbezüglichen Bedenken bestehen daher teilweise fort.

„Bewegungsbild“ und Sekundärnutzung

§ 38 Abs. 2 SPolDVG sieht die Möglichkeit vor, die durch eine elektronische Aufenthaltsüberwachung erhobenen Daten zu einem Bewegungsbild zu verbinden. Diese Verknüpfung von Einzeldaten ist aus datenschutzrechtlicher Sicht ein zentraler Intensivierungsfaktor, weil sie eine Profilbildung über Zeiträume hinweg ermöglicht. Der ursprüngliche Entwurf knüpfte hierbei systematisch an den Primärzweck – die Überwachung des Aufenthaltsortes – an. Mit Blick auf die technische Funktionsweise der elektronischen Aufenthaltsüberwachung[2] ergab diese Konstruktion aus unserer Sicht jedoch keinen sinnvollen Mehrwert: Die Standortbestimmung setzt ohnehin eine fortlaufende Datenerhebung voraus. Naheliegender war, dass die Verbindung zu einem Bewegungsbild eine Nutzung für Sekundärzwecke (Gefahrenabwehr oder Strafverfolgung) jenseits der unmittelbaren Aufenthaltskontrolle ermöglichen sollte, etwa um Bewegungsmuster nachträglich auszuwerten. Zur Klarstellung der gesetzgeberischen Intention regten wir deshalb dringend an, die Regelung zu überarbeiten, insbesondere im Hinblick auf Zweckbindung, Zugriffsvoraussetzungen und Kontrollmechanismen. Dies wurde überwiegend aufgegriffen: Durch Anpassungen der systematischen Stellung und der Formulierung ist die Vorschrift nun besser auslegungsfähig und dürfte die vom Gesetzgeber intendierten Fallkonstellationen eher erfassen. Die beibehaltene Voraussetzung eines Richtervorbehalts für diese Situationen begrüßten wir ausdrücklich. Unser Vorschlag, zusätzlich eine rechtssichere Legaldefinition des Begriffs „Bewegungsbild“ aufzunehmen, wurde dagegen nicht umgesetzt. Dies halten wir weiterhin für nachteilig, weil unklare Begriffe bei einer derart eingriffsintensiven Datenverarbeitung zu weit reichenden Auslegungsmöglichkeiten führen können.

---

2) Die Überwachung des Aufenthaltsorts soll die Feststellung ermöglichen, ob der Träger des Geräts eine geografische Einschlusszone unerlaubt verlässt bzw. eine geografische Ausschlusszone unerlaubt betritt und eine Alarmierung im Falle der Zuwiderhandlung auslösen. Hierfür ist technisch jedoch nur eine punktuelle Feststellung des Aufenthaltsortes erforderlich und gerade nicht die Anfertigung eines Bewegungsbilds.

Dauer der Anordnung

Der Entwurf sah ferner vor, die bisherige Höchstdauer von Anordnungen (und etwaigen Verlängerungen) von drei auf vier Monate zu erhöhen. Da die Dauer einer Überwachungsmaßnahme wesentlich für die Intensität des Grundrechtseingriffs ist, kann eine Fristverlängerung die Verhältnismäßigkeit einer Eingriffsbefugnis zusätzlich belasten. Maßgeblich war dabei auch, dass (auch wiederholte) Verlängerungen bereits nach geltendem Recht zulässig sind, ein konkreter Nutzen der Fristverlängerung in der Begründung nicht dargelegt wurde und eine spätere Überprüfung der Maßnahme die Rechtsposition der betroffenen Person zusätzlich belastet hätte. Aus datenschutzrechtlicher Sicht haben wir daher von dieser Änderung abgeraten. Die geplante Fristverlängerung wurde im weiteren Gesetzgebungsverfahren verworfen.

Transparenz, Benachrichtigung und Betroffenenrechte

Nicht aufgegriffen wurde insbesondere unser Vorschlag, wesentliche Aspekte der Datenverarbeitung nach § 38 SPolDVG stärker in die Benachrichtigungsvorschriften einzubetten (u. a. § 10 Abs. 5 SPolDVG). Zwar erfolgt die elektronische Aufenthaltsüberwachung regelmäßig in dem Sinne offen, dass die verpflichtete Person von der Datenerhebung Kenntnis hat. Für eine wirksame Wahrnehmung datenschutzrechtlicher Rechte genügt jedoch nicht allein die Kenntnis, „dass" Daten erhoben werden. Erforderlich ist vielmehr eine hinreichend konkrete Information über Umfang und Reichweite der Verarbeitung: Welche Daten werden in welcher Frequenz erhoben? Zu welchen Zwecken dürfen sie verarbeitet werden (Primär- und Sekundärzwecke)? Wer erhält Zugriff, unter welchen Voraussetzungen und mit welchen Protokollierungen? Wie lange werden die Daten gespeichert, wann werden sie gelöscht, und welche Rechtsbehelfe stehen zur Verfügung? Gerade bei eingriffsintensiven Maßnahmen ist Transparenz ein wesentliches Korrektiv, um Rechtsklarheit zu schaffen und Vertrauen in die Rechtmäßigkeit der Verarbeitung zu ermöglichen. Eine entsprechende Verbesserung wäre aus unserer Sicht wünschenswert gewesen.

Einordnung des „spanischen Modells“

Abschließend ist darauf hinzuweisen, dass erst nach der Anhörung im Ausschuss durch einen Abänderungsantrag eine ausdrückliche Rechtsgrundlage für das „spanische Modell“ in den Gesetzestext aufgenommen wurde (vgl. § 38 Abs. 2 SPolDVG). Zu dieser Änderung hatte unsere Behörde keine Gelegenheit mehr zur Stellungnahme. Gerade weil das Modell eine weitere betroffene Person einbezieht, halten wir die Festlegung besonders klarer gesetzlicher Rahmenbedingungen für wichtig. Neben technischen Fragen (z. B. welche Daten der gefährdeten Person tatsächlich erhoben und übermittelt werden) kommt es hier insbesondere auf die Ausgestaltung der Freiwilligkeit, Informationspflichten, Datensparsamkeit sowie effektive Schutzmechanismen gegen missbräuchliche Nutzung an.

Die Neufassung des § 38 SPolDVG wurde durch das Gesetz Nr. 2166 zur Erweiterung der elektronischen Aufenthaltsüberwachung auf Fälle häuslicher Gewalt am 19. Februar 2025 vom Landtag des Saarlandes beschlossen und im Amtsblatt vom 10. April 2025 verkündet.[3] Sie gilt seit dem 11. April 2025. Der saarländische Gesetzgeber hat die elektronische Aufenthaltsüberwachung zudem in den Katalog der Maßnahmen nach § 42 SPolDVG aufgenommen. Die dort genannten polizeilichen Befugnisse unterliegen gemäß § 5 Abs. 2 SPolDVG einer regelmäßigen Kontrolle durch unsere Behörde. Wir beabsichtigen daher, den praktischen Einsatz der elektronischen Aufenthaltsüberwachung in absehbarer Zeit in unsere Prüfungsplanung aufzunehmen. Im Fokus werden dabei insbesondere die tatsächlichen Datenflüsse (einschließlich möglicher Sekundärnutzungen), die Voraussetzungen und Praxis der Bewegungsbildgenerierung, die Umsetzung von Speicher- und Löschkonzepten, die Protokollierung von Zugriffen sowie die Transparenz gegenüber den betroffenen Personen stehen. Damit soll sichergestellt werden, dass das legitime Ziel eines verbesserten Schutzes vor häuslicher Gewalt mit den Anforderungen an eine rechtsstaatlich und datenschutzkonform begrenzte Datenverarbeitung in Einklang gebracht wird.

---

3) Amtsblatt des Saarlandes I, Nr. 13/2025, S. 332.

2.2 Weitere Beteiligung beim Maßregelvollzugsgesetz

Wie bereits im vergangenen Jahr berichtet[4], wurden wir im Zusammenhang mit der Novellierung des Maßregelvollzugsgesetzes (MRVG) beteiligt. Auch im anschließenden parlamentarischen Verfahren zum Gesetzentwurf (LT-Drs. 17/1333) brachten wir erneut datenschutzrechtliche Gesichtspunkte ein und hielten die noch offenen Punkte aus unserer Stellungnahme aus 2024 aufrecht. Im Mittelpunkt standen dabei insbesondere die Regelungen zur Speicherung und Löschung personenbezogener Daten sowie zur Videoüberwachung.

Speicherung und Löschung nach Ende der Unterbringung

Wir regten dringend an, die vorgesehene Löschregelung in § 40 MRVG zu überarbeiten. Der Entwurf enthielt Fristen, innerhalb derer Daten nach Beendigung der jeweiligen Unterbringung zu löschen gewesen wären. Damit wurden zwar zeitliche Grenzen der Aufbewahrung adressiert; es fehlte jedoch nach unserem Verständnis eine hinreichend bestimmte Rechtsgrundlage, die eine Verarbeitung – und damit insbesondere eine Speicherung – über die Dauer der Unterbringung hinaus überhaupt erlaubt hätte.

Die allgemeine Datenverarbeitungsbefugnis in § 38 MRVG knüpft an eine Verarbeitung „zur Durchführung des Maßregelvollzugs“ an und erfasst damit primär die Zeit des tatsächlichen Aufenthalts in der Einrichtung. Soweit das zuständige Ministerium der Justiz einen Bedarf sah, bestimmte Informationen auch nach Entlassung oder Verlegung für eine begrenzte Zeit – vor allem aus Gründen der Dokumentation – vorzuhalten, bedurfte es daher einer ausdrücklichen, zweckgebundenen und verhältnismäßigen Ermächtigung. Wir haben empfohlen, § 40 MRVG so auszugestalten, dass Zwecke, Datenkategorien, Zugriffsberechtigungen sowie differenzierte Speicher- und Löschfristen klar geregelt werden. Dadurch wird nicht nur die Rechtsposition der Betroffenen gestärkt, sondern auch die notwendige Rechtssicherheit für die Einrichtungen geschaffen, die andernfalls zwischen

4) Vgl. 33. Tätigkeitsbericht Datenschutz 2024, Kapitel 2.2.

Dokumentationsinteressen und Löschpflichten in einen unauflösbaren Konflikt geraten können.

Klarstellung zur Videoüberwachung

Ein weiterer Schwerpunkt unserer Stellungnahme ergab sich aus einem Termin mit der Saarländischen Klinik für Forensische Psychiatrie (SKFP) in Merzig. Im Zusammenhang mit einer geplanten Erneuerung und Ausweitung der Videoüberwachung zeigte sich, dass unsere Behörde und das Ministerium der Justiz den Inhalt der im Entwurf enthaltenen Videoüberwachungsnorm (§ 42 MRVG) insbesondere im Hinblick auf den Begriff des „Außenbereichs" unterschiedlich auslegten.[5] Gegen die weitergehende Auslegung des Ministeriums bestanden im Grundsatz keine durchgreifenden datenschutzrechtlichen Einwände, sofern die Maßnahme an klare Zwecke gebunden, räumlich begrenzt und mit angemessenen Garantien versehen ist. Um Missverständnisse zu vermeiden und die praktische Anwendung zu vereinheitlichen, hielten wir jedoch eine Konkretisierung im Wortlaut sowie in der Gesetzesbegründung für erforderlich. Ziel war es, die Reichweite der Norm und die damit verbundenen Schutzmechanismen so eindeutig zu formulieren, dass sowohl Betroffene als auch Verantwortliche die Grenzen der Zulässigkeit erkennen können.

Ergebnis der Beteiligung und offene Punkte

Zu beiden Schwerpunktthemen unterbreiteten wir konkrete Formulierungsvorschläge. Diese wurden vom zuständigen Ausschuss im Wege eines Abänderungsantrags übernommen.

Damit konnten zentrale Punkte zur rechtssicheren Ausgestaltung der Datenaufbewahrung nach Ende der Unterbringung sowie zur Klarstellung der Videoüberwachungsregelung erreicht werden.

---

5) Siehe hierzu den vorliegenden Bericht unter Ziffer 6.4.

Nicht durchsetzen konnten wir demgegenüber weitere datenschutzrechtliche Anmerkungen, insbesondere zur Vollständigkeit der Verweisungen in § 36 Abs. 1 MRVG auf Regelungen des Justizvollzugsdatenschutzgesetzes (JVollzDSG), zur Ausgestaltung der Norm über Maßnahmen der Telekommunikationsüberwachung sowie zum Kernbereichsschutz. Diese Themen bleiben aus unserer Sicht für die Anwendungspraxis bedeutsam und werden von uns weiterhin im Blick behalten, insbesondere bei der Bewertung der praktischen Umsetzung der Datenverarbeitung in der Einrichtung.

Die Novellierung des Maßregelvollzugsgesetzes wurde im Rahmen des Gesetzes Nr. 2168 zur Novellierung des Maßregelvollzugsrechts vom 19. März 2025 durch den Landtag des Saarlandes beschlossen und im Amtsblatt vom 30. April 2025 verkündet.[6] Es gilt seit dem 01. Mai 2025.

6) Amtsblatt des Saarlandes I, Nr. 16/2025, S. 370.

VOLLZUGSPRAXIS

3. VOLLZUGSPRAXIS

Ein nicht unerheblicher Teil der Tätigkeit des Unabhängigen Datenschutzzentrums Saarland entfällt auf die Zusammenarbeit mit den Datenschutzbehörden der anderen Länder sowie des Bundes. Diese Kooperation ist für einen einheitlichen und damit wirksamen Vollzug der Datenschutz-Grundverordnung von besonderer Bedeutung. Rechtsfragen sollen einheitlich bewertet werden und Verantwortliche sollen – unabhängig davon, in welchem Bundesland sie ihren Sitz haben – mit vergleichbaren Verfahrensstandards rechnen können. Betroffene profitieren davon, dass die Aufsichtsbehörden in zentralen Fragen nach möglichst einheitlichen Maßstäben vorgehen und Entscheidungen nachvollziehbar begründen. Schließlich ermöglicht eine abgestimmte Praxis auch eine effizientere Aufgabenerfüllung: Erfahrungen aus Einzelfällen können geteilt, bewährte Vorgehensweisen übernommen und Ressourcen gezielter eingesetzt werden.

Ein wichtiges Forum zur Abstimmung auf Arbeitsebene bilden die Arbeitskreise der Datenschutzkonferenz. Speziell im Arbeitskreis Rechtsdurchsetzung werden insbesondere Fragen des behördlichen Vorgehens bei der Durchsetzung datenschutzrechtlicher Pflichten und der Ahndung etwaiger Verstöße beraten. Im Berichtszeitraum standen zwei Vorhaben im Mittelpunkt, die zu einer weiteren Harmonisierung und Professionalisierung des behördlichen Bußgeldvollzugs beitragen.

3.1 Musterrichtlinien für das Verfahren über Geldbußen

Die Datenschutzbehörden sind gem. Art. 58 Abs. 2 lit. i DSGVO i. V. m. § 16 Abs. 1 BDSG sowie den jeweiligen landesrechtlichen Vorschriften befugt, bei Datenschutzverstößen Geldbußen zu verhängen. Aufgrund der föderalen Struktur der Datenschutzaufsicht waren die Verfahrensabläufe und Beurteilungsmaßstäbe in der Praxis jedoch nicht immer einheitlich. Vor diesem Hintergrund verfolgte der Arbeitskreis Rechtsdurchsetzung das Ziel, im Rahmen der Entwicklung von Leitlinien leitende und zugleich praxistaugliche Vorgaben zu machen, die den Behörden bei der Bearbeitung von Verfahren über Geldbußen nach der DSGVO Orientierung geben und die Vergleichbarkeit der Verfahren stärken sollen.

Dieses Ziel wurde mit den Musterrichtlinien für das Verfahren über Geldbußen der Datenschutzaufsichtsbehörden (MRiDaVG) erreicht. Die DSK verabschiedete die MRiDaVG am 16. Juni 2025; im Saarland wurden sie durch Verwaltungsvorschrift vom 23. Juli 2025 umgesetzt. Sie gelten für Bußgeldverfahren im nichtöffentlichen Bereich.

Die Richtlinien enthalten auf den Regelfall bezogene Vorgaben zum Verfahrensablauf, zur Ermessensausübung sowie zur Anwendung und Auslegung deutscher Rechtsnormen im Rahmen von Bußgeldverfahren nach der DSGVO. Sie gelten für Bußgeldverfahren (nicht für Verwaltungsverfahren), sind auch in grenzüberschreitenden Konstellationen zu beachten und stellen klar, dass Vorgaben des Europäischen Datenschutzausschusses im Verhältnis zu den Richtlinien vorrangig sind.

Inhaltlich gliedern sich die MRiDaVG in mehrere Teile:

- Allgemeine Leitlinien und Verfahrensgrundsätze: Im Allgemeinen Teil bündeln die MRiDaVG zentrale Leitplanken für ein unionsrechtskonformes Bußgeldverfahren. Sie stellen klar, dass das nationale Verfahrensrecht im Lichte des Unionsrechts anzuwenden ist und Entscheidungen im Verfahren (von der Einleitung bis zur Beendigung und zur Sanktion) nach pflichtgemäßem, transparent auszuübendem Ermessen zu treffen sind.

Maßgeblicher Orientierungsrahmen sind dabei die Sanktionskriterien der DSGVO. Zugleich ordnen die Richtlinien das Zusammenspiel von Abhilfemaßnahmen und Bußgeldverfahren sowie die Koordination in unionsrechtlichen Kooperations- und Kohärenzverfahren, um ein abgestimmtes und konsistentes Vorgehen sicherzustellen.

- Weiter Betroffenenbegriff und Verbandshaftung: Als „Betroffene" im Bußgeldverfahren werden nicht nur natürliche Personen verstanden. Vielmehr haften Verantwortliche, Auftragsverarbeiter sowie Zertifizierungs- und Überwachungsstellen bußgeldrechtlich unabhängig von ihrer Rechtsform. Die MRiDaVG stellen die unmittelbare Verbandshaftung für das Handeln von Organen, Vertretern oder sonstigen Personen im Rahmen der unternehmerischen Tätigkeit heraus und leiten daraus prozessuale Konsequenzen ab (u. a. keine Behandlung als bloße Nebenbeteiligte, soweit einschlägige Verfahrensvorschriften ihrem Wesen nach anwendbar sind).

- Zuständigkeit und Organisation: Bußgeldverfahren sind organisatorisch von Verwaltungsverfahren (z. B. Beschwerde- oder von Amts wegen geführte Verfahren) zu trennen; es ist eine gesonderte Bußgeldakte zu führen. Zugleich eröffnen die MRiDaVG die Möglichkeit, Unterlagen und Beweisstücke aus dem Verwaltungsverfahren zu übernehmen. Für Konstellationen mehrfacher Zuständigkeit wird angeregt, Übertragungsmöglichkeiten im Ordnungswidrigkeitenrecht zu nutzen, um Verfahren zu beschleunigen oder zu vereinfachen, insbesondere wenn eine Zuständigkeitskonzentration sachgerecht erscheint.

- Ablauf des Bußgeldverfahrens: Die Richtlinien strukturieren vor allem das „Wie" des Verfahrens: Sie beschreiben die Entscheidungs- und Dokumentationsschritte bei Einleitung, Fortführung und Beendigung (insbesondere auch bei einer Einstellung) und legen fest, welche internen bzw. externen Stellen in diesen Konstellationen ggf. zu beteiligen oder zu informieren sind. Daneben regeln sie organisatorische und verfahrenspraktische Fragen, etwa Aktenführung, Adressierung bei juristischen Personen und Personengesellschaften sowie die Ausgestaltung von Auskunftsersuchen an öffentliche und nichtöffentliche Stellen.

- Ermessensentscheidung, Einstellung und Bescheidinhalt: Die MRiDaVG präzisieren insbesondere, welche Kriterien bei der pflichtgemäßen Ermessensausübung im Bußgeldverfahren heranzuziehen und nachvollziehbar zu dokumentieren sind – maßgeblich sind hierbei die in Art. 83 Abs. 2 Satz 2 DSGVO genannten Bemessungs- und Gewichtungsgesichtspunkte. Wenn statt einer Geldbuße eine Verwarnung als Abhilfemaßnahme in Betracht kommt, ist dies zu dokumentieren und an die zuständige Organisationseinheit weiterzugeben. Zum Inhalt des Bußgeldbescheides wird klargestellt, dass nationale Formerfordernisse i. S. d. Art. 66 Abs. 1 OWiG unionsrechtskonform anzuwenden sind und sich der konkrete Bescheidinhalt an den materiellen Anforderungen der DSGVO orientieren muss. Bei unmittelbarer Verbandshaftung ist außerdem hervorzuheben, dass im Bescheid grundsätzlich keine natürliche Person als Betroffener benannt werden muss.

Weitere Regelungen betreffen die Zusammenarbeit mit der Staatsanwaltschaft, den Umgang mit Asservaten sowie die Herausgabe bzw. Übermittlung von Informationen über Bußgeldverfahren. Hierzu zählen Mitteilungen an besondere Aufsichts- bzw. Berufsaufsichtsstellen, Eintragungs- und Unterrichtungspflichten (z. B. Gewerbezentralregister/Gewerbeaufsicht) sowie Auskünfte an Dritte auf Ersuchen unter Berücksichtigung entgegenstehender schutzwürdiger Interessen. Für die Öffentlichkeitsarbeit enthält die Richtlinie Leitplanken: Auskünfte sollen sachlich und wahrheitsgemäß erfolgen, Ermittlungszweck und faires Verfahren dürfen nicht gefährdet werden; über den Erlass eines Bußgeldbescheides soll die Öffentlichkeit grundsätzlich erst nach Zustellung bzw. sonstiger Bekanntgabe informiert werden.

3.2 Merkblatt zu Verständigungen in Bußgeldverfahren

Die Möglichkeit, eine gerichtliche oder außergerichtliche Verständigung herbeizuführen, kennt man aus verschiedenen Rechtsgebieten. Insbesondere ist der Vergleich ein gängiges Instrument zur Beendigung zivilrechtlicher Verfahren, die ansonsten für die Parteien einen ungewissen Ausgang bergen. Auch im Strafverfahren sind Verständigungen bzw.

Settlements, umgangssprachlich auch als „Deal“ bezeichnet, etabliert und seit Einführung des § 257c StPO im Jahr 2009 gesetzlich normiert.

Im datenschutzrechtlichen Bußgeldverfahren fehlte es bislang an einem einheitlichen Rahmen, wann und wie ein Verfahren durch eine einvernehmliche Lösung beendet werden kann. Vor diesem Hintergrund hat die Datenschutzkonferenz ein Merkblatt zu Verständigungen in datenschutzrechtlichen Verfahren über Geldbußen (Stand: Dezember 2025) beschlossen.

Das Merkblatt gilt für nationale Bußgeldverfahren ohne grenzüberschreitenden Bezug; Vorgaben des Europäischen Datenschutzausschusses gehen im Kollisionsfall stets vor. Inhaltlich richtet es sich vor allem an Bußgeldverfahren wegen Verstößen gegen die DSGVO sowie – soweit die Datenschutzaufsichtsbehörden zuständig sind – gegen das TDDDG. Da die DSGVO die verfahrensrechtliche Ausgestaltung von Bußgeldverfahren nicht im Detail regelt, verortet das Merkblatt die Verständigung im Zusammenspiel von Art. 83 Abs. 8 DSGVO und den nationalen Verfahrensregelungen (insbesondere § 41 BDSG mit Verweis auf OWiG und StPO). Zugleich stellt es klar, dass die Grundsätze der Geldbußenzumessung nach Art. 83 Abs. 1 und 2 DSGVO und den hierzu ergangenen Leitlinien nicht zur Disposition der Verfahrensbeteiligten stehen.

- Voraussetzungen und Reichweite: Eine Verständigung kommt nur „in geeigneten Fällen“ in Betracht. Typischer Anwendungsfall sind Verfahren, in denen andernfalls ein erheblicher zusätzlicher Aufwand zu erwarten ist – etwa durch umfangreiche rechtliche Auseinandersetzungen im Bescheid, eine absehbare Abgabe an die Staatsanwaltschaft bei umfangreichen Einspruchsbegründungen oder eine intensive Unterstützung von Gericht und Staatsanwaltschaft im gerichtlichen Verfahren. Eine Verständigung kann sowohl von Betroffenen angeregt als auch von der Behörde aufgegriffen werden; sie erfolgt freiwillig, ein Anspruch hierauf besteht nicht. Ob (und in welchem Umfang) eine Verständigung angestrebt wird, entscheidet allein die zuständige Aufsichtsbehörde. Grundsätzlich ist eine Verständigung in jedem Stadium des behördlichen Bußgeldverfahrens möglich; mit zunehmendem Verfahrensfortschritt

verringert sich allerdings regelmäßig der Spielraum für eine bußgeldmindernde Berücksichtigung, weil bereits Aufwand entstanden ist.

Bevor die Behörde einer Verständigung zustimmt, soll sie die Beweislage prüfen: Die Tat muss – gegebenenfalls auf Basis des Verständigungsergebnisses – mit der für eine Verurteilung erforderlichen Wahrscheinlichkeit nachweisbar sein. Zwingender Kern einer Verständigung ist eine geständige Einlassung. Daneben soll sich die oder der Betroffene auch zu weiteren, für die Zumessung relevanten Umständen einlassen; die Behörde unterzieht diese Angaben vor einer Verwertung einer Plausibilitätsprüfung. Ergänzend kann eine Mitwirkung an der Sachverhaltsaufklärung – etwa der Verzicht auf Beweisanträge – eine Rolle spielen.

- Verständigungsgespräch und Dokumentation: Das sog. Verständigungsgespräch stellt einen zentralen Aspekt einer Verständigung dar. Im Sinne effizienter Verfahrensführung soll der Termin auf das notwendige Maß begrenzt bleiben; der Schwerpunkt liegt regelmäßig auf der Rechtsfolgenseite, insbesondere der avisierten Geldbuße. Ein abgebrochenes Gespräch schließt weitere Gespräche nicht aus, sofern die Voraussetzungen weiterhin vorliegen. Wesentlich ist die Dokumentationspflicht: Der Kern der Erörterung ist – unabhängig davon, ob es zu einer Verständigung kommt – aktenkundig zu machen.

- Minderung der Geldbuße: Die Behörde kann einen Abschlag auf die ohne Verständigung beabsichtigte Geldbuße gewähren. Bei der Bestimmung dieses Abschlags sind unter Wahrung der Sanktionszwecke (Art. 83 Abs. 1 und 2 DSGVO) insbesondere der bisherige Verfahrensverlauf, Umfang und Qualität der vorliegenden Beweismittel sowie der im Streitfall zu erwartende weitere Aufwand zu berücksichtigen.

- Form, Inhalt und Grenzen: Die Verständigungserklärung ist an keine bestimmte Form gebunden. Inhaltlich empfiehlt das Merkblatt u. a. eine kurze Bezeichnung der Tat (ggf. durch Verweis auf eine bereits erfolgte Anhörung), die Angabe der Geldbuße (als konkreter Betrag oder als Korridor), eine klare Darstellung der erwarteten Art und des Umfangs

der Einlassung sowie Hinweise auf mögliche Folgen eines späteren Einspruchs. Außerdem wird auf die sinngemäße Anwendung von § 257c Abs. 4 StPO hingewiesen, wonach ausnahmsweise die Bindung an eine Verständigung entfallen kann. Zugleich zieht das Merkblatt klare Grenzen: Ein Verzicht auf Rechtsmittel oder Regelungen, die etwa die Rückgabe sichergestellter Gegenstände oder Registereintragungen betreffen, sollen nicht Gegenstand einer Verständigung sein.

- Kurzbescheid und Folgen eines Einspruchs: Wird das Verfahren durch Verständigung beendet, wird der Verstoß regelmäßig mit einem Bußgeldbescheid geahndet, der sich auf die Mindestangaben nach § 66 OWiG beschränkt („Kurzbescheid"). In diesen Fällen kann die rechtliche Würdigung entfallen; insbesondere muss die Zumessung nicht begründet werden. Legt der oder die Betroffene dennoch Einspruch ein, kann die Behörde den Kurzbescheid zurücknehmen und einen neuen, ausführlich begründeten Bescheid – gegebenenfalls mit höherer Geldbuße – erlassen.

3.3 Data Act/EU-Datenverordnung

Neben der Vereinheitlichung des behördlichen Bußgeldvollzugs führen neue unionsrechtliche Vorgaben zum Datenzugang und zur Datennutzung jenseits des klassischen Datenschutzrechts zu Abgrenzungs-, Auslegungs- und Zuständigkeitsfragen, die für einen kohärenten und rechtssicheren Vollzug frühzeitig geklärt werden müssen.

Seit dem 12. September 2025 ist die Verordnung (EU) 2023/2854 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung („EU-Datenverordnung/Data Act")[7], in weiten Teilen (siehe Art. 50 Data Act) anwendbar. Auch wenn die Verordnung nicht als

7) Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung), abrufbar unter https://eur-lex.europa.eu/eli/reg/2023/2854/oj/deu.

Datenschutzrechtsakt angelegt ist, betrifft sie die Tätigkeit der Datenschutzaufsichtsbehörden unmittelbar: Sie schafft neue Zugangs- und Weitergaberechte zu Daten, die bei der Nutzung vernetzter Produkte und zugehöriger digitaler Dienste anfallen, und wirft dabei Auslegungs- und Abgrenzungsfragen im Zusammenspiel mit der DSGVO auf.

Kern der Datenverordnung ist die Stärkung der Kontrolle der Nutzerinnen und Nutzer über nutzungsgenerierte Daten. Anbieter vernetzter Produkte (etwa Smart-Home-Geräte, Wearables oder vernetzte Fahrzeuge) müssen sicherstellen, dass Nutzer grundsätzlich Zugang zu den durch die Nutzung erzeugten Daten erhalten. Daneben kann der Nutzer verlangen, dass der Dateninhaber diese Daten an einen Dritten (bspw. Reparatur- oder Wartungsdienstleister, Vergleichs- oder Analyseanbieter) übermittelt bzw. weitergibt. Diese Rechte zielen darauf ab, Lock-in-Effekte zu reduzieren, nachgelagerte Märkte zu öffnen und datenbasierte Innovation zu erleichtern.[8]

Die EU-Datenverordnung gilt, wie sich aus deren Art. 1 Abs. 2 ergibt, sowohl für personenbezogene als auch für nicht-personenbezogene Daten. In der praktischen Anwendung werden jedoch häufig Mischdatensätze betroffen sein. Viele Nutzungs- und Telemetriedaten erlauben Rückschlüsse auf eine identifizierte oder identifizierbare Person – etwa weil sie Geräte einem Nutzerkonto zuordnen, Standort- oder Bewegungsprofile abbilden oder Nutzungsgewohnheiten erkennen lassen. Hinzu kommt, dass vernetzte Produkte oftmals auch Daten über Dritte erfassen, die nicht selbst Nutzer des Produkts sind (bspw. Mitfahrende im Fahrzeug, Besucherinnen in einem smarten Gebäude oder zufällig erfasste Personen im Umfeld). Gerade in solchen Konstellationen verschärfen sich die datenschutzrechtlichen Implikationen: Datenzugangs- und Weitergabeverlangen sind so zu gestalten, dass Rechte Dritter nicht unangemessen beeinträchtigt werden (bspw. durch Datenminimierung, technische Filterung oder Pseudonymisierung).

8) Erwägungsgrund 1 und 2 des Data Acts.

Für personenbezogene Daten stellt die EU-Datenverordnung klar, dass der Data-Act-Mechanismus keine eigenständige datenschutzrechtliche Erlaubnis begründet. Soweit die Bereitstellung oder Übermittlung personenbezogener Daten erfolgt, müssen die Anforderungen der DSGVO eingehalten werden (Art. 1 Abs. 5 Data Act); insbesondere bedarf es einer Rechtsgrundlage sowie der Beachtung der Grundsätze der Verarbeitung gemäß Art. 5 DSGVO (z. B. Zweckbindung, Transparenz, Datenminimierung). Im Ergebnis ist ein angemessener Ausgleich herzustellen zwischen dem Interesse an Datennutzung und Innovation einerseits und dem Schutz der Rechte und Freiheiten betroffener Personen andererseits.

Die praktische Wirksamkeit des Data Act hängt in Deutschland von der nationalen Aufsichts- und Kontrollstruktur ab. Hierzu hatte der Bundesgesetzgeber mit dem Referentenentwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2023/2854 (Data Act-Durchführungsgesetz – DA-DG) erste Regelungsvorschläge unterbreitet. In ihrer Stellungnahme vom 13. März 2025 zu diesem Referentenentwurf eines Data Act-Durchführungsgesetzes beanstanden die Datenschutzaufsichtsbehörden der Länder unter anderem die vorgesehene Verlagerung datenschutzrechtlicher Zuständigkeiten auf die Bundesebene:[9]

- Unionsrechtliche Bedenken/Kohärenz mit der DSGVO: Die Aufsichtsbehörden der Länder halten die vorgesehene Verschiebung der Zuständigkeit auf die BfDI für unionsrechtswidrig. Art. 37 Abs. 3 Satz 1 Data Act knüpfe an die bereits nach der DSGVO zuständigen Aufsichtsbehörden an, um eine Zuständigkeitszersplitterung zu vermeiden; eine Befugnis der Mitgliedstaaten hiervon abweichende Zuständigkeitsregeln zu schaffen, lasse die Vorschrift nach Auffassung der DSK nicht erkennen.

  Die Landesaufsichtsbehörden betonen zudem, dass der europäische Gesetzgeber aus sachlichen Gründen von dem Grundsatz ausgehe, die Bewertung von Datennutzungsanliegen und die Beurteilung der dadurch

9) www.datenschutzkonferenz-online.de/media/st/Data_Act_Umsetzung_Laenderstellungnahme.pdf.

erlangten personenbezogenen Daten sollen möglichst durch dieselbe Behörde erfolgen. Darüber sind verwaltungsrechtliche Verfahrenskonstruktionen, in denen eine datenschutzaufsichtliche Bewertung nur als „Beurteilungsbeitrag" in einer Gesamtentscheidung einer anderen Behörde sichtbar wird, zu kritisieren. Dies könne die unionsrechtlich zugewiesenen Aufgaben der Datenschutzaufsicht (u. a. im Beschwerdekontext) verkürzen und den effektiven Rechtsschutz erschweren.

- Verfassungsrechtliche Bedenken/föderale Kompetenzordnung: Die Datenschutzaufsichtsbehörden der Länder sehen außerdem Konflikte mit der verfassungsrechtlichen Verteilung der Verwaltungskompetenzen. Der Data Act erfasse vernetzte Produkte und Dienste nicht nur im Bereich der „Wirtschaft", sondern auch in vielen Feldern, die in die Zuständigkeit der Länder fallen (z. B. medizinische Versorgung, Lehre und Forschung, Schulen, Kultureinrichtungen, Medien, Gerichte, Vereine, Verbände und Kammern).

  Hinzu komme, dass eine generelle Aufsicht einer Bundesbehörde über Datenverarbeitungen von Landesbehörden grundlegenden föderalen Ordnungsprinzipien widerspreche – insbesondere, weil Landesbehörden im Anwendungsbereich des EU-Data-Acts unterschiedliche Rollen einnehmen können (Nutzer, Dateninhaber, Datenempfänger).

- Praktikabilität und Rechtsicherheit: Schließlich beanstanden die Datenschutzaufsichtsbehörden der Länder die geplante Struktur als nicht praktikabel. Datenschutzfragen „im Rahmen" des Data Act ließen sich häufig nicht trennscharf von vorgelagerten oder nachgelagerten Verarbeitungen von Daten derselben Akteure abgrenzen. Dies führe – entgegen dem Ziel der Vereinfachung – zu Doppelaufsicht, parallelen Verfahren und einem erhöhten Risiko divergierender Bewertungen. Dies hat Konsequenzen für Betroffene und Unternehmen: Statt kurzer Wege zu vertrauten Ansprechpartnern vor Ort drohten Verfahren bei entfernten Stellen und eine Zersplitterung des Rechtsschutzes; insgesamt nehme die Rechtsunsicherheit zu, während Ressourcen doppelt gebunden würden.

Ergänzend wird hervorgehoben, dass die Landesdatenschutzbehörden über gewachsene Beratungsstrukturen verfügen und regionale Akteure, Branchen und Vollzugspraxis gut kennen – ein Standortvorteil, der nicht ohne belastbaren Mehrwert aufgegeben werden sollte.

Aus diesen unionsrechtlichen, verfassungsrechtlichen und praktischen Gründen empfehlen die Landesdatenschutzbehörden, die vorgesehene Sonderzuständigkeit grundlegend zu überarbeiten und die Effektivität und Rechtssicherheit der Aufsicht als Voraussetzung digitaler Innovation stärker in den Vordergrund zu stellen.

Auch der Bundesrat hat im Gesetzgebungsverfahren in seiner Sitzung am 19. Dezember 2025 beschlossen, eine Stellungnahme zu dem Gesetzentwurf abzugeben.[10] Darin werden mehrere Punkte aufgegriffen, die in der Sache mit der Kritik der Landesaufsichtsbehörden korrespondieren. So sieht auch der Bundesrat einen erhöhten Abstimmungsbedarf und warnt vor parallelen Verfahren und divergierenden Beurteilungen. Es drohe die Gefahr einer Zersplitterung und Reduzierung des Rechtsschutzes (u. a. unterschiedliche Gerichtsstände). Zweifelhaft sei schließlich, ob Art. 37 Abs. 3 Data Act überhaupt abweichende nationale Regelungen zulässt. Der Bundesrat fordert zudem eine Ausnahme, damit die Prüfung bestimmter Datenverlangen von Landesbehörden nicht bei der Bundesnetzagentur zentralisiert wird; dies wird ausdrücklich mit föderalen Ordnungsprinzipien begründet.

Für die Aufsichtspraxis bleibt damit absehbar, dass die Umsetzung des Data Act in Deutschland nicht nur technische Fragen des Datenzugangs betrifft, sondern vor allem auch eine klar begründete, kohärente Zuständigkeitsordnung erfordert, die Doppelstrukturen vermeidet und den Rechtsschutz der Betroffenen sichert.

10) https://dserver.bundestag.de/btd/21/035/2103508.pdf.

WIRTSCHAFT

4. WIRTSCHAFT

4.1 Das Auskunftsrecht in der Kreditwirtschaft

Auch im Bereich der Kreditwirtschaft war unsere Behörde in einer Anzahl von Verfahren mit den Voraussetzungen des Anspruchs auf Auskunft nach Art. 15 DSGVO befasst.

Auskunft über Datenempfänger nach irrtümlicher Schließfachöffnung

Ein Beschwerdeführer hatte bei seiner Bank ein Schließfach angemietet, in dem er diverse Unterlagen und Gegenstände aufbewahrte. Neben Bargeld befand sich auch ein handschriftliches Testament im Schließfach, das unter anderem den Namen des Beschwerdeführers und weitergehende, eine Erbschaft betreffende Informationen enthielt. Bei der Bank sollte nun das Schließfach einer verstorbenen Kundin im Rahmen einer Nachlassabwicklung geöffnet werden, da der zugehörige Schlüssel nicht aufzufinden war. Aufgrund eines Irrtums bezüglich der Schließfachnummer durch eine mitarbeitende Person der Bank wurde aber anstatt des Schließfachs der Verstorbenen das Schließfach des Beschwerdeführers geöffnet und die Inhalte des Schließfachs an einen Rechtsanwalt als Nachlasspfleger herausgegeben. Der Nachlasspfleger nahm Einsicht in die Unterlagen und brachte diese, nachdem er festgestellt hatte, dass es sich nicht um Gegenstände und Unterlagen der Verstorbenen handelte, wieder zurück in die Bankfiliale. Nachdem er von der Bank nach Art. 34 DSGVO über den Vorfall benachrichtigt worden war, beantragte der Beschwerdeführer gegenüber der Bank, dass ihm nach Art. 15 DSGVO Auskunft über etwaige Empfänger seiner personenbezogenen Daten im Zusammenhang mit dem Vorfall erteilt wird.

Der Beschwerdeführer hatte sinngemäß dargelegt, dass aus seiner Sicht das Risiko bestehe, dass der Nachlasspfleger, der unberechtigt von den Schließfachinhalten – insbesondere dem Testament – Kenntnis genommen hat, ggf. in eine erbrechtliche Auseinandersetzung mit ihm verwickelt sein könnte. Die Bank hingegen weigerte sich in der Folge über die Identität des Nachlasspflegers Auskunft zu geben und begründete dies unter anderem mit einer Nichtanwendbarkeit der DSGVO sowie mit Schutzinteressen des Nachlasspflegers, der sich ansonsten der Gefahr einer mutmaßlich unberechtigten Rechtsverfolgung durch den Beschwerdeführer ausgesetzt sehen könnte.

Hiesiger Auffassung nach war Art. 15 DSGVO im vorliegenden Fall aber anwendbar und es bestand dem Grunde nach auch ein Anspruch des Beschwerdeführers aus Art. 15 Abs. 1 lit. c DSGVO auf Auskunft über die Identität des Nachlasspflegers.

Nach Art. 2 Abs. 1 DSGVO gilt die Verordnung für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Hervorzuheben ist, dass Verarbeitungen personenbezogener Daten damit bereits dann in den sachlichen Anwendungsbereich der DSGVO fallen, wenn sie nur teilweise automatisiert erfolgen, mithin wenn auch nur einzelne Verarbeitungsschritte des Gesamtverarbeitungsvorganges mittels Informationstechnik durchgeführt werden.[11] Auch gänzlich manuelle Verarbeitungen sind umfasst, sofern die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, in einem Dateisystem gespeichert sind. Bejaht hat der Europäische Gerichtshof dies etwa für die mündliche Übermittlung personenbezogener Daten aus einem Dateisystem.[12] Irrelevant sei laut EuGH zudem, ob es sich bei diesem Dateisystem i. S. d. Art. 4 Nr. 6 DSGVO um physische Akten oder eine elektronische Datenbank handele.[13]

11) Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 2 Rn. 14.
12) EuGH, Urteil vom 07.03.2024 - C-740/22, Rn. 35.
13) EuGH, a. a. O.

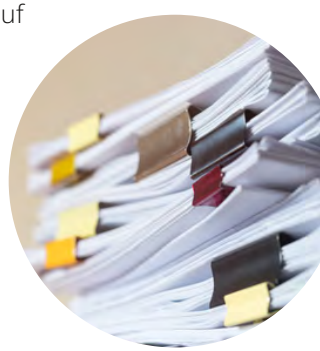
Der EuGH statuiert daher, dass

„ (...) diese Verordnung genauso für die automatisierte wie für die manuelle Verarbeitung personenbezogener Daten gilt, damit der Schutz, den diese Verordnung den von der Datenverarbeitung betroffenen Personen verleiht, nicht von den verwendeten Techniken abhängt und nicht ernsthaft Gefahr läuft, umgangen zu werden."

Voraussetzung sei lediglich,

„(...) dass die Daten, die Gegenstand dieser Verarbeitung sind, in einem „Dateisystem" „gespeichert" sind oder „gespeichert werden sollen", damit diese Verarbeitung in den sachlichen Anwendungsbereich der DSGVO fällt."

Auch der Begriff der Verarbeitung ist nach Art. 4 Nr. 2 DSGVO denkbar weit auszulegen, da er jeden Vorgang im Zusammenhang mit personenbezogenen Daten umfasst, unabhängig davon, ob er mit oder ohne Hilfe automatisierter Verfahren ausgeführt wird.



Erfolgt also eine Offenlegung von Informationen, die sich auf eine identifizierbare Person beziehen, gegenüber Dritten, ist ohne Belang, auf welche konkrete Art und Weise die Offenlegung erfolgt. Sie kann mittels informationstechnischer Systeme, mündlich oder etwa auch durch schlichtes Handeln erfolgen, sofern dieses dazu geeignet ist, dass sich Dritte der entsprechenden Informationen gewahr werden können. Denn um dem Grundrecht einer Person auf Schutz der sie betreffenden personenbezogenen Daten aus Art. 8 Abs. 1 Grundrechtecharta der Europäischen Union hinreichend Geltung und Wirksamkeit zu verschaffen, darf es für eine Anwendbarkeit der datenschutzrechtlichen Vorschriften nicht darauf ankommen, wie Informationen gegenüber Dritten offengelegt werden.

Zusammenfassend unterfallen solche Vorgänge der DSGVO, bei denen personenbezogene Daten gegenüber Dritten offengelegt werden, solange die Informationen einem Dateisystem entstammen, unabhängig davon, ob das Dateisystem digital oder analog geführt wird.

Einerseits lag der Bank die Information, dass der Beschwerdeführer als Mieter des Schließfachs Kunde war, zweifelsfrei analog oder digital innerhalb eines etwaigen Kundenmanagementsystems vor. Durch Übergabe der Schließfachinhalte an den Nachlasspfleger und dessen Einsichtnahme in diese – darunter in das handschriftliche Testament – wurde zumindest die Vertragspartnereigenschaft des Beschwerdeführers in Bezug auf die Bank, aber auch die personenbezogenen Informationen innerhalb des Testaments, gegenüber diesem Dritten offengelegt und damit verarbeitet im Sinne des Art. 4 Nr. 2 DSGVO.

Zudem hatte die Bank auch die personenbezogenen Daten innerhalb des Testaments als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO verarbeitet, da im Nachgang zur Öffnung des Schließfachs die Schließfachinhalte und die von der Datenoffenlegung umfassten Datenkategorien aus dem Testament – für Zwecke einer Benachrichtigung nach Art. 34 DSGVO an den Beschwerdeführer – protokolliert wurden. Da der Vorfall von der Bank damit offensichtlich als Datenschutzverletzung im Sinn des Art. 4 Nr. 12 DSGVO qualifiziert und diesbezügliche Maßnahmen nach Art. 33 und 34 DSGVO ergriffen wurden, muss das der unbeabsichtigten Datenoffenlegung zugrundeliegende Verarbeitungshandeln von der Verantwortlichen daher auch selbst als Verarbeitung nach Art. 4 Nr. 2 DSGVO eingeordnet worden sein.[14]

Der Nachlasspfleger war ferner als Empfänger im Sinne des Art. 4 Nr. 9 DSGVO zu qualifizieren; hierfür ist es nicht erforderlich, dass der Empfänger die personenbezogenen Daten bspw. als Verantwortlicher mit eigener Zwecksetzung selbst erhebt oder speichert, da eine Offenlegung bereits

14) Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 4 Nr. 12 Rn. 5, beck-online.

in dem Moment erfolgt, in dem ein Dritter eine tatsächliche Möglichkeit zur Kenntnisnahme erhält.[15]

Auch standen einer Auskunftserteilung keine Interessen oder Rechte des Nachlasspflegers entgegen. Insoweit stellt Art. 6 Abs. 4 in Verbindung mit Art. 6 Abs. 1 lit. c[16] oder f[17] in Verbindung mit Art. 15 Abs. 1 lit. c DSGVO eine hinreichende Rechtsgrundlage für die mit der Auskunft über etwaige Empfänger verbundene Verarbeitung personenbezogener Daten dar. Zudem konnte Art. 15 Abs. 4 DSGVO nicht für eine Beschränkung des Auskunftsrechts nach Art. 15 Abs. 1 DSGVO herangezogen werden, da Art. 15 Abs. 4 DSGVO ausschließlich auf Art. 15 Abs. 3 DSGVO verweist und damit nicht für die Informationen nach Art. 15 Abs. 1 lit. a–h DSGVO gilt.[18] Auch standen im nationalen Recht geregelte Ausnahmen der Auskunftserteilung nicht entgegen. Zwar sieht etwa § 29 Abs. 1 Satz 2 BDSG vor, dass ein Recht auf Auskunft nicht besteht, „soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen." Gerade für den Fall eines „Berufsgeheimnisträgers" – mithin einer rechtskundigen Person, die in diesem Zusammenhang ausschließlich in ihrer beruflichen Sphäre adressiert wird – drängen sich solche überwiegenden berechtigten Interessen an einem Ausschluss der Auskunft jedoch nicht auf. Im Übrigen wurden von der Verantwortlichen auch keine Tatsachen vorgetragen, die hinreichend substantiiert hätten, dass § 29 Abs. 1 Satz 2 BDSG oder sonstige Ausnahmetatbestände einschlägig sind.

Ferner ist das Recht aus Art. 15 DSGVO nicht an weitere Voraussetzungen, wie das Vorliegen eines spezifischen, zu bezeichnenden Grundes für den Antrag geknüpft. So kann eine Auskunft über konkrete Empfänger gerade dem Zweck dienen, die betroffene Person in die Lage zu versetzen, etwaige

15) Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 4 Nr. 2 Rn. 25, beck-online.
16) Taeger/Gabel/Taeger, 4. Aufl. 2022, DS-GVO Art. 6 Rn. 81, beck-online..
17) BGH, Urteil vom 22.02.2022 - VI ZR 14/21, Rn. 19, juris.
18) Europäischer Datenschutzausschuss, Leitlinien 01/2022, S. 61, Rn. 169.

Risiken einer ggf. rechtswidrigen Offenlegung eigenständig zu bewerten oder weitergehende Betroffenenrechte geltend zu machen.[19] So wurde von dem Beschwerdeführer vorgetragen, es bestehe ein abstraktes Risiko, dass der Nachlasspfleger, dem die Inhalte des Schließfachs übergeben worden sind, selbst mit einer den Beschwerdeführer betreffenden Erbauseinandersetzung befasst sein könnte. Ungeachtet der Frage, wie wahrscheinlich es gewesen sein mag, dass der konkrete Nachlasspfleger zugleich anwaltlicher Vertreter der Gegenseite in einem sonstigen Rechtsstreit des Betroffenen war, ermöglicht Art. 15 DSGVO dem Betroffenen damit aber eine eigenständige Einschätzung des Sachverhalts, etwaiger Risiken und der aus seiner Sicht notwendigen Folgemaßnahmen.

Nachdem die verantwortliche Bank im Hinblick auf eine beabsichtigte Anordnung zur Auskunftserteilung im obigen Sinne nach § 28 VwVfG angehört wurde, ist sie dem Antrag des Beschwerdeführers „ohne Anerkennung einer Rechtspflicht" nachgekommen. Da sich die Beschwerdegegnerin der Rechtsauffassung der Aufsichtsbehörde inhaltlich somit nicht anschloss, wurde für den Fall zukünftiger, vergleichbar gelagerter Sachverhalte eine Warnung nach Art. 58 Abs. 2 lit. a DSGVO ausgesprochen.

Auskunft über Zugriffe durch Mitarbeitende

Ein Kunde beantragte bei seiner Bank Auskunft über die zu seiner Person gespeicherten personenbezogenen Daten. Insbesondere forderte er Informationen darüber, welche Mitarbeitenden der Bank im Laufe der letzten Jahre Zugriff auf sein Konto genommen hatten, da er befürchtete, dass diese Zugriffe rechtswidrig und ohne berechtigten Anlass erfolgt sein könnten. Das Kreditinstitut hatte den Beschwerdeführer sodann aufgefordert, einen etwaigen Verdacht bezüglich unrechtmäßiger Kontozugriffe unter Nennung des Namens konkreter Mitarbeitenden und des Zeitraums des unberechtigten Zugriffs zu spezifizieren, da aus datenschutzrechtlichen Gründen nur dann weitere Auskünfte erteilt werden könnten. Der Beschwerdeführer hatte anschließend gegenüber seiner Bank klargestellt,

19) EuGH, Urteil vom 12.01.2023 - C-154/21, Rn. 33 ff.

dass sein Antrag nach Art. 15 DSGVO auch die Zurverfügungstellung einer Kopie seiner personenbezogenen Daten bedinge, was insbesondere auch sämtliche Protokolldaten, aus denen etwaige Zugriffe auf sein Konto durch Mitarbeitende der Bank ersichtlich sind, umfasse. Das Kreditinstitut vertrat weiterhin die Auffassung, dass eine Auskunft über die Identität konkreter Mitarbeitender ohne Mitteilung eines belastbaren Verdachts nicht möglich sei. Der Betroffene wandte sich daher mit einer Beschwerde an unsere Dienststelle.

Grundsätzlich ergibt sich aus Art. 15 Abs. 1 lit. c DSGVO ein Anspruch der betroffenen Person auf Auskunft über Empfänger, gegenüber denen personenbezogene Daten offengelegt wurden:

Mitarbeitende einer verantwortlichen Stelle sind dabei in der Regel nicht als Empfänger im Sinne des Art. 4 Nr. 9 DSGVO einzuordnen, wenn sie personenbezogene Daten lediglich unter Aufsicht der verantwortlichen Stelle und im Einklang mit deren Weisungen verarbeiten.[20] Vor diesem Hintergrund ist über konkrete Mitarbeitende allenfalls dann Auskunft zu geben, sofern diese in einem sog. Mitarbeiterexzess handeln, mithin rechtswidrig bzw. außerhalb der bankinternen Regularien Zugriff auf (Konto-)Informationen genommen haben. Erhält das Kreditinstitut von einem solchen Vorgang Kenntnis, ist es seinerseits nach Art. 33 DSGVO zur Meldung des Vorfalls verpflichtet. Es ist dabei grundsätzlich zweckmäßig und zulässig, wenn das Kreditinstitut zumindest die Glaubhaftmachung eines Verdachts fordert, dass Mitarbeitende ggf. entgegen internen Weisungen auf ein Konto zugegriffen haben, sofern im Übrigen durch interne, technisch-organisatorische Maßnahmen hinreichend sichergestellt ist, dass in der Regel keine weisungswidrigen Zugriffe erfolgen.

Entgegen der Aussage der Bank erfordert dies im Rahmen der Geltendmachung des Auskunftsrechts aber nicht zwangsläufig die Nennung eines konkreten Namens oder Zeitraums des unberechtigten Zugriffs durch die um Auskunft ersuchende Person, da ihr diese Informationen in der Regel

20) EuGH, Urteil vom 22.06.2023 - C-579/21.

gerade nicht vorliegen dürften; Anforderung ist daher allenfalls, dass der Betroffene Umstände darlegt, die einen weisungswidrigen Zugriff denkbar erscheinen lassen. In diesem Fall hat das Kreditinstitut die Pflicht, den Sachverhalt weitergehend aufzuklären. Denn nur nach interner Aufklärung ist es dazu in der Lage zu entscheiden, ob die Identität eines Mitarbeitenden nach Art. 15 DSGVO offenzulegen ist, weil dieser beim Zugriff auf Informationen eines Kunden im Mitarbeiterexzess gehandelt hat.

Mit Blick auf die Anforderung einer Kopie etwaiger Protokolldaten, war darauf hinzuweisen, dass der Begriff des personenbezogenen Datums im Sinne des Art. 4 Nr. 1 DSGVO in der Regel weit auszulegen ist. Daher sind auch Protokolldaten, die etwaige Kontozugriffsvorgänge beinhalten, als personenbezogene Daten des Kontoinhabers einzuordnen. Auch diese sind damit im Falle der Anforderung einer Kopie nach Art. 15 Abs. 3 DSGVO zu beauskunften.

Dabei ist nach Art. 15 Abs. 4 DSGVO zu berücksichtigen, dass in der angeforderten Kopie der Protokolldaten ggf. Namen von Mitarbeitenden geschwärzt werden können, die weisungsgemäß auf die Kundeninformationen zugegriffen haben. Dies erfordert in jedem Einzelfall aber die positive Feststellung, dass die Tatbestandsvoraussetzungen aus Art. 15 Abs. 4 DSGVO erfüllt sind; danach darf das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen, was eine umfassende Abwägung der widerstreitenden Interessen von Antragsteller und den Mitarbeitenden erfordert. Dabei kann für die Abwägung von Bedeutung sein, ob die jeweiligen Mitarbeitenden bestimmungsgemäß auch im unmittelbaren Kundenkontakt arbeiten oder ob der Zugriff im Wege eines Mitarbeiterexzesses erfolgte. Denn soweit ein sich im Exzess handelnder Mitarbeiter ohnehin nach Art. 15 Abs. 1 lit. c DSGVO benannt werden muss, hat dieser auch kein schutzwürdiges Interesse an einer Schwärzung in den Protokolldaten. Die vorbezeichneten Fälle sind daher in aller Regel ein Indiz dafür, dass schutzwürdige Interessen der Mitarbeitenden nicht überwiegen, wenngleich auch hier eine Abwägung im Einzelfall erforderlich bleibt.

Aus hiesiger Sicht war es daher erforderlich, dass der Beschwerdeführer einerseits eine Kopie der Zugriffsprotokolle erhält, und eine Prüfung durch die Bank erfolgt, inwieweit eine Schwärzung etwaiger Namen bzw. Kennungen von Mitarbeitenden in den Protokolldaten zulässig ist. Im Rahmen eines Hinweises nach Art. 58 Abs. 1 lit. d DSGVO wurde der auskunftsverpflichteten Bank die hiesige Rechtsauffassung mitgeteilt. Das Verfahren war zum Ende des Berichtszeitraums noch nicht abgeschlossen.

4.2 Ausschluss des Auskunftsanspruchs durch gerichtlichen Vergleich

In unserem Tätigkeitsbericht für das Jahr 2023[21] befassten wir uns bereits näher mit der rechtlichen Möglichkeit einer vertraglichen Einschränkung bzw. des vertraglichen Ausschlusses des Auskunftsanspruchs aus Art. 15 Abs. 1, Abs. 3 DSGVO, insbesondere im arbeitsrechtlichen Kontext. Diese Thematik wird in der Literatur, soweit ersichtlich aber auch in der aufsichtsbehördlichen Praxis, bislang nicht einheitlich behandelt. So reichen die Positionen von einer generellen Verfügungsbefugnis des Betroffenen über diesen Anspruch bis hin zu dessen strikter Unabdingbarkeit, gegebenenfalls auch gegen den ausdrücklichen Willen des Betroffenen.[22]

In unserem 32. Tätigkeitsbericht legten wir unsere diesbezügliche Rechtsauffassung umfassend dar. Selbige ist getragen von dem Gedanken der Selbstbestimmtheit und Eigenverantwortlichkeit des Betroffenen, was auch dessen Verfügungsbefugnis über seine datenschutzrechtlichen Betroffenenrechte (Art. 12 ff. DSGVO) beinhalten muss. Das Verwaltungsgericht des Saarlandes[23] in erster sowie das Oberverwaltungsgericht des Saarlandes in zweiter Instanz[24] haben sich dieser Rechtsauffassung angeschlossen.

---

21) 32. Tätigkeitsbericht Datenschutz 2023, Kapitel 8.2.
22) Zusammenfassend: Fuhlrott/Garden: Vergleichsweise Erledigung des datenschutzrechtlichen Auskunftsanspruchs, NZA 2021, S. 530.
23) VG Saarland, Urteil vom 10.07.2024 - 5 K 979/22.
24) OVG Saarland, Urteil vom 13.05.2025 - 2 A 165/24.

Die Gerichte teilen insbesondere unsere Auffassung, dass ein Anspruchsverzicht hinsichtlich Datenverarbeitungen der Vergangenheit möglich sein soll. Im Rahmen einer vertraglichen Einigung oder eines gerichtlichen Vergleichs soll man folglich auf diejenigen Betroffenenrechte (Auskunftsansprüche) verzichten können, welche auf Datenverarbeitungen vor Vergleichsschluss abzielen.

Nun könnte man diesbezüglich einwenden, die Speicherung der Daten stelle keine solche Datenverarbeitung der Vergangenheit dar, sondern umfasse als andauernder und fortlaufender Prozess auch gegenwärtige und zukünftige Verarbeitungen. Entscheidender Bezugspunkt ist jedoch der Zeitpunkt der Datenerhebung und damit der Zeitpunkt der Festlegung des Verarbeitungszwecks. Wurden die Daten zeitlich vor dem erklärten Anspruchsverzicht des Betroffenen erhoben, so umfasst dieser Verzicht auch die Betroffenenrechte hinsichtlich der künftigen Speicherung dieser Daten, zumindest dann, wenn sich der weitere Verarbeitungszweck nicht wesentlich verändert hat. Auf die Konstellation eines Arbeitsverhältnisses bezogen bedeutet dies, dass der Arbeitnehmer (Betroffene) auf die künftige Auskunft der durch den Arbeitgeber verarbeiteten Daten verzichten kann, wenn die Erhebung dieser Daten zur Begründung und Durchführung des Arbeitsverhältnisses erfolgte, in aller Regel daher zeitlich vor dem Verzicht lag, und der Arbeitgeber diese Daten auch in Zukunft für diese Zwecke verarbeitet (speichert). Letzteres ist auch dann der Fall, wenn die Daten aufgrund rechtlicher Vorschriften Mindestspeicherfristen unterliegen, welche u. U. weit über das Ende des Arbeitsverhältnisses hinausreichen.

Neben der dogmatischen Richtigkeit dieser Rechtsauffassung, erachten wir diese auch für praktikabel und interessengerecht. Sie führt weder zu einer subjektiven Benachteiligung des Betroffenen noch zu einer objektiven Herabsetzung des Datenschutzniveaus im Bereich der Betroffenenrechte. Ist es der freie erklärte Wille von Verantwortlichem und Betroffenen, in Zukunft nichts mehr miteinander zu tun zu haben und folglich sämtliche offenen oder verborgenen Ansprüche gegenseitig auszuschließen, so wäre es ein untragbares Ergebnis, sie aufgrund vermeintlicher datenschutzrechtlicher Erfordernisse weiterhin aneinander zu binden oder eine

abschließende gütliche Einigung hieran scheitern zu lassen. Es liegen auch keine von den subjektiven Interessen losgelösten objektiven Interessen der Allgemeinheit vor, die es erfordern würden, dass die datenschutzrechtlichen Betroffenenrechte zwischen den Parteien nicht disponibel sein sollten.

Es bleibt abzuwarten, wie sich die Rechtsauffassung in diesem Bereich weiterentwickelt. Durch die vorgenannten gerichtlichen Entscheidungen sehen wir uns in unserer Behördenpraxis jedenfalls bestätigt und werden auch künftige gleichgelagerte Fälle in diesem Sinne entscheiden.

4.3 Wenn Algorithmen über Mobilität entscheiden

In urbanen Räumen können Carsharing-Angebote eine wichtige Ergänzung individueller Mobilität darstellen. Ein nach Einholung einer Bonitätsauskunft ohne Interventionsmöglichkeit automatisiert erklärter Nutzungsausschluss kann daher für Betroffene in erheblichem Maße nachteilige Effekte nach sich ziehen. Werden, wie dies in einem beschwerdegegenständlichen Verfahren im Berichtszeitraum untersucht wurde, in einem Buchungsprozess eines Carsharing-Anbieters Interessentinnen und Interessenten allein gestützt auf einen extern eingeholten Score-Wert ohne weitere Interventionsmöglichkeit durch Mitarbeitende des Verantwortlichen abgelehnt, kann dies einen Verstoß gegen Art. 22 Abs. 1 DSGVO darstellen. Hiernach hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Im Rahmen des aufsichtsbehördlichen Verfahrens erklärte der Verantwortliche zwar, dass für den Buchungsprozess im Fall einer bonitätsbedingt drohenden Ablehnung zunächst eine Kontaktmöglichkeit mit kundenbetreuenden Mitarbeitenden vorgesehen war, diese Vorgabe sei allerdings letztlich nicht operationalisiert worden, so dass Buchungsanfragen

einzelner Interessentinnen und Interessenten aufgrund eingeholter Bonitätsauskünfte automatisiert abgewiesen wurden. Diese ohne weitere menschliche Prüfung erfolgte Ablehnung des Vertragsabschlusses war als erhebliche Beeinträchtigung im Sinne des Art. 22 Abs. 1 DSGVO zu qualifizieren.

Allein die subjektive Wahrnehmung einer Entscheidung als belästigend, unangenehm oder benachteiligend reicht dabei regelmäßig nicht aus, um von einer erheblichen Beeinträchtigung auszugehen; ob durch eine automatisierte Entscheidung diese Erheblichkeitsschwelle überschritten wird, ist im Einzelfall unter objektiven Gesichtspunkten zu beurteilen.[25] Während dies unter Berücksichtigung von Erwägungsgrund 71 der DSGVO beispielsweise für den Fall der Ablehnung eines Online-Kreditantrags oder bei Online-Einstellungsverfahren ohne menschliches Zutun gelten kann, kann dies nicht für jedwede Vertragsablehnung unterstellt werden. Würden substanzielle Nachteile im Sinne der Vorschrift allerdings vorrangig auf die Angebotsebene von Quasi-Monopolisten oder Versorgungsunternehmen[26] beschränkt werden, würde der Schutzzweck der Norm überwiegend ins Leere laufen. Überzeugender ist es daher darauf abzustellen, ob die der Vertragsablehnung vorausgehende automatisierte Entscheidung für die Lebensführung einer betroffenen Person spürbare Auswirkungen haben kann.[27]

Unstrittig ist ein von einem privaten Unternehmen angebotenes Carsharing kein Bestandteil des öffentlichen Personennahverkehrs (ÖPNV), jedoch sind solche Angebote integrale, den ÖPNV ergänzende Elemente multimodaler Mobilitätskonzepte und damit für die Gewährleistung individueller Mobilität im urbanen Raum durchaus als wesentlich zu betrachten. Ein derartiger automatisierter Vertragsausschluss kann für die individuelle Lebensführung und die Angewiesenheit auf ergänzende Mobilitätsangebote deutlich

25) von Lewinski, in BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg, 53. Edition, Art. 22 Rn. 38, beck-online.
26) von Lewinski a. a. O., Rn. 39a, beck-online.
27) Buchner, in Kühling/Buchner, 4, DS-GVO BDSG 4. Auflage 2024, Art. 22, Rn. 27, beck-online; Martini, in Paal/Pauly, DS-GVO BDSG 3. Auflage 2021, Art. 22, Rn. 27; Scholz, in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2. Auflage 2025, Rn. 38.

nachteiligere Auswirkungen entfalten als die Ablehnung eines Erwerbs von Allerweltsgegenständen.[28]

Da überdies keine Ausnahme nach Art. 22 Abs. 2 DSGVO vorgelegen hat – insbesondere war die Entscheidung nicht für den Abschluss oder die Erfüllung eines Vertrags erforderlich – wurde aufsichtsbehördlich ein Verstoß festgestellt. Der Verantwortliche modifizierte daraufhin den Buchungsprozess entsprechend seiner eigenen ursprünglichen Vorgabe.

4.4 Telefonwerbung: Wer darf was – und wer kontrolliert?

Auch im siebten Jahr nach Geltungseintritt der DSGVO sind im Bereich der Direktwerbung wesentliche Fragen zu datenschutzrechtlichen Pflichten der Verantwortlichen und der Aufsichtszuständigkeit der Datenschutzbehörden noch klärungsbedürftig. Das Bundesverwaltungsgericht (BVerwG) und der Europäische Gerichtshof (EuGH) haben sich im Berichtszeitraum mit dem Verhältnis zwischen Datenschutzrichtlinie für elektronische Kommunikation – Richtlinie 2002/58/EG (RL 2002/58/EG) und DSGVO auseinandergesetzt und hierzu unterschiedliche Aussagen getroffen.

Im Januar des Berichtszeitraums hat das BVerwG über einen Sachverhalt zur werblichen Datenverarbeitung im B2B-Bereich, der bereits im Jahr 2016 unsere Behörde als Eingabe erreicht hat, abschließend entschieden.[29] Nach diesem höchstrichterlichen Urteil vom 29. Januar 2025 – BVerwG 6 C 3.23 – erfolgte die bereits im Jahr 2017 aufsichtsbehördlich untersagte Verarbeitung personenbezogener Daten von Einzelzahnärztinnen und –ärzten für Zwecke der telefonischen Direktwerbung durch ein auf den Dentalgoldhandel spezialisiertes Unternehmen in datenschutzrechtlich unzulässiger Weise. Das BVerwG statuierte, dass für die streitgegenständliche Werbeansprache keine (mutmaßliche) Einwilligung im Sinne des § 7 Abs. 2 Nr. 1

28) Buchner a. a. O.
29) Vgl. 27. Tätigkeitsbericht Datenschutz 2017/2018, Kapitel 14.3., S. 132 ff; 30. Tätigkeitsbericht Datenschutz 2021, Kapitel 4.22, S. 112 ff.

Gesetz gegen den unlauteren Wettbewerb (UWG) vorgelegen hat und mit der ihr zugrundeliegenden Datenverarbeitung damit auch kein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit. f DSGVO verfolgt werden konnte.

Auch wenn die Revision gegen das Urteil des Oberverwaltungsgerichts des Saarlandes (OVG) vom 02. Mai 2023 – A 111/22[30] – damit letztlich zurückgewiesen wurde und unsere bereits im Jahr 2016 erlassene Untersagungsverfügung letztinstanzlich bestätigt wurde, erkannte das BVerwG in der angegriffenen Entscheidung der Vorinstanz Verstöße gegen revisibles Recht. So hatte das OVG statuiert, dass mit Blick auf die Öffnungsklausel in Art. 13 Abs. 3 RL 2002/58/EG und die nationale Umsetzung in § 7 Abs. 2 Nr. 1 UWG im zu entscheidenden Fall ausschließlich auf die Einwilligung der Werbeadressaten nach Art. 6 Abs. 1 lit. a DSGVO abgestellt werden könne und ein Rückgriff auf die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO ausscheide. Das BVerwG stellt allerdings unter Bezugnahme auf Art. 95 DSGVO und das Verhältnis zwischen der RL 2002/58/EG und der DSGVO fest, dass Art. 13 Abs. 3 RL 2002/58/EG in der Form der mitgliedstaatlichen Umsetzung in § 7 Abs. 2 Nr. 1 UWG und Art. 6 Abs. 1 lit. f DSGVO nebeneinander anzuwenden sind; im Fall der Wettbewerbswidrigkeit der Werbeansprache wird somit kein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit. f DSGVO verfolgt und die zugrundeliegende Verarbeitung der personenbezogenen Daten für Zwecke der Direktwerbung war als datenschutzrechtlich unzulässig zu qualifizieren.

Diese Entscheidung des BVerwG begegnete in der Literatur im Hinblick auf die Auslegung von Art. 95 DSGVO und des Verhältnisses der beiden Rechtsakte RL 2002/58/EG und DSGVO teilweise grundsätzlicher Kritik.[31] Danach suspendiere Art. 95 DSGVO lediglich zusätzliche Pflichten der DSGVO, soweit der Verantwortliche besonderen Pflichten nach der RL 2002/58/EG unterliegt, die dasselbe Ziel verfolgen. Für eine Werbeansprache würden ausschließlich die spezifischen Regelungen nach Art. 13 RL 2002/58/EG in Form des § 7 UWG gelten, so dass ein Rückgriff auf Art. 6 DSGVO

30) Vgl. 32. Tätigkeitsbericht Datenschutz 2023, Kapitel 11.3.
31) Golland, Alexander „Schnittstelle Wettbewerbs- und Datenschutzrecht: Anforderungen an die Zulässigkeit von Direktwerbung", in Datenschutz-Berater Nr. 05/2025, S. 140–142.

ausgeschlossen und eine Datenschutzaufsichtsbehörde nicht für die mit der Werbeansprache verbundene Datenverwendung aufsichtszuständig sei. Damit korrespondiert zunächst auch, dass der EuGH mittlerweile zur einwilligungsfreien Bestandskundenwerbung entschieden hat, dass für einen werblichen E-Mailversand, der die Voraussetzungen von Art. 13 Abs. 2 RL 2002/58/EG[32] kumulativ erfüllt, keine zusätzlichen datenschutzrechtlichen Voraussetzungen nach Art. 6 Abs. 1 DSGVO zu prüfen sind.[33]

Allein mit Blick auf das angeführte Urteil des EuGH ergeben sich für Verantwortliche – gleichgültig, ob diese Telefon- oder E-Mail-gestützte Direktwerbung betreiben – jedoch keine wesentlichen Erleichterungen hinsichtlich der Berücksichtigung datenschutzrechtlicher Vorgaben oder potenzieller Prüfmaßnahmen der Datenschutzaufsichtsbehörden. Angesichts der Entscheidung des EuGH zur Bestandskundenwerbung ist für die Versendung der Werbe-E-Mails abschließend das Vorliegen der Voraussetzungen von Art. 13 Abs. 2 RL 2002/58/EG resp. § 7 Abs. 3 UWG zu prüfen. Für dieser Datennutzung vor- und nachgelagerte Schritte der Verarbeitung personenbezogener Daten von Werbeadressaten – wie Erhebung, Abgleich mit Werbesperrlisten, Speicherung, Veränderung, Übermittlung etc. – sowie Informations- und Betroffenenrechte gelten die datenschutzrechtlichen Vorgaben uneingeschränkt.[34] Der einheitliche Vorgang der unternehmerischen Werbetätigkeit wird damit hinsichtlich der Zulässigkeitsbedingungen rechtlich fragmentiert. Gerade für außerhalb bestehender Geschäftsbeziehungen erfolgende Werbemaßnahmen zur Kundengewinnung („Kaltakquise") und der damit verbundenen Datenverarbeitung bedeutet dies ferner, dass einer nach RL 2002/58/EG resp. UWG rechtswidrigen Datennutzung für Werbe-Anrufe/-E-Mails regelmäßig keine nach der DSGVO zulässige Datenerhebung und -speicherung vorausgehen kann.
Ob datenschutzrechtliche Pflichten nach der DSGVO gegebenenfalls doch für den Fall noch maßgeblich sein können, wenn die Voraussetzungen von Art. 13 Abs. 2 RL 2002/58/EG beziehungsweise § 7 UWG für die

32) Umgesetzt in nationales Recht in § 7 Abs. 3 UWG.
33) EuGH, Urteil vom 13.11.2025 - C-654/23, Rn. 69.
34) EuGH, a. a. O., Rn. 48.

Datenverwendung nicht erfüllt sind, ist zumindest diskussionswürdig. Der Generalanwalt Szpunar hat in seinen der EuGH-Entscheidung vorausgehenden Schlussanträgen[35] ausgeführt, dass ein Rückgriff auf Art. 6 DSGVO dann nicht erforderlich ist, wenn „[...] die Verarbeitung personenbezogener Daten auf der Grundlage dieser Bestimmung [Art. 13 Abs. 2 RL 2002/58/EG] für rechtmäßig befunden worden ist." Der EuGH seinerseits statuiert, dass datenschutzrechtliche Vorgaben nach Art. 6 Abs. 1 DSGVO nicht gelten, wenn der werbliche E-Mail-Versand gemäß Art. 13 Abs. 2 RL 2002/58/EG stattfindet.[36]

Die Aussagen des Generalanwalts und des Gerichts lassen damit einen Auslegungsspielraum zu, wonach Art. 13 RL 2002/58/EG nur dann die werbliche Datennutzung abschließend und ohne Notwendigkeit des Rückgriffs auf die DSGVO regelt, wenn die Voraussetzungen der Vorschrift kumulativ erfüllt sind und die Werbeansprache danach rechtmäßig erfolgt. Dies hieße im Umkehrschluss, dass bei einer nicht nach Art. 13 Abs. 2 RL 2002/58/EG gestatteten Datenverwendung Art. 6 Abs. 1 lit. f DSGVO wieder als Prüf- und Zulässigkeitsmaßstab in Frage kommen könnte.[37] Überdies stellt die in Art. 13 Abs. 1 RL 2002/58/EG normierte Einwilligung als Voraussetzung für werbliche Kontaktaufnahmen den Regelfall dar. Über Art. 2 lit. f RL 2002/58/EG in Verbindung mit Art. 94 Abs. 2 DSGVO gelten für diese Einwilligung die Wirksamkeitsvoraussetzungen der DSGVO, so dass über diesen Verweis eine Legitimationsgrundlage im Sinne des Art. 4 Nr. 11 in Verbindung mit Art. 6 Abs. 1 lit. a DSGVO gegeben sein muss.

Auch in der Annahme, dass die Zulässigkeitsbedingungen für die Werbeansprachen unter Verwendung elektronischer Kommunikationsmittel und die damit verbundene Datennutzung ausschließlich nach den Vorgaben der RL 2002/58/EG ohne Rückgriff auf Art. 6 DSGVO zu beurteilen ist, kann eine Aufsichtszuständigkeit der Datenschutzaufsichtsbehörden unterstellt

35) Generalanwalt beim EuGH, 27.03.2025 - C-654/23, Rn. 52.
36) EuGH, a. a. O., Rn. 69.
37) Allerdings kann nach der BVerwG-Entscheidung mit einer wettbewerbswidrigen Datenverwendung kein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit. f DSGVO verfolgt werden.

werden. Nach § 20 Abs. 1 Saarländisches Datenschutzgesetz kontrolliert die saarländische Landesbeauftragte für Datenschutz und Informationsfreiheit die Einhaltung der Vorschriften der DSGVO und anderer datenschutzrechtlicher Bestimmungen. Ungeachtet der Form der nationalen Umsetzung, handelt es sich bei den Vorschriften der RL 2002/58/EG um solche mit datenschutzrechtlichem Wesenskern, die laut Rechtsprechung der sachlichen Prüfungskompetenz der Datenschutzaufsichtsbehörden unterworfen sein können.[38]

Soweit vor diesem Hintergrund in der Literatur vertreten wird, dass angesichts unterschiedlicher Schutzzwecke und -güter der RL 2002/58/EG und der DSGVO eine Aufsichtszuständigkeit der Datenschutzbehörden nicht vorliegen könne, kann dies nicht überzeugen. Art. 13 Richtlinie 2002/58/EG dient mit Blick auf Erwägungsgrund 40 der Richtlinie zunächst dem Privatsphärenschutz im Sinne von Art. 7 Grundrechtecharta der Europäischen Union (GRCh); der Schutzbereich der Richtlinie ist allerdings auch anhand der in Art. 1 Abs. 1 in Verbindung mit Abs. 2 RL 2002/58/EG und Erwägungsgrund 2 konturierten normativen Zielsetzung, wonach ein gleichwertiger Schutz der Grundrechte und Grundfreiheiten „insbesondere des Rechts auf Privatsphäre, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation […]“ in der Gemeinschaft gewährleistet werden soll, und unter Berücksichtigung des Verhältnisses des den Rechtsakten zugrundeliegenden Primärrechts zu beurteilen. Der Privatsphärenschutz nach Art. 7 GRCh und der Schutz personenbezogener Daten nach Art. 8 GRCh werden dabei nicht als autonome Schutzgüter interpretiert, sondern es wird vielmehr von korrespondierenden Schutzzielen und einer „einheitlichen Schutzverbürgung“ ausgegangen,[39] die letztlich für eine Aufsichtszuständigkeit der Datenschutzbehörden für die Datenverwendung im Rahmen der E-Mail- und Telefon-gestützten Direktwerbung spricht.

---

38) Verwaltungsgericht des Saarlandes, Urteil vom 29.10.2019 - 1 K 732/19, Rn. 117, juris; zu § 25 Telekommunikation-Telemedien-Datenschutzgesetz: Verwaltungsgericht Hannover, Urteil vom 19.03.2025 – 10 A 5385/22, Rn. 65 ff., juris..
39) EuGH, Urteil vom 17.06.2021 – C-597/19, Rn. 113 ff. Bundesverfassungsgericht, Beschluss vom 06.11.2019 - 1 BvR 276/17, BVerfGE 152, 216-274, Rn. 99-101, juris.

4.5 Videoüberwachung

Soweit Beschwerden und Hinweise zu Videoüberwachungsmaßnahmen seit Jahren den Löwenanteil der an das Datenschutzzentrum adressierten Anliegen ausmachen, war im zurückliegenden Berichtszeitraum erneut ein erheblicher Anstieg der Fallzahlen von 255 (2024) auf 343 zu verzeichnen. Während die Anzahl der vorgetragenen Videoüberwachungsmaßnahmen im unternehmerischen Kontext, hier vor allem im Gastgewerbe und hinsichtlich der Überwachung von Mitarbeitenden, weitgehend auf konstantem Niveau blieb, sind Anfragen und Beschwerden zu von Privatpersonen betriebenen Überwachungsmaßnahmen erheblich angestiegen.

Dabei sind die faktischen Möglichkeiten der Aufsichtsbehörde bezüglich einer noch einzelfallangemessenen Sachbefassung mit Anliegen zur privaten Videoüberwachung und die Erwartungshaltung der beschwerdeführenden Personen häufig nicht deckungsgleich. Oftmals werden zeitnahe Aufsichtsmaßnahmen, Vorortprüfungen, die Entfernung von Kameras und die Verhängung von Geldbußen verlangt, ohne dass dies mit den gegebenen Ressourcen überhaupt leistbar oder sachgerecht wäre. Dem liegt häufig auch eine datenschutzferne Motivlage zugrunde, soweit streitbehaftete Nachbarschaftsverhältnisse zu wechselseitigen Beschwerden, zu einer erheblichen Aufladung von Verfahren und damit zwangsläufig auch zu einer generellen Zunahme der Verfahrensdauern führen.

Überwachung von Verkaufsautomaten

Im Berichtszeitraum adressierten wiederholt Beschwerden und Kontrollanregungen die kameragestützte Überwachung von Verkaufsautomaten. Im öffentlichen Raum sind mittlerweile eine Vielzahl von Warenautomaten zu finden, mit denen ganztägig unterschiedlichste Bedürfnisse in einem zumeist niedrigpreisigen Marktsegment gedeckt werden können. Die angebotenen Produktsortimente sind dabei genauso vielgestaltig wie die anzutreffenden Überwachungsszenarien.

Im Rahmen der durchgeführten Untersuchungen wurde dabei oftmals erkennbar, dass den Kameraeinsätzen keine tragfähigen datenschutzrechtlichen Rahmenkonzepte zugrunde gelegt wurden oder Vorüberlegungen vorausgegangen sind, sondern diese nahezu beliebig ausgestaltet waren. So konnten die mit der Überwachung verfolgten Zwecke bzw. die angeführten Gefährdungen häufig nicht auf eine belastbare Tatsachengrundlage gestützt werden oder die räumliche Ausdehnung der Überwachung ging erheblich über das zur Wahrnehmung der verfolgten Schutzzwecken erforderliche Maß hinaus; in Einzelfällen wurde so statt der fokussierten Überwachung eines einzelnen Verkaufsautomaten die vollkommen unverhältnismäßige Erfassung ganzer Straßenzüge festgestellt. Auch eine hinreichende Transparenz durch eine Informationserteilung im Sinne des Art. 13 DSGVO durch geeignete Hinweisschilder war oftmals nicht gewährleistet. In einem der untersuchten Fälle wurde ein Verfahren nach dem Ordnungswidrigkeitengesetz eingeleitet.

Grundsätzlich kann eine kameragestützte Überwachung solcher Verkaufsautomaten zulässig sein, wenn die Rahmenbedingungen nach Art. 6 Abs. 1 lit. f DSGVO Berücksichtigung finden, d. h. wenn der Kameraeinsatz zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und schutzwürdige Interessen und Grundfreiheiten der betroffenen Personen nicht überwiegen.

- Als berechtigtes Interesse gilt nicht nur ein rechtliches, sondern auch jedes nicht von der Rechtsordnung missbilligte tatsächliche Interesse wirtschaftlicher oder ideeller Art. Das Interesse an der Videoüberwachung muss objektiv begründbar sein und sich aus einer konkreten Sachlage ergeben. So kann im Kontext der Warenautomaten die Verhütung von Vandalismusschäden oder der Schutz vor Eigentumsdelikten als berechtigtes Interesse Berücksichtigung finden, jedoch muss die Gefahr durch konkrete, einzelfallbezogene Tatsachen begründbar sein; das heißt, der Kamerabetreiber muss konkrete Tatsachen anführen, aus denen sich eine Gefährdungslage ergibt, die über das allgemeine Lebensrisiko hinausgeht.[40]

40) BVerwG, Urteil vom 27.03.2019 - 6 C 2.18, Rn. 28, juris.

Für Automatenbetreiber ist daher entscheidend, dass durch eine hinreichende Dokumentation von bereits eingetretenen Schadensereignissen (bspw. in Form von Schadensmeldungen an Versicherungen oder Polizeidienststellen) eine konkrete Gefährdungslage belegt werden kann. Zwar kann auch eine prognostische Beschreibung eines spezifischen Gefährdungsrisikos zur Glaubhaftmachung ausreichend sein, allerdings muss die Gefahrenprognose objektiv belastbar sein. So ist es nicht ausreichend, wenn ein Überfallrisiko auf Mitarbeitende skizziert wird, allerdings weder das niedrigpreisige Warensortiment noch die regelmäßig geringe Bargeldmenge allein für ein solches Gefährdungsrisiko für Mitarbeitende sprechen.

- Ein belastbares berechtigtes Interesse reicht allein nicht aus, die Überwachungsmaßnahme muss für die Erreichung dieser Zwecke auch erforderlich sein. Das Erforderlichkeitsmerkmal ist ausschließlich dann gegeben, wenn der Verarbeitungszweck nicht in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden kann, die weniger stark in die Grundrechte und -freiheiten der betroffenen Personen eingreifen. Zudem ist die Erforderlichkeit gerade auch unter Berücksichtigung des Grundsatzes der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO zu beurteilen und für kameragestützte Überwachungsmaßnahmen dementsprechend eine Beschränkung der Überwachung in räumlichem und/oder zeitlichem Kontext auf das notwendige Maß hin zu prüfen.

  Da Schadenshandlungen zumeist unmittelbar in räumlicher Nähe zum Verkaufsautomaten drohen, kann eine weiträumige Erfassung eines ganzen Straßenzuges nicht mit dem Erforderlichkeitsmerkmal und dem Grundsatz der Datenminimierung in Einklang stehen. Zulässig kann allenfalls eine räumlich fokussierte Überwachung des nahen Umfelds des Verkaufsautomaten sein und gegebenenfalls ist zu prüfen, inwiefern durch eine geänderte Aufstellung die mit der Überwachung verbundene Eingriffstiefe reduziert werden kann.

- Im Rahmen der eigentlichen Interessenabwägung sind die grundrechtlich geschützten Positionen des Kamerabetreibers – hier vor allem die

unternehmerische Freiheit im Sinne des Art. 16 Grundrechtecharta der Europäischen Union (GRCh) und der Schutz des Eigentums aus Art. 17 GRCh – gegen das Grundrecht der Betroffenen auf Datenschutz (Art. 8 GRCh) abzuwägen. Die Interessen und Grundrechte und Grundfreiheiten von Verkehrsteilnehmern, Passanten sowie Anwohnern, die im Rahmen räumlich weitreichender Überwachungsmaßnahmen im öffentlichen Verkehrsraum und auf fremden Grundstücken betroffen sind, überwiegen dabei regelmäßig das verfolgte Überwachungsinteresse. Zwar werden diese im öffentlichen Raum nur in ihrer Sozialsphäre tangiert, jedoch streitet für die betroffenen Personen der Umstand, dass ihre Interessen oder Grundrechte und Grundfreiheiten, die in die Abwägung miteinzubeziehen sind, gerade auch mit Blick auf Erwägungsgrund 47 durch die spezifische vernünftige Erwartungshaltung der betroffenen Personen konturiert werden.

Im Fall einer räumlich ausgedehnten Überwachung von Verkaufsautomaten geben erfasste Personen überwiegend weder Anlass zu ihrer Überwachung noch können sie sich ihr je nach Ausgestaltung entziehen. Mit Blick auf die zumeist unmittelbar an einem Verkaufsautomaten angebrachten Hinweisschilder haben Betroffene vor Betreten des überwachten Bereichs auch häufig keine Gelegenheit, diese Pflichtinformationen nach Art. 13 DSGVO zur Kenntnis zu nehmen. Vor diesem Hintergrund kann datenschutzrechtlich allenfalls eine räumlich eng begrenzte, klar auf den Automaten ausgerichtete Kameraüberwachung zulässig sein.

Transparenz als Zulässigkeitsmaßstab für Kameraeinsätze

Die Herstellung hinreichender Transparenz gegenüber der von einer Datenverarbeitung betroffenen Person ist zwingende Folge der bereits in Art. 5 Abs. 1 lit. a DSGVO normierten Nachvollziehbarkeit. Während für die Einwilligung nach Art. 4 Nr. 11 in Verbindung mit Art. 6 Abs. 1 lit. a DSGVO eine hinreichende Informiertheit eine bereits tatbestandliche Wirksamkeitsvoraussetzung darstellt, erkannte die Rechtsprechung im Zusammenhang mit der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO in einer unzureichenden Umsetzung des Transparenzgebots zwar auch einen

sanktionswürdigen Verstoß, verneinte allerdings eine unmittelbare Auswirkung des Transparenzdefizits auf die Zulässigkeit der zugrundeliegenden Datenverarbeitung; d. h. trotz des Fehlens oder der Unvollständigkeit einer Information nach Art. 13 DSGVO gegenüber der betroffenen Person, konnte die für sie intransparente Datenverarbeitung als zulässig erachtet werden.[41]

Während gemessen am Maßstab der vernünftigen Erwartung der betroffenen Person im Sinne des Erwägungsgrunds 47 der DSGVO bei Transparenzdefiziten eine für die von einer Datenverarbeitung betroffenen Person objektiv fernliegende, überraschende Datenverarbeitung grundsätzlich kaum nach Art. 6 Abs. 1 lit. f DSGVO legitimiert werden konnte, schärft der Europäische Gerichtshof[42] die unmittelbare Bedeutung von Transparenz für die Zulässigkeit der damit verbundenen Datenverarbeitung nach. Das Gericht statuiert dabei, dass eine Nichterfüllung der Information über das durch den Verantwortlichen verfolgte berechtigte Interesse zum Zeitpunkt der Datenerhebung zur Folge hat, dass eine Datenverarbeitung sodann nicht auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden kann.

So einleuchtend diese Auslegung des EuGH zunächst klingt, so weitreichend sind die Folgen für die Bandbreite möglicher kameragestützter Verarbeitungshandlungen, die ganz überwiegend ausschließlich gestützt auf die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO erfolgen können. Während sich hinreichende Transparenz durch Hinweisschilder für stationäre Überwachungsmaßnahmen weitestgehend unproblematisch erreichen lässt, kann eine Informationserteilung für mobile Kameraeinsätze oftmals nicht garantiert werden; denn potenziell nicht begrenzte Erfassungsbereiche erschweren die Herstellung hinreichender Transparenz gegenüber allen von der Überwachung betroffenen Personen. Die bisher offene Frage, ob dabei Informationspflichten

41) Bspw. Österreichisches Bundesverwaltungsgericht, Urteil vom 11.12.2023 - W137 2259819-1; Schleswig-Holsteinisches Verwaltungsgericht, Urteil vom 07.08.2024 - 8 A 159/20, Rn. 54 ff., juris.
42) EuGH, Urteil vom 09.01.2025 – C-394/23, Rn. 52.

nach Art. 13[43] oder Art. 14 DSGVO[44] gelten, ist mit dem Urteil des EuGH vom 18. Dezember 2025[45] zugunsten von Art. 13 DSGVO entschieden worden.

Da eine Anzahl an Beschwerden und Kontrollanregungen gerade auch mobile Kameraeinsätze zum Gegenstand hat, ergeben sich in diesem Zusammenhang mit Blick auf das nunmehr zwingende Transparenzgebot grundsätzliche Fragen zur Einsatzzulässigkeit. Angesichts einer Zunahme an Verfahren betreffend den Einsatz von Dashcams in privaten Fahrzeugen, ist unter Zugrundelegung der Rechtsprechung des EuGH einstweilen offen, wie eine solche Datenverarbeitung, der typischerweise Beweissicherungsinteressen im Zusammenhang mit Unfallgeschehen zugrunde liegen, datenschutzrechtlich legitimiert sein kann; denn selbst für den Fall der Anbringung eines den Vorgaben nach Art. 13 DSGVO genügenden Hinweisschildes ist aufgrund der häufig anzutreffenden räumlichen Ausdehnung der Erfassungsbereiche gerade räumlich-situativ nicht gewährleistet, dass betroffene Passanten, Verkehrsteilnehmer und sonstige Dritte Gelegenheit haben, das angebrachte Schild und die darin enthaltenen Information zur Kenntnis zu nehmen. Dabei können für die Betroffenheit auch spezifische technische Rahmenbedingungen der Datenverarbeitung bspw. die Aufnahme lediglich wenige Sekunden umfassender Loops, die nur im Ereignisfall länger gespeichert werden, oder sog. Blackbox-Verfahren keinen Unterschied machen.

4.6 E-Mail an den Chef: Forderungsdurchsetzung als Datenschutzverstoß

Eine Verarbeitung personenbezogener Daten zur Verfolgung und Durchsetzung zivilrechtlicher Ansprüche ist in weitem Umfang datenschutzrechtlich zulässig. Gläubiger einer Forderung haben grundsätzlich ein berechtigtes Interesse rechtlicher und wirtschaftlicher Art daran, bestehende oder

43) Schleswig-Holsteinisches Verwaltungsgericht, a. a. O., Rn. 44 ff.; Europäischer Datenschutzausschuss, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Rn. 110.
44) Verwaltungsgericht Ansbach, Beschluss vom 22.03.2024 – AN 14 K 22.00995 (nicht veröffentlicht).
45) EuGH, Urteil vom 18.12.2025 - C-422/24, Rn. 33 ff.

vermeintliche Forderungen gegenüber ihren Schuldnern durchzusetzen, entweder selbst oder unter Zuhilfenahme einer damit beauftragte dritten Person, beispielsweise einen Rechtsanwalt. Die Rechtsgrundlage für die Verarbeitung der diesbezüglichen Betroffenendaten (Schuldnerdaten) folgt regelmäßig aus Art. 6 Abs. 1 lit. f DSGVO.[46]

Auch zu Zwecken der Kontaktaufnahme mit dem Schuldner ist es neben den gesetzlich geregelten Registerabfragen, in erster Linie der Melderegisterabfrage nach den §§ 44 f. Bundesmeldegesetz, daher zulässig, dass Gläubiger oder Rechtsanwälte auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO eigenständig Recherchen über das Internet oder die sozialen Netzwerke durchführen, um die Anschrift des Schuldners in Erfahrung zu bringen. Zu berücksichtigen ist jedoch, dass hierbei die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit gewahrt werden und der Gläubiger neben seinem Anspruchsverfolgungsinteresse auch die berechtigten Interessen seines Schuldners im Blick hat.

In einem uns im Berichtszeitraum zugetragenen Sachverhalt ist letzteres nicht passiert. Dort hatte ein mit der Geltendmachung einer Forderung eines Energieversorgungsunternehmens beauftragter Rechtsanwalt die Kontaktmöglichkeit zu dem mutmaßlichen Schuldner bzw. zu einer dieser nahestehenden Person über deren Arbeitgeber gesucht.

Hintergrund des Mandats waren ausstehende Forderungen aus Versorgungsleistungen für eine leerstehende Immobilie einer verstorbenen Person. Nach erfolgloser Recherche der Wohnadressen näherer Angehöriger und potenzieller Erben ermittelte der Rechtsanwalt über das Internet eine Person gleichen Nachnamens, deren Vornamen er auch der Todesanzeige der verstorbenen Schuldnerin entnehmen konnte. Dies genügte ihm sodann, um zunächst telefonisch und daraufhin via E-Mail-Kontakt zu dieser Person über deren Arbeitgeber zu suchen, welchen er ebenfalls über das Internet ausfindig machen konnte. Die E-Mail adressierte er dabei an eine Funktionsadresse des Arbeitgebers, welche ihm hierzu

46) Buchner/Petri, in: Kühling/Buchner, DSGVO (4. Aufl. 2024), Art 6 Rn. 166e.

von diesem genannt worden war. Er schilderte hierin kurz den Sachverhalt, ging insbesondere auf die noch bestehenden Forderungen ein, und bat die betroffene Person um Rückmeldung, falls es sich bei ihr um die Ehefrau oder die Tochter des Sohnes der verstorbenen Schuldnerin handeln sollte.

Diese Form der Kontaktaufnahme war rechtswidrig und verletzte die betroffene Arbeitnehmerin in ihren datenschutzrechtlichen Positionen. Zwar kann die Kontaktaufnahme zu einem Schuldner auch am Ort des Arbeitgebers gesucht werden, insbesondere, wenn andere Mittel der Adressermittlung ausgeschöpft sind; der Kontakt muss hierbei jedoch in diskreter Form aufgenommen werden, d. h. ohne Benennung des Grundes und in einer Weise, welche sicherstellt, dass nur die betroffene Person selbst und nicht das Arbeitsumfeld hiervon Kenntnis erlangt.

Letzteres kann in der Regel durch ein Schriftstück erfolgen, welches im Adressfeld des Umschlags einen Vermerk wie „Persönlich", „Vertraulich" oder „Eigenhändig" enthält. Hierdurch wird sichergestellt, dass das Schriftstück nur von dem genannten Empfänger geöffnet werden darf und nicht von Arbeitskollegen oder der Poststelle.
Die betroffene Person sah durch die E-Mail, welche zudem noch von einer Arbeitskollegin gelesen werden konnte, zu Recht eine ehrverletzende Wirkung ausgehen, und sah nicht zuletzt auch ihre Reputation gegenüber ihrem Arbeitgeber gefährdet.

Als Konsequenz des festgestellten Verstoßes gegen das Datenschutzrecht wurde gegenüber dem handelnden Rechtsanwalt als Verantwortlichem nach Art. 4 Nr. 7 DSGVO eine Verwarnung nach Art. 58 Abs. 2 lit. b DSGVO ausgesprochen.

WOHNUNGSWIRTSCHAFT

5. WOHNUNGS-WIRTSCHAFT

Das Verarbeitungshandeln im Bereich der Wohnungsvermietung und -verwaltung war auch im zurückliegenden Berichtszeitraum häufiger Gegenstand von an das Datenschutzzentrum adressierten Beschwerden und Beratungsanfragen. Die Bandbreite an potenziellen Verstößen ist erheblich; trotzdem wiederholen sich regelmäßig aber im Wesentlichen Sachverhalte, soweit Datenweitergaben durch Vermieterinnen und Vermieter oder durch Wohnungsverwaltungen sowie ein überschießender oder intransparenter Umgang mit Daten von Mieterinnen und Mieter vorgetragen werden.

5.1 Gesundheitsdaten im Mietverhältnis

Auch wenn ein wohlmeinender Zweck verfolgt wurde und diese im Interesse der betroffenen Person erfolgen soll, sind bei der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO im Rahmen eines Mietverhältnisses spezifische Rahmenbedingungen zu berücksichtigen. Sollen in einem Mietobjekt, das vor allem von Seniorinnen und Senioren bewohnt wird, die Daten der Mieterinnen und Mieter um Angaben zu behandelnden Ärztinnen und Ärzten, Pflegediensten und –stufen ergänzt werden, handelt es sich dabei um Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO in Verbindung mit Art. 9 Abs. 1 DSGVO, für die die Verarbeitungsbedingungen nach Art. 9 Abs. 2 DSGVO gelten.

Der Begriff der Gesundheitsdaten – mithin personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen – ist dabei nach der Rechtsprechung[47] weit auszulegen und erfasst auch Informationen, bei welchen Ärztinnen oder Ärzten eine betroffene Person in Behandlung steht.[48]

Im Fall der Beschwerde einer Bewohnerin konnte die diesbezügliche Datenverarbeitung entgegen der Rechtsauffassung des Verantwortlichen nicht auf Art. 6 Abs. 1 lit. d DSGVO gestützt werden, wonach die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen. Diese Vorschrift kann gemäß Satz 2 des Erwägungsgrunds 46 der DSGVO nur dann Berücksichtigung finden, wenn – bspw. in Akut- oder Ausnahmesituationen – nicht auf eine andere datenschutzrechtliche Legitimationsgrundlage zurückgegriffen werden kann. Soweit im verfahrensgegenständlichen Zusammenhang eine institutionalisierte, aktenmäßige Verarbeitung von Gesundheitsdaten von Mieterinnen und Mieter für den Eventualfall stattfinden sollte, konnte mithin nicht auf Art. 6 Abs. 1 lit. d DSGVO, sondern nur auf die ausdrückliche Einwilligung der betroffenen Personen nach Art. 9 Abs. 2 lit. a DSGVO abgestellt werden.

Nach Übersendung einer Warnung nach Art. 58 Abs. 2 lit. a DSGVO erwiderte der Vermieter, dass die Erhebung und Verarbeitung dieser Gesundheitsdaten ohnehin auf freiwilliger Basis erfolgt sei, auch wenn dies den betroffenen Personen gegenüber nicht hinreichend deutlich gemacht wurde. Da letztlich glaubhaft war, dass die Interessen des Vermieters und der Mieterinnen und Mieter deckungsgleich waren und der Prozess umgehend umgestaltet wurde, blieb es bei der Warnung als aufsichtsrechtliche Maßnahme.

---

47) EuGH, Urteil vom 04.10.2024 – C-21/23.
48) Österreichisches Bundesverwaltungsgericht – Urteil vom 03.06.2024 – BVwG W 292 22282284-1.

5.2 Anbahnung und Beendigung von Mietverhältnissen

Häufig thematisieren Kontrollanregungen Wohnungsannoncen, in denen Immobilienmaklerinnen und –makler oder Vermieterinnen und Vermieter die Übersendung von Mietselbstauskünften und Bonitätsauskünften zur Vereinbarung von Besichtigungsterminen voraussetzen. In derartigen Fällen werden regelmäßig kombinierte Hinweise nach Art. 58 Abs. 1 lit. d DSGVO und Warnungen nach Art. 58 Abs. 1 lit. a DSGVO unter Hinweis auf die „Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressent:innen“[49] an die jeweiligen Verantwortlichen gesandt; unter Berücksichtigung eines gestuften Mietanbahnungsprozesses ist eine Verarbeitung von Daten von Mietinteressentinnen und -interessenten aus einer Selbstauskunft als Voraussetzung für die Einräumung eines Besichtigungstermins regelmäßig nicht nach Art. 5 Abs. 1 lit. a in Verbindung mit Art. 6 Abs. 1 lit. b oder f DSGVO und Art. 5 Abs. 1 lit. c DSGVO legitimiert.

Die datenschutzrechtliche Bewertung von Mietanbahnungsprozessen beschränkt sich indes nicht auf Selbstauskünfte und Bonitätsnachweise, sondern umfasst auch den Umgang mit Daten aus früheren Mietverhältnissen. Gelegentlich kennen sich Vermieterinnen und Vermieter sowie Wohnungsinteressentinnen und -interessenten aus früheren Mietverhältnissen und nicht immer sind diese einvernehmlich und konfliktfrei geendet. Frühere Mieterinnen und Mietern, die sich treuwidrig verhalten oder erhebliche Mietrückstände hinterlassen haben, sind für Vermieterinnen und Vermieter dabei bei Eingehung eines erneuten Mietverhältnisses regelmäßig nicht erste Wahl. Insoweit können bzw. müssen Vermieterinnen und Vermietern Daten aus früheren Mietverhältnissen verarbeiten, allerdings gilt es für Datenverarbeitungen im Rahmen von Blacklists spezifische Anforderungen zu beachten.

---

49) abrufbar unter https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/alle_Dateien_und_Ordner_bis_2025/themen/OH_Mietinteresse_DSK_240124_V1.pdf..

In einem Beschwerdeverfahren wurde vorgetragen, dass ein Mietinteressent von einem potenziellen Vermieter aufgrund von Außenständen aus einem früheren Mietverhältnis eine Absage erhalten habe. Mit Blick auf eine bereits erteilte Restschuldbefreiung nach einem Privatinsolvenzverfahren, unter Berücksichtigung des erheblichen Alters der noch dokumentierten Mietforderung und mangels einer transparenten Information über diese Datenverarbeitung, sah sich der Mietinteressent in seinen Rechten verletzt. Der Beschwerdegegner teilte mit, dass gestützt auf Art. 6 Abs. 1 lit. f DSGVO das berechtigte Interesse verfolgt werde, sich vor Mietnomaden, Schuldnern und Negativmietern – insbesondere dann, wenn diese bereits Mieter waren – zu schützen. Laut Löschkonzept wurden personenbezogene Daten in diesem Zusammenhang für einen Zeitraum von 15 Jahren gespeichert. Dokumentierte Forderungen allein seien allerdings kein Ausschlusskriterium, da eine positive Bonitätsauskunft – die standardmäßig eingeholt werde – zur Anbahnung eines Mietverhältnisses beitragen kann. Eine transparente Information im Sinne der Art. 13 oder 14 DSGVO sei nicht erfolgt, da die Datenerhebung vor Inkrafttreten der DSGVO erfolgt sei.[50] Ob in dem konkreten Fall Maßnahmen zur Forderungsbetreibung ergriffen oder Vollstreckungstitel erwirkt wurden, war nicht dokumentiert.

Letztlich war allerdings die langjährige Datenspeicherung für den verfolgten Zweck angesichts des festgestellten Informationsdefizits, der vernünftigen Erwartungen des Beschwerdeführers und überwiegender schutzwürdige Interessen und Grundrechte/-freiheiten nicht legitimiert:

- Das dargelegte Interesse – die Minimierung des Risikos eines erneuten Forderungsausfalls durch Eingehung eines Mietverhältnisses mit einem in der Vergangenheit säumigen Mieter – war als wirtschaftliches Interesse berechtigt und als Ausdruck der grundrechtlich geschützten Privatautonomie anerkennenswert. Die langjährige Datenspeicherung über einen Forderungsausfall erfolgte auf Vorrat – soweit sie ausschließlich Relevanz für den Fall entfaltet, dass die betroffene Person erneut als Mietinteressent in Erscheinung tritt – und von dieser ging

50) Art. 99 DSGVO: Inkrafttreten: 24.05.2016; Geltungseintritt: 25.05.2018.

mit Blick auf die potenziellen Folgen für die betroffene Person eine benachteiligende Wirkung aus.[51] Berechtigte Interessen des Verantwortlichen und schutzwürdige Interessen der betroffenen Person sind damit vor dem Hintergrund eines langjährigen Verarbeitungshandelns und sich im Zeitablauf verändernder Positionen abzuwägen. Je länger die Daten über einen Forderungsausfall von betroffenen Mieterinnen und Mietern gespeichert werden sollen, um so schwerer wiegen im Zeitablauf ihre schutzwürdigen Interessen und um so höher werden die Anforderungen, die an das berechtigte Interesse zu stellen sind.

Grundsätzlich ist ein Blacklisting, das Daten zu vertrags-/treuwidrigem Verhalten oder Mietausfällen umfasst, möglich, allerdings müssen in diesem Zusammenhang die Grundsätze der Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 DSGVO, insbesondere mit Blick auf Transparenz, Zweckbindung und Datenminimierung, ausreichend operationalisiert werden. Da im beschwerdegegenständlichen Fall keine transparente Informationserteilung hinsichtlich der Datenverarbeitung für ein solches Blacklisting im Sinne des Art. 13 oder 14 DSGVO erfolgt war,[52] kein Nachweis für die Umsetzung eines geeigneten Informationsprozesses für Altfälle als organisatorische Maßnahme geführt werden konnte oder überhaupt nach Beendigung des Mietverhältnisses irgendeine Kontaktaufnahme mit dem Beschwerdeführer hinsichtlich des Mietausfalls dokumentiert war, war nicht ersichtlich, dass dieser vernünftigerweise mit der ihn betreffenden Datenverarbeitung (noch) rechnen musste. Auch eine erteilte Restschuldbefreiung prägte vor dem Hintergrund des Informationsdefizits die Erwartungshaltung entscheidend, da diese gerade darauf abzielt, eine erneute Teilnahme am Wirtschaftsleben[53] zu ermöglichen.

---

51) EuGH, Urteil vom 07.12.2023 – C 26/22 und C 64/22, Rn. 94; Simitis/Hornung/Spiecker gen. Döhmann, a. a. O., Rn. 109, beck-online.
52) Da die Datenerhebung vor Inkrafttreten der DSGVO erfolgt ist, bedingt Art. 94 DSGVO die Notwendigkeit der Prüfung der Datenverarbeitungen, die vor dem 25.05.2018 eingesetzt haben. Auch ein Datenverarbeitungshandeln, dass nach der Rechtslage bis zum 24.05.2018 datenschutzrechtlich ggfls. zulässig erfolgt sein kann, musste notwendigerweise auf die Zulässigkeit der Verarbeitungsbedingungen nach Geltungseintritt der DSGVO geprüft werden.
53) EuGH, a. a. O., Rn. 98.

- Auch wäre der Verantwortliche für den Fall einer früheren Datenlöschung nicht schlechter gestellt, da dieser vor Eingehung des Mietverhältnisses Bonitätsauskünfte über Mietinteressentinnen und -interessenten einholte und damit ein hinreichend geeignetes Instrument eingesetzt wurde, um die Kreditwürdigkeit bei der Mietanbahnung zu prüfen und das Risiko von zukünftigen Mietausfällen zu reduzieren.

Der Verantwortliche wurde daher zur Löschung der für Zwecke des Blacklistings verarbeiteten Daten des Beschwerdeführers und zur Erstellung eines geänderten Löschkonzepts aufgefordert. Im Übrigen wurde unter Berücksichtigung der festgestellten strukturellen Defizite ein Verfahren nach dem Ordnungswidrigkeitengesetz eingeleitet.

5.3 Risiken im Immobilienmanagement

Die Weitergabe personenbezogener Daten in der datenschutzrechtlichen Verantwortlichkeit von Vermieterinnen und Vermietern oder Verwaltern nach dem Wohnungseigentumsgesetz (WEG) wurde im Berichtszeitraum in zahlreichen Fällen mit verschiedensten Ausprägungen von beschwerdeführenden Personen vorgetragen.

In folgenden typischen Fallgestaltungen war eine Datenoffenlegung an die empfangenden Stellen oder Personen datenschutzrechtlich nicht zu beanstanden:

- Datenweitergaben zur Terminabstimmung an Handwerksbetriebe[54] und – im Fall einer Veräußerungsabsicht – an Immobilienmakler stellen nahezu den Beschwerdestandardfall dar und erfolgen nach einer vorausgegangenen transparenten Informationserteilung nach Art. 13 DSGVO mittels häufig von Verbänden zur Verfügung gestellten, dem jeweiligen Mietvertrag angehängten Musterdatenschutzinformationen, datenschutzrechtlich in zulässiger Weise.

54) Vgl. 30. Tätigkeitsbericht Datenschutz 2021, 4.23.1.

- Vor dem Hintergrund vermeintlich stattgefundener Störungen innerhalb einer Hausgemeinschaft – wie beispielsweise Ruhestörungen oder aber auch der Anbau von Cannabispflanzen in einem Privatkeller – werden oftmals Maßnahmen gegen Mieterinnen und Mieter ergriffen, denen für die Adressaten erkennbar Beschluss- oder Sachbefassungen durch Wohnungseigentümergemeinschaften zugrunde liegen. Ungeachtet dessen, ob die Verursachung zunächst objektiv zutreffend einer Mietpartei zugeschrieben werden kann, können Sondereigentümerinnen oder -eigentümer im Rahmen des Informationsaustausches und Willensbildungsprozesses innerhalb der Gemeinschaft der Wohnungseigentümer derartige Beeinträchtigungen personenbezogen adressieren, um ein vermietendes Mitglied, aus dessen Sondereigentum eine Störung potenziell hervorgeht, zur Einwirkung anzuhalten; denn Sondereigentümerinnen und -eigentümer sind über § 14 Abs. 2 Nr. 1 WEG verpflichtet, das Sondereigentum der übrigen Mitglieder der Gemeinschaft nicht zu beeinträchtigen bzw. die Gemeinschaft der Wohnungseigentümer hat nach § 14 Abs. 1 Nr. 2 WEG gegenüber dem Sondereigentümer den Anspruch, dass Regelungen – bspw. Hausordnungen und darin vorgesehene Verhaltenspflichten – gerade auch nach Einwirkung auf die mietende Person[55] eingehalten werden.

- Die Weitergabe personenbezogener Daten von Mieterinnen und Mieter – bspw. durch Zurverfügungstellung einer Kopie des Mietvertrags – an Rechtsanwältinnen/Rechtsanwälte anlässlich einer mietrechtlichen Auseinandersetzung, ist regelmäßig nach Art. 6 Abs. 1 lit. b DSGVO – im Rahmen der Abwicklung der mietvertraglichen Beziehung[56] – oder nach Art. 6 Abs. 1 lit. f DSGVO zulässig und stellt keinen Verstoß gegen das

55) BeckOGK/Falkner, 01.3.2025, WEG § 14 Rn. 44, beck-online.
56) Kühling/Buchner/Buchner/Petri, 4. Aufl. 2024, DS-GVO Art. 6 Rn. 33, beck-online; BeckOK DatenschutzR/Albers/Veit, 51. Ed. 01.02.2025, DS-GVO Art. 6 Rn. 43, beck-online; Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 30, beck-online; A. A. Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 6 Abs. 1 Rn. 32, beck-online.

Datenminimierungsgebot aus Art. 5 Abs. 1 lit. c DSGVO dar. Relevante Unterlagen müssen von Vermieterinnen und Vermietern vor Weitergabe an den oder die mandatierte(n) Bevollmächtige(n) nicht dahingehend „vorgeprüft" werden, ob und welche Informationen für die Rechtsdurchsetzung letztlich erforderlich sind.

In nachfolgenden typischen Fallgestalten erfolgt eine Datenoffenlegung ohne datenschutzrechtliche Legitimationsgrundlage:

- Eine Weitergabe der Information über die Kündigung eines Mietverhältnisses aufgrund von Zahlungsrückständen durch einen Vermieter an eine andere Mieterin per Messengernachricht, war als Verstoß gegen Art. 5 Abs. 1 lit. a in Verbindung mit Art. 6 Abs. 1 lit. f DSGVO zu qualifizieren. Vor dem Hintergrund einer freundschaftlichen Verbundenheit von Adressatin und gekündigter Mieterin sowie dem vermeintlich wohlgemeinten Interesse des Vermieters, die geschasste Mieterin durch gutes Zureden der Freundin zum Auszug zu bewegen und dieser – sowie sich selbst – somit Rechtsverfolgungskosten zu ersparen, war die Datenweitergabe nicht erforderlich und es standen überwiegend schutzwürdige Interessen der Mieterin entgegen. Es wurde in diesem Fall eine Verwarnung nach Art. 58 Abs. 2 lit. b DSGVO ausgesprochen.

- Die Übermittlung einer privat genutzten Mobilfunk- und Festnetznummer eines Sondereigentümers durch einen Verwalter an einen Miteigentümer konnte nicht gestützt auf Art. 6 Abs. 1 DSGVO erfolgen, soweit damit aufgrund anhaltender Ruhestörungen aus dem Sondereigentum die Gewährleistung der Einhaltung der Hausordnung, die Streitbeilegung und die Vermeidung von Rechtsverfolgungskosten verfolgt werden sollte.

  Ein von Lärmbelästigungen aus der vermieten Nachbarwohnung betroffener Sondereigentümer bat den Verwalter um Zurverfügungstellung der Anschrift des Vermieters, um sich bei diesem unmittelbar über die Störungen beschweren zu können. Der Verwalter nahm dies zum Anlass, dem Sondereigentümer nicht nur die erbetene Anschrift, sondern auch Telefonnummern des vermietenden Miteigentümers

mitzuteilen. Nach Ansicht des Verwalters war diese Weitergabe der Telefonnummern gestützt auf die Einwilligung des betroffenen Sondereigentümers, den Verwaltervertrag und die Interessenabwägung zulässig. Die unmittelbare Übermittlung der Telefonnummern effektiviere die Streitbelegung, da der vermietende Sondereigentümer so angerufen werden könne, um Ruhestörungen mithören zu können. Überdies sei es nicht Sache der Gemeinschaft der Wohnungseigentümer, sich mit den angeführten Beeinträchtigungen auseinanderzusetzen. Zudem stünden den Mitgliedern der Eigentümergemeinschaft ohnehin weitreichende Einsichtsrechte in die Verwaltungsunterlagen zu.

Weder die vorgelegte Einwilligung noch der Verwaltervertrag oder sich daraus ergebende Sekundärpflichten gaben jedoch Anhaltspunkte dafür her, dass diese Datenweitergabe legitimiert sein könnte. Soweit der lärmgeplagte Sondereigentümer lediglich eine Anschrift begehrte, wurde durch die unverlangte Übermittlung der Telefonnummern der Informationswunsch übererfüllt, so dass bereits eine Erforderlichkeit im Sinne des Art. 6 Abs. 1 lit. f DSGVO nicht gegeben war. Zudem war die Weitergabe dieser vor allem für unmittelbare Kommunikation mit dem Verwalter hinterlegten Kontaktdaten für den betroffenen Sondereigentümer nicht objektiv erwartbar. Auch der Hinweis auf das in § 18 Abs. 4 WEG geregelte Einsichtsrecht stritt letztlich nicht für Zulässigkeit; denn das passive, durch den Verwalter für die Gemeinschaft zu gewährende Einsichtsrecht unterscheidet sich zum einen konzeptionell von der beschwerdegegenständlichen proaktiven Weitergabe von Kontaktinformationen, zum anderen ist die Zulässigkeit einer Ausdehnung dieses Einsichtsrechts auf über die ladungsfähige Anschriften hinausgehende Kontaktinformationen der Mitglieder der Gemeinschaft strittig.[57]

Gegenüber dem Verwalter wurde vor diesem Hintergrund eine Verwarnung nach Art. 58 Abs. 2 lit. b DSGVO ausgesprochen.

57) BeckOK WEG/Elzer, 61. Ed. 1.7.2025, WEG § 18 Rn. 171, beck-online.

JUSTIZ

6. JUSTIZ

6.1 Übermittlungspflicht in Ermittlungsverfahren

Bei der Ermittlung strafrechtlich relevanter Sachverhalte sind Staatsanwaltschaft und Polizei häufig auf Informationen angewiesen, die bei privaten Stellen vorhanden sind. In vielen Fällen handelt es sich dabei um personenbezogene Daten, etwa Kontoinhaberdaten bei Kreditinstituten, Vertrags- und Bestandsdaten bei Unternehmen (z. B. Energieversorgern) oder von Videodaten aus privaten Überwachungssystemen.

Im Berichtszeitraum sahen sich zahlreiche Unternehmen und Institutionen im Saarland mit entsprechenden Anfragen der Polizei oder Staatsanwaltschaft konfrontiert. Unsere Behörde wurde von einigen privaten Verantwortlichen um datenschutzrechtliche Einordnung gebeten, nachdem entsprechende Anfragen der Polizei eingegangen waren. Im Mittelpunkt standen dabei insbesondere die Fragen, ob eine Befugnis oder sogar eine Pflicht zur Übermittlung besteht, welche Rechtsgrundlage hierfür einschlägig ist und ob die betroffene Person über die zweckändernde Verwendung ihrer Daten zu informieren ist.

Die Unsicherheiten resultieren dabei nicht zuletzt aus der komplexen rechtlichen Gemengelage, die sich aus dem Zusammenspiel von Strafprozess- und Datenschutzrecht ergibt. Während die Ermittlungsbehörden auf Grundlage der Strafprozessordnung handeln, müssen private Stellen die Vorgaben der DSGVO beachten.

Rechtliche Grundlagen des Datenaustauschs

Die datenschutzrechtliche Bewertung solcher Anfragen erfordert eine klare Trennung der beteiligten Verarbeitungsvorgänge. Nach dem vom Bundesverfassungsgericht entwickelten Doppeltürmodell vollzieht sich ein Datenaustausch zwischen zwei verantwortlichen Stellen in zwei miteinander korrespondierenden Schritten: Während auf Seiten der auskunftsersuchenden Ermittlungsbehörde personenbezogene Daten erhoben werden, übermittelt die ersuchte Stelle diese Daten. Bei einem solchen Datenaustausch stellen sowohl die Abfrage als auch die Bereitstellung personenbezogener Daten selbstständige Eingriffe in das Recht auf informationelle Selbstbestimmung dar und bedürfen jeweils einer eigenständigen Rechtsgrundlage.[58]

Für nichtöffentliche Stellen richtet sich die Zulässigkeit der Übermittlung personenbezogener Daten an Ermittlungsbehörden grundsätzlich nach der Datenschutz-Grundverordnung. Eine Datenübermittlung an Polizei oder Staatsanwaltschaft ist demnach nur rechtmäßig, wenn sie sich auf eine Rechtsgrundlage nach Art. 6 DSGVO stützen lässt. In der Praxis stehen hierbei vor allem Art. 6 Abs. 1 lit. c DSGVO (Erfüllung einer rechtlichen Verpflichtung) und Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse nach Abwägung) im Vordergrund. Welche dieser Grundlagen einschlägig ist, entscheidet sich maßgeblich danach, ob die Anfrage der Ermittlungsbehörden lediglich auf freiwillige Kooperation zielt oder ob sie eine verbindliche Herausgabe begründet.

Strafprozessuale Befugnisse – datenschutzrechtlichen Implikationen

Die Strafprozessordnung sieht unterschiedliche Befugnisse für die Anforderung personenbezogener Daten vor, die sich in ihrer Verbindlichkeit und ihren Voraussetzungen deutlich unterscheiden. Die zentralen Normen sind die Generalklauseln der §§ 161, 163 StPO sowie das Herausgabeverlangen nach § 95 StPO.

---

58) BVerfG, Beschluss vom 24.01.2021 – 1 BvR 1299/05, BVerfGE 130, 151, Rn. 123.

Die §§ 161 Abs. 1 Satz 1, 163 Abs. 1 Satz 2 StPO ermöglichen den Ermittlungsbehörden sogenannte Auskunftsersuchen gegenüber privaten Stellen. Anders als die ebenfalls dort geregelten Auskunftsverlangen gegenüber Behörden, begründen Auskunftsersuchen keine rechtliche Verpflichtung zur Datenübermittlung, sondern setzen auf die freiwillige Kooperation der angesprochenen Stelle. Die verantwortliche Stelle kann in diesen Fällen eine eigene Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO vornehmen und auf dieser Grundlage entscheiden, ob sie die Daten herausgibt. Praktisch hilfreich ist es, wenn die Ermittlungsbehörden zumindest Grundinformationen zum Tatvorwurf und zum Zweck der Anfrage mitteilen, damit die verantwortliche Stelle die Abwägung belastbar vornehmen kann. Eine solche Informationsweitergabe ist jedoch keine rechtliche Voraussetzung für die Wirksamkeit des Ersuchens.

Davon zu unterscheiden sind verbindliche Herausgabeverlangen nach § 95 Abs. 1 StPO. Ein Herausgabeverlangen nach § 95 Abs. 1 StPO begründet für die ersuchte Stelle eine rechtliche Verpflichtung zur Datenübermittlung i. S. d. Art. 6 Abs. 1 lit. c DSGVO. Diese Vorschrift, die ursprünglich auf die Herausgabe körperlicher Gegenstände abzielte, findet nach ständiger Rechtsprechung auch auf immaterielle Daten Anwendung.[59] Verweist die Ermittlungsbehörde in ihrer Anfrage ausdrücklich auf § 95 StPO, so ist die private Stelle verpflichtet, die angeforderten Daten herauszugeben, sofern die Voraussetzungen der Norm erfüllt sind. Dies setzt voraus, dass die Daten konkret bezeichnet sind und sich mit Gewissheit im Gewahrsam der ersuchten Stelle befinden.

Pauschale Anfragen, mit denen die Behörden zunächst die Existenz von Daten klären möchten, können sich nicht auf § 95 StPO stützen; sie sind typischerweise im Rahmen der allgemeinen Ermittlungsbefugnisse nach §§ 161, 163 StPO einzuordnen. Wegen der Anknüpfung an die

59) BVerfG, Urteil vom 16.06.2009 - 2 BvR 902/06, NJW 2009, 2431 [2434]; BVerfG, Beschluss vom 12.04.2005 - 2 BvR 1027/02, NJW 2005, 1917 [1920].

Beschlagnahmeregelungen des § 94 StPO setzt § 95 StPO voraus, dass sich das Verlangen auf hinreichend konkretisierte Datenbestände bezieht, die sich mit Gewissheit im Gewahrsam des Adressaten befinden. Der herausverlangte „Beweisgegenstand" muss so genau bezeichnet sein, dass Umfang und Inhalt der angeforderten Daten eindeutig erkennbar sind, etwa anhand eines klaren Personenbezugs (Name, Kennung) und eines konkret benannten Zeitraums.

Exkurs: In solchen Konstellationen, in denen es um die Reaktion auf verpflichtend zu erfüllende behördliche Anfragen der Ermittlungsbehörden geht, ist § 24 Abs. 1 Nr. 1 BDSG, nach der eine zweckändernde Verarbeitung durch nichtöffentliche Stellen u. a. dann zulässig ist, wenn sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist, regelmäßig nicht der passende datenschutzrechtliche Anknüpfungspunkt. Der Grund liegt darin, dass § 24 BDSG eine eigene Abwägungsentscheidung des Verantwortlichen verlangt. § 24 Abs. 1 Nr. 1 BDSG erlaubt die Übermittlung, verpflichtet die nichtöffentliche Stelle jedoch nicht dazu[60], was mit der Herausgabepflicht in den Fällen des § 95 StPO kollidiert. § 24 BDSG tritt daher hinter der spezialgesetzlichen Regelung des Art. 6 Abs. 1 Abs. 1 lit. c DSGVO i. V. m. § 95 Abs. 1 StPO zurück. Der praktische Anwendungsbereich dieser Norm bleibt auf Fälle beschränkt, in denen der Verantwortliche in eigenem Interesse und aus eigener Initiative personenbezogene Daten für Anzeigen oder Hinweise gegenüber Sicherheits- oder Ordnungsbehörden nutzen möchte.

Abgrenzung und Verfahrenshinweise für die Praxis

Die Abgrenzung zwischen einem bloßen Auskunftsersuchen und einem verbindlichen Herausgabeverlangen ist in der Praxis von erheblicher Bedeutung, da sie darüber entscheidet, ob die verantwortliche Stelle eine eigene Interessenabwägung vorzunehmen hat oder zur Datenübermittlung

60) BeckOK DatenschutzR/Albers, 54. Ed. 01.08.2025, BDSG § 24 Rn. 15, beck-online.

verpflichtet ist. Unbestimmte Paragrafenketten sind in der Praxis besonders fehleranfällig, weil sie bei den Empfängern Unsicherheit erzeugen, ob eine Pflicht besteht oder eine Abwägungsentscheidung zu treffen ist. Soll eine rechtliche Verpflichtung begründet werden, muss die Anfrage dies erkennbar machen und ausdrücklich auf § 95 Abs. 1 StPO Bezug nehmen. Aus diesem Grund ist den Ermittlungsbehörden dringend anzuraten, ihre Anfragen präzise zu formulieren und die zugrundeliegende Rechtsgrundlage klar zu benennen. Die Staatsanwaltschaft Saarbrücken hat uns signalisiert, dies bei zukünftigen Ermittlungsverfahren berücksichtigten zu wollen.

Private Stellen sollten bei unklaren Anfragen zeitnah eine Konkretisierung verlangen, um rechtssicher handeln zu können. Wird die Anfrage hingegen eindeutig auf § 95 Abs. 1 StPO gestützt, so können ohne Verstoß gegen datenschutzrechtliche Vorgaben auf Basis von Art. 6 Abs. 1 lit. c DSGVO personenbezogene Daten den Ermittlungsbehörden zur Verfügung gestellt werden.

Datenschutzrechtliche Pflichten der verantwortlichen Stellen

Unabhängig davon, ob die Datenübermittlung auf einer rechtlichen Verpflichtung oder einer freiwilligen Kooperation beruht, müssen verantwortliche Stellen stets prüfen, ob sie die betroffenen Personen über die zweckändernde Verarbeitung ihrer personenbezogenen Daten informieren müssen. Die Übermittlung personenbezogener Daten an Ermittlungsbehörden stellt regelmäßig eine solche Zweckänderung dar, über die die betroffene Person gemäß Art. 13 Abs. 3 oder Art. 14 Abs. 4 DSGVO zu unterrichten ist.

Diese Informationspflicht entfällt nur dann, wenn einer der in den §§ 32, 33 BDSG vorgesehenen Ausnahmefälle vorliegt. Die verantwortliche Stelle muss im Einzelfall prüfen, ob die Voraussetzungen dieser Ausnahmen erfüllt sind. Hierzu kann es erforderlich sein, zusätzliche Informationen von den Strafverfolgungsbehörden einzuholen, insbesondere dann, wenn eine Information an die betroffene Person den Ermittlungserfolg gefährden

würde. Sofern die Voraussetzungen des § 32 Abs. 1 Nr. 3 oder § 33 Abs. 1 Nr. 2 lit. b BDSG erfüllt sind, entfällt lediglich die Informationspflicht. § 32 Abs. 1 Nr. 3 bzw. § 33 Abs. 1 Nr. 2 lit. b BDSG normieren hingegen kein Informationsverbot. Der verantwortlichen Stelle bleibt es unbenommen, nach eigenem Ermessen zu entscheiden, ob sie die betroffene Person überobligatorisch informieren möchte.

Bei der Entscheidung, die betroffene Person trotz Wegfall der Informationspflicht zu informieren, sollte allerdings berücksichtigt werden, ob die Ermittlungsbehörden ein verdecktes Vorgehen für erforderlich halten, beispielsweise weil der Tatverdächtige noch keine Kenntnis von dem Verfahren hat. In solchen Fällen könnte eine Information der betroffenen Person den Ermittlungserfolg gefährden und unter Umständen sogar den Tatbestand der Strafvereitelung nach § 258 StGB erfüllen.

Ein ausdrückliches, verpflichtendes Offenbarungsverbot kann von Ermittlungsbehörden einseitig nur unter den Voraussetzungen des § 95a StPO im Kontext von Beschlagnahmeverfahren erwirkt werden. Der bloße Hinweis, eine Information solle „unterbleiben", ersetzt eine solche gesetzliche Grundlage nicht; umso wichtiger ist es, die jeweilige Verfahrenslage und den konkreten Inhalt behördlicher Hinweise sorgfältig einzuordnen.

Für private Stellen ist bei Anfragen von Polizei oder Staatsanwaltschaft entscheidend, ob ein freiwilliges Auskunftsersuchen oder ein verbindliches Herausgabeverlangen vorliegt. Während Ersuchen auf Grundlage der allgemeinen Ermittlungsbefugnisse typischerweise eine eigenständige Abwägungsentscheidung nach Art. 6 Abs. 1 lit. f DSGVO erfordern, begründet ein hinreichend konkretes Herausgabeverlangen nach § 95 Abs. 1 StPO regelmäßig eine rechtliche Verpflichtung zur Übermittlung personenbezogener Daten im Sinne des Art. 6 Abs. 1 lit. c DSGVO. Flankierend ist die Frage der Informationspflichten über eine Zweckänderung konsequent mitzudenken; dabei sind sowohl die gesetzlichen Ausnahmen der §§ 32, 33 BDSG als auch besondere Konstellationen verdeckter Ermittlungen und ein etwaiges Offenbarungsverbot nach § 95a StPO zu berücksichtigen.

6.2 Informationspflichten bei der Verkehrsüberwachung

Anfang 2025 erreichte uns eine Beschwerde, die sich auf eine Anlage zur Verkehrsüberwachung bezog (umgangssprachlich als „Panzer-Blitzer“ bezeichnet). Ein Bürger beanstandete, dass an der betreffenden Anlage kein Hinweisschild mit Informationen zum Datenschutz angebracht gewesen sei. Bei anderen vergleichbaren Einrichtungen habe er hingegen eine Beschilderung mit Hinweisen entsprechend Art. 13 DSGVO vorgefunden. Aufgrund des fehlenden Hinweises sei er nicht in der Lage gewesen, seine Betroffenenrechte effizient geltend zu machen; insbesondere habe er weder einen Verantwortlichen noch Kontaktmöglichkeiten zu einer Datenschutzaufsicht ohne Weiteres ermitteln können.

Wir teilten dem Beschwerdeführer mit, dass eine Beschilderung an der Anlage selbst nicht zwingend auf Grundlage der DSGVO zu erfolgen hat. Denn die DSGVO ist auf den geschilderten Sachverhalt nicht anwendbar. Nach Art. 2 Abs. 2 lit. d DSGVO sind Datenverarbeitungen von den Regelungen der Verordnung ausgenommen, sofern sie durch zuständige Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung erfolgen. Maßgeblich ist dabei eine unionsrechtliche Auslegung. Sie erfasst nicht nur klassische Strafverfahren im nationalen Sinne, sondern auch solche Verfahren, die nach deutschem Recht als Ordnungswidrigkeiten eingeordnet sind, soweit sie der staatlichen Verfolgung und Ahndung von Rechtsverstößen dienen. Für den durch Art. 2 Abs. 2 lit. d DSGVO ausgenommenen Bereich gilt stattdessen die Richtlinie (EU) 2016/680 (sog. JI-Richtlinie). Deren Vorgaben sind in Deutschland in verschiedenen Rechtsakten umgesetzt, insbesondere im dritten Teil des Bundesdatenschutzgesetzes sowie in spezialgesetzlichen Regelungen des Strafverfahrens- und Polizeirechts.

Geschwindigkeitskontrollen dienen dazu, verkehrswidriges Verhalten zu erkennen, zu dokumentieren und – sofern erforderlich – in einem Ordnungswidrigkeitenverfahren zu verfolgen und zu ahnden.

Zugleich entfalten sie eine präventive Wirkung, indem sie zur Einhaltung der Verkehrsregeln anhalten und Verstöße bereits im Vorfeld verhindern sollen. Die Datenerhebung und -verarbeitung steht damit in einem funktionalen Zusammenhang mit der Verfolgung von Rechtsverstößen durch zuständige Behörden; folglich sind die Voraussetzungen der vorgenannten Bereichsausnahme erfüllt. Soweit der Beschwerdeführer darauf hinwies, er habe an anderen Geschwindigkeitsüberwachungsanlagen Hinweise nach Art. 13 DSGVO vorgefunden, lässt sich daraus keine rechtliche Verpflichtung im hier geprüften Fall ableiten.

Auch im Anwendungsbereich der JI-Richtlinie bestehen Transparenzpflichten, die jedoch anders ausgestaltet sind als die Informationspflichten nach Art. 13 DSGVO. Für Ordnungswidrigkeiten gelten über die Verweisung in § 46 Abs. 1 OWiG die Vorschriften der Strafprozessordnung. Im Hinblick auf die datenschutzrechtliche Information der betroffenen Personen ist dabei insbesondere § 55 BDSG einschlägig. Danach hat der Verantwortliche bestimmte Informationen in allgemeiner Form und in einer für jedermann zugänglichen Weise bereitzustellen. Hierzu gehören – der Sache nach vergleichbar mit Art. 13 DSGVO – insbesondere:

- die Zwecke der Verarbeitung personenbezogener Daten,
- die Betroffenenrechte, insbesondere auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,
- Name und Kontaktdaten des Verantwortlichen sowie des Datenschutzbeauftragten,
- der Hinweis auf das Beschwerderecht bei der zuständigen Datenschutzaufsichtsbehörde einschließlich deren Kontaktdaten.

Anders als nach Art. 13 DSGVO müssen diese Informationen betroffenen Personen jedoch nicht zwangsläufig zeitgleich mit der Erhebung der Daten zur Verfügung gestellt werden. Entscheidend ist vielmehr, dass die Hinweise so erteilt werden, dass betroffene Personen ihre Rechte effektiv wahrnehmen können. Dies setzt eine hinreichende Auffindbarkeit und Verständlichkeit voraus. Die Information kann auf unterschiedlichen Wegen bereitgestellt werden; naheliegend ist insbesondere eine Veröffentlichung

auf den Internetauftritten der jeweils verantwortlichen Stellen. Dort sollten die Hinweise so platziert und benannt werden, dass sie ohne besondere Vorkenntnisse gefunden werden können (z. B. über einen klar bezeichneten Menüpunkt zu „Datenschutzhinweisen im Ordnungswidrigkeitenverfahren" oder über eine Suchfunktion). Zugleich kann es sinnvoll sein, die Informationen mit kurzen Erläuterungen zum Verfahrenskontext (z. B. Verkehrsüberwachung, Anhörungsverfahren, Bußgeldbescheid) zu versehen, um die Zuordnung zu erleichtern.

Für Maßnahmen der Verkehrsüberwachung können im Saarland unterschiedliche Stellen zuständig sein. Regelmäßig führt die Vollzugspolizei entsprechende Kontrollen durch. Innerhalb geschlossener Ortschaften können für die Überwachung des ruhenden und fließenden Verkehrs aber auch Ortspolizeibehörden zuständig sein. Unsere weiteren Prüfungen, die durch die Beschwerde angestoßen wurden, zeigten jedoch erhebliche Transparenzdefizite in Bezug auf Datenverarbeitungen in Ordnungswidrigkeitenverfahren (vgl. § 46 Abs. 1 OWiG i. V. m. den einschlägigen strafprozessualen Regelungen und § 55 BDSG). Auf nahezu keiner der in Augenschein genommenen Webseiten verantwortlicher saarländischer Stellen waren ausreichende Hinweise zu entsprechenden Datenverarbeitungen auffindbar. Teilweise fanden sich zwar allgemeine Datenschutzerklärungen für den jeweiligen Internetauftritt, diese enthielten jedoch keine spezifischen Informationen zum JI-Regime bzw. zu Datenverarbeitungen im Ordnungswidrigkeitenkontext und waren daher für die effektive Wahrnehmung von Betroffenenrechten nur eingeschränkt geeignet.

Gemeinsam mit dem externen Datenschutzbeauftragten mehrerer betroffener Kommunen entwickelten wir daher ein Muster für Datenschutzhinweise, das von den verantwortlichen Stellen an die jeweiligen Gegebenheiten angepasst und in den Internetportalen integriert bzw. veröffentlicht werden kann. Ziel war es, eine praxistaugliche und zugleich rechtssichere Grundlage zu schaffen, die sowohl die erforderlichen Mindestinformationen nach § 55 BDSG abdeckt als auch eine bürgerfreundliche Darstellung ermöglicht. Bis zum Redaktionsschluss des vorliegenden Tätigkeitsberichts war die Umsetzung der vorgesehenen Änderungen jedoch noch nicht abgeschlossen.

Wir werden die verantwortlichen Stellen weiterhin bei der Ausgestaltung und Implementierung entsprechender Hinweise unterstützen und die Entwicklung im Rahmen unserer Aufsichtstätigkeit begleiten.

Abschließend ist darauf hinzuweisen, dass sich die Informationspflichten nach § 55 BDSG nicht auf Ordnungswidrigkeitenverfahren im Kontext „Verkehr" beschränken. Das Erfordernis, Datenschutzhinweise im Sinne des JI-Regimes in allgemeiner Form bereitzustellen, gilt auch für andere Arten von Ordnungswidrigkeiten, etwa in Bereichen der kommunalen Gefahrenabwehr, des Gewerbe- oder Umweltrechts, soweit die Verarbeitung der Verfolgung und Ahndung von Rechtsverstößen dient. Verantwortliche Stellen sind daher gehalten, sobald sie personenbezogene Daten in diesem Kontext verarbeiten, entsprechende Informationen allgemein zugänglich vorzuhalten und die Auffindbarkeit für Betroffene sicherzustellen. Wir unterstützen die verantwortlichen Stellen hierbei im Rahmen unserer Aufgaben beratend.

6.3 Datenschutz hinter Gefängnismauern

Datenschutzrechtliche Beschwerden von Inhaftierten in Justizvollzugsanstalten (JVA) sind im Saarland zwar eher selten, gleichwohl wenden sich auch Strafgefangene und – nach der Entlassung – ehemalige Gefangene immer wieder mit Anliegen an die Datenschutzaufsicht. Dies ist nicht ungewöhnlich: Der Strafvollzug ist ein Bereich, in dem staatliche Stellen in besonderer Weise in Grundrechte eingreifen und wo personenbezogene Daten in einem Umfang verarbeitet werden, der weit über viele andere Verwaltungsbereiche hinausgeht. Der Vollzug erfordert eine Vielzahl sicherheits- und ordnungsbezogener Maßnahmen, eine engmaschige vollzugliche Begleitung sowie eine umfassende Dokumentation. Gerade wegen dieser spezifischen Rahmenbedingungen ist es aus datenschutzrechtlicher Sicht wichtig, den Blick nicht nur auf einzelne Beschwerden zu richten, sondern die zugrunde liegenden Strukturen und Verfahren regelmäßig und systematisch zu prüfen.

Denn weder Grund- noch Datenschutzrechte machen vor den Pforten eines Gefängnisses vollständig Halt. Auch im Strafvollzug gilt das Recht auf informationelle Selbstbestimmung fort; es wird durch die vollzuglichen Erfordernisse zwar in zulässigem Umfang beschränkt, aber nicht aufgehoben. Der Umgang mit personenbezogenen Daten muss daher auch im Vollzug auf einer gesetzlichen Grundlage beruhen, sich an den Grundsätzen der Zweckbindung und Datenminimierung orientieren, transparent ausgestaltet sein und durch geeignete technisch-organisatorische Maßnahmen abgesichert werden. In einem Bereich, der durch ein strukturelles Machtgefälle, eingeschränkte Ausweichmöglichkeiten der Betroffenen und eine erhöhte Vulnerabilität geprägt ist, kommt zudem dem Schutz vor unberechtigten Zugriffen, einer konsequenten Protokollierung und einer klaren Rollen- und Verantwortungszuordnung besondere Bedeutung zu.

Vor diesem Hintergrund führten wir im Berichtszeitraum eine Datenschutzprüfung in den saarländischen Justizvollzugsanstalten durch. Ziel war es, unabhängig von konkreten Beschwerden einen aktuellen, ganzheitlichen Überblick über zentrale Datenverarbeitungen zu gewinnen, Risiken frühzeitig zu identifizieren und – wo erforderlich – datenschutzrechtliche Nachsteuerungen anzustoßen. Im Fokus standen zwei Themenkomplexe, die für den Vollzug von erheblicher praktischer Relevanz sind: (1) das IT-Fachverfahren „Buchhaltungs- und Abrechnungssystem im Strafvollzug“ (BASIS-Web), das in den Anstalten als umfassendes Verwaltungs- und Dokumentationssystem genutzt wird, sowie (2) die Videoüberwachung in den Anstalten, die sowohl im Außenbereich als auch – in bestimmten Grenzen – im Innenbereich eingesetzt wird.

Die Prüfung umfasste dabei sowohl rechtliche als auch technisch-organisatorische Aspekte. Wir ließen uns die bestehenden Prozesse, Zuständigkeiten und Sicherheitskonzepte erläutern, prüften die Einbindung des Datenschutzes in die System- und Verfahrensgestaltung, bewerteten den Zugriffsschutz und die Protokollierung sowie die Regelungen zu Speicherung, Aufbewahrung, Löschung und Einschränkung der Nutzung.

Bei der Videoüberwachung betrachteten wir insbesondere die Frage, in welchen Bereichen und zu welchen Zwecken eine Beobachtung erfolgt, wie die Arbeitsplätze der Videobeobachtung ausgestaltet sind, welche Speicher- und Löschkonzepte bestehen und wie die Sicherung von Sequenzen zu Beweiszwecken dokumentiert und begrenzt wird.

BASIS-Web: Einsatz und Funktionsumfang

Bei BASIS-Web handelt es sich um ein länderübergreifend eingesetztes System, das federführend in Nordrhein-Westfalen entwickelt wurde und von nahezu allen Bundesländern sowie auch vom Großherzogtum Luxemburg genutzt wird. Die Systemarchitektur und grundlegende Funktionen sind daher im Kern vergleichbar; zugleich können sich konkrete Module, Schnittstellen, Parameter und organisatorische Abläufe je nach Einsatzort unterscheiden. Diese Unterschiede sind nicht nur technisch bedingt, sondern spiegeln auch die unterschiedlichen rechtlichen Rahmenbedingungen der Länder wider. Seit der Föderalismusreform im Jahr 2006 fällt der Justizvollzug in die Gesetzgebungskompetenz der Länder. Dadurch divergieren die gesetzlichen Vorgaben, etwa zu Dokumentationspflichten, Aufbewahrung und Löschung, zu besonderen Sicherungsmaßnahmen oder zu Zuständigkeiten im Vollzug. In der Folge kann auch der konkrete Bedarf an Funktionen eines Verwaltungs- und Dokumentationssystems in wesentlichen Punkten variieren.

Im Saarland wird BASIS-Web in den Justizvollzugsanstalten Saarbrücken und Ottweiler eingesetzt. Das System entstand ursprünglich als Software für Buchhaltung und Abrechnung im Vollzug. Es hat sich jedoch im Laufe der Jahre zu einer integrativen IT-Organisationslösung entwickelt, die weite Teile des Vollzugsalltags abbilden kann. Neben Buchhaltung, Kassen- und Zahlungsverkehr werden in der Praxis unter anderem Funktionen für die Arbeitsverwaltung, Verpflegung, Logistik und – je nach Ausprägung – auch für vollzugsbezogene Dokumentationen genutzt. Dadurch kann das System eine erhebliche Informationsdichte über einzelne Gefangene aufweisen. Auch wenn nicht jede Funktion zwingend genutzt wird und Informationen teils in anderen Systemen oder Akten geführt werden, entsteht ein sehr umfassendes Lagebild, das sowohl für die Vollzugssteuerung als auch für

Sicherheits- und Verwaltungszwecke relevant ist. Aus Sicht des Datenschutzes folgt daraus: Je zentraler ein System ist und je mehr Datenkategorien es zusammenführt, desto höher sind die Anforderungen an Zugriffsschutz, Rollen- und Berechtigungskonzepte, Protokollierung sowie Zwecktrennung.

Eine datenschutzrechtliche Prüfung eines solchen Systems kann sich daher nicht auf eine abstrakte Betrachtung der Software beschränken. Entscheidend ist vielmehr, wie das System konkret im Saarland eingesetzt wird: Welche Module sind aktiviert? Welche Daten werden tatsächlich erfasst? Wer hat Zugriff auf welche Informationen? Welche Schnittstellen bestehen zu anderen Verfahren? Wie werden Auswertungen und Exporte gehandhabt? Und wie wird sichergestellt, dass der Zugriff auf besonders sensible Informationen (z. B. Gesundheitsdaten oder Daten zu besonderen Sicherungsmaßnahmen) nur einem eng begrenzten Personenkreis möglich ist?

Technische Infrastruktur, Sicherheitskonzepte und Notfallvorsorge

Im ersten Teil der Prüfung widmeten wir uns der eingesetzten technischen Infrastruktur und den Sicherheitskonzepten. In einer Justizvollzugsanstalt sind IT-Systeme regelmäßig nicht nur „Hilfsmittel", sondern Teil zentraler Verwaltungs- und Vollzugsprozesse. Ein Ausfall kann unmittelbare Auswirkungen auf Abläufe im Haftalltag haben, etwa bei der Verwaltung von Konten, bei Arbeitszuweisungen, bei der Ausgabe von Verpflegung oder bei organisatorischen Abläufen in Besuchs- und Transportprozessen. Daraus folgt einerseits ein hoher Bedarf an Verfügbarkeit, andererseits dürfen Verfügbarkeitsanforderungen nicht zulasten von Vertraulichkeit und Integrität gehen.

Wir ließen uns daher die zentralen Bausteine der Infrastruktur erläutern, insbesondere die Systeme, auf denen BASIS-Web betrieben wird, die Netzsegmentierung, die Einbindung in Authentifizierungs- und Benutzerverwaltungssysteme sowie Maßnahmen zur Absicherung gegen unberechtigte Zugriffe. Besonderes Augenmerk legten wir auf Sicherheitskonzepte, die für den Schutz personenbezogener Daten maßgeblich sind (z. B. zum Disaster-Recovery/Notfallwiederherstellung bei Ausfall von IT-Komponenten).

Rollen- und Berechtigungskonzept: „Need-to-know“ als Leitprinzip

Ein Schwerpunkt unserer Prüfung war die Ausgestaltung der Zugriffsrechte in BASIS-Web. Ein zentrales Datenschutzprinzip ist dabei das „Need-to-know“-Prinzip: Vollzugsmitarbeitende dürfen nur auf die personenbezogenen Daten zugreifen, die sie zur Erfüllung ihrer konkreten Aufgaben benötigen. In einer Justizvollzugsanstalt arbeiten unterschiedliche Bereiche zusammen – Vollzugsdienst, Verwaltung, Zahlstelle, Arbeitsbetriebe, ggf. medizinischer Dienst –, deren Informationsbedarfe sich deutlich unterscheiden. Ein System, das diese Bereiche technisch zusammenführt, muss daher zugleich eine differenzierte Zugriffstrennung ermöglichen.

Wir ließen uns das vorhandene Rollen- und Rechtekonzept detailliert vorstellen und prüften insbesondere:

- Rollenbildung und Standardisierung: Sind Rollen so definiert, dass sie typische Aufgabenprofile abdecken (z. B. Zahlstelle, Arbeitsverwaltung) und nicht auf Einzelpersonen zugeschnitten sind? Werden Rollen zentral gepflegt oder entstehen „Sonderrollen“, die mit der Zeit unübersichtlich werden?

- Rechtevergabeprozesse: Wer beantragt, wer genehmigt, wer setzt um? Gibt es ein Vier-Augen-Prinzip bei besonders weitreichenden Berechtigungen? Wie wird dokumentiert, warum eine Berechtigung erforderlich ist?

- Aktualität und Entzug von Rechten: Wie wird sichergestellt, dass Berechtigungen bei Aufgabenwechsel, Versetzung oder längerer Abwesenheit angepasst bzw. entzogen werden? Gibt es regelmäßige Überprüfungen der vergebenen Rechte?

- Protokollierung und Kontrolle: Werden Zugriffe und Bearbeitungen protokolliert? Sind Protokolle auswertbar und werden sie – zumindest anlassbezogen oder stichprobenartig – tatsächlich geprüft? Wie wird mit Auffälligkeiten umgegangen?

- Datenschutzfreundliche Voreinstellungen: Werden bei der Systemkonfiguration und bei Standardrollen eher restriktive Voreinstellungen gewählt, die einen Zugriff nur bei Bedarf freischalten („least privilege“), oder werden weite Zugriffe vergeben, die später eingeschränkt werden sollen?

Für die Praxis ist dabei entscheidend, dass Rollen- und Berechtigungskonzepte nicht nur „auf dem Papier“ existieren, sondern gelebte Prozesse sind. Gerade in komplexen Organisationen kann eine zunächst sinnvolle Struktur im Laufe der Zeit durch Ausnahmen, personelle Veränderungen und organisatorische Notwendigkeiten erodieren. Eine regelmäßige Überprüfung und eine klare Zuständigkeit für die Pflege des Berechtigungskonzepts sind daher essenziell.

Aufbewahrung, Löschung und Nutzungseinschränkung

Ein wiederkehrendes Thema in Beschwerden und Beratungsanfragen ist die Frage, ob und wie lange Daten nach einer Entlassung gespeichert bleiben dürfen. Betroffene nehmen häufig an, dass mit dem Ende der Haft automatisch „alles gelöscht“ werden müsse. Tatsächlich sind die gesetzlichen Vorgaben differenziert: Einerseits müssen Daten gelöscht werden, sobald sie für zulässige Zwecke nicht mehr erforderlich sind; andererseits können Aufbewahrungsfristen, Dokumentationspflichten oder archivrechtliche Vorgaben einer sofortigen Löschung entgegenstehen. Für die Praxis bedeutet dies, dass Lösch- und Aufbewahrungsprozesse transparent, dokumentiert und überprüfbar gestaltet sein müssen.

Für den Saarländischen Strafvollzug enthält das Saarländische Justizvollzugsdatenverarbeitungsgesetz (JVollzDSG) maßgebliche Vorgaben. Nach § 59 JVollzDSG sind personenbezogene Daten zu löschen, soweit ihre weitere Verarbeitung nicht mehr zulässig ist oder sie aus anderen Gründen für die Erfüllung vollzuglicher Zwecke oder für wissenschaftliche bzw. statistische Zwecke nicht mehr erforderlich sind. Ab dem Zeitpunkt der Entlassung oder einer dauerhaften Verlegung ist die Erforderlichkeit einer weiteren Speicherung jährlich zu überprüfen. Zudem enthält das Gesetz eine Regellöschfrist: Personenbezogene Daten sind grundsätzlich nach fünf Jahren zu

löschen (§ 59 Abs. 3 Satz 1 JVollzDSG). Dies betrifft insbesondere Daten, die in IT-Systemen wie BASIS-Web gespeichert sind.

Daneben gilt für bestimmte Aktenarten eine abweichende Logik. Für Gefangenenpersonal- und Gesundheitsakten sieht die Verordnung über die Aufbewahrung von Schriftgut in der Justiz und der Justizverwaltung (JSchrA-VO) andere Aufbewahrungsfristen vor, typischerweise zehn bzw. zwanzig Jahre. Diese Unterschiede sind in der Praxis häufig schwer vermittelbar, aber rechtlich bedeutsam. Das JVollzDSG greift dies in § 60 Abs. 1 Nr. 5 auf und erlaubt, dass in diesen Fällen eine Löschung zunächst unterbleiben kann, wenn die Akten einer umfassenden Nutzungseinschränkung unterliegen.

Eine solche Nutzungseinschränkung bedeutet, dass die betroffenen Akten nicht mehr in der laufenden Verwaltung verfügbar sind. Sie sind gesondert aufzubewahren und dürfen nur noch in gesetzlich vorgesehenen Fällen geöffnet werden. Der Zugriff ist auf einen eng begrenzten Personenkreis zu beschränken, und es sollte nachvollziehbar dokumentiert sein, wann und zu welchem Anlass eine Einsicht erfolgt. Die Nutzungseinschränkung ist damit ein Mittel, um die fortbestehende Aufbewahrungspflicht mit dem Datenschutzprinzip der Zweckbindung und Erforderlichkeit in Einklang zu bringen: Die Daten werden nicht „frei verfügbar" vorgehalten, sondern in einen Zustand überführt, der eine Nutzung nur noch in Ausnahmefällen erlaubt.

Für Betroffene ist es wichtig zu wissen, dass ihnen neben Akteneinsichtsrechten auch datenschutzrechtliche Auskunftsrechte nach §§ 54 ff. JVollzDSG zustehen. Gerade weil die rechtlichen Vorgaben zu Speicherung, Löschung und Nutzungseinschränkung komplex sind und die Betroffenen die Zulässigkeit einer Aufbewahrung häufig nur schwer selbst einschätzen können, unterstützen wir als Aufsichtsbehörde bei Fragen in diesem Kontext beratend. In der Praxis ist dabei nicht nur die Rechtslage entscheidend, sondern auch, ob die Einrichtungen über nachvollziehbare, dokumentierte Lösch- und Aufbewahrungsprozesse verfügen, die eine konsistente Anwendung der Vorgaben gewährleisten.

Videoüberwachung im Justizvollzug: Sicherheitserfordernisse und Grenzen der Beobachtung

Neben dem Einsatz zentraler Verwaltungssoftware ist die Videoüberwachung ein besonders sensibler Bereich der Datenverarbeitung im Strafvollzug. Kameras können zur Sicherheit beitragen, bergen aber zugleich erhebliche Risiken für die Rechte der Betroffenen – sowohl der Gefangenen als auch von Bediensteten und Dritten. Daher sind Videoüberwachungsmaßnahmen strikt an gesetzlichen Vorgaben auszurichten, auf das Erforderliche zu begrenzen und durch konkrete Schutzvorkehrungen zu flankieren.

Im Rahmen der Prüfung betrachteten wir die Videoüberwachung in den Justizvollzugsanstalten Saarbrücken und Ottweiler. Dabei ging es einerseits um die Frage, wo überwacht wird und auf welcher Rechtsgrundlage dies geschieht, andererseits um die technisch-organisatorische Ausgestaltung der Videobeobachtung, insbesondere hinsichtlich Zugriffsschutz, Speicherdauer, Löschung und Sicherung von Sequenzen.

- Videoüberwachung im Außenbereich: Kameras werden in den Justizvollzugsanstalten zunächst zur Sicherung der Grenzen und des unmittelbaren Umfelds eingesetzt. Trotz hoher Mauern und baulicher Sicherungen kommt es in der Praxis zu Versuchen, Außenwände zu überwinden oder unerlaubte Gegenstände in die Anstalt zu verbringen, etwa durch „Überwürfe" von Drogen, Mobiltelefonen oder anderen verbotenen Gegenständen. Der Gesetzgeber hat daher eine Beobachtung des Umfelds in § 30 JVollzDSG gestattet.

  Datenschutzrechtlich ist dabei entscheidend, dass schützenswerte Belange Dritter hinreichend berücksichtigt werden. Die Überwachung darf nicht dazu führen, dass private Grundstücke, Wohnbereiche oder öffentliche Wege in einem Umfang erfasst werden, der für die Sicherung der Anstalt nicht erforderlich ist. In der Praxis kann dies durch eine geeignete Ausrichtung der Kamera, durch Begrenzung des Erfassungsbereichs oder – soweit technisch erforderlich – durch Unkenntlichmachung (Schwärzung, Verpixelung) erreicht werden. Entscheidend ist,

dass solche Maßnahmen nicht nur theoretisch möglich sind, sondern tatsächlich eingesetzt und regelmäßig überprüft werden.

- Videoüberwachung im Innenbereich: Neben dem Außenbereich können auch bestimmte Freiflächen und Räume innerhalb der Anstalten Gegenstand einer Videoüberwachung sein. § 31 JVollzDSG gestattet eine Beobachtung, soweit dies aus Gründen der Sicherheit erforderlich ist. Typische Zwecke sind die Aufsicht über Bereiche, in denen eine unmittelbare Sichtkontrolle nicht möglich ist, die Verhinderung von unbefugtem Betreten bestimmter Zonen oder die Unterstützung bei der Bewältigung sicherheitsrelevanter Situationen.

  Im Rahmen unserer Prüfung in der JVA Saarbrücken wurde uns unter anderem die Videoüberwachung in einer Werkhalle vorgestellt. Dort existieren Bereiche, die vom zentralen Arbeitsplatz der Bediensteten aus nicht ohne Weiteres eingesehen werden können. Eine videogestützte Beobachtung kann in solchen Konstellationen dazu beitragen, Gefährdungen frühzeitig zu erkennen oder im Ereignisfall schneller reagieren zu können. Datenschutzrechtlich bleibt jedoch maßgeblich, dass der Einsatz auf die konkret erforderlichen Bereiche begrenzt wird und dass alternative, weniger eingriffsintensive Mittel geprüft werden, soweit sie gleich geeignet sind. Zudem ist sicherzustellen, dass die Videobeobachtung nicht zu einer „Dauerüberwachung ohne Anlass“ wird, die über das Sicherheitsbedürfnis hinausgeht.

- Besondere Sicherungsmaßnahmen und Überwachung in Hafträumen: Hafträume sind grundsätzlich von Videoüberwachung auszunehmen. Auch inhaftierten Personen ist ein Mindestmaß an Privatsphäre zuzugestehen. Ein vollständiger Verlust von Rückzugsräumen wäre mit den Grundrechten nicht vereinbar. Nur unter engen Voraussetzungen – insbesondere im Rahmen besonderer Sicherungsmaßnahmen bei konkreter Eigen- oder Fremdgefährdung – kann eine kameragestützte, für den Gefangenen erkennbare Beobachtung auf gesetzlicher Grundlage zulässig sein (§ 32 JVollzDSG). Hierzu dienen speziell dafür vorgesehene Räume (z. B. Monitorhafträume, besonders gesicherte Hafträume), die nicht dem

regulären Haftraumstandard entsprechen und deren Nutzung regelmäßig auf konkrete Gefährdungslagen bezogen und zeitlich begrenzt sein muss.

Auch bei einer zulässigen Überwachung sind weitere Schutzvorkehrungen zwingend: Es ist auf die elementaren Bedürfnisse der Gefangenen und auf die Wahrung der Intimsphäre Rücksicht zu nehmen. Insbesondere müssen sanitäre Einrichtungen zuverlässig von der Beobachtung ausgenommen werden. Nach den uns dargestellten Abläufen erfolgt dies in den saarländischen Anstalten durch Verpixelung bzw. Schwärzung des Toilettenbereichs. Für den Datenschutz ist hierbei nicht nur die Existenz einer Maskierung relevant, sondern auch deren Wirksamkeit: Maskierungen müssen so eingerichtet sein, dass sie nicht ohne Weiteres deaktiviert werden können, und ihre Funktionsfähigkeit sollte regelmäßig überprüft werden.

In besonders sensiblen Bereichen – etwa im medizinischen Bereich (Behandlungszimmer) oder in Räumen, in denen Entkleidungsdurchsuchungen stattfinden – findet nach den uns dargestellten Informationen keine Videoüberwachung statt.

Organisatorische Ausgestaltung der Videobeobachtung

Neben der Frage der räumlichen Zulässigkeit ist die technisch-organisatorische Ausgestaltung der Videobeobachtung entscheidend. Auch eine grundsätzlich zulässige Kamera kann datenschutzrechtlich problematisch werden, wenn der Zugriff auf Livebilder und Aufzeichnungen nicht hinreichend beschränkt ist, wenn Speicherfristen unangemessen lang sind oder wenn keine klaren Regeln für die Sicherung und Weitergabe von Sequenzen bestehen.

Wir betrachteten daher insbesondere:

- Videobeobachter-Arbeitsplätze: Sind Monitore so positioniert, dass Unbefugte keine Einsicht nehmen können? Gibt es Sichtschutzmaßnahmen? Sind Arbeitsplätze nur für berechtigte Personen zugänglich?

- Zugriffssteuerung: Wer darf Livebilder sehen, wer darf Aufzeichnungen abrufen, wer darf Sequenzen exportieren? Gibt es Rollen- und Berechtigungsmodelle auch für Videoanlagen?

- Speicher- und Löschkonzepte: Werden Aufzeichnungen nur so lange gespeichert, wie es zur Zweckerreichung erforderlich ist? Erfolgt eine automatische Löschung? Sind Fristen dokumentiert und überprüfbar?

- Sicherung zu Beweiszwecken: Wenn Sequenzen für Ermittlungs- oder Disziplinarverfahren gesichert werden, muss dies nachvollziehbar dokumentiert werden (Anlass, Zeitraum, Zugriff, Empfänger). Zudem ist sicherzustellen, dass gesicherte Sequenzen besonders geschützt sind und nach Abschluss des Verfahrens gelöscht werden, soweit keine weiteren gesetzlichen Gründe entgegenstehen.

- Protokollierung: Werden Zugriffe auf Aufzeichnungen protokolliert? Können Protokolle ausgewertet werden? Wird dies tatsächlich durchgeführt?

Zwischenfazit

Im Rahmen der Prüfung wurden keine gravierenden Defizite festgestellt, die sich nicht mit datenschutzrechtlichen Anforderungen vereinbaren ließen. Insgesamt ergaben sich vielmehr Hinweise darauf, dass die besonderen Anforderungen des Strafvollzugs mit dem Schutz personenbezogener Daten grundsätzlich in Einklang gebracht werden können, wenn klare rechtliche Grundlagen, ein restriktives Berechtigungskonzept und belastbare organisatorische Schutzmechanismen konsequent umgesetzt werden.

Gleichwohl zeigt sich – wie in vielen komplexen IT- und Sicherheitsumgebungen – ein fortlaufender Bedarf an Präzisierung und Pflege. Dies betrifft insbesondere die kontinuierliche Aktualisierung von Rollen- und Berechtigungen in zentralen Fachverfahren, die Auswertung von Zugriffsprotokollen, die konsequente Umsetzung und Dokumentation von Lösch- und Nutzungseinschränkungen sowie die klare, anlassbezogene

Handhabung der Sicherung von Videosequenzen. Wir werden die Ergebnisse der Prüfung mit dem Justizministerium erörtern und – soweit erforderlich – Empfehlungen zur weiteren datenschutzfreundlichen Ausgestaltung der Datenverarbeitung im Justizvollzug aussprechen.

Für Inhaftierte und ehemalige Inhaftierte gilt: Wer unsicher ist, ob und welche Daten zur eigenen Person bei der Justiz gespeichert sind, kann – neben den jeweils bestehenden Akteneinsichtsrechten – datenschutzrechtliche Auskunftsansprüche geltend machen. Gerade weil die gesetzlichen Vorgaben komplex sind und die tatsächliche Praxis für Betroffene schwer durchschaubar sein kann, unterstützen wir als Aufsichtsbehörde bei Fragen in diesem Bereich weiterhin beratend.

6.4 Kameras im Maßregelvollzug

Psychisch kranke oder suchtkranke Straftäterinnen und Straftäter, gegen die eine Maßregel der Besserung und Sicherung nach den §§ 61 ff. StGB angeordnet wurde, werden im Saarland regelmäßig nicht in einer Justizvollzugsanstalt, sondern in der Saarländischen Klinik für Forensische Psychiatrie (SKFP) in Merzig untergebracht. Auch im Maßregelvollzug dient die Unterbringung dem Schutz der Allgemeinheit vor weiteren Straftaten. Neben der psychiatrisch-medizinischen Behandlung sind deshalb angemessene bauliche und technische Sicherungsmaßnahmen erforderlich.

Eine solche Maßnahme kann die Beobachtung mittels optisch-elektronischer Einrichtungen (Videoüberwachung) sein. Voraussetzungen und Grenzen regelt § 42 MRVG[61]. Im Berichtsjahr begleiteten wir ein Beratungsvorhaben zur geplanten Erweiterung der Kameraüberwachung in der SKFP.

Zu Beginn unserer Beteiligung stand eine Novellierung der einschlägigen Videoüberwachungsbefugnisse im Raum. In den Abstimmungen erwies sich insbesondere die Auslegung des in § 42 MRVG verwendeten Begriffs der „Außenanlage“ als klärungsbedürftig. Aus Sicht unserer Behörde

61) Vgl. 33. Tätigkeitsbericht Datenschutz 2024, Kapitel 2.2.

umfasste der Begriff nach Entwurfsbegründung vor allem Grün- und Freiflächen innerhalb der gesicherten Anstaltsgrenzen (etwa Innenhöfe). Die Projektverantwortlichen wollten hingegen auch angrenzende Bereiche der unmittelbaren Umgebung außerhalb der Klinik einbeziehen. Wir haben darauf hingewirkt, den Anwendungsbereich im weiteren Gesetzgebungsverfahren durch Wortlaut und Begründung zu konkretisieren und den Einzelfall stärker an den räumlichen Gegebenheiten auszurichten. Diese Präzisierung wurde umgesetzt und schafft eine rechtssicherere Grundlage für die Planung.

Auf dieser Basis bewerteten wir die vorgesehenen Erweiterungen der Videoüberwachungsmaßnahme in der Klink und deren Umfeld. Die ergänzende Überwachung der Hauptpforte begegnete keinen datenschutzrechtlichen Bedenken. Auch für die Videoüberwachung der auf dem Gelände gelegenen Mitarbeiterparkplätze wurden gewichtige Gründe angeführt. Zugleich wiesen wir darauf hin, dass die Abwehr akuter Gefahrenlagen – etwa Übergriffe oder schwerwiegende Manipulationen an Fahrzeugen – regelmäßig vor allem durch ein situationsbezogenes Live-Monitoring wirksam unterstützt werden kann; dies ist bei der Ausgestaltung (Zugriffs- und Berechtigungskonzept) zu berücksichtigen.

Weiterhin wurde seitens der SKFP der Bedarf angemeldet, Teile einer auf dem Gelände verlaufenden Stichstraße zu überwachen. In diesem Bereich befindet sich ein Unterstand, den untergebrachte Personen mit gewährtem Freigang in ihrer Freizeit nutzen dürfen. Hier gaben wir zu bedenken, dass Bereiche mit Freizeit- und Rückzugsfunktion einer Videoüberwachung nur eingeschränkt zugänglich sind und gegebenenfalls ausgenommen oder zeitlich zu begrenzen sind; zudem kommen technische Maßnahmen wie Blickwinkelbegrenzung oder Maskierungen in Betracht.

Schließlich berieten wir zur Umsetzung der Transparenzpflichten. Nach § 42 Abs. 4 Satz 2 MRVG ist die Beobachtung kenntlich zu machen. Da die

Videoüberwachung zwar auf dem Grundstück der Einrichtung erfolgt, dort jedoch auch Wege und Straßen liegen, die unproblematisch von Dritten genutzt werden können, empfahlen wir eine ausreichende und korrekt gestaltete Hinweisbeschilderung an den maßgeblichen Zugangspunkten und Zugangswegen.

ÖFFENTLICHE VERWALTUNG

7. ÖFFENTLICHE VERWALTUNG

7.1 Baby-Begrüßungsbesuche

Gratulationen der Kommunen zu besonderen Anlässen gehören vielerorts zur gelebten Verwaltungspraxis. Sie können die Verbundenheit innerhalb der örtlichen Gemeinschaft stärken und sind aus datenschutzrechtlicher Sicht grundsätzlich möglich. Bereits in unserem Tätigkeitsbericht 2017/2018[62] haben wir ausführlich dargelegt, dass das Beglückwünschen von Einwohnerinnen und Einwohnern zu bestimmten Jubiläen – etwa zu runden Geburtstagen oder Ehejubiläen – durch kommunale Mandatsträger mit Blick auf § 50 Abs. 2 Bundesmeldegesetz (BMG) als Aufgabe der kommunalen Selbstverwaltung eingeordnet und bei entsprechender Ausgestaltung satzungsrechtlich geregelt werden kann.

Anders zu bewerten ist jedoch die immer wieder geäußerte Idee, anlässlich der Geburt eines Kindes persönlich zu gratulieren und hierbei unangekündigt einen Hausbesuch durchzuführen oder eine „Baby-Willkommensbox" zu überbringen. Die Geburt eines Kindes ist ein sehr persönliches Ereignis.

62) Vgl. 27. Tätigkeitsbericht Datenschutz 2017/2018, Kapitel 6.4.

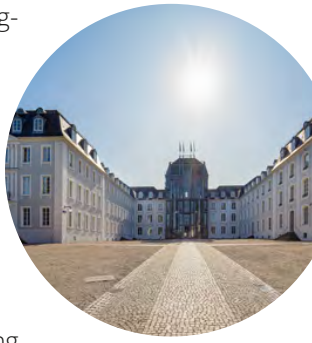
Im Gegensatz zu einem runden Geburtstag ist ein Besuch der Verwaltung in dieser Situation weder sozial üblich noch erwartbar. Ein unangekündigter Vor-Ort-Besuch kann – auch unabhängig von der Freundlichkeit der Geste – als erheblicher Eingriff in die private Lebensgestaltung wahrgenommen werden.

Diese besondere Schutzbedürftigkeit ist nicht nur eine Frage der sozialen Angemessenheit, sondern hat unmittelbare datenschutzrechtliche Konsequenzen. Denn ein Baby-Begrüßungsbesuch setzt regelmäßig eine vorgelagerte Datenverarbeitung voraus: Die Kommune benötigt Informationen über die Geburt sowie Namen und Anschrift der Eltern, um den Besuch zu organisieren. Eine dem § 50 Abs. 2 BMG entsprechende rechtliche Befugnis für diese Datenverarbeitung existiert nicht, so dass die Möglichkeit einer satzungsrechtlichen Regelung für die Kommune ausscheidet. Werden für die Gratulation zur Geburt Daten erhoben und an eine andere Stelle innerhalb der Kommune (z. B. Bürgermeisterbüro, Ortsvorsteher) weitergegeben, die ursprünglich im Melde- oder Standesamtskontext verarbeitet wurden, liegt eine Verarbeitung zu einem anderen Zweck vor. Für eine solche Datenverarbeitung zu Gratulationszwecken reicht eine bloße Ankündigung des Vorhabens – etwa im Amtsblatt oder auf der Internetseite – nicht aus, selbst wenn den Eltern darin eine Widerspruchsmöglichkeit („Opt-out“) eingeräumt wird. Ebenso wenig kann eine Einwilligung der Eltern stillschweigend unterstellt werden, da eine solche grundsätzlich ausdrücklich erteilt werden muss.

Baby-Begrüßungsbesuche sind daher so zu gestalten, dass sie nur auf der Grundlage einer vorherigen, unmissverständlichen Einwilligung der betroffenen Personen erfolgen. Das bedeutet: Eltern müssen das Angebot bewusst annehmen („Opt-in“), etwa indem sie sich bei der Gemeinde melden oder ein entsprechendes Formular (online oder in Papierform) ausfüllen. Hierfür kann die Kommune allgemein – etwa im Gemeindeblatt oder auf der Internetseite – über ein freiwilliges Willkommensangebot informieren und einen einfachen Weg zur Anmeldung bereitstellen. Erst dann dürfen die hierfür erforderlichen Daten verarbeitet und – soweit notwendig – intern weitergegeben werden.

7.2 Live-Streaming von Ratssitzungen

Zur Stärkung demokratischer Teilhabe nutzen staatliche und kommunale Gremien seit langem audiovisuelle Formate. Während Übertragungen von Parlamentsdebatten auf Landes- und Bundesebene etabliert sind, wächst auch im kommunalen Bereich das Interesse, öffentliche Sitzungen von Gemeinderäten und Kreistagen per Live-Stream zugänglich zu machen oder im Nachgang als Aufzeichnung bereitzustellen. Solche Angebote können Transparenz fördern und den Zugang für Menschen erleichtern, die Sitzungen nicht vor Ort verfolgen können. Die rechtlichen Voraussetzungen hierfür regelt § 40 Abs. 1 Satz 3 und 4 KSVG. Danach darf der Gemeinderat bzw. Kreistag in öffentlichen Sitzungen Ton- und Bildübertragungen sowie Ton- und Bildaufzeichnungen veranlassen und der Allgemeinheit über das Internet zur Verfügung stellen. Datenschutzrechtlich stützt sich die Verarbeitung personenbezogener Daten regelmäßig auf Art. 6 Abs. 1 lit. e DSGVO i. V. m. Art. 6 Abs. 3 DSGVO, da sie der Wahrnehmung einer Aufgabe im öffentlichen Interesse dient und in § 40 KSVG gesetzlich näher ausgestaltet ist.



Reichweite der Ermächtigung und Betroffenenkreis

Adressat der gesetzlichen Regelung sind die kommunalen Mandatsträgerinnen und Mandatsträger. § 40 KSVG ermöglicht damit eine mediale Abbildung des kommunalpolitischen Meinungsaustauschs, nicht jedoch eine allgemeine Erfassung der Saalöffentlichkeit. Besucherinnen und Besucher nehmen öffentliche Sitzungen aufgrund des Öffentlichkeitsgrundsatzes grundsätzlich „bedingungslos“ wahr: Sie dürfen nicht faktisch vor die Wahl gestellt werden, entweder auf Anwesenheit zu verzichten oder eine Veröffentlichung ihrer Person hinzunehmen. Daher hat die Kommune organisatorisch und technisch sicherzustellen, dass Aufnahmen auf den für die Beratung maßgeblichen Bereich (z. B. Rednerpult, Sitzbereich des Rates) begrenzt werden und Publikumsbereiche nicht erfasst werden. Hinweise am Eingang sind gleichwohl erforderlich, ersetzen aber keine tragfähige Rechtsgrundlage für Publikumsaufnahmen.

Widerspruchsrecht der Ratsmitglieder

§ 40 Abs. 1 Satz 4 KSVG gewährt jedem Ratsmitglied das Recht zu verlangen, dass die Übertragung und Aufzeichnung seines Redebeitrags bzw. die Veröffentlichung der Aufzeichnung unterbleibt. Dieses individuelle, voraussetzungslose Widerspruchsrecht verdeutlicht zweierlei: Erstens obliegt die Grundentscheidung über Live-Stream und/oder Aufzeichnung dem Kollegialorgan, regelmäßig durch Regelungen in der Geschäftsordnung. Einzelne Ratsmitglieder können die Durchführung nicht insgesamt verhindern, wohl aber die mediale Verwertung des eigenen Redebeitrags. Zweitens muss die Kommune ein praktikables Verfahren vorsehen, um Widersprüche zuverlässig umzusetzen (z. B. vorherige Abfrage, Möglichkeit des kurzfristigen Widerspruchs, klare Zuständigkeiten). Technisch kommen etwa Stummschaltung, Abblenden/Standbild oder eine Kameraführung ohne Abbildung der widersprechenden Person in Betracht. Dass hierdurch in Übertragung oder Aufzeichnung inhaltliche Lücken entstehen und daraus Rückschlüsse auf die widersprechende Person möglich sind, ist als gesetzlich angelegte Folge hinzunehmen.

Veröffentlichung und Speicherdauer

Für die öffentliche Bereitstellung aufgezeichneter Sitzungen enthält § 40 KSVG keine ausdrücklichen Speicherfristen. Maßgeblich ist daher der Grundsatz der Speicherbegrenzung: Die Dauer der Veröffentlichung muss am Zweck der Information und Rechenschaft ausgerichtet sein. Als Orientierungswert halten wir eine Bereitstellung für die laufende Legislaturperiode regelmäßig für angemessen. Diese Begrenzung beruht maßgeblich auf der Erwägung, dass mit dem Ende der Legislaturperiode regelmäßig auch das Mandat der betroffenen Ratsmitglieder endet und sich damit der unmittelbare Aktualitäts- und Rechenschaftsbezug der veröffentlichten Redebeiträge deutlich abschwächt. Spätestens zu diesem Zeitpunkt sollte daher eine Depublikation erfolgen oder zumindest eine erneute Prüfung der Erforderlichkeit und Verhältnismäßigkeit vorgenommen werden. Davon zu trennen sind Aufbewahrungen zu internen Zwecken, etwa zur Dokumentation oder für das Kommunalarchiv. Solche Archivierungen können zulässig

sein, müssen jedoch mit einem eigenen Zweck, klaren Zugriffsregelungen und einer deutlichen Trennung von der frei zugänglichen Mediathek verbunden werden.

Insgesamt können Live-Streams und Aufzeichnungen die kommunale Öffentlichkeit sinnvoll erweitern – datenschutzgerecht sind sie aber nur, wenn Rechtsgrundlage, Betroffenenkreis, Widerspruchsverfahren, Kameraführung und Speicherkonzept konsequent aufeinander abgestimmt werden

7.3 Bekanntgabe von Schulnoten

Situationen, in denen die Lehrerin oder der Lehrer schulische Leistungen im Klassensaal vor den übrigen Mitschülerinnen und Mitschülern benotet, dürften viele von uns, sicherlich mit gemischten Gefühlen, noch vor Augen haben.

Aus datenschutzrechtlicher Sicht kann eine solche individuelle Notenverkündung in der Klasse nur dann zulässig sein, wenn sie sich auf eine Rechtsgrundlage stützen kann.

Im saarländischen Schulrecht findet sich indes keine rechtliche Verankerung dieser Praxis. Im Gegenteil lässt der *„Erlass zur Leistungsbewertung in den Schulen des Saarlandes“*[63] vielmehr den Schluss zu, dass schulrechtlich lediglich die Veröffentlichung eines nicht individualisierten (pseudonymisierten) Notenspiegels zulässig ist und dies auch nur im Bereich der weiterführenden Schulen. Für die Grund- und Förderschulen untersagt der Erlass die Bekanntgabe des Notenspiegels (vgl. Nr. 2.4.2, 2.4.4, 3.4.2 und 4.4.2.).

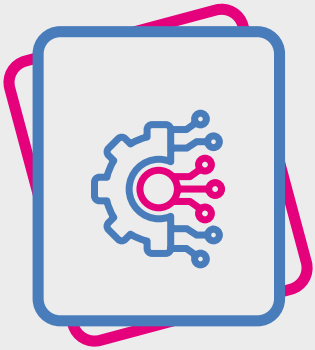
Eine derartige Praxis der Datenoffenlegung kann nicht auf den allgemeinen schulischen Bildungs- und Erziehungsauftrag (§ 1 Schulordnungsgesetz) gestützt werden und ist daher nicht in das Ermessen des Lehrpersonals gestellt. Eine Datenverarbeitung von einer derartigen Eingriffsqualität in die grundrechtlichen Positionen der Schülerinnen und Schüler verlangt

63) Amtsblatt des Saarlandes I, Nr. 28/2024, S. 506 ff.

vielmehr nach einer bereichsspezifischen eindeutigen Gesetzesgrundlage (vgl. Art. 6 Abs. 1 lit. e, Abs. 3 lit. b DSGVO), welche wie bereits erwähnt, nicht existiert.

Auch kann sich eine diesbezügliche Befugnis daneben weder aus einer ausdrücklichen noch einer konkludenten (stillschweigenden) Einwilligung der Schüler ergeben. Selbst für den Fall, dass man die formalen Bedingungen einer Einwilligung nach Art. 7 DSGVO in punkto Informiertheit und Eindeutigkeit sicherzustellen vermag, so dürfte es regelmäßig an der Freiwilligkeit einer solchen Einwilligung fehlen. Die Schüler können sich nämlich einer solchen Praxis schwerlich bis gar nicht entziehen. In vielen Fällen werden sie bereits aus einem Gruppenzwang innerhalb der Klasse der Verkündung ihrer Noten zustimmen, selbst wenn ihnen dies unangenehm oder nicht Recht sein sollte. Diejenigen Schülerinnen und Schüler, welche sich einer Veröffentlichung ihrer Noten in einer solchen Situation versperren, müssten mit dem falsch verstandenen Makel der unausgesprochen schlechten Zensur leben, was diskriminierenden Charakter haben kann und für die schulische Entwicklung sicherlich nicht förderlich ist.

Die Bewertung oder Benotung schulischer Leistungen vor den übrigen Mitschülern ist demnach datenschutzrechtlich unzulässig. Hieran vermag auch eine gut gemeinte Absicht der Motivation der Schülerinnen und Schüler nichts zu ändern. Dies kann auch durch ein individuelles Gespräch mit dem Lehrpersonal erreicht werden, ohne das Ergebnis einer Bloßstellung einzelner Schülerinnen und Schüler zu riskieren.



TECHNISCH-ORGANISATORISCHER DATENSCHUTZ

8. TECHNISCH-ORGANISATORISCHER DATENSCHUTZ

8.1 Risikobewertung bei Datenschutzverletzungen

Dass im Zuge der Verarbeitung personenbezogener Daten auch Fehler passieren, seien sie technischer oder menschlicher Natur, ist unvermeidlich. Die DSGVO trägt diesem Umstand in den Art. 33 und 34 DSGVO Rechnung. Diese Vorschriften sehen ein Fehlerfolgensystem vor, welches, je nach Konstellation und Schwere der dem Fehler zugrunde liegenden Datenschutzverletzung, zwei Stufen vorsieht.

Wird durch den Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten i. S. d. Art. 4 Nr. 12 DSGVO erkannt oder besteht zumindest eine hohe Wahrscheinlichkeit einer solchen Datenschutzverletzung, so hat er dies nach Art. 33 DSGVO auf erster Stufe unverzüglich und möglichst binnen 72 Stunden der gemäß Art. 55 DSGVO zuständigen Aufsichtsbehörde zu melden. Von einer solchen Meldung darf der Verantwortliche nur dann absehen, wenn die Verletzung des Schutzes personenbezogener Daten nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche auf einer zweiten Stufe – zusätzlich zu der zuständigen Aufsichtsbehörde – auch die betroffene Person unverzüglich von der Verletzung. Diese Benachrichtigung muss u. a. in klarer und einfacher Sprache erfolgen, eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung oder Abmilderung ihrer möglichen nachteiligen Auswirkungen für die betroffene Person enthalten. Damit soll es der betroffenen Person ermöglicht werden, bereits eigenständig die erforderlichen Vorkehrungen zu treffen.

Sowohl im Rahmen des Art. 33 Abs. 1 DSGVO (Meldung an die Aufsichtsbehörde) als auch im Rahmen des Art. 34 Abs. 1 DSGVO (Benachrichtigung der betroffenen Person) ist es der unbestimmte Begriff des „Risikos" der Verletzung, welcher den Dreh- und Angelpunkt des weiteren Vorgehens bildet. Zwar gibt die DSGVO in ihrem Erwägungsgrund 85 dem Verantwortlichen hierbei eine gewisse Hilfestellung, indem sie bestimmte Risikoarten – wohlgemerkt in nicht abschließender Form – beispielhaft aufzählt. Der Verantwortliche muss den Begriff gleichwohl mit Leben ausfüllen, indem er konkrete Überlegungen und Prognosen anstellt. Es verbietet sich dabei von vornherein, sich hierbei ausschließlich vorgefertigter Formulare oder Checklisten zu bedienen, auch wenn diese womöglich den Anspruch erheben sollten, eine rechtskonforme Bewertung zeitsparend und vollumfänglich durchführen zu können.

Anhand der Meldung einer Datenschutzverletzung einer örtlichen Kindertageseinrichtung kann exemplarisch dargestellt werden, welche Überlegungen der Verantwortliche hierbei anzustellen hat. Hintergrund war eine Meldung nach § 47 SGB VIII (Kindeswohlgefährdung) aufgrund eines gegenüber anderen Kindern mutmaßlich auffällig gewordenen Kindes. Um den Sachverhalt zu klären, wurde durch die Kommune via E-Mail zeitnah Kontakt zu der Leitung der Kindestageseinrichtung gesucht, wobei ihr ein folgenschwerer Fehler in Form der Verwechselung zweier E-Mail-Verteilerlisten

unterlief. Anstelle einer E-Mail-Adresse der Kita-Leitung fand ein namensgleicher Verteiler Verwendung, mit der Folge, dass eine große Anzahl von Eltern derzeitig und ehemals betreuter Kinder von dem Vorfall Kenntnis erhielt.

Dieser Fehler wurde zeitnah bemerkt und unsere Behörde auch fristgemäß hiervon nach Art. 33 DSGVO in Kenntnis gesetzt. Auch wurden die Empfänger der E-Mail darum gebeten, diese zu löschen und über deren Inhalt Stillschweigen zu wahren; das Wichtigste wurde jedoch Unterlassen, nämlich auch die Eltern des betroffenen Kindes zeitnah nach Art. 34 Abs. 1 DSGVO zu benachrichtigen. Ohne weitere Begründung vertrat hier die Gemeinde die Auffassung, aus dem Datenschutzverstoß resultiere kein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen.

Dies ist jedoch zu kurz gegriffen, denn der in Art. 34 DSGVO niedergeschriebene Risikobegriff („hohes Risiko“) umfasst gerade nicht nur eine Gefährdung physischer oder materieller Rechte. Aus Erwägungsgrund 85 der DSGVO geht vielmehr hervor, dass auch immaterielle Güter hierunter zu subsumieren sind. So wird auch die Gefahr einer durch die Datenschutzverletzung drohenden Diskriminierung in dem Erwägungsgrund explizit als Beispiel genannt.

Ein solches hohes Risiko drängte sich vorliegend jedoch geradezu auf. Zu dem Zeitpunkt, in welchem der Fehler erkannt wurde, ging es nicht mehr darum einen womöglich entstandenen Schaden rückgängig zu machen. Nach erfolgter Offenlegung der sensiblen Informationen über ihren Sohn an einen unbestimmten Adressatenkreis anderer Eltern konnte die Datenschutzverletzung nicht mehr „geheilt“ werden. Sprichwörtlich war das Kind zu diesem Zeitpunkt bereits in den Brunnen gefallen. Trotzdem war eine sofortige Benachrichtigung der Eltern in dieser Situation alles andere als überflüssig. Den Eltern wäre hierdurch die Möglichkeit gegeben worden, sich auf die Situation einzustellen, konkret, sich darauf gefasst zu machen, von anderen Personen auf den Sachverhalt angesprochen zu werden und

sich bereits im Vorfeld darauf vorzubereiten. Es ging mithin darum, eine Überrumpelungssituation zu verhindern und womöglich auch das eigene Kind mental darauf einzustellen, in der Kindertageseinrichtung oder im sonstigen sozialen Umfeld mit der Sache konfrontiert zu werden.

Führt man sich diese Überlegungen vor Augen, so wäre eine sofortige Benachrichtigung der Eltern absolut naheliegend gewesen. Um dies zu erkennen, braucht es jedoch tatsächlicher eigener Überlegungen und Bewertungen des Verantwortlichen.

8.2 Datenschutzverletzungen durch Phishing und Drittanbieter-Produkte

Im Jahr 2025 erreichten das Unabhängige Datenschutzzentrum Saarland 914 Meldungen von Datenschutzverletzungen nach Art. 33 DSGVO. Wenngleich jede Meldung einen individuell zu bewertenden Einzelfall darstellt, so lassen sich drei wesentliche Trends erkennen: Ein Teil der Vorfälle geht auf menschliche oder organisatorische Fehler zurück. So wurden beispielsweise Daten von Betroffenen aufgrund von Tippfehlern in der E-Mail-Empfängerleiste an falsche Empfänger gesendet oder Daten ohne Rechtsgrundlage erhoben. Ein weiterer Teil lässt sich auf Phishing zurückführen: Als eine Form des sogenannten Social Engineering werden dabei häufig E-Mails gefälscht, um Mitarbeitende einer Institution zur Preisgabe von Zugangsdaten zu verleiten. Mit den so erbeuteten Zugangsdaten können Kriminelle sich dann in die Systeme der Institution einloggen, dort Daten abgreifen oder weitere unbefugte Handlungen vornehmen. Den dritten großen Bereich stellen Sicherheitsvorfälle im Zusammenhang mit Drittanbieter-Hard- und -Software dar. Dabei treten Sicherheitslücken in eingekauften IT-Systemen auf und führen zur Kompromittierung der verarbeiteten personenbezogenen Daten, ohne dass dies unmittelbar von der angegriffenen Institution ausgeht. Im Folgenden soll der Blick auf die beiden letzten Kategorien gerichtet werden. Neben relevanten potenziellen Fallstricken werden auch Empfehlungen und Handlungsoptionen aufgezeigt, mit denen sich derartige Vorfälle vermeiden lassen.

Kompromittierung von Zugangsdaten durch Phishing

Analog zu anderen Formen des Social Engineering wird auch beim Phishing die Gutgläubigkeit der Opfer ausgenutzt. So wird in der Regel ein Vorwand konstruiert, unter dem bspw. Mitarbeitende einer Institution darum gebeten werden, ihre Zugangsdaten zu bestimmten IT-Systemen auf einer Webseite anzugeben bzw. zu bestätigen. Bekannt sind diese Angriffe oft aus dem Umfeld von Banken: Private E-Mail-Konten erhalten Nachrichten, dass die Zugangsdaten zum Konto bei einer beliebigen Bank dringend aktualisiert werden müssten. Auch im beruflichen Umfeld häufen sich Phishing-Mails. Mit Hilfe weniger, öffentlich einsehbarer Informationen lassen sich E-Mails formulieren, die angeblich von Vorgesetzten stammen und dringend um Zugangsdaten oder direkt um Geld, etwa in Form von Bezahlkarten, bitten. Durch die Nutzung großer Sprachmodelle (Large Language Models, LLMs) ist es für Kriminelle überdies ein Leichtes, auch umfangreiche, sprachlich korrekte E-Mails mit komplexen und glaubwürdigen Vorwänden zu formulieren.

Opfer von Phishing haben derweil nicht nur mit dem unmittelbar entstandenen Schaden zu kämpfen. Oft fürchten sie Ärger oder Repressionen im beruflichen Umfeld für das „Hereinfallen" auf derartige Angriffe. In einigen Fällen führt dies dazu, dass erfolgreiche Phishing-Angriffe erst spät gemeldet werden und sich durch die verspätete Reaktion der Schaden noch vergrößert.

Regelmäßig werden bei Phishing-Angriffen personenbezogene Daten kompromittiert. Dazu zählen etwa Daten der Opfer selbst aber auch von weiteren Mitarbeitenden, dienstlichen Kontakten oder Kunden. In mehreren, dem UDZ gemeldeten Fällen wurden Adressbücher und E-Mail-Accounts nach Kontakten durchsucht, um über das gekaperte E-Mail-Konto weitere Spam- oder Phishing-Mails zu versenden.

Für die betroffenen Institutionen ist es oft schwer, abzuschätzen, welches Ausmaß der Angriff insgesamt hat und damit auch, welche personenbezogenen Daten konkret betroffen sind. Diese Information ist jedoch

nicht nur zur Eindämmung und Bekämpfung des unmittelbaren Angriffs entscheidend, sondern muss auch Bestandteil der Meldung nach Art. 33 DSGVO an die Datenschutzbehörde sein. Diese prüft die von dem Verantwortlichen vorgenommene Risikoeinschätzung und berät über weitere Schritte.

Eine obere Grenze für den möglichen Schaden durch Phishing lässt sich aus den Zugriffsrechten der betroffenen Nutzerkonten ableiten. Haben Angreifer durch Phishing Zugriff auf ein Nutzerkonto erlangt, können sie in der Regel auf alle Inhalte zugreifen, für die dieses Konto freigeschaltet ist. Können konkrete Zugriffe also nicht durch Protokolldaten oder ähnliches nachgewiesen oder ausgeschlossen werden, so muss davon ausgegangen werden, dass alle zugreifbaren Daten vom Angriff betroffen sind. Dies verdeutlicht auch, wie wichtig eine effektive Verwaltung von Zugriffsrollen und -rechten sowie eine Segmentierung der Datenbestände sind. Das sogenannte „Principle of Least Privilege" (dt. etwa Prinzip des minimalen Zugriffsrechts) ist tief in der IT-Sicherheit verwurzelt und besagt, dass ein Zugriff nur auf die Daten möglich sein darf, die zur Erfüllung der gegebenen Aufgaben notwendig sind. Im Datenschutzrecht hat dieser Grundsatz in Form der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO Einzug gehalten.

Zur Vermeidung und Bekämpfung von Phishing-Angriffen können eine Reihe weiterer Maßnahmen getroffen werden. Das BSI[64] hat eine Informationsseite eingerichtet, ebenso informiert die Verbraucherzentrale NRW[65] laufend über aktuelle Phishing-Kampagnen. Im Folgenden sind noch einmal einige Empfehlungen zusammengefasst.

Für Verantwortliche:

- die Einrichtung und Anpassung von Spamfiltern sowie weiterer E-Mail-Sicherheitsmechanismen wie SPF, DKIM und DMARC,

64) https://www.bsi.bund.de/dok/passwortdiebstahl-durch-phishing.
65) https://www.verbraucherzentrale.nrw/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnungen-6059.

- die Anzeige vollständiger E-Mail-Adressen im E-Mail-Client (ggf. werden sonst nur Namen angezeigt, die jedoch vollständig vom Absender der Mail kontrolliert werden können und daher nicht vertrauenswürdig sind),

- die Umsetzung eines Rollen- und Rechtekonzepts nach dem „Principle of Least Privilege“ und die Beachtung des Grundsatzes der Datenminimierung,

- die Schulung von Mitarbeitenden, um Phishing-Angriffe zu erkennen und ggf. zu melden,

- die Etablierung einer (Fehler- bzw. Arbeits-)kultur, in der Opfer von Sicherheitsvorfällen zur Meldung ermutigt werden.

Für Einzelpersonen:

- die Anzeige vollständiger E-Mail-Adressen im E-Mail-Client (s. o.),

- die Schärfung des eigenen Bewusstseins für Spam- und Phishing-Mails,

- eine gesunde Skepsis gegenüber spontanen oder ungewöhnlichen Anfragen (ggf. ist es ratsam, vor potenziell schädlichen Handlungen wie der Eingabe von Zugangsdaten eine Bestätigung auf einem anderen „Kanal“, bspw. per Telefon, einzuholen).

Kompromittierung von Drittanbieter-Systemen

In einigen gemeldeten Fällen ließen sich die Vorfälle auf Soft- oder Hardwaresysteme von Drittanbietern zurückführen, die von den Verantwortlichen eingesetzt wurden. So ist es bspw. üblich, in Betrieben mit einem hohen Maß an Außendienst oder für Mitarbeitende im Home-Office ein VPN („Virtual Private Network“) einzurichten, das eine verschlüsselte Verbindung zwischen dem Endgerät (Laptop, Smartphone o. ä.) und der IT-Infrastruktur

des Arbeitgebers herstellt. Oft kommen dabei kommerzielle Produkte, sog. VPN-Gateways, zum Einsatz. Diese bieten eine Rundum-Lösung: Sie müssen lediglich einmalig in die IT-Infrastruktur integriert werden und stellen dann entsprechende Anwendungsprogramme und/oder Konfigurationsdateien zur Verfügung, die sich auf den Endgeräten installieren lassen. Auch bei Firewalls werden in der Regel kommerzielle Produkte eingesetzt, die sich mit geringem Aufwand konfigurieren lassen und weitestgehend autonom arbeiten.

Häufig ist der Einsatz von (nicht nur kommerziellen) Drittanbieter-Systemen alternativlos, etwa weil nur begrenzte technische Expertise vorhanden ist oder weil ein vergleichbares Sicherheits- bzw. Qualitätsniveau nicht mit anderen Mitteln hergestellt werden kann. Die Nutzung entbindet Institutionen jedoch nicht von ihrer datenschutzrechtlichen Verantwortlichkeit. Es muss also sichergestellt werden, dass die Systeme aktualisiert und ggf. ersetzt werden. Auf der Webseite des CERT-Bund[66] warnt etwa das BSI vor bekannten Schwachstellen in zahlreichen Hard- und Softwarekomponenten. Diese Informationen sowie Informationen der Hersteller über eventuell verfügbare Updates sollten Verantwortliche beobachten. Manche Quellen lassen sich „abonnieren", sodass eine E-Mail-Benachrichtigung erfolgt, wenn eine Schwachstelle in einem selbst eingesetzten Produkt auftritt oder ein Update verfügbar ist.

Im Auge behalten sollten Verantwortliche auch den Lebenszyklus der eingesetzten Systeme. Endet die Unterstützung des Herstellers für ein bestimmtes System, werden in der Regel keine Updates mehr bereitgestellt. Wird dann dennoch eine Sicherheitslücke bekannt, besteht eine akute Gefahr für die IT-Sicherheit und damit in der Regel auch das Risiko einer Datenpanne. Zeichnet sich also ab, dass ein eingesetztes System das Ende seines Lebenszyklus erreicht – meist informieren Hersteller über das geplante Ende der Unterstützung – sollte rechtzeitig der Ersatz geplant und umgesetzt werden.

---

66) https://wid.cert-bund.de/portal/wid/kurzinformationen.

Das BSI[67] stellt einige Hinweise für die Aktualisierung von Software bereit. Im Folgenden sind noch einmal wichtige Empfehlungen zusammengefasst:

- Verfügbare Updates zeitnah installieren, Meldungen über verfügbare Updates abonnieren oder beobachten,
- Sicherheitsmeldungen eines CERT und/oder des Herstellers abonnieren oder beobachten,
- Veraltete Systeme vor Ende des Herstellersupports aktualisieren oder austauschen,
- Notfallpläne erstellen, falls Systeme abgeschaltet werden müssen, weil Sicherheitslücken bekannt sind und (noch) keine Updates bereitstehen.

8.3 Pflichten von Auftragsverarbeitern

Auch wenn Verantwortliche über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden und damit nach Art. 4 Nr. 7 DSGVO die Hauptlast der datenschutzrechtlichen Pflichten tragen, sind Auftragsverarbeiter – mithin unterstützende Stellen, derer sich die Verantwortlichen im Rahmen ihrer Datenverarbeitungsprozesse bedienen – ebenso Adressaten von Vorgaben der DSGVO. Ungeachtet der in Art. 29 DSGVO normierten Weisungsgebundenheit im Rahmen der Verarbeitung personenbezogener Daten im Auftrag des datenschutzrechtlich Verantwortlichen, wird ausdrücklich auch der Auftragsverarbeiter nach Art. 32 DSGVO verpflichtet, ausreichende Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu ergreifen und läuft spiegelbildlich für den Fall eines Verstoßes gegen diese Pflichten Gefahr, Adressat von aufsichtsbehördlichen Abhilfe- und Sanktionsmaßnahmen zu werden.

67) https://www.bsi.bund.de/dok/504184.

Potenzielle Verstöße von Auftragsverarbeitern gegen Pflichten aus Art. 32 DSGVO wurden der Aufsichtsbehörde im Berichtszeitraum durch Meldungen über Datenschutzverletzungen nach Art. 33 DSGVO bekannt, die von den Verantwortlichen oder – ohne dass diese eine Meldepflicht nach der Vorschrift treffen würde – von den Auftragsverarbeitern abgegeben wurden, aber auch durch Mitteilungen früherer Kundinnen und Kunden oder betroffener Personen.

Fehlender Nachweis geeigneter Prozesse

Eine Sicherheitslücke bei einem Softwareentwickler führte zu einer potenziellen Zugriffsmöglichkeit auf eine hohe sechsstellige Anzahl an Kundendatensätzen eines Verantwortlichen. Den diesbezüglichen Meldungen nach Art. 33 DSGVO sowohl des Verantwortlichen als auch dessen Auftragsverarbeiters lag dabei im Wesentlichen zugrunde, dass durch einen Fehler beim Auftragsverarbeiter statt randomisierter Daten eine vollständige Kopie der Kundendatenbank des Verantwortlichen an den Softwareentwickler weitergegeben wurde. Auch wenn sich letztlich keine Anhaltspunkte für einen Datenabfluss ergeben haben, wurde im Rahmen der Untersuchung des Sachverhalts erkennbar, dass eine unzureichende Operationalisierung der Vorgaben des Auftragsverarbeitungsvertrags nach Art. 28 Abs. 3 Satz 1 DSGVO sowohl beim Verantwortlichen als auch beim Auftragsverarbeiter einen wesentlichen Beitrag zu dieser unbeabsichtigten Datenweitergabe geleistet haben.

Art. 32 Abs. 4 DSGVO adressiert gleichermaßen Verantwortliche und Auftragsverarbeiter und verpflichtet diese zur Implementierung entsprechender prozeduraler Schritte. Nur durch hinreichende Dokumentationsprozesse ist sichergestellt, dass der Auftragsverarbeiter ihnen erteilte Weisungen unmissverständlich ausführen und eine weisungskonforme Erledigung nachweisen bzw. der Verantwortliche den ihm nach Art. 5 Abs. 2 DSGVO obliegenden Kontrollpflichten mit Blick auf die Ausführung seiner Weisungen nachkommen kann.

Der vorliegend geschlossene Auftragsverarbeitungsvertrag sah in Umsetzung von Art. 28 Abs. 3 Satz 2 lit. a DSGVO zwar vor, dass mündlich

erteilte Weisungen schriftlich zu bestätigen sind, allerdings hatte der Auftragsverarbeiter keine internen Vorgaben operationalisiert, wie mit mündlich erteilten Weisungen im konkreten Fall umzugehen ist, damit die Umsetzung der auftragsvertraglichen Maßgaben prozesshaft gewährleistet ist. Ferner hatten in dem untersuchten Fall letztlich weder der Verantwortliche noch der Auftragsverarbeiter die erteilte Weisung schriftlich dokumentiert, so dass der Auftragsverarbeiter, der die Weitergabe einer vollständigen Kopie der Kundendatenbank veranlasst hatte, nicht nur den konkreten Wortlaut, der die Datenweitergabe veranlassenden Weisung nicht glaubhaft machen konnte, sondern gerade auch die prozedurale Gewährleistung einer weisungskonformen Erfüllung nicht garantieren konnte.

Gegen den Auftragsverarbeiter wurde wegen eines Verstoßes gegen Art. 28 Abs. 3 Satz 2 lit. a DSGVO und Art. 32 Abs. 4 DSGVO ein Verfahren nach dem Ordnungswidrigkeitengesetz eingeleitet.

Fakultative Auftragsverarbeitungsverträge

Ein Hersteller hat den seine Produkte vertreibenden freien Händlerinnen und Händlern eine softwareseitige Unterstützung zur Verarbeitung der Daten von Endkundinnen und -kunden angeboten; im Zusammenhang mit dem angebotenen Kundendatenmanagementtool und der damit verbundenen Verarbeitung der Daten von Endkundinnen und –kunden verfolgte der Hersteller keine eigenen Zwecke und handelte damit nicht als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO, sondern lediglich als Auftragsverarbeiter.

Nach einem Hinweis eines ehemaligen Händlers wurde eine aufsichtsbehördliche Untersuchung eingeleitet und festgestellt, dass die Händlerinnen und Händler von dem Unternehmen zwar wiederholt auf die Möglichkeit des Abschlusses eines Vertrags nach Art. 28 Abs. 3 Satz 1 DSGVO hingewiesen wurden, der Hersteller diesen im Übrigen aber den Abschluss eines solchen Auftragsverarbeitungsvertrags als Wahlmöglichkeit überließ. Der Hersteller war dabei der Ansicht, dass es Sache der Händlerinnen und Händler als Verantwortliche im Sinne des Art. 4 Nr. 7

DSGVO für die Verarbeitung ihrer Kundendaten sei, den Abschluss eines solchen Auftragsverarbeitungsvertrags zu gewährleisten; die Mehrzahl der Händlerinnen und Händler hätten dabei von der Wahlmöglichkeit Gebrauch gemacht und einen Vertrag nach Art. 28 Abs. 3 Satz 1 DSGVO abgeschlossen. Im Fall des hinweisgebenden Händlers existierte indes kein Auftragsverarbeitungsvertrag und die Daten der Endkundinnen und -kunden wurden nach einer einseitigen Beendigung der Vertriebstätigkeit durch den Hersteller durch diesen ohne Weisung des Händlers gelöscht.

Zutreffend war die Auffassung, dass die Händlerinnen und Händler, die sich für den Einsatz des Kundendatenmanagementtools entschieden haben, grundsätzlich als Verantwortliche zu qualifizieren waren, allerdings war auch der Hersteller, der eine solche Verarbeitungsinfrastruktur für die Händlerinnen und Händler anbietet, verpflichtet, eine verordnungsgemäße Datenverarbeitung zu gewährleisten. Durch das festgestellte rein reaktive Verhalten des Herstellers, dem durch die Zurverfügungstellung eines Kundendatenmanagementtools für alle Händlerinnen und Händler gerade eine wesentliche Gestaltungsmacht bei der Institutionalisierung der Zusammenarbeit der beteiligten Akteure zukommt, konnte weder eine zweifelsfreie Zuordnung von Verantwortlichkeiten und Pflichten noch eine streng weisungsgebundene Datenverarbeitung systematisch garantiert werden. Ausschließlich durch eine standardisierte, für alle Händlerinnen und Händler geltende Pflicht zum Abschluss von Auftragsverarbeitungsverträgen – im Sinne einer organisatorischen Maßnahme nach Art. 32 DSGVO – im Zusammenhang mit der Nutzungsvereinbarung des Kundendatenmanagementtools hätte ein solches datenschutzrechtliches Rollenverständnis geschärft und das Risiko einer weisungswidrigen Datenverarbeitung hinreichend reduziert werden können.

Das Unternehmen nahm das Verfahren zum Anlass, die Auftragsverarbeitung nach Art. 28 DSGVO standardmäßig in die Nutzungsvereinbarung mit den Händlerinnen und Händlern aufzunehmen; wegen eines Verstoßes gegen Art. 28 Abs. 3 Satz 1 DSGVO und Art. 32 Abs. 4 DSGVO wurde gegen den Hersteller ein Verfahren nach dem Ordnungswidrigkeitengesetz eingeleitet.

Effektive Wirksamkeitskontrollen

Durch ein ethisch handelndes Hackerkollektiv wurde ein saarländischer Auftragsverarbeiter, welcher bundesweit sektoral verwendete Softwarelösungen anbietet, auf eine Anzahl festgestellter Schwachstellen, die einen Zugriff auf personenbezogene Daten potenziell ermöglicht hatten, aufmerksam gemacht. Das Kollektiv übersandte die an das Unternehmen adressierte Information über die festgestellten Sicherheitslücken dabei auch an die saarländische Datenschutzaufsichtsbehörde und lancierte den Sachverhalt unter Nennung von Namen exponierter Personen, die von den Sicherheitslücke potenziell betroffen waren.

Der Auftragsverarbeiter räumte dabei das Bestehen der festgestellten Sicherheitslücken ein, ergriff umgehend Abhilfemaßnahmen, um diese Sicherheitslücken zu schließen und betonte, dass – mit Ausnahme des Hackerkollektivs – keine Anhaltspunkte für einen nicht autorisierten Datenzugriff bzw. -abfluss festgestellt werden konnte. Im Zuge der aufsichtsbehördlichen Untersuchung war vor allem die Frage zu klären, welche Mechanismen zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung im Sinne des Art. 32 Abs. 1 2. Halbsatz lit. d DSGVO implementiert waren und aus welchem Grund die festgestellten Sicherheitslücken trotz dieser Maßnahmen nicht frühzeitig detektiert und vermieden wurden.

Für Auftragsverarbeiter, deren Geschäftsmodell vorrangig in der Bereitstellung von online abrufbaren Anwendungen besteht (Software-as-a-Service), sind Penetrationstests – simulierte Angriffe auf eine IT-Infrastruktur mit dem Ziel Sicherheitslücken zu detektieren – eine geeignete Maßnahme, um potenzielle Schwachstellen identifizieren zu können. Ein zielführender Mechanismus der Wirksamkeitskontrolle setzt dabei voraus, dass Penetrationstests nicht nur regelmäßig, sondern auch anlassbezogen – bspw. nach einem größeren Update – wiederholt werden.[68]

68) Martini, in Paal/Pauly, 4. Aufl. 2026, VO (EU) 2016/679 Art. 32 Rn. 45, beck-online.

Das Unternehmen konnte zwar Testate und Ergebnisse von in der Vergangenheit durchgeführten Penetrationstest vorlegen, an einer internen Richtlinie, die Zeitabstände und Anlässe zur Durchführung sowie Kriterien zur Vergabe von Penetrationstest systematisch und verbindlich vorgegeben hätte, fehlte es allerdings. Gerade mit Blick auf das Geschäftsmodell des Auftragsverarbeiters und eines damit verbundenen spezifisch erhöhten Risikos, Ziel eines Angriffs zu werden, war die Gewährleistung einer effektiven Wirksamkeitskontrolle als Schutzmaßnahme im Sinne des Art. 32 Abs. 1 2. Halbsatz lit. d DSGVO unabdingbar. Der Auftragsverarbeiter nahm den Vorfall und die sich anschließende Untersuchung zum Anlass, seine Compliance-Vorkehrungen vollständig zu überarbeiten.

Auch wenn durch das Ergebnis einer forensischen Untersuchung glaubhaft gemacht werden konnte, dass eine Datenexfiltration nicht wahrscheinlich war und die Sicherheitslücken umgehend geschlossen wurden, war die unzureichende Operationalisierung von Maßnahmen zur Wirksamkeitskontrolle durch den Auftragsverarbeiter als Verstoß zu qualifizieren. Zum Redaktionsschluss war die Untersuchung noch nicht abgeschlossen und über aufsichtsbehördliche Abhilfebefugnisse noch nicht entschieden.

8.4 Patientendaten im Müll

Das ordnungsgemäße Löschen und Vernichten personenbezogener Daten ist ein wesentlicher Aspekt eines datenschutzkonformen Verarbeitungshandelns. Verantwortliche müssen Informationen nicht nur rechtmäßig erheben und nutzen, sondern auch sicherstellen, dass Daten nicht länger gespeichert werden, als es für die Zwecke erforderlich ist (Grundsatz der Speicherbegrenzung). Sobald der Zweck entfällt und keine gesetzlichen oder sonstigen verpflichtenden Aufbewahrungsfristen mehr entgegenstehen, sind Unterlagen und Datenträger so zu löschen bzw. zu vernichten, dass eine Wiederherstellung praktisch ausgeschlossen ist. Zugleich verlangt die DSGVO angemessene technische und organisatorische Maßnahmen, um personenbezogene Daten vor unbefugtem Zugriff zu schützen (insbesondere Art. 24 und 32 DSGVO). Dies gilt in besonderem Maße für Gesundheitsdaten als besonders schützenswerte Datenkategorie.

Gleichwohl zeigt die Aufsichtspraxis immer wieder, dass gerade bei der Aussonderung und Entsorgung von Unterlagen Fehler passieren – häufig an Schnittstellen: beim Übergang zwischen laufendem Betrieb, Archivierung und endgültiger Vernichtung, aber auch dort, wo Hilfspersonal oder externe Dienstleister eingebunden werden. Solche Versäumnisse wiegen besonders schwer, weil sie regelmäßig die Vertraulichkeit der betroffenen Personen unmittelbar gefährden.

So hatten wir im Berichtszeitraum einen Hinweis auf das unsachgemäße Entsorgen von Patientendaten einer Arztpraxis erhalten. Im Rahmen einer Außenprüfung in einer innerstädtischen Fußgängerzone wurde festgestellt, dass sich tatsächlich zahlreiche medizinische Unterlagen der Arztpraxis obenauf in mehreren gemeinsam genutzten Papiertonnen eines Mehrparteienhauses befanden. Die Tonnen waren nicht verschlossen und die Dokumente, darunter Diagnoseberichte und Laborbefunde, für jedermann frei zugänglich. Zum Schutz der betroffenen Personen wurden die Unterlagen noch vor Ort durch Mitarbeiter unserer Behörde gesichert und in Verwahrung genommen.

Eine derartige Ablage stellt regelmäßig eine Verletzung des Schutzes personenbezogener Daten dar, weil Unbefugte Kenntnis nehmen können. Verantwortliche müssen organisatorisch sicherstellen, dass Unterlagen bis zur Vernichtung geschützt gelagert und die Vernichtung selbst in einem geregelten, nachvollziehbaren Verfahren erfolgt. Auch ein Rekurrieren auf mögliche den Verstoß verursachende Dritte, wie bspw. das Reinigungspersonal, exkulpiert den Verantwortlichen in der Regel nicht, da er seinen Geschäfts- und Praxisbetrieb derart zu organisieren hat, dass nur vertrauenswürdige Personen nach einem vorgegebenen Verfahren mit der Vernichtung/Entsorgung von personenbezogenen Unterlagen/Daten betraut sind.

Aufsichtsrechtlich sind in solchen Fällen grober Verstöße, insbesondere im Bereich sensibler Gesundheitsdaten, regelmäßig sowohl Abhilfemaßnahmen (z. B. Anordnungen zur Einführung sicherer Entsorgungswege,

Schulungen, Nachweispflichten) als auch – je nach Schwere und Umständen des Einzelfalls – ordnungswidrigkeitenrechtliche Schritte zu prüfen.

Zum Schutz der Patientinnen und Patienten und auch im eigenen Interesse sollten Verantwortliche insbesondere:

- ein Lösch- und Vernichtungskonzept mit Zuständigkeiten, Fristen und Abläufen etablieren,
- Unterlagen bis zur Vernichtung in verschlossenen Behältern aufbewahren und den Zugriff strikt beschränken,
- Aktenvernichtung nur mit geeigneten Geräten (z. B. Partikelschnitt) oder durch professionelle Dienstleister durchführen lassen,
- bei externen Dienstleistern eine Auftragsverarbeitung vertraglich absichern und Vernichtungsnachweise verlangen,
- Mitarbeitende regelmäßig unterweisen und die Einhaltung der Verfahren stichprobenartig kontrollieren.

Im zugrundeliegenden Fall wurde das Verfahren an unsere Bußgeldstelle abgegeben.

8.5 Datenintegrationszentrum am UKS

Um medizinische Forschung mit Daten aus der klinischen Versorgung zu ermöglichen, betreibt das Universitätsklinikum des Saarlandes (UKS) in Kooperation mit der Universität des Saarlandes (UdS) ein sog. Datenintegrationszentrum (DIZ) ein. Vergleichbare Strukturen wurden im Zuge der Medizininformatik-Initiative[69] an mehreren Universitätskliniken etabliert; auch im Saarland soll damit ein Rahmen geschaffen werden, der Forschungsvorhaben auf einer belastbaren Datenbasis unterstützt und

69) https://www.medizininformatik-initiative.de/de/start.

zugleich die Rechte der Patientinnen und Patienten wahrt. Um dies zu ermöglichen ist es Aufgabe des Datenintegrationszentrums, Daten aus unterschiedlichen Systemen der Patientenversorgung (typischerweise Krankenhausinformationssysteme, Labor-, Radiologie-, Pathologiesysteme etc.) zusammenzuführen und so zu verarbeiten, dass sie datenschutzgerecht, qualitativ abgesichert und standardisiert für die medizinische Forschung nutzbar werden, so dass auch Erkenntnisse aus der Forschung wieder in die Versorgung zurückfließen können.

Unsere Behörde begleitete das Projekt im Berichtszeitraum eng und stand insbesondere im ersten Halbjahr in kontinuierlichem Austausch mit dem UKS. Im Mittelpunkt der Beratung standen die rechtlichen Anforderungen an die Verarbeitung von Gesundheitsdaten sowie die technische und organisatorische Ausgestaltung des Schutzkonzepts.

Als Rechtsgrundlage der Datenverarbeitung innerhalb des DIZ dient die Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO. Es ist vorgesehen, dass die Patienten bei ambulanter oder stationärer Aufnahme um Einwilligung in eine Weiterverarbeitung ihrer Daten ersucht werden. Die hiernach erhobenen Daten sollen sodann an das DIZ übermittelt und in die dortigen Systeme eingepflegt werden. Für die Wirksamkeit der Einwilligung ist entscheidend, dass sie freiwillig, informiert und eindeutig erteilt wird und jederzeit widerrufen werden kann. Entsprechend war auch zu klären, wie Einwilligungen dokumentiert, Widerrufe umgesetzt und Datenflüsse daran ausgerichtet werden (z. B. Sperr- und Löschprozesse, Nachvollziehbarkeit und Protokollierung).

Wesentliche Voraussetzung der Datenschutzkonformität ist eine konsequente Pseudonymisierung. Pseudonymisierung bedeutet, dass Daten ohne zusätzliche Informationen nicht mehr einer Person zugeordnet werden können und dass diese zusätzlichen Informationen getrennt aufbewahrt und durch technische und organisatorische Maßnahmen geschützt werden. Im DIZ dient das Pseudonym als eindeutige Kennziffer, mit der Behandlungsdaten einer Patientin oder eines Patienten über verschiedene Behandlungsfälle und Dokumentationssysteme hinweg zusammengeführt

werden können, ohne dass Forschende oder die mit der Aufbereitung der medizinischen Daten befassten Stellen die Identität der Patientin oder des Patienten kennen müssen. Vor der Bereitstellung an Forschende durchlaufen diese Daten eine weitere Pseudonymisierung. Im Bereich der eigentlichen Forschungstätigkeit liegt demnach eine zweifache Pseudonymisierung der Daten vor, welche es den Forschungstreibenden unmöglich macht, den Ursprung der Daten zu eruieren, geschweige denn, eine Patientenzuordnung zu treffen.

Verwendung findet das im DIZ erzeugte Pseudonym auch im Rahmen des Betriebs der das Datenintegrationszentrum flankierenden Biobank der medizinischen Fakultät der Universität des Saarlandes. In dieser Einrichtung wird auf Basis von Einwilligungen der jeweiligen Patienten Biomaterial (Blut- und Gewebeproben etc.) zu Zwecken medizinischer Forschung vorgehalten. Die Biobank speist sich dabei aus Material, welches ihr von den Kliniken des UKS zugesendet wird. Im Rahmen der Übersendung an die Biobank wurde das entnommene Biomaterial bis dato unter Aufdruck des im DIZ hinterlegten Pseudonyms des Patienten etikettiert und in der Biobank sodann unter diesem Pseudonym geführt.

Hier sahen wir für das Datenintegrationszentrum insgesamt die Funktion des Pseudonyms, eine unmittelbare Personen-/Patientenzuordnung zu erschweren, gefährdet. Das DIZ-Pseudonym soll im Sinne der oben beschriebenen Trennung gerade dazu beitragen, dass medizinische Daten nur unter einer Kennung verarbeitet werden und die Identitätsinformationen hiervon getrennt bleibt. Wird dasselbe DIZ-Pseudonym jedoch im Moment der Probenentnahme offen mit der identifizierten Person „zusammengebracht" (weil Mitarbeitende beim Etikettieren Patient und Pseudonym zugleich kennen), entsteht eine Zuordnungsinformation außerhalb der im DIZ vorgesehenen Abschottung. Damit bestand das Risiko, dass die im DIZ angelegten technischen und organisatorischen Schutzmaßnahmen zur Trennung von Identität und medizinischen Daten faktisch unterlaufen werden.

Um diese Schwachstelle des Pseudonymisierungsverfahrens zu schließen, wurde auf unsere Anregung ein angepasstes Etikettierungs- und Übersendungsverfahren eingeführt. Auf die Etiketten werden nun zufallsgenerierte, temporäre Kennungen gedruckt. Das eigentliche Pseudonym wird zwar weiterhin übermittelt, jedoch nicht mehr offen, sondern in verschlüsselter Form auf dem Etikett angebracht und erst in der Biobank entschlüsselt. Mitarbeitenden des UKS ist es damit nicht mehr möglich, das im DIZ und in der Biobank verwendete Pseudonym einer Patientin oder einem Patienten zuzuordnen. Zugleich bleibt die notwendige interne Zuordenbarkeit innerhalb der beteiligten IT-Systeme für zulässige, einwilligungsbasierte Forschungsprozesse erhalten.

So konnten wir zu einer datenschutzkonformen Lösung im Rahmen unserer Beratungstätigkeit für das UKS beitragen.

UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Fritz-Dobisch-Str. 12 • 66111 Saarbrücken
Postfach 10 26 31 • 66026 Saarbrücken

Telefon 0681 94781 – 0
Telefax 0681 94781 – 29

E-Mail poststelle@datenschutz.saarland.de

www.datenschutz.saarland.de
www.informationsfreiheit.saarland.de