# 32. Tätigkeitsbericht

## der Landesbeauftragten für Datenschutz und Informationsfreiheit

## Berichtszeitraum: 2023

Dem Landtag und der Landesregierung
vorgelegt am 24. April 2024
(Landtagsdrucksache 17/811)

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

# Vorwort

Das zurückliegende Berichtsjahr 2023 hat erneut die europäische Dimension des Datenschutz- und Digitalrechts verdeutlicht. Zahlreiche Rechtsakte der EU wurden als Reaktion auf technische Entwicklungen und Begehrlichkeiten im Bereich datengetriebener transnationaler Geschäftsmodelle bereits verabschiedet oder befinden sich auf der Zielgeraden; sie alle werden mitunter weitreichende Auswirkungen auf unseren digitalen Alltag haben. Wenngleich die im Rahmen der EU-Digitalstrategie ergangenen Rechtsetzungsakte die DSGVO unberührt lassen, stehen die Regelungskomplexe nicht isoliert nebeneinander, sondern es ergeben sich vielmehr vielschichtige Wechselwirkungen und damit auch erhebliche Auswirkungen auf die Beratungs- und Vollzugspraxis aller europäischen Datenschutzaufsichtsbehörden.

Besonders deutlich wird dies bei dem Thema Künstliche Intelligenz (KI); obwohl KI bereits seit Jahren Einzug in unseren Alltag hält, tritt ihr eigentliches transformatives Potenzial vor allem in jüngster Vergangenheit verstärkt in Erscheinung. Trotz aller derzeit noch bestehenden Unzulänglichkeiten und Grenzen lassen sich den großen Sprachmodellen, wie GPT, Llama, PaLM oder Gemini, nachhaltige Auswirkungen auf das Mensch-Maschine-Verhältnis und – mit Blick auf die Vielgestaltigkeit der Einsatzszenarien – disruptive Effekte auf nahezu alle Lebensbereiche ableiten. Solche Anwendungen werden zu einem großen Teil mit personenbezogenen Daten trainiert und führen dadurch auch zu neuen Risiken und Gefahren für die Grundrechte Betroffener. Wenn auch Kompetenz- und Verfahrensfragen zur Umsetzung der KI-Verordnung noch gesetzlich zu regeln sein werden, ergeben sich jetzt schon umfangreiche datenschutzrechtliche Fragestellungen von Bürgerinnen und Bürgern, Unternehmen und öffentlichen Stellen, die auch durch die Datenschutzaufsichtsbehörden zu beantworten sind.

Während der europäische Gesetzgeber den regulatorischen Rahmen für den Umgang mit Daten weiter verdichtet, hat der Europäische Gerichtshof (EuGH) im zurückliegenden Berichtszeitraum mit einer Reihe von Grundsatzentscheidungen nicht nur wesentliche Aussagen zur Auslegung der DSGVO, sondern auch zur Vereinbarkeit des nationalen Rechts mit dem Unionsrecht getroffen. Diese Entscheidungen führten neben Klarstellungen zu zentralen Fragen, wie dem Auskunftsrecht betroffener Personen oder der Verhängung von Geldbußen unmittelbar gegenüber juristischen Personen, auch zu einer Klärung hinsichtlich des Umfangs der gerichtlichen Kontrolle in Bezug auf Entscheidungen der Aufsichtsbehörden. Ebenso wie der Bundesgesetzgeber mit Blick auf die neuere Rechtsprechung des EuGH notwendige Anpassungen im Bundesdatenschutzgesetz vornehmen wird, wird auch für das Saarländische Datenschutzgesetz eine Revision im Lichte der Rechtsprechung des Gerichtshofs erfolgen müssen.

Anpassungen angesichts veränderter Anforderungen und Rahmenbedingungen sind im Berichtsjahr auch innerhalb unserer Dienststelle erforderlich geworden. Um die Behörden auf Landes- und auf Kommunalebene bei der Bewältigung der komplexen Aufgabe der Verwaltungsdigitalisierung fundiert beraten sowie Lösungen für die aktuellen datenschutzrechtlichen und technischen Herausforderungen bei der anspruchsvollen Aufgabe der Verwaltungsdigitalisierung anbieten zu können, haben wir unter interner Umstrukturierung einen Schwerpunkt auf diesen Aufgabenbereich gelegt.

Zudem ist es uns unter Nutzung freier Stellenanteile gelungen, den Bereich der Bearbeitung von Bußgeldverfahren personell zu verstärken. Zwar liegt der Fokus der Aufsichtstätigkeit nach wie vor auf unterstützender Zusammenarbeit, allerdings ist den datenschutzrechtlichen Vorgaben im Einzelfall auch durch das Ergreifen von Sanktionsmaßnahmen Geltung zu verschaffen. So war auch im Berichtsjahr eine Zunahme der Anzahl und des Umfangs der ausgesprochenen Geldbußen zu verzeichnen.

Da es in dem hochdynamischen Gefüge aus sich stetig wandelnden regulatorischen und technischen Rahmenbedingungen zunehmend herausfordernder wird, Schritt zu halten, danke ich ganz besonders meinen zwanzig Mitarbeiterinnen und Mitarbeitern, die trotz ihrer vielgestaltigen Aufgaben stets den Überblick behalten und mit großem Engagement die Fortentwicklung des Datenschutzrechts gestaltend begleiten.

Saarbrücken, im April 2024

Monika Grethel

*Landesbeauftragte für Datenschutz*
*und Informationsfreiheit*

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# I.

# 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 und die Parlamente über aktuelle Entwicklungen im Datenschutzrecht dar. Um einen ersten und allgemeinen Überblick über die Anzahl der Sachverhalte zu geben, mit denen sich die deutschen Aufsichtsbehörden im Berichtszeitraum befasst haben und um die Transparenz und Vergleichbarkeit der Tätigkeit der Aufsichtsbehörden zu erhöhen, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) gemeinsame Kriterien zur statistischen Darstellung von Tätigkeitsschwerpunkten aufgestellt, welche im Folgenden dargestellt werden.

## 1.1 Beschwerden

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

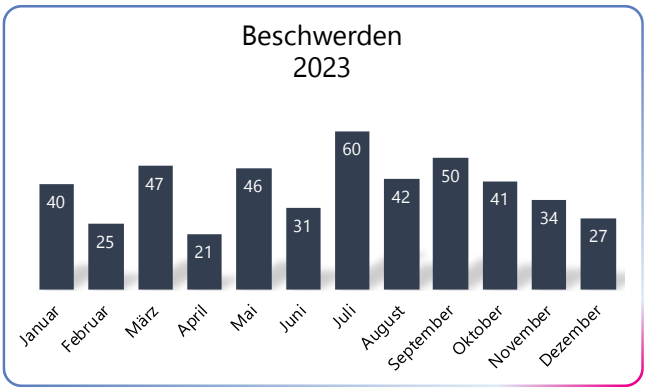


Abb. 1: Beschwerden (gesamt) 2023

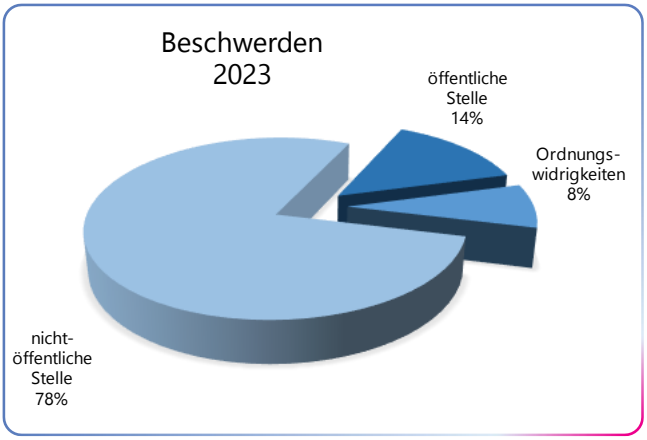


Abb. 2: Beschwerden (Aufteilung) 2023

## 1.2 Beratungen

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

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

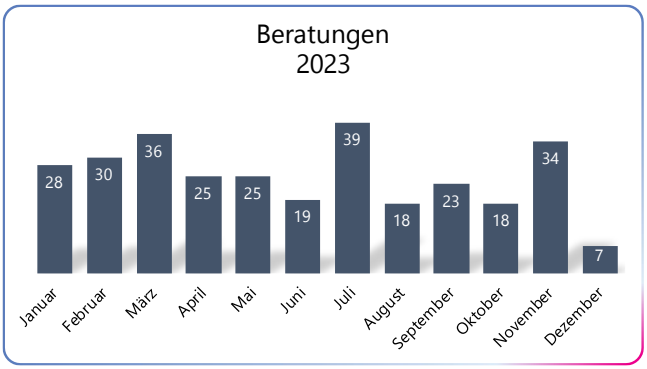


Abb. 3: Beratungen (gesamt) 2023

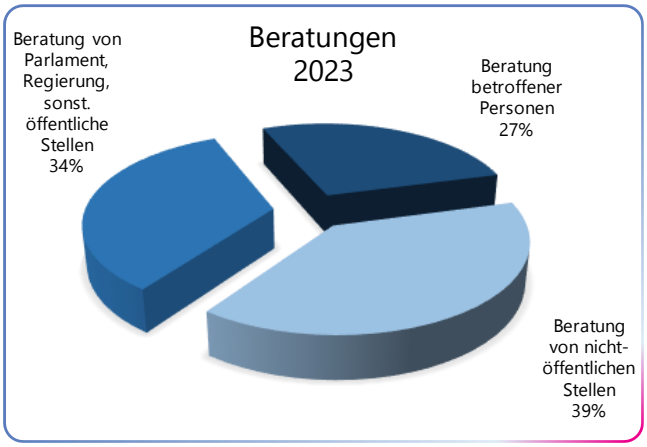


Abb. 4: Beratungen (Aufteilung) 2023

## 1.3 Meldungen von Datenschutzverletzungen

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

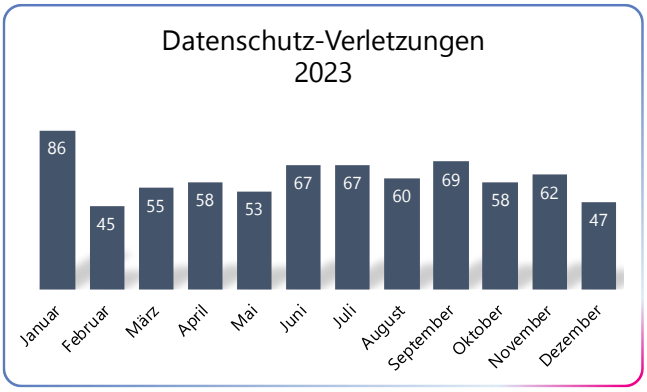


Abb. 5: Datenschutzverletzungen 2023

## 1.4 Abhilfemaßnahmen

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

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

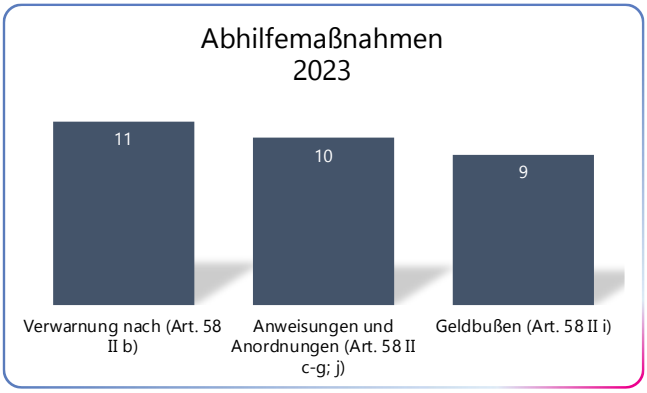


Abb. 6: Abhilfemaßnahmen (gesamt) 2023

## 1.5 Europäische Verfahren

Einen zunehmenden 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 die-

ser Mehraufwand wiederum durch den für alle Seiten gewinnbringenden europäischen Austausch gerechtfertigt.

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

| | Bundesrepublik Deutschland | Saarland |
|---|---|---|
| Verfahren mit Betroffenheit Art. 56 Abs. 1 | 418 | 1 |
| Verfahren mit Federführung Art. 56 Abs. 2 | 51 | 0 |
| Verfahren gem. Kapitel VII DSGVO | 2540 | 1367 |

Abb. 7: Europäische Verfahren (gesamt) 2023

Zu diesem Zweck hatte auch das UDZ im Jahr 2023 in insgesamt 418 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 beispielweise eine Niederlassung der verarbeitenden Stelle im Saarland existiert oder weil auch saarländische Bürger von einer konkreten Verarbeitung erheblich betroffen sein könnten.

In einem Fall wurde diese Betroffenheit für das UDZ bejaht.

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

Darüber hinaus wurden mehrere freiwillige Amtshilfeersuchen europäischer Aufsichtsbehörden an das UDZ gerichtet, im Rahmen derer ein allgemeiner Austausch über diverse datenschutzrechtliche Fragestellungen erfolgte.

## 1.6 Förmliche Begleitung von Rechtsetzungsvorhaben

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

Im Berichtzeitraum wurde das UDZ hiernach in 11 Rechtsetzungsvorhaben verfahrensbegleitend tätig.

## 1.7 Gerichts- und gerichtliche Bußgeldverfahren

In 2023 wurden gegen durch das UDZ verhängte Abhilfemaßnahmen gemäß Art. 58 Abs. 2 DSGVO insgesamt 8 Gerichts- und gerichtliche Bußgeldverfahren geführt.

## 1.8 Presseanfragen

In 2023 wurden insgesamt 32 Presseanfragen an hiesige Dienststelle gerichtet.

# II.

# Rückblick – Entwicklungen seit dem 31. Tätigkeitsbericht 2022

# 2 Rückblick – Entwicklungen seit dem 31. Tätigkeitsbericht 2022

Im 31. Tätigkeitsbericht für das Berichtsjahr 2022 wurde im Kontext des Datenschutzes im öffentlichen Bereich über mehrere Prüfungen und Verfahren berichtet, die zum Zeitpunkt des Redaktionsschlusses noch nicht vollständig beendet waren. Über deren Ausgang bzw. zu deren derzeitigem Verfahrensstand soll an dieser Stelle informiert werden.

## 2.1 Prüfung der Videoüberwachungsanlage Johanneskirche

Über die Prüfung der polizeilichen Videoüberwachungsanlage am Standort Johanneskirche wurde im vergangenen Tätigkeitsbericht unter Punkt 3.1 berichtet. Zum Zeitpunkt des Redaktionsschlusses stand eine ausführliche Stellungnahme des Landespolizeipräsidiums noch aus. Zwischenzeitlich erhielt das UDZ eine entsprechende Rückmeldung, in der weitgehende Anpassungen der polizeilichen Maßnahme zugesichert wurden. Nicht nur fand eine Überarbeitung und Ausweitung der vorhandenen Privatzonenmaskierung statt, auch die Transparenzkennzeichnung vor Ort wurde durch weitere Hinweisschilder ausgebaut. Zudem fand eine Aktualisierung der im Internet verfügbaren Transparenz- und Datenschutzinformationen („Polizeilicher Videoschutz in Saarbrücken“) statt.

In einzelnen Punkten der technischen und organisatorischen Abläufe konnten wir bislang jedoch keine Anpassung bewirken. So divergieren die Auffassungen noch zu bestimmten Aufbewahrungsfristen von Sicherheitskopien und zur Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung (abseits einer vorhandenen Errichtungsanordnung) für die Videoüberwachungsanlage. Diesbezüglich haben wir nochmals auf die Stellungnahme des LPP reagiert. Wir gehen davon aus, dass auch diese Punkte noch geklärt werden können.

## 2.2 Kontrolle des Schengener Informationssystems

Die Kontrolle des Schengener Informationssystems der zweiten Generation (SIS II) war Gegenstand des vergangenen Tätigkeitsberichts unter Punkt 3.2. Auch hier stand zum Zeitpunkt des Redaktionsschlusses eine ausführliche Stellungnahme des Landespolizeipräsidiums noch aus. Zwischenzeitlich informierte das LPP über eingehende Prozessanpassungen bei den relevanten Fahndungsausschreibungen zur polizeilichen Beobachtung. Hierzu gehörten Sensibilisierungen der Polizeibediensteten zu den erforderlichen Ausschreibungsvoraussetzungen, eine strengere Beachtung von Aussonderungsprüf- und Löschfristen sowie eine Verbesserung der Begründungs- und Dokumentationsweisen.

Da es sich bei der Kontrolle des SIS II um eine mit diversen anderen Aufsichtsbehörden (auf Bundes- und Landesebene) koordinierte Prüfung gehandelt hatte, wurde im Juli 2023 nochmals eine kurze Zusammenfassung der gesamtdeutschen Ergebnisse an das LPP übermittelt.

Das bereits seit einiger Zeit in Aufbau befindliche erweiterte Schengener Informationssystem der dritten Generation (SIS 3.0) nahm zwischenzeitlich – am 07.03.2023 – seinen Wirkbetrieb auf. Das UDZ wird die diesbezüglichen Datenverarbeitungen weiter im Blick behalten. Insbesondere, da mit dem neuen Rechtsrahmen erhebliche Änderungen einhergehen – etwa die Schaffung von Möglichkeiten biometrischer Recherche und automatisierten Fingerabdruckabgleichs.

## 2.3 Beendigung des Projekts „PoC - Datenkonsolidierung“

Bereits seit mehreren Jahren begleitete das UDZ den „Proof of Concept (PoC) – Datenkonsolidierung“, eine in Kooperation der Landeskriminalämter der Länder Nordrhein-Westfalen und Rheinland-Pfalz sowie des Landespolizeipräsidiums Saarland durchgeführte Machbarkeitsstudie. Die Aufsichtsbehörden der

verantwortlichen Länder sprachen im Jahr 2022 eine koordinierte Warnung aus (siehe 31. Tätigkeitsbericht, Punkt 5.1). Erhebliches Gewicht erlangte auch ein seitens des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Auftrag gegebenes und zwischenzeitlich veröffentlichtes Gutachten, das ebenfalls Bedenken an der Umsetzbarkeit eines solchen Projekts aufwarf.[1]

Mittlerweile wurde uns insbesondere durch andere Projektteilnehmer mitgeteilt, dass die Projektentwicklung zum „PoC – Datenkonsolidierung" eingestellt wurde. Eine Weiterführung des Vorhabens sei nicht avisiert und die diesbezüglich vorgesehenen Ressourcen seien anderweitig verteilt worden. Ein Projektabschlussbericht werde jedoch noch verfasst.

Aufgrund der in unserer Warnung ausgesprochenen Bedenken begrüßen wir diese Entscheidung der Projektverantwortlichen. Dennoch ist vor dem Hintergrund des Gesamtprojekts P 20 (früher: Polizei 20/20) davon auszugehen, dass die kritischen Fragestellungen in mehreren anderen Konstellationen erneut Relevanz erlangen werden.

## 2.4 Antrag „kleiner Waffenschein"

Im 31. Tätigkeitsbericht berichteten wir unter Punkt 4.2 außerdem über die durch uns begleitete Umgestaltung des Antragsformulars für den „kleinen Waffenschein". Während die Antragsformulare einvernehmlich und abschließend überarbeitet werden konnten, ergaben sich weitere Detailfragen hinsichtlich der ebenfalls zu aktualisierenden Datenschutzerklärungen. Dies führte dazu, dass sich das Verfahren trotz der bereits im letzten Jahr in Aussicht gestellten, baldigen Umsetzung auf unbestimmte Zeit verzögerte.

[1] Rechtsgutachten von Prof. Dr. Matthias Bäcker, LL.M., Universität Mainz: Polizeirechtlicher und verfassungsrechtlicher Rahmen eines polizeilichen Informationsverbunds der Länder, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2023/Gutachten-polizeilicher-Informationsverbund.html (letzter Abruf: 11.12.2023).

Kernpunkt dieser neuen Fragestellung waren und sind die Aufbewahrungs- und Speicherfristen im Kontext waffenrechtlicher Aktenführung, die in den relevanten Vorschriften des Waffengesetzes (WaffG) nur in sehr geringem Umfang gesetzlich vorgeschrieben sind.

Wir stehen diesbezüglich mit der Abteilung für Waffenrecht beim Ministerium für Inneres, Bauen und Sport (MIBS) in Kontakt und erhoffen uns eine baldige Klärung der offenen Problemstellungen. Dies insbesondere auch, da im Zuge des Online-Zugangsgesetzes (OZG) bei einzelnen Behörden zwischenzeitlich auch eine Beantragung waffenrechtlicher Erlaubnisse auf elektronischem Wege möglich ist und zunehmende Digitalisierungsbemühungen (etwa von analoger zu digitaler Aktenführung) das Aufkommen weiterer datenschutzrechtlicher Fragestellungen wahrscheinlich machen.

## 2.5 Einführung der Online-Zeugenvernehmung

Im vergangenen Tätigkeitsbericht (Punkt 4.5) berichteten wir über das Vorhaben des Landesverwaltungsamts (LaVA), die bestehende Möglichkeit der Online-Anhörung von Betroffenen einer Verkehrsordnungswidrigkeit künftig auch auf eine Online-Vernehmung von Zeugen auszuweiten, und schilderten die in diesem Kontext gesehenen Bedenken des UDZ mit Blick auf Gewährleistung von Authentizität sowie Integrität der so erlangten Daten.

Im Frühjahr 2023 erörterten wir die Thematik mit Vertretern des LaVA. Eine Verständigung auf die vom UDZ konkret vorgeschlagenen Identifikationsmethoden konnte derweil nicht erzielt werden, da unsere geäußerten Bedenken überwiegend nicht geteilt wurden und man die Implementierung der eID-Authentifikation im Massenverfahren als nicht praxistauglich bewertete. Dennoch wurde nach Rücksprache mit dem Anbieter des Fachverfahrens versichert, neben der einfachen Anmeldung des Bürgers via in gleichem Schreiben übersandter Kennung und Passwort auch bis Ende 2023 die Möglichkeit zu

schaffen, zusätzlich über einen Button optional die Daten der AusweisAPP auslesen und die abgegebene Erklärung damit authentifizieren zu lassen.

Dem UDZ wurde zudem zugesichert, dass bei breiter Akzeptanz der eID-Funktion künftig auf eine reine Authentifizierung mittels elektronischem Personalausweis umgestiegen werden könne. Wir wiesen zudem nochmals darauf hin, dass dem Bürger bei der Wahl der Anmeldemethode größtmögliche Transparenz zuteil werden und er deswegen im Vorfeld der Entscheidung zur Art der Authentifizierung über die verschiedenen Möglichkeiten informiert werden muss. Auch hat aus Sicht des UDZ im Backend eine Kennzeichnung des Datensatzes zu erfolgen, ob dieser nach sicherer Authentifizierung mittels ePA erfasst wurde oder die Eingabe ohne diesen Faktor erfolgte.

Vor dem Hintergrund der ausführlichen Gespräche sahen wir damit unsere Beratungsfunktion als erfüllt und weitergehende aufsichtsbehördliche Maßnahmen trotz offener Kritikpunkte als nicht erforderlich an. Nach hiesigem Kenntnisstand befindet sich die Online-Zeugenvernehmung zwischenzeitlich im Wirkbetrieb.

# III.

# Digitalisierung der Verwaltung

# 3 Digitalisierung der Verwaltung

Unsere Behörde leistet einen wichtigen Beitrag bei der Beratung der saarländischen Landesbehörden und Kommunen in Bezug auf die Berücksichtigung datenschutzrechtlicher Aspekte bei Digitalisierungsvorhaben. Die Bedeutung des Datenschutzes für das Vertrauen der Bürger in die Digitalisierung kann nicht genug betont werden. Angesichts dieser Tatsache haben wir einen unserer aufsichtsbehördlichen Schwerpunkte auf die Durchführung dieser Beratungsfunktion verlagert und priorisieren entsprechende Verfahren. Unser Ziel ist es, durch fundierte Expertise und Beratung einen wesentlichen Beitrag zur Gewährleistung eines hohen Datenschutzniveaus in sämtlichen Digitalisierungsprojekten der saarländischen Verwaltung zu leisten.

## 3.1 Beratung der Landesregierung zum Einsatz von Microsoft 365

Zu Beginn des Jahres 2023 ist eine oberste Landesbehörde an uns herangetreten, da eine neue Videokonferenzlösung beschafft werden sollte. Der Vertrag über das bisher zum Einsatz kommende Produkt sollte nicht verlängert werden. Als Wunschlösung wurde der Einsatz von MS Teams anvisiert.

Es war bekannt, dass sich die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bereits seit langem sehr intensiv mit der Möglichkeit einer datenschutzkonformen Nutzung von Microsoft 365 (MS 365) und damit auch von MS Teams als einem der in MS 365 enthaltenen Dienste durch öffentliche Stellen beschäftigte. Da die Bearbeitung der durch die DSK aufgeworfenen Fragen ein vertieftes Verständnis der zugrundeliegenden datenschutzrechtlichen Problemstellungen erfordert, wurde unsere Behörde gebeten, die vertraglichen Verhandlungen mit Microsoft in Bezug auf die Aspekte des Datenschutzes beratend zu begleiten. Dieser Bitte sind wir gerne nachgekommen.

Seit März 2023 fanden daher in regelmäßigen Abständen Termine zwischen der Landesbehörde und unserer Behörde unter Einbeziehung von Microsoft statt, um die bestehenden rechtlichen Hindernisse eingehend zu erörtern und Lösungsansätze zu erarbeiten. Ausgangspunkt der Besprechungen war dabei die Stellungnahme der DSK zum Einsatz von Teams im öffentlichen Bereich aus November 2022.[2]

Zum Zeitpunkt der Erstellung dieses Tätigkeitsberichtes befand sich unsere Behörde noch immer im Abstimmungsprozess mit der Landesbehörde, weshalb an dieser Stelle eine Darstellung des vorläufigen Zwischenergebnisses erfolgt.

Schwerpunkt der Beratungen waren die vertraglichen Bedingungen, die Microsoft im sog. Data Protection Addendum (DPA) zum Umgang mit personenbezogenen Daten im Zusammenhang mit der Erbringung seiner Online-Dienste vereinbart. Die DSK hat in ihrer Stellungnahme insgesamt sieben Themenkomplexe, welche vereinzelt wiederum in Teilbereiche untergliedert sind, untersucht und datenschutzrechtlich bewertet:

1. Festlegung von Art und Zweck der Verarbeitung, Art der personenbezogenen Daten
2. Eigene Verantwortlichkeit Microsofts
3. Weisungsbindung, Offenlegung verarbeiteter Daten, Erfüllung rechtlicher Verpflichtungen, CLOUD Act, FISA 702
4. Umsetzung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO
5. Löschung und Rückgabe personenbezogener Daten
6. Information über Unterauftragsverarbeiter
7. Datenübermittlungen in Drittstaaten

[2] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf.

Anhand dieser Aufstellung wurden während der Beratungsgespräche die Regelungen des Data Protection Addendum (DPA) erörtert, notwendige Änderungsbedarfe identifiziert und Anpassungsvorschläge diskutiert.

In einigen Punkten ist es gelungen, gemeinsam mit allen Beteiligten Änderungen am DPA herbeizuführen, die die Kritikpunkte der DSK adressieren. So wurden etwa Änderungen bei den Daten- und Personenkategorien vorgenommen oder auch Klarstellungen über bestimmte Arten der Verarbeitung im DPA aufgenommen. Zudem hat sich Microsoft in diversen Punkten dazu bereiterklärt, dem Verantwortlichen weitere Dokumente und Informationen zu überlassen, um seinen Verpflichtungen aus der DSGVO nachkommen zu können.

### Drittstaatentransfer

Bezüglich der Übermittlung von Daten in Drittstaaten gab es noch während unserer Verhandlungen eine Veränderung der Rechtslage. Zu Beginn der Gespräche mit Microsoft war Grundlage für den Transfer von Daten in ein Drittland, wie schon zum Zeitpunkt des Abschlussberichtes der DSK, die Einbindung von Standardvertragsklauseln. Entsprechend beschränkte sich die Bewertung der DSK auf eine Möglichkeit des Datentransfers unter Berücksichtigung der Standardvertragsklauseln, die Microsoft Irland mit der Microsoft Corporation abgeschlossen hatte (sog. SCC Processor-to-Processor; „Modul 3“[3]).

Seitdem die Europäische Kommission am 10. Juli 2023 den Angemessenheitsbeschluss für den Datenschutzrahmen EU-USA (EU-U.S. Data Privacy Framework – EU-U.S. DPF) angenommen hat, steht wieder eine datenschutzrechtliche Grundlage entsprechend Art. 45 DSGVO für den Datentransfer zu Unternehmen in den USA zur Verfügung. Microsoft sichert im DPA zu, entsprechend dem EU-U.S. DPF zertifiziert zu sein, womit ein Teil der Problematik des Datentransfers (vorläufig)

[3] Abrufbar unter: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

aufgelöst werden konnte. Am 11. Januar 2024 gab Microsoft zudem bekannt, sein im Rahmen der Aussetzung des Privacy Shield etabliertes Konzept der EU-Datengrenzen nun auf alle Daten in der Microsoft Cloud auszuweiten. So sollen perspektivisch alle personenbezogenen Daten von EU-Bürgern aus Azure, Microsoft 365, Power Platform und Dynamics 365 die EU nicht mehr verlassen[4].

Die Problematik des Drittlandtransfers wurde mit Blick auf den Angemessenheitsbeschluss mithin vorläufig für erledigt erklärt. Die Erweiterung der EU-Datengrenze wird von uns ebenfalls begrüßt.

### Offenlegungsersuchen

Keine Einigung konnte bislang indes bezüglich der Offenlegungsbefugnisse (z.B. Cloud Act) erzielt werden. Hier wurde seitens Microsoft vorgetragen, dass die von der DSK aufgeworfenen Fragen mit dem EU-U.S. DPF erledigt seien. Diesen Ausführungen konnten wir nicht folgen und mit der EU-Datengrenze („EU Data Boundary“[5]) gewinnt diese Problematik an neuer Bedeutung. Anders als bisher verarbeitet Microsoft im Rahmen der EU-Datengrenze personenbezogene Daten des Kunden vorwiegend im EWR und nicht mehr in den USA. Soweit sich eine Anfrage einer US-Behörde auf in Europa verarbeitete Daten bezieht, kann das EU-U.S. DPF keine Anwendung finden, da keine grenzüberschreitende Verarbeitung vorliegt. Denn die im EU-U.S. DPF vorgesehenen Garantien in Bezug auf den Zugang von US-Behörden gelten nur, soweit die Daten zuvor innerhalb des EU-US-Datenschutzrahmens in die USA übermittelt wurden[6].

---

[4] Inwiefern dies tatsächlich alle Online-Dienste betreffen wird, ist zweifelhaft; derzeit jedenfalls sind die Ausnahmen von der EU-Datengrenze noch vielfältig.

[5] Abrufbar unter: https://blogs.microsoft.com/eupolicy/2022/12/15/eu-data-boundary-cloud-rollout/?culture=de-de&country=de.

[6] Abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/ip_23_3721. Siehe auch Beschluss der Kommission EU 2023/1795, Gliederungspunkt 2.2.6.

Bei Anfragen von US-Behörden auf Zugang zu in Europa verarbeiteten Daten wird es erst im Zeitpunkt der Herausgabe durch Microsoft Irland an die Drittstaatsbehörde zu einer Drittstaatsproblematik bzw. einem Drittstaatstransfer, der dann an den allgemeinen Regelungen des Kapitels V der DSGVO und dort insbesondere an Art. 48 DSGVO zu messen ist.

### Löschfristen

Ebenfalls noch keine Einigung erzielten wir bezüglich der Löschfristen. Zunächst hatte Microsoft in Aussicht gestellt, dass sie eine neue Formulierung insbesondere für den bisher strittigen Abschnitt „es sei denn, Microsoft ist durch dieses DPA zur Aufbewahrung autorisiert" wählt. Allerdings entsprach auch die vorgeschlagene Formulierung nicht den Vorgaben der DSGVO. Microsoft erläuterte diesbezüglich, dass man davon ausgehe, im Zweifel auch den Aufforderungen von U.S.- Recht zu unterliegen und daher hier keine Einschränkung auf den Wortlaut der DSGVO vornehmen könne. Von unserer Seite wurde klargestellt, dass eine Verlängerung der Löschfristen aufgrund gesetzlicher Verpflichtungen, die nicht aus europäischem Recht resultieren, gegen die DSGVO verstößt. Insofern geht es auch hier um das Spannungsverhältnis zwischen EU-Recht und US-amerikanischem Recht.

Als Ergebnis kann festgehalten werden, dass der bekanntermaßen steinige Weg zu einem datenschutzkonformen Einsatz von MS Teams auch in Zukunft noch einige Herausforderungen mit sich bringen wird. Wir konnten in den Gesprächen mit den Beteiligten einige Änderungen im DPA anregen und umsetzen. Auf diese Weise wurden mehrere Kritikpunkte umfassend behandelt und möglichst den Anforderungen der DSGVO angenähert. Allerdings lassen sich auch unter Berücksichtigung der erzielten Änderungen und der Garantien, die das EU-U.S. DPF mit sich bringt, noch immer nicht alle Widersprüche zwischen dem Recht der USA und der DSGVO, insbesondere im öffentlichen Bereich, aus dem Weg räumen.

Unabhängig davon sind die Stellen, die nunmehr beabsichtigen MS 365 in ihrer Behörde einzusetzen, als Verantwortliche für die Datenverarbeitung verpflichtet, die Risiken, die mit der Verarbeitung einhergehen, im Rahmen einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO zu adressieren. Auf Grundlage dieser Risikoermittlung müssen, ergänzend zu den bereits erwirkten Änderungen im DPA, angemessene technische und organisatorische Maßnahmen umgesetzt werden.

Auch weiterhin werden wir die Landesregierung beratend bei der Einführung von MS Teams und dem fortlaufenden Anpassungsprozess der vorgelegten Rahmen-Datenschutz-Folgenabschätzung unterstützen. Um die bisher positiven Bestrebungen der Landesregierung zu einem Abschluss zu bringen, wird auch weiterhin eine umfassende Mitwirkung von Microsoft erforderlich sein.

## 3.2 Studierenden-Energiepreispauschalengesetz

Um die finanziellen Auswirkungen der stark gestiegenen Energiekosten für die Bürgerinnen und Bürger abzumildern, hatte die Bundesregierung im Jahr 2022 mit drei Entlastungspaketen umfangreiche Maßnahmen zur Entlastung und sozialen Unterstützung auf den Weg gebracht.

Auf Grund eines Beschlusses des Koalitionsausschusses vom 3. September 2022 sollten auch „alle Studentinnen und Studenten sowie Fachschülerinnen und Fachschüler" eine Einmalzahlung in Höhe von 200 Euro erhalten, um auch sie von den gestiegenen Energiekosten zu entlasten.

Ein entsprechendes Gesetz zur Zahlung einer einmaligen Energiepreispauschale für Studierende, Fachschülerinnen und Fachschüler sowie Berufsfachschülerinnen und Berufsfachschüler in Bildungsgängen mit dem Ziel eines mindestens zweijährigen berufsqualifizierenden Abschlusses (Studierenden-Energiepreispauschalengesetz – EPPSG) trat zum 21.12.2022 in Kraft. Dieses sah im Ergebnis vor, dass insgesamt rund 2,95 Millionen Studierende und etwa 450.000 Fachschülerinnen und Fachschüler,

die am 1. Dezember 2022 an einer in Deutschland gelegenen Ausbildungsstätte immatrikuliert waren, anspruchsberechtigt waren. Der Vollzug des EPPSG sollte den Ländern obliegen. Die Beantragung und Zahlbarmachung der Einmalzahlung sollte über eine zentral betriebene digitale Plattform erfolgen, die Bund und Länder noch erarbeiten mussten.

Zum Jahreswechsel 2022/2023 wurden wir durch das saarländische Ministerium für Finanzen und Wissenschaft erstmalig mit der Bitte um datenschutzrechtliche Beratung kontaktiert. Ein Schwerpunkt unserer Beratung war dabei die Art und Weise der Bereitstellung der Daten aller im Saarland immatrikulierten Studierenden und Fachschülerinnen und Fachschüler. Die zum damaligen Zeitpunkt von einer Bund-/Länderarbeitsgruppe erarbeiteten Konzepte sahen vor, dass jede Ausbildungsstätte, die bei ihr vorhandenen, für die Anspruchsberechtigung relevanten Daten [Namen, Geburtsdaten, Adressinformationen, sonstige Kontaktdaten (E-Mail, Telefon), Matrikelnummer] an die zentral betriebene Antragsplattform übermitteln sollte, damit dort dann im Zeitpunkt der Antragstellung eine automatisierte Prüfung der Berechtigung erfolgen könne.

Das Ministerium für Finanzen und Wissenschaft hatte Zweifel daran, dass eine solche Übermittlung der Daten aller Anspruchsberechtigten datenschutzrechtlich zulässig sei. Diese Zweifel wurden von uns geteilt.

Vor der Beantragung der Energiepreispauschale sollten nach dem ursprünglichen Konzept personenbezogene Daten aller Anspruchsberechtigten an den Betreiber der zentralen Antragsplattform übermittelt werden, unabhängig davon, ob ein konkreter Antrag auf Zahlung bereits vorlag. Eine geplante Verschlüsselung sollte lediglich den Transportweg der Daten absichern. Trotz dieser Maßnahme erhielt der Betreiber der Antragsplattform bereits zu einem Zeitpunkt Kenntnis von den personenbezogenen Daten aller Anspruchsberechtigten, zu dem noch kein Antrag auf Auszahlung des Unterstützungsbetrags gestellt worden war.

Aus datenschutzrechtlicher Perspektive stellt die Bereitstellung der Liste mit personenbezogenen Daten für den späteren elektronischen Antragsprozess bereits eine rechtfertigungsbedürftige Übermittlung personenbezogener Daten dar. Eine solche Übermittlung erfordert eine gesetzliche Grundlage, die die Art und den Umfang der Weitergabe der personenbezogenen Daten aller Anspruchsberechtigten der Ausbildungsstätte erlaubt. Weder war eine solche Rechtsgrundlage im EPPSG vorgesehen noch bestand die Möglichkeit, eine solche Rechtsgrundlage im Rahmen einer in diesem Gesetz vorgesehenen Verordnung zu schaffen. Daher wäre ein ergänzendes formelles Landesgesetz erforderlich gewesen, um die personenbezogenen Daten der Anspruchsberechtigten bereits vorab an den Betreiber der Antragsplattform übermitteln zu dürfen, um so eine spätere, rein automatisierte Prüfung und Auszahlung zu ermöglichen. Ein solches Gesetzgebungsverfahren hätte jedoch erhebliche Verzögerungen mit sich gebracht.

Als Alternative zu einer gesetzlichen Lösung haben wir daher ein Konzept für eine technische Lösung entwickelt, das unserer Meinung nach den datenschutzrechtlichen Anforderungen entspricht. Im Gegensatz zu den ursprünglichen Vorgaben des EEPSG sollten nach unserem Vorschlag die von den jeweiligen Ausbildungsstätten bereitgestellten Datensätze individuell verschlüsselt und das zur Entschlüsselung erforderliche Passwort nur dem Antragsberechtigten zur Verfügung gestellt werden. Durch die Eingabe dieses Passworts könnte der Anspruchsberechtigte dann die bereits verschlüsselten Daten für den Betreiber der Plattform freigeben, um eine automatisierte Prüfung und Zahlung seines Anspruchs zu ermöglichen. Ein solcher Ansatz hätte den Vorteil, dass die personenbezogenen Daten der Anspruchsberechtigten erst zum Zeitpunkt der Antragstellung durch das vom Antragsteller bereitgestellte Passwort entschlüsselt würden. Bis zu diesem Zeitpunkt lägen nur verschlüsselte Daten vor.

Im Ergebnis wurde der Prozess der Datenbereitstellung durch die Ausbildungsstätten nach diesem Konzept durch den IT-

Dienstleister, der für den Betrieb der Antragsplattform verantwortlich war, bundesweit realisiert. Darüber hinaus haben wir das datenschutzrechtliche Freigabeverfahren nach § 15 SDSG begleitet und konnten so die Ausbildungsstätten bei der Erstellung der notwendigen datenschutzrechtlichen Unterlagen und Informationen für die Betroffenen unterstützen. Unsere Beratung hat somit wesentlich dazu beigetragen, den Studierenden und Fachschülerinnen und -schülern ein datenschutzfreundliches Antragsverfahren zur Verfügung zu stellen.

**Fazit**

In Anbetracht des beschriebenen Falles wird deutlich, dass nicht immer die Schaffung gesetzgeberischer Maßnahmen die einzige Lösung zur Bewältigung komplexer datenschutzrechtlicher Herausforderungen darstellt. Oftmals werden technische Alternativen vernachlässigt, obwohl sie potenziell effektive Lösungen bieten können. Insbesondere im vorliegenden Kontext des EPPSG wurde deutlich, dass eine rein gesetzgeberische Herangehensweise nicht ausreichte, um den datenschutzrechtlichen Bedenken hinsichtlich der Übermittlung personenbezogener Daten gerecht zu werden. Stattdessen erwies sich ein technisches Konzept zur individuellen Verschlüsselung und kontrollierten Freigabe der Daten durch die Anspruchsberechtigten als geeignete Alternative. Dies verdeutlicht die Notwendigkeit, bei der Entwicklung von Lösungsansätzen für Datenschutzprobleme vermehrt technische Aspekte zu berücksichtigen und entsprechende Lösungen zu erforschen, zu entwickeln und einzusetzen.

## 3.3 Entwicklung und Betrieb von Informationssystemen

Nicht immer und so etwa auch beim intraföderalen Betrieb von Informationssystemen, wie die Antrags- und Prozessplattform Civento, lassen sich datenschutzrechtliche Fragen alleine durch einen Blick in die DSGVO lösen. Die Umsetzung des Onlinezu-

gangsgesetzes, das Bund und Länder verpflichtet, all ihre Verwaltungsleistungen online anzubieten, führt dazu, dass Behörden in Zukunft Daten im großen Umfang durch IT-Systeme verarbeiten lassen. Insbesondere deshalb, weil zahlreiche Digitalisierungsvorhaben dem Prinzip „Einer-für-Alle" (EfA) folgen, können auch verfassungsrechtliche Aspekt bei der datenschutzrechtlichen Beurteilung eine Rolle spielen.

EfA bedeutet, dass ein Land oder eine Allianz aus mehreren Ländern eine Leistung zentral entwickelt und betreibt – und diese anschließend anderen Ländern und Kommunen zur Verfügung stellt, die den Dienst dann mitnutzen können. Hierfür müssen sich die mitnutzenden Stellen mittels standardisierter Schnittstellen anbinden. Die Kosten für Betrieb und Weiterentwicklung des Dienstes teilt sich das bereitstellende Land mit den angeschlossenen Ländern und Kommunen.[7] Zusammenarbeit auf föderaler und kommunaler Ebene ist daher im Bereich der Digitalisierung eher die Regel als die Ausnahme.

### Staatsverträge und Verwaltungsabkommen als Mittel der Zusammenarbeit

Auch das Grundgesetz (GG) verankert dieses Recht der Länder zur Zusammenarbeit in Art. 91 c. Dort heißt es in Absatz 3: „*Die Länder können darüber hinaus den gemeinschaftlichen Betrieb informationstechnischer Systeme sowie die Errichtung von dazu bestimmten Einrichtungen vereinbaren*.". Aufgabe der Länder und Kommunen ist es nunmehr, die Fragen, die sich aus der geplanten Zusammenarbeit, wie auch der Nachnutzung von entwickelten EfA-Lösungen ergeben, vertraglich zu regeln. Unter den Begriff „vereinbaren" in Art. 91 c GG fallen dabei sowohl die Möglichkeit einer Verwaltungsvereinbarung wie auch der Abschluss von (intraföderalen) Staatsverträgen. Dabei greifen die Behörden in der bisherigen Praxis in aller Regel auf eine Verwaltungsvereinbarung zurück. Diese Lösung

[7] Abrufbar unter: https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/efa/efa-node.html

bietet den Vorteil, dass eine Beteiligung des Parlaments unterbleiben kann und die Vereinbarungen daher innerhalb kurzer Zeitspannen umsetzbar sind.

Allerdings eignet sich nicht jeder zu regelnde Sachverhalt für den Abschluss einer Verwaltungsvereinbarung, so dass in manchen Fällen ein Staatsvertrag zu schließen ist. Im Gegensatz zu Verwaltungsvereinbarungen erfordern Staatsverträge die Zustimmung des Parlaments gemäß Art. 95 Abs. 2 der Verfassung des Saarlandes. Die Regierung bringt den Staatsvertrag mit dem Entwurf eines Zustimmungsgesetzes in das Parlament ein, welches dem Vertrag zustimmen oder diesen ablehnen kann. Stimmt das Parlament zu, erfolgt die Transformation des Vertrages in Landesrecht durch ein sogenanntes Zustimmungsgesetz.[8]

Die Notwendigkeit eines Staatsvertrages ergibt sich für die Länder immer dort, wo eine Materie geregelt werden soll, die dem Vorbehalt des Gesetzes unterliegt. Dies ist der Fall, wenn die Grundrechte der Bürger tangiert werden oder es um die Regelung grundlegender Bereiche geht (Wesentlichkeitslehre). Das Bundesverfassungsgericht nennt als Kriterien für das Vorliegen der Wesentlichkeit etwa den Umfang des Adressatenkreises, die Langzeitwirkung einer Regelung, gravierende finanzielle Auswirkungen, erhebliche Auswirkungen auf das Staatsgefüge, Konkretisierung offenen Verfassungsrechts, die Auswirkungen auf das Gemeinwesen sowie die Unmittelbarkeit und Finalität einer gesetzlichen Regelung. Wohingegen z.B. das Erfordernis flexibler Regelungen oder das Vorliegen entwicklungsoffener Sachverhalte gegen die Wesentlichkeit sprechen sollen.[9]

Die Notwendigkeit von Staatsverträgen auch im IT-Bereich wird man daher immer dann annehmen müssen, wenn Länder

[8] Aktueller Begriff Nr. 48/07 vom 19. September 2007 „Staatsverträge zwischen den Bundesländern".

[9] Kriterien der Wesentlichkeitslehre des Bundesverfassungsgerichts, WD 3 - 3000 - 152/19.

Teile ihrer originären Zuständigkeit gemeinsam auslagern wollen, etwa durch Schaffung einer gemeinsamen Einrichtung, die mit hoheitlichen Aufgaben betraut wird (z.B. Staatsvertrag über die Einrichtung einer Gemeinsamen elektronischen Überwachungsstelle der Länder – GÜL-Staatsvertrag). Ebenso, wenn der zu regelnde Sachverhalt die Gesetzgebung der Länder beeinflusst. Als Beispiel hierfür ist der IT-Staatsvertrag zwischen dem Bund und den Ländern zu nennen, da auf dessen Basis für die Länder bindende Entscheidungen durch den IT-Planungsrat getroffen werden, die auch die Gesetzgebung z.B. in Form des E-Government Gesetzes betreffen können.

Im Übrigen stellt gerade die Weiterentwicklung der landeseigenen Informationstechnik in den meisten Fällen einen Bereich dar, der mit Blick auf die stetigen Entwicklungen und Fortschritte im Bereich IT und Digitalisierung flexibel gehandhabt werden muss. Allein die rasanten Entwicklungen der letzten Jahre zeigen, dass es sich hier um ein entwicklungsoffenes Themenfeld handelt, das ein hohes Maß an Anpassung erfordert. Zum gegenwärtigen Zeitpunkt sind daher Verwaltungsvereinbarungen oft, aber eben nicht immer, ein adäquates Mittel, um den Rahmen einer Kooperation zu regeln.

### Fazit

Die Zusammenarbeit der Länder und Kommunen bleibt auch aus Sicht des Datenschutzes ein Themengebiet, das immer neue Herausforderungen bereithalten wird. In der Vergangenheit erarbeitete rechtliche Bewertungen finden ihre Grenzen oft dort, wo bisher unbekannte, technische Sachverhalte geregelt werden müssen. Insbesondere mit Blick auf den Einsatz KI-basierter Technologien wird man etwa die Intensität der Grundrechtseingriffe bei der Datenverarbeitung durch IT-Systeme in Zukunft immer wieder neu bewerten müssen. Es bleibt somit eine Frage des Einzelfalls, ob die zu regelnde Materie dem Vorbehalt des Gesetzes unterliegt und somit einen Staatsvertrag notwendig macht.

## 3.4 VOIS-Saarland

Das kommunale Meldewesen bildet die zentrale personenbezogene Datengrundlage der öffentlichen Verwaltung. Die in seinem Rechtsrahmen geregelten Datenverarbeitungen sind mannigfaltig und reichen von rein öffentlichen Zwecken wie der Pass- und Ausweisverwaltung bis hin zu den vornehmlich privaten Zwecken einer Registerauskunft. Vor diesem Hintergrund ist es nicht übertrieben, das Meldewesen als das *„informationelle Rückgrat"* der staatlichen Verwaltung zu bezeichnen.[10] Es liegt auf der Hand, dass aufgrund dieser herausragenden Bedeutung die Funktionsfähigkeit des Meldewesens und die jederzeitige Verfügbarkeit der hierin verarbeiteten Daten oberstes Gebot sein muss. Der jederzeitigen Datenverfügbarkeit ist vor allem dann ein besonderes Augenmerk zu widmen, wenn Überlegungen einer Zusammenführung der informationstechnischen Systeme in Form einer mehr oder weniger stark ausgeprägten Zentralisierung der Meldedatenverarbeitung angestellt werden.

Bei einer zentralisierten Datenverarbeitung besteht die Gefahr, dass ein einziger Fehler oder ein Ausfall des zentralen Systems (Single point of failure) die gesamte Datenverfügbarkeit beeinträchtigen kann. Zudem steigt die Abhängigkeit von zentralen Dienstleistern für die Bereitstellung und Wartung der IT-Infrastruktur bzw. für den Betrieb des zentralen Systems. Schließlich erhöht eine Zentralisierung das Risiko von Datenschutzverletzungen und Cyberangriffen.

Vor diesem Hintergrund war unsere Behörde in die datenschutzrechtliche Bewertung einer geplanten Meldeplattform für die saarländischen Kommunen eingebunden. Die von den saarländischen Gemeinden als zuständige Meldebehörden gemäß § 1 Satz 1 Saarl. Bundesmeldegesetz-Ausführungsgesetz (SaarlBMG AG) nach § 2 Abs. 2 Satz 1 BMG zu führen-

[10] Bundesministerium des Inneren und für Heimat, https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsrecht/meldewesen/meldewesen-node.html

den Melderegister sollten nach diesen Planungen künftig in Form einer Auslagerung der kommunalen melderechtlichen IT-Infrastruktur betrieben werden. In diesem Rahmen sollte den teilnehmenden Kommunen ein Meldewesen-Fachverfahren als Clientanwendung zur Verfügung gestellt werden. Geplant war, dass das Verfahren durch den kommunalen Zweckverband des Saarlandes im Wege einer Auftragsverarbeitung nach Art. 28 DSGVO in technischer Hinsicht betrieben und betreut wird. Der Zweckverband wollte sich hierfür wiederum im Wege einer Unterbeauftragung zweier privatrechtlicher IT-Unternehmen bedienen. Die Server für die Datenverarbeitung sollten bei einem externen privaten Dienstleister (Rechenzentrum) aufgestellt und betrieben werden.

Im Rahmen unserer Beteiligung gemäß § 19 Abs. 2 Satz 2 Saarländisches Datenschutzgesetz (SDSG) waren für uns vor allem folgende Punkte und Überlegungen von besonderer Bedeutung.

Das Bundesmeldegesetz (BMG) überträgt in § 2 Abs. 2 den Meldebehörden die Pflicht zur Führung von Melderegistern. Diese Melderegister sind rechtlich voneinander getrennt, d. h. jede Meldebehörde ist sowohl melderechtlich als auch datenschutzrechtlich zunächst einmal selbst verantwortlich für die Verarbeitung der innerhalb ihres Meldedatenbestands geführten (verarbeiteten) Daten. Die Gemeinden als Meldebehörden sind damit zugleich datenschutzrechtlich Verantwortliche i. S. d. Art. 4 Nr. 7 DSGVO. Im Rahmen ihrer gesetzlich zugewiesenen Aufgabenwahrnehmung dürfen sich die Meldebehörden grundsätzlich eines Auftragsverarbeiters gemäß Art. 28 DSGVO bedienen (vgl. § 7 Abs. 1 BMG). Eine solche Auftragsverarbeitung sehen wir auch im Rahmen der eigentlichen Meldedatenverarbeitung, d. h. im Rahmen von Vorgängen mit und an Meldedaten gemäß Art. 4 Nr. 2 DSGVO, als grundsätzlich zulässig an. Aufgrund der überragenden Bedeutung und der Sensibilität dieser Verarbeitungsmaterie sind hierbei indes erhebliche Anforderungen an die Auswahl des Auftragsverarbeiters sowie an die technischen und organisatorischen Maß-

nahmen zu stellen; dies umso mehr, je weiter die Auftragsdatenverarbeitung die Gestalt eines Outsourcings der öffentlichen Verarbeitungssysteme in den privatrechtlichen Bereich annimmt.

### 3.4.1 Auftragsverarbeiter und technisch-organisatorische Maßnahmen

Art. 28 Abs. 1 DSGVO legt dem Verantwortlichen die Pflicht auf, nur mit denjenigen Auftragsverarbeitern zusammenzuarbeiten, „die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen [der DSGVO] erfolgt und den Schutz der Rechte der betroffenen Person gewährleisten."

Ein besonderes Augenmerk im Rahmen der Auswahl liegt hierbei auf der Integrität, der Verfügbarkeit und der Vertraulichkeit der zu verarbeitenden Meldedaten (Art. 5 Abs. 1 lit. f DSGVO). Selbige dürfen weder durch unbefugte Dritte eingesehen noch auf sonstige Art und Weise kompromittiert werden können. Auch dürfen die Daten nicht durch ein eigenes versehentliches Handeln oder ein Versäumnis des Auftragsverarbeiters bzw. durch ein diesem evtl. nicht zurechenbares Ereignis von außen in ihrer Verfügbarkeit beeinträchtigt werden. Die sich hieraus ergebenden Pflichten werden in Art. 32 DSGVO sowie in Erwägungsgrund 39 Satz 12 der DSGVO konkretisiert.

Es bedarf keiner näheren Erläuterung, dass die hieraus resultierenden technisch-organisatorischen Maßnahmen und Anforderungen an den Auftragsverarbeiter auf die jeweilige Datenverarbeitung ausgelegt, mehr noch, auf diese „maßgeschneidert" und konkret bezeichnet sein müssen. „Konkret" ist hier im wortwörtlichen Sinne zu verstehen. Die ergriffenen Maßnahmen müssen vollumfänglich und, vor allem in technischer Hinsicht, detailliert beschrieben sein. Wenig geeignet sind hingegen abstrakt im Vorhinein vertraglich festgelegte Schutzziele oder allgemein aufgeführte Schutzmechanismen, welche

mehr oder weniger im Rahmen jeder Datenverarbeitung und Auftragsverarbeitung einzuhalten sind.

Eine Festlegung der zu ergreifenden technisch-organisatorischen Maßnahmen kann nur dann in sinnvoller Art und Weise erfolgen, wenn man sich zunächst der Risiken bewusst wird, auf deren Ausschluss bzw. Minimierung die Maßnahmen abzielen. In Bezug auf eine Auftragsverarbeitung von Meldedaten steht aus hiesiger Sicht daher am Anfang der Ermittlung der diesbezüglich zu ergreifenden technisch-organisatorischen Maßnahmen eine Datenschutz-Folgeabschätzung nach Art. 35 DSGVO. Die geplante Datenverarbeitung hat bereits aufgrund ihres Umfanges sowie der Art (Sensibilität) der zu verarbeitenden Daten ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen im Hinblick darauf, dass sich die Meldebehörden durch eine räumlich teilweise oder vollständige Auslagerung der Meldedatenspeicherung (Datenbankserver) weitgehend ihrer tatsächlichen Einflussmöglichkeiten hinsichtlich der Verfügbarkeit der Daten begeben. Dieser Verlust der direkten und jederzeitigen Verfügungsmöglichkeit über die Daten muss durch umfangreiche vertragliche Regelungen kompensiert werden, welche die Verarbeitungsmodalitäten beim Auftragsverarbeiter und dessen Pflichten präzise, detailreich und unmissverständlich regeln. Dies kann nur geschehen, wenn die Datenverarbeitung sowie die konkreten Verarbeitungsbeiträge der Auftragsverarbeiter detailliert beschrieben und auf Fehleranfälligkeit hin untersucht werden. Nur dann können die Risiken abgeschätzt und Überlegungen angestellt werden, mit welchen Maßnahmen technischer und/oder organisatorischer Art diese Risiken minimiert werden können. Zwingend erforderlich ist hierfür eine Analyse und schriftliche Dokumentation der einzelnen Datenflüsse und Verarbeitungsschritte. Ist dies von Seiten des Verantwortlichen erfolgt, so hat sich dieser sodann insbesondere folgenden Punkten zu widmen:

### 3.4.2 Trennung der Meldedatenbestände

Wie bereits oben ausgeführt, bleibt jede Gemeinde (Meldebehörde) alleinige verantwortliche Stelle für die Verarbeitung der ihr zugewiesenen Meldedatenbestände. Nach der gesetzlichen Grundintention bedeutet dies, dass jede Gemeinde zunächst mit eigenen technischen Mitteln die ihr zugewiesenen Meldedaten zu verarbeiten hat, ohne dass diese Verarbeitung in irgendeiner Form mit dem Melderegister einer anderen Gemeinde verbunden oder gar von dieser abhängig wäre. Grundsätzlich bedeutet dies den Betrieb von 52 informationstechnisch autarken kommunalen Meldesystemen im Saarland, welche auch räumlich voneinander zu trennen wären.[11]

Eine solche strikte Trennung ginge mit Blick auf das Ausfallrisiko eines oder mehrerer Meldesysteme mit einer Risikostreuung einher. Fiele ein Meldesystem, aus welchen Gründen auch immer aus, so würde dies die übrigen Meldesysteme zunächst nicht tangieren. Eine strikte Trennung der Meldesysteme, auch in physischer Hinsicht, d. h. in getrennte Datenserver, liefe jedoch den Vorstellungen einer ressourcenschonenden zentralen Meldedatenverarbeitung entgegen, geht es hier doch vor allem darum, die Verwaltung der Meldedatenbestände auf einige wenige Akteure zu verteilen und damit insgesamt wirtschaftlicher zu gestalten. Unfreiwillige Folge einer solchen vollständigen oder teilweisen Zentralisierung könnte jedoch sein, dass eine Kompromittierung der an einem zentralen Ort betriebenen technischen Systeme mit einer Offenlegung oder dem Verlust sämtlicher Melderegister (Melderegisterdaten) verbunden sein könnte.

Konsequenz hieraus muss sein, dass im Rahmen der für mehrere Meldebehörden (Gemeinden) durchzuführenden Auf-

[11] Die Pflicht zur Führung einzelner Melderegister ist dabei von der Möglichkeit der Errichtung eines zentralen Meldedatenbestands (§ 55 Abs. 3 BMG) zu trennen. Die Errichtung eines zentralen Meldedatenbestands (vgl. § 3 Abs. 1 Saarl. Bundesmeldegesetz-Ausführungsgesetz) führt nicht zu einem Wechsel der Verantwortlichkeit nach § 2 Abs. 2 S. 1 BMG.

tragsverarbeitung, welche die Meldedatenverarbeitung an einer oder an mehreren zentralen Örtlichkeiten und auf gemeinsamen technischen Systemen (Anwendungsserver, Datenbankserver, Storage-Hardware) durchführt, Mechanismen vorgesehen werden müssen, welche trotz der örtlichen und technischen Zusammenführung gleichwohl eine effektive Trennung der Meldedatenbestände verwirklichen. Diese Trennung hat vor allem zweierlei sicherzustellen. Zum einen soll sie bewirken, dass der Ausfall eines Verarbeitungssystems sich nicht auf die übrigen Systeme auswirkt. Die Meldebehörden müssen auch nach dem beschriebenen Verfahren jederzeit und unabhängig voneinander in der Lage sein, ihre gesetzlich zugewiesene Datenverarbeitung autark zu betreiben. Zum anderen soll verhindert werden, dass im Fall eines vorsätzlichen rechtswidrigen Zugriffs auf die technischen Einrichtungen, sei es von außen durch Dritte, oder von innen, etwa durch einen oder mehrere Administratoren, ein Zugriff auf sämtliche Melderegister (Meldedaten) möglich ist.

Erforderlich hierfür ist eine *echte* Mandantentrennung auf Seiten des Auftragsverarbeiters. Eine bloß logische Mandantentrennung auf Anwenderseite, etwa in der Form, dass jede Meldebehörde in einem zentralen Verarbeitungssystem aufgrund eines Rechte- und Rollenkonzeptes nur Zugriff auf die sie betreffenden Meldedaten hat, reicht nicht aus, dem anzustrebenden hohen Schutzniveau Genüge zu tun. Welche datenschutzrechtlichen Anforderungen an eine effektive Trennung der einzelnen Verarbeitungstätigkeiten dabei gestellt werden, wird im Rahmen des von der Datenschutzkonferenz herausgegebenen Standarddatenschutzmodells (Version 3) näher beschrieben. Dessen Vorgaben und Empfehlungen können für Behörden und sonstige öffentliche Stellen als Leitlinien begriffen werden. In seinem Baustein 50 (Baustein 50 „Trennen“, Version V.1.0 vom 6.10.2020[12)] beinhaltet das Standard-

[12] Abrufbar unter: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Trennen_V1.0.pdf

datenschutzmodell einen Maßnahmenkatalog mit Trennungsanforderungen an Daten, Systeme und Dienste sowie Prozesse sowohl innerhalb einer Organisation als auch von miteinander zusammenarbeitenden Organisationen. In Bezug auf gemeinsam genutzte Dienste und Systeme geht das SDM bereits bei einem *mittleren Schutzniveau* von dem Erfordernis einer logischen Trennung von Fachapplikationen aus, von der jeweils eine Instanz (Fachapplikation) in einem eigenen virtuellen Betriebssystem betrieben wird (3. lit. e). Ein *hohes Schutzniveau* wird in einer physikalischen Trennung von Fachapplikationen gesehen, bei der jede Fachapplikation in einem Betriebssystem auf einer eigenen IT-Hardware in unterschiedlichen Räumen eines Gebäudes oder an unterschiedlichen Orten (Rechenzentren) betrieben wird (3 lit. g, h).

Selbst wenn man das Erfordernis eines hohen Schutzniveaus vorliegend ablehnen sollte, so ist aus hiesiger Sicht zumindest die Gewährleistung eines mittleren Schutzniveaus unabdingbar, mit der Folge, dass die einzelnen Meldedaten durch die Meldebehörden nur auf eigens eingerichteten und virtuell – und damit getrennt – betriebenen Betriebssystemen verarbeitet werden dürfen.

### 3.4.3 Nachweis eines Standards der Informationssicherheit

Mit Blick auf die Auswahl eines die Anforderungen des Art. 28 Abs. 1 DSGVO entsprechenden Auftragsverarbeiters sind wir weiter der Überzeugung, dass eine umfassende Zertifizierung desselben regelmäßig erforderlich ist. Den Standard der ISO 27000-Familie oder eines vergleichbaren Standards erachten wir dabei für obligatorisch. Es handelt sich hierbei um eine international anerkannte Zertifizierung eines Informationssicherheits-Managementsystems (ISMS).[13] Eine solche Zertifizierung spricht, jedenfalls in informationstechnischer Hinsicht, für die Zuverlässigkeit des Auftragsverarbeiters und er-

[13] Vgl. *Sohr/Kemmerich*, in: Kipker, Cybersecurity (1. Aufl. 2020) S. 74 ff.

möglicht es den verantwortlichen Stellen oftmals erst eine dahingehende Bewertung und Auswahl zu treffen.

Zusammenfassend lässt sich festhalten, dass die Einrichtung/Zurverfügungstellung einer zentralen Meldedatenverarbeitungsinstanz für die saarländischen Kommunen durch ein privates Unternehmen im Wege einer Auftragsverarbeitung grundsätzlich möglich ist, dem Gesetz insbesondere keine dahingehenden Verarbeitungsverbote zu entnehmen sind. Die tatsächliche Ausgestaltung dieser Auftragsverarbeitung in technisch-organisatorischer Sicht muss mit erheblicher Sorgfalt und Genauigkeit betrieben werden und insbesondere weitreichende Risikoanalysen beinhalten.

Das Melderecht geht im Grundsatz von einer dezentralisierten Datenverarbeitung durch viele Akteure (Meldebehörden) aus. Die Nichtexistenz eines, immer mal wieder diskutierten, zentralen Bundesmelderegisters spricht in unseren Augen dafür, dass der Gesetzgeber die derzeitige Verteilung auf die verantwortlichen kommunalen Meldebehörden beibehalten will. Zwar muss sich die hieraus resultierende behördliche Kleingliedrigkeit des Meldewesens nicht zwingend in den Verarbeitungsprozessen widerspiegeln, d. h. ein Zusammenarbeiten, etwa in Form einer Zusammenlegung von IT-Infrastruktur und Personal, ist grundsätzlich möglich. Wird dieser Weg gewählt, so muss jedoch sichergestellt werden, dass trotzdem jede verantwortliche Kommune (Meldebehörde) in der Lage ist, die Aufgabe unmittelbar und ohne zeitliche Zäsur weiterzuführen, sollte die ausgegliederte Infrastruktur ausfallen und/oder ein Auftragsverarbeiter, aus welchen Gründen auch immer, von heute auf morgen nicht mehr zur Verfügung stehen.

Darüber hinaus bietet allerdings schon der derzeitige Rechtsrahmen (§ 55 Abs. 3 BMG) die Möglichkeit, jedenfalls auf Ebene der Bundesländer durch Landesrecht die Voraussetzungen für das Einrichten und Führen zentraler Meldedatenbestände zu regeln. Bisher hat der Landesgesetzgeber von dieser Befugnis keinen Gebrauch gemacht. Wir haben daher angeregt, dass

die betroffenen Kommunen bzw. der Zweckverband das Gespräch mit dem für das Melderecht zuständigen Ministerium für Inneres, Bauen und Sport suchen, um zunächst zu erörtern, inwiefern das geplante Vorhaben von den derzeitigen Regelungen des Melderechts überhaupt gedeckt ist. Eine Rückmeldung seitens des Zweckverbands steht derzeit noch aus.

## 3.5 Funkwasserzähler

Die Abrechnung von Verbrauchswerten via digitaler Messsysteme ist bereits seit vielen Jahren Standard in den Bereichen der Strom-, Gas-, und Heizwasserversorgung. Auch im Bereich der Versorgung mit Frischwasser werden die alten analogen Wasserzähler sukzessive durch ihre digitalen Pendants ausgetauscht. Mit diesem Wechsel eröffnet sich die Möglichkeit, das so erfasste Messergebnis kontaktlos mittels Funk zu übertragen.

Im 26. Tätigkeitsbericht für die Jahre 2015/2016 (S. 79 ff.) hatte sich unsere Behörde – damals noch unter der alten Rechtslage – bereits eingehend mit dieser Thematik auseinandergesetzt und kam zu dem Ergebnis, dass ein Einsatz sog. „intelligenter" Wasserzähler durch öffentliche Stellen in Form einer Funkübertragung des Messergebnisses nur aufgrund vorheriger schriftlicher Einwilligung des Betroffenen rechtlich zulässig ist. Diese Rechtsfolge ergab sich unmittelbar aus der damaligen Vorschrift des § 32 Abs. 1 Saarländischen Datenschutzgesetz (SDSG) i. d. F. vom 18.05.2011. Nach dieser Vorschrift stand der betroffenen Person auch die jederzeitige Möglichkeit des Widerrufs ihrer Einwilligung zu.

Das novellierte SDSG aus dem Jahr 2018 sieht keine vergleichbare bereichsspezifische Rechtsgrundlage mehr vor. Hieraus folgt, dass sich die Zulässigkeit der diesbezüglichen Datenverarbeitung vor allem nach den allgemeinen Bestimmungen der DSGVO beurteilt.

Mit ihrer Stellungnahme vom 11. Mai 2023[14] verortete die Datenschutzkonferenz (DSK) hier ein Regelungsdefizit und forderte die Einführung möglichst bundeseinheitlicher spezialgesetzlicher Regelungen, welche den Einsatz funkbasierter Kaltwasserzähler – in Analogie zu den bereits bestehenden Regelungen im Bereich der Strom- und Gasversorgung – nach Zweck, Art sowie den technisch-organisatorischen Anforderungen explizit regeln.

Ohne, dass bislang entsprechende gesetzliche Regelungen verabschiedet wurden, begannen in der zweiten Hälfte des Berichtsjahres 2023 einige saarländische Wasserversorger mit der Umstellung ihres Abrechnungswesens hin zu einem funkbasierten Fernerfassen der Verbrauchswerte. Die diesbezügliche Intensivierung des Austauschs der alten Wasserzähler durch neue Funkwasserzähler führte bei unserer Behörde zu einem erhöhten Beschwerdeaufkommen hiervon betroffener Kunden.

### 3.5.1 Einordnung der Ausgangslage

Bei Funkwasserzählern handelt es sich um Messeinrichtungen mit einer Kommunikationszusatzeinrichtung, die das Auslesen des Messergebnisses (den Zählerstand) zusammen mit einigen Statusinformationen (z.B. Leckage, Rückfluss, Umgebungstemperatur) aus der Ferne ermöglichen. Hierbei wird zwischen zwei Arten von Geräten unterschieden. Geräte mit unidirektionaler Kommunikationsschnittstelle senden die gesammelten Daten (Mess- und Statusinformationen) periodisch (in Zeitabständen von in der Regel 16 Sekunden) autonom aus. Dieses Funksignal kann sodann durch den Wasserversorger/ Netzbetreiber oder einen beauftragten Dritten durch Vorbeifahren (drive-by) ohne weiteres Zutun des Vertragskunden/Hauseigentümers erfasst und genutzt werden. Bei Geräten mit bidirektionaler Kommunikationsschnittstelle werden die

[14] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/st/2023-05-11_DSK-Stellungnahme_Funkwasserzaehler.pdf

gesammelten Daten erst auf Abruf durch den Wasserversorger/Netzbetreiber bereitgestellt. In beiden Fällen allerdings erhält der Kunde von dem Erfassungsvorgang (Ablesevorgang) in der Regel keine Kenntnis. Nach hiesigem Kenntnisstand finden bei saarländischen Wasserversorgern bisher nur Geräte mit unidirektionaler Kommunikationsschnittstelle Verwendung. Die nachfolgende rechtliche Bewertung bezieht sich folglich allein auf diese Geräteart.

Beim Bereitstellen der öffentlichen Wasserversorgung handelt es sich um Daseinsvorsorge und damit um eine öffentliche Aufgabe. Auch das Verhältnis zwischen Wasserversorger und Kunden ist öffentlich-rechtlich geprägt. Im Regelfall besteht ein Anschluss- und Benutzungszwang. Lediglich die vertragliche Ausgestaltung dieses Versorgungsverhältnisses des Wasserversorgers mit dem Kunden ist – nach unseren bisherigen Kenntnissen – ausschließlich privatrechtlich ausgestaltet. Inhalt des diesbezüglichen Versorgungsvertrages sind allgemeine Bedingungen über die Versorgung von Tarifkunden mit Wasser, die in der Verordnung über Allgemeine Bedingungen für die Versorgung mit Wasser (AVBWasserV) auf der Grundlage des § 27AGBG (außer Kraft) vom Bundesministerium für Wirtschaft im Einvernehmen mit dem Bundesministerium der Justiz und mit Zustimmung des Bundesrates erlassen wurden.

Die Wasserversorger nutzen Funkwasserzähler dabei im Wesentlichen für zwei Zwecke. Zum einen sollen die Funkwasserzähler den Wasserversorgern die Durchführung der jährlichen Verbrauchsdatenerfassung und -abrechnung erleichtern. Zum anderen dienen diese Geräte auch der Pflege und Wartung der Wasserversorgungsnetze und damit einem öffentlichen Interesse, indem die Wasserversorger auch unterjährig Verbrauchsdaten und Statusinformationen auslesen können, die sie dann zur Kapazitätsplanung und Störungsbeseitigung verwenden können. Für diese beiden verschiedenen Verarbeitungszwecke gelten unterschiedliche datenschutzrechtliche Anforderungen.

### 3.5.2 Einsatz eines Funkwasserzählers zu Abrechnungszwecken

Die Datenverarbeitung, deren Zweck darauf gerichtet ist, dass ein Funkwasserzähler den jeweils aktuellen Zählerstand in kurzen periodischen Zeitabständen aussendet und dadurch eine unterjährige Erfassung des Wasserverbrauchs durch den Wasserversorger ermöglicht, kann nach hiesiger Auffassung derzeit ausschließlich auf eine diesbezügliche Einwilligung des Kunden (Art. 6 Abs. 1 lit. a DSGVO) gestützt werden.

Eine Datenverarbeitung zur Vertragserfüllung gemäß Art. 6 Abs. 1 lit. b) scheidet schon deshalb als Rechtsgrundlage aus, weil durch das periodische Aussenden des Verbrauchswertes dem Wasserversorger personenbezogene Daten des Kunden auch dann i. S. d. Art. 4 Nr. 2 DSGVO bereitgestellt werden und zugänglich sind, wenn er diese Daten nicht bzw. noch nicht zu Abrechnungszwecken benötigt. Das periodische Aussenden des Zählerstands geht über das hinaus, was zur Erfüllung des Vertrags bzw. zur Abrechnung erforderlich ist und verstößt damit gegen den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO. Hier läge es vielmehr bereits aus Gründen der Datenminimierung nahe, die Datenübertragung nur anlassbezogen durchzuführen. Insbesondere bei einem herkömmlichen Tarif, bei dem nur die verbrauchte Gesamtmenge eines bestimmten Zeitraumes relevant ist, dürfte es nicht erforderlich sein, weitere Daten aufzuzeichnen und zu übertragen. Hiermit ist es nicht zu vereinbaren, dass alle 16 Sekunden der jeweils aktuelle Zählerstand übertragen wird, dies erst recht, wenn zum jeweiligen Zeitpunkt keine turnusmäßige Abrechnung ansteht.

Denkbar wäre es allenfalls, dass im Zähler die konkreten Abrechnungsstichtage einprogrammiert werden und nur zu diesem Zeitpunkt, ggf. unter Berücksichtigung einer Toleranz von mehreren Tagen, eine Übertragung des Zählerstandes stattfindet.

Auch ergibt sich aus § 18 Abs. 2 AVBWasserV[15], wonach das Wasserversorgungsunternehmen über die Art der verwendeten Messeinrichtungen bestimmt, keine gesetzliche Gestattung für die Installation von funkbasierten Messeinrichtungen und die damit zusammenhängende Übertragung personenbezogener Daten.

Soweit in § 18 Abs. 2 S. 2 AVBWasserV von „Art" der Messeinrichtungen gesprochen wird, werden damit lediglich die unterschiedlichen Bauarttypen (Flügelradwasserzähler, Volumenzähler, Verbundwasserzähler, Messkapselzähler) in Bezug genommen. Die Vorschrift soll im Verhältnis zwischen Wasserversorger und Kunde sicherstellen, dass der Wasserversorger auf eine homogene Betriebsinfrastruktur zurückgreifen kann und er nicht bei jedem Kunden mit einem anderen Wasserzählermodell konfrontiert wird. Die Vorschrift des § 18 AVBWasserV gibt dem Wasserversorger darüber hinaus keine Befugnis, den Wasserzähler mit Zusatzeinrichtungen, insbesondere mit Datenübertragungs- und Kommunikationseinrichtungen auszurüsten.

§ 18 AVBWasserV hat keinerlei datenschutzrechtlichen Regelungsgehalt, sondern verweist in seinem Absatz 1 ausschließlich auf eichrechtliche Vorschriften. Die Vorschrift kann demnach auch keine Rechtsgrundlage für die funkbasierte Verarbeitung personenbezogener Daten im Zusammenhang mit dem Einsatz eines Funkwasserzählers bilden.

Auch den übrigen Regelungen der AVBWasserV, insbesondere § 20, kann keine Befugnis zum Fernauslesen entnommen werden. Die gegenteilige Auffassung, die den Begriff der „Ablesung" technikoffen verstehen will und über den Wortlaut hinaus auch ein „Auslesen" hierunter subsumieren will, verkennt die Systematik des § 20 AVBWasserV. Nicht anders lässt sich sonst § 20 Abs. 2 AVBWasserV erklären, welcher dem Wasser-

[15] „Das Wasserversorgungsunternehmen hat dafür Sorge zu tragen, daß eine einwandfreie Messung der verbrauchten Wassermenge gewährleistet ist. Es bestimmt Art, Zahl und Größe sowie Anbringungsort der Meßeinrichtungen."

versorger die Möglichkeit einer Schätzung einräumt, sollten die Räume des Kunden nicht zum Zwecke der Ablesung betreten werden können. Auch die in § 20 Abs. 1 S. 1 AVBWasserV gegebene Möglichkeit der Selbstablesung durch den Kunden ist letztlich dahingehend zu deuten, dass dieser gerade nicht dazu verpflichtet ist, eine von ihm nicht wahrnehmbare und daher im Zeitpunkt der Ablesung auch nicht kontrollierbare Ablesung via funkbasierter Fernauslesung zu dulden.

### 3.5.3 Einsatz eines Funkwasserzählers aus Gründen des öffentlichen Interesses

Neben den Abrechnungszwecken dient die Installation eines Funkwasserzählers auch dazu, die Pflichtaufgabe der Wasserversorgung zu erfüllen und insbesondere die Betriebssicherheit und Hygiene der Wasserversorgungseinrichtung besser kontrollieren und gewährleisten zu können. Auch in diesem Bereich bedürften jedoch Art und Umfang der damit zusammenhängenden Verarbeitung personenbezogener Daten einer bereichsspezifischen, förmlichen gesetzlichen Grundlage, an der es derzeit im Saarland fehlt.

Art. 6 Abs. 1 lit. b DSGVO und die Regelungen der AVBWasserV kommen schon deswegen nicht als Rechtsgrundlage in Betracht, da bei der Gewährleistung der Trinkwasserversorgung die öffentliche Aufgabenwahrnehmung und nicht die Abwicklung des Vertragsverhältnisses mit dem Kunden im Vordergrund steht.

Auch den Normen des Wasserhaushaltsgesetzes (WHG), insbesondere den § 50 WHG lassen sich in Verbindung mit Art. 6 Abs. 1 lit.e DSGVO keine Verarbeitungsgrundlagen entnehmen. Eingriffe in das Recht auf informationelle Selbstbestimmung bedürfen grundsätzlich einer förmlichen, parlamentarischen Ermächtigung, die die zu erhebenden personenbezogenen Daten als solche, den Anlass und den spezifischen Zweck der Erhebung, die Art und Dauer der Aufbewahrung sowie ihre Löschung normenklar und bestimmt regelt und den

Grundsatz der Verhältnismäßigkeit wahrt.[16] Diesen Anforderungen, die sich zudem auch aus Art. 6 Abs. 3 DSGVO ergeben, werden die § 50 WHG mit ihrem generalklauselartigen Wortlaut nicht gerecht.

Zusammenfassend ist nach Auffassung unserer Behörde eine normenklare bereichsspezifische Regelung der funkbasierten Auslesung von Wasserzählern unabdingbar, welche im Saarland bis dato jedoch nicht existiert. Die Freischaltung entsprechender Funktionalitäten an bereits installierten oder noch zu installierenden Wasserzählern bedarf daher einer Einwilligung des jeweiligen Vertragspartners.

[16] Vgl. zuletzt BVerfG 27.05.2020 1 BvR 1873/13 u.a.; BVerfGE 65, 1ff (44 ff., 151 ff.).

# IV.

# Inneres

# 4 Inneres

## 4.1 Kontrollen der Antiterror- und Rechtsextremismus-Datei

Wie zuletzt im 30. Tätigkeitsbericht unserer Behörde dargestellt (dort: Punkt 4.5), sind in turnusmäßigen Abständen (mindestens alle zwei Jahre) Datenschutzprüfungen im Zusammenhang mit der Antiterrordatei (ATD) und der Rechtsextremismus-Datei (RED) durchzuführen. Bei diesen standardisierten und beim BKA zentral geführten Informationssystemen handelt es sich um Datenbestände, die zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland bzw. des gewaltbezogenen Rechtsextremismus geschaffen wurden und den Informationsaustausch zwischen den Polizeien und Nachrichtendiensten verbessern sollen.[17]

In den Zuständigkeitsbereich der saarländischen Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) fallen die „Abteilung V – Verfassungsschutz" des Ministeriums für Inneres, Bauen und Sport sowie das saarländische Landespolizeipräsidium (LPP). Aufgrund der hohen Prüfdichte gerade im Sicherheitsbereich und der geringen Personalkapazität unserer Behörde werden die ATD und die RED bei der Abteilung V und beim LPP derzeit alternierend kontrolliert. Die Prüfung der Abteilung V wurde bereits im Jahr 2022 begonnen, konnte allerdings erst im Frühjahr des Jahres 2023 abgeschlossen werden. Direkt im Anschluss wurde die für das Jahr 2023 vorgesehene Prüfung beim LPP initiiert und durchgeführt. Im Rahmen des diesjährigen Tätigkeitsberichts berichten wir deswegen über beide Kontrollen.

[17] Vgl. BT-Drs. 17/8672 (RED-G) und BT-Drs. 16/2950 (ATDG), jew. S. 1.

### 4.1.1 Kontrolle bei der Verfassungsschutzbehörde

Die turnusmäßige Kontrolle bei der saarländischen Verfassungsschutzbehörde zeigte auf, dass die überprüften Zentraldateien nach wie vor von eher geringer Bedeutung für die praktische Arbeit der abruf- und speicherberechtigten Stellen sind. Zum Stichtag der Prüfung verantwortete die saarländische Verfassungsschutzbehörde hier nur sehr wenige Personendatensätze.

Im Rahmen der Kontrolle konnte deren ursprüngliche Einspeicherung als rechtmäßig beurteilt werden. Den Verarbeitungen lag jeweils ein entsprechender Anfangsverdacht im Sinne des § 2 Abs. 1 Antiterrordateigesetz (ATDG) bzw. Rechtsextremismusdatei-Gesetz (RED-G) zugrunde. Zur ATD konnte nachvollziehbar begründet werden, warum die betroffenen Daten weiterhin in der Zentraldatei hinterlegt sein sollten. Im Rahmen der Prüfung zur RED kündigte die Verfassungsschutzbehörde noch im Vor-Ort-Termin an, dass die Erforderlichkeit einer fortgesetzten Speicherung mit Blick auf bestimmte Informationen zwischenzeitlich nicht mehr gesehen werde. Unserer Behörde wurde deswegen eine baldige Löschung zugesichert, die auch kurz darauf stattfand.

Bereits im Jahr 2024 wird aufgrund des verpflichtenden Prüfturnus erneut eine Prüfung bei der Verfassungsschutzbehörde durchzuführen sein.

### 4.1.2 Kontrolle beim Landespolizeipräsidium

Wie schon im Rahmen der Kontrolle bei der Abteilung V zeigte sich auch beim LPP, dass die praktische polizeiliche Arbeit nur in sehr geringem Maße von der Existenz und den Inhalten der geprüften Zentraldateien abhängig ist. Zwar verantwortete die saarländische Polizei ungleich mehr Fälle als die Verfassungsschutzbehörde. Dennoch war zu vermerken, dass der Datenbestand seit der letzten Prüfung im Jahr 2020/2021 geschrumpft war. Zudem konnte anhand der angeforderten Protokolldaten festgestellt werden, dass im Jahr 2023 (bis zum Prüfzeitpunkt

im Juni) nur wenige Neueinspeicherungen stattgefunden hatten (von denen ein Datensatz bereits wenige Wochen später wieder gelöscht wurde) und keine einzige länderübergreifende Recherche in den Zentraldateien durchgeführt worden war.

Zum Gegenstand der Einzelfallkontrolle wurden insgesamt sechs Sachverhalte gemacht, deren Speicherung mit Blick auf die in § 2 ATDG / RED-G niedergelegten Voraussetzungen aber keinen datenschutzrechtlichen Bedenken begegneten. Mit Blick auf die Dokumentation der Vorgänge war positiv zu vermerken, dass das in der letzten turnusmäßigen Prüfung noch nicht genutzte, abgestimmte Dokumentationsformblatt (siehe 30. TB 2020, Punkt 4.5) mittlerweile Verwendung fand. Zur konkreten Ausgestaltung des Formulars und weiterer Verarbeitungsnachweise konnte unsere Behörde aufgrund nunmehr bestehender Erfahrungsberichte aus der Praxis weitere Verbesserungen (insbesondere in Bezug auf die Dokumentation der Erforderlichkeit von Eintragungen) vorschlagen.

Die nächste Prüfung der ATD und RED beim Landespolizeipräsidium wird aufgrund der turnusmäßigen Prüfverpflichtung voraussichtlich im Jahr 2025 stattfinden.

## 4.2 Kontrolle zu PHW und EHW

Zur Unterstützung bei der Wahrnehmung ihrer Aufgaben greift auch die saarländische Polizei auf das zu Fahndungs- und Auskunftszwecken betriebene zentrale Informationssystem der deutschen Polizei (INPOL) zurück. In diesem können unter anderem diverse Angaben zu Einzelpersonen gespeichert werden, denen aufgrund ihres Inhalts teils erhebliches Eingriffsgewicht zu bescheinigen ist. Neben den Grunddaten zu einzelnen Personen bzw. deren Personalien sind dies vor allem Daten aus erkennungsdienstlichen Behandlungen und Kriminalaktennachweisen. Ebenso können im System sogenannte „personengebundene Hinweise“ (PHW) und „ermittlungsunterstützende Hinweise“ (EHW) gespeichert werden.

In Koordination mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) führte unsere Behörde (beginnend im Jahr 2022 und abschließend im Berichtsjahr 2023) eine Kontrolle dieser Hinweis-Kennzeichnungen durch.

### 4.2.1 Die Rechtsgrundlage der Kennzeichnung und deren mögliche Inhalte

Die für die Speicherung von PHW und EHW relevanten Rechtsgrundlagen finden sich für die Eintragung im polizeilichen Informationsverbund in § 16 Abs. 6 des Bundeskriminalamtgesetzes (BKAG) und für den Landesdatenbestand in § 21 Abs. 2 des Saarländischen Gesetzes über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG).

Die im Wesentlichen inhaltsgleichen Regelungen sehen vor, dass das Bundeskriminalamt (BKA) bzw. die saarländische Vollzugspolizei zu bereits in den polizeilichen Informationssystemen aus anderen Gründen vorhandenen Daten von Beschuldigten, Verdächtigten oder Gefährdern – soweit erforderlich – personengebundene sowie ermittlungsunterstützende Hinweise anreichernd bzw. ergänzend speichern darf. Das Anlegen einer Person, allein um diese mit einem Hinweis zu versehen (isolierte Vergabe), ist unzulässig und wird auch durch die technische Ausgestaltung des Systems grundsätzlich verhindert.

Problematisch ist derweil, dass die *gesetzlichen* Regelungen für die Vergabe von Hinweisen – trotz des damit verbundenen, vertiefenden Eingriffs in das Recht auf informationelle Selbstbestimmung – keine sehr konkreten Kriterien aufweisen und so im Konflikt mit den aus Rechtsstaats- und Demokratieprinzip herzuleitenden Grundsätzen der Bestimmtheit und Normenklarheit stehen. Nicht zuletzt deswegen ist derzeit eine Verfassungsbeschwerde, im Besonderen gegen § 16 Abs. 6 Nr. 2

BKAG (Vergabe von ermittlungsunterstützenden Hinweisen), beim Bundesverfassungsgericht anhängig.[18]

Nach den bis dato verfassungsrechtlich unbeanstandeten Regelungen ist eine Vergabe zulässig

- bei PHW**,** wenn der Hinweis zum Schutz der betroffenen Person selbst oder zur Eigensicherung der Polizeibeamten erforderlich ist und
- bei EHW**,** wenn der Hinweis geeignet ist, dem Schutz Dritter oder der Gewinnung von Ermittlungsansätzen zu dienen.

Unter anderem aufgrund umfassender Kritik der Datenschutzaufsichtsbehörden am Fehlen formalgesetzlicher Vorgaben zur Vergabe der einzelnen Hinweise,[19] haben das BKA und die Innenressorts der Länder in Kooperation zwei Leitfäden entwickelt, um jedenfalls klarere und einheitliche Kriterien für die Vergabe von PHW und EHW zu schaffen. Den oben genannten verfassungsrechtlichen Bedenken wird damit jedoch nur teilweise begegnet.

Die Leitfäden sehen vor, dass die Vergabe personengebundener und ermittlungsunterstützender Hinweise nur in Form standardisierter Hinweiskategorien erfolgen darf. Hierzu definieren die Leitlinien unterschiedliche Typen von PHW und EHW und legen einheitliche Kriterien für deren Vergabe fest. Der EHW-Leitfaden ist hierbei als Verschlusssache (VS-NfD) eingestuft; der PHW-Leitfaden besitzt keine Einstufung.

Eine etwaig vorhandene Kennzeichnung wird Polizeibeamten, die den Datensatz einer Person im Informationssystem recherchieren, entsprechend angezeigt. Zu den Hinweisen, die im Rahmen der gegenständlichen Prüfung näher untersucht wurden, gehören die Folgenden:

[18] Das Verfahren vor dem BVerfG wird unter dem Aktenzeichen 1 BvR 1160/19 geführt.
[19] Siehe hierzu die Darstellung des BfDI in dessen 24. Tätigkeitsbericht (2011, 2012), Kapitel 7.4.5, S. 98.

- PHW PSYV (psychische und Verhaltensstörung)
- PHW BTMK (Betäubungsmittelkonsument)
- EHW Reisender Täter
- EHW BTM-Handel (Betäubungsmittelhandel)

### 4.2.2 Feststellungen des Prüfverfahrens

Das Prüfverfahren wies sowohl mit Blick auf die Vergabepraxis an sich als auch in Bezug auf eine nachvollziehbare Dokumentation der diesbezüglichen Einzelfallentscheidung erhebliche Defizite auf.

So fordert bspw. der PHW-Leitfaden für die Vergabe des Hinweises PSYV, dass das Bestehen einer psychischen Erkrankung des Betroffenen, aus der Gefahren für ihn selbst oder für Polizeibedienstete resultieren, durch einen ärztlichen Befund in Form eines Attests oder Gutachtens festgestellt wurde. Im Zuge einer Stichprobenkontrolle wurden mehrere Einzelfälle auf das Vorhandensein solcher Dokumente untersucht. Im Vor-Ort-Termin konnten zu einem Großteil der Personendatensätze keine entsprechenden Befunde vorgewiesen werden. Teilweise basierten die Eintragungen auf eigenen Angaben der betroffenen Personen selbst oder auf Wahrnehmungen Dritter, was den im Leitfaden geforderten Kriterien nicht genügt.

Auch wenn der PHW BTMK mit der Bezeichnung „Betäubungsmittelkonsument" darauf hindeutet, dass damit Personen gekennzeichnet werden können, die Betäubungsmittel (BtM) konsumieren, reicht dies für sich genommen für eine Vergabe dieses Hinweises nicht aus. Sowohl § 16 Abs. 6 Nr. 1 BKAG / § 21 Abs. 2 Nr. 1 SPolDVG als auch der PHW-Leitfaden verlangen weiter, dass aus dem Gebrauch der Substanzen erhebliche Gesundheitsgefahren für die betroffene Person selbst oder für Polizeibedienstete resultieren können. Dies wäre insbesondere zu vermuten, wenn für den Konsum erfahrungsgemäß gefährliche Utensilien mitgeführt werden (Fixerbesteck) oder in Folge der BtM-Aufnahme besonders aggressives Verhalten zu erwarten ist. In einem Großteil der kontrollierten

Einzelfälle konnte im Prüftermin ein solcher Konnex zwischen Konsum und Gefährdung aber gerade nicht hinreichend belegt werden.

Sowohl die Vergabe des EHW Reisender Täter als auch die des EHW BTM-Handel war im Rahmen der Prüfung kritisch zu bewerten. Dies bereits mit Blick auf die im EHW-Leitfaden festgelegten Vergabevoraussetzungen selbst, die nach Sicht unserer Behörde eine hohe Gefahr der Stigmatisierung bieten und teilweise sehr unbestimmt formuliert wurden. Aber auch die konkret durchgeführte Einzelfallkontrolle zeigte Defizite bei der Anwendung dieser Kriterien auf. So konnte nach unserer Auffassung in fast keinem der überprüften Sachverhalte das Vorliegen der letztlich geforderten Speichergründe ausreichend nachgewiesen oder eine einheitliche Vergabepraxis dargelegt werden.

Letztlich zeigte sich bei der Vor-Ort-Prüfung auch, dass die in den Leitfäden ausdrücklich geforderte Dokumentation der Einzelfallentscheidung bei der Hinweisvergabe nur sehr eingeschränkt existierte. Dies erschwerte es im Prüfverfahren zusätzlich, die seitens der Polizei vorgenommenen kriminalistischen Einschätzungen und Prognosen gebührend nachvollziehen zu können.

### 4.2.3 Mitteilung der Prüfergebnisse und Ausblick

Das Landespolizeipräsidium wurde in zeitlicher Nähe zum Redaktionsschluss dieses Tätigkeitsberichts über die Ergebnisse der vorbeschriebenen Kontrolle unterrichtet. Über eine zu erwartende Stellungnahme kann deswegen zum jetzigen Zeitpunkt noch nicht berichtet werden. In unserem umfangreichen Prüfbericht fordern wir jedoch eine Evaluation der derzeitigen Vergabe- und Dokumentationspraxis sowie zusätzliche Bemühungen, die Anforderungen der Leitfäden künftig streng einzuhalten.

Nicht nur aufgrund der vielen bislang noch nicht näher überprüften Hinweiskategorien, sondern auch wegen der zuneh-

menden Entwicklungsfortschritte hin zu einer neuen Informations- und Systemarchitektur der deutschen Polizeien im Rahmen des Projekts P20 (früher Polizei 20/20) gehen wir davon aus, dass wir künftig noch häufiger Kontrollen zur Vergabe von PHW und EHW durchführen werden.

## 4.3 Prüfung zu Datenübermittlungen an Europol

Mit der „Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit im Bereich der Strafverfolgung (Europol)" (im Folgenden: Europol-VO) wurde das bereits seit 1991 existierende und 2009 in neue rechtliche Fundamente gegossene europäische Polizeiamt (Europol) durch die seither existierende, europäische Agentur „Europol" abgelöst. Ihr kommt dabei die Aufgabe zu, „*die Tätigkeit der zuständigen Behörden der Mitgliedstaaten sowie deren Zusammenarbeit bei der Prävention und Bekämpfung von organisierter Kriminalität, Terrorismus und anderen Formen schwerer Kriminalität zu unterstützen und zu verstärken, wenn zwei oder mehr Mitgliedstaaten betroffen sind*".

Im Zuge dieser Kooperation werden regelmäßig Daten von den mitgliedstaatlichen Sicherheitsbehörden an Europol übermittelt. Den rechtlichen Rahmen für diese Verarbeitung relevanter Daten bilden die Vorgaben der Europol-VO und der nationalen Vorschriften im Europol-Gesetz (EuropolG). Um eine effektive Kontrolle der Einhaltung dieser Vorgaben europaweit zu gewährleisten, vereinbarten der Europäische Datenschutzbeauftragte (EDSB) und die mitgliedstaatlichen Datenschutzaufsichtsbehörden bereits im Jahr 2022, künftig regelmäßige Prüfungen in diesem Bereich durchzuführen. Als Ziel wurde eine jährliche Untersuchung solcher Datenübermittlungen angestrebt, bei denen personenbezogene Daten Minderjähriger betroffen sind. Im Zuge der erstmalig durchgeführten, koordinierten Prüfaktion im Jahr 2023 war auch unsere Behörde involviert, da bei einer Auswertung der Datenströme des den Kontakt zu Europol als Zentralstelle pflegenden Bundes-

kriminalamts (BKA) auch eine einzelne durch das Saarländische Landespolizeipräsidium initiierte Übermittlung von Daten eines Minderjährigen aus dem Jahr 2018 nachgewiesen wurde.

Hiesige Behörde nutzte das so einzuleitende Verfahren, um allgemeine Erkenntnisse zur Übermittlung von Daten an Europol zu erlangen und eine Einzelfallkontrolle hinsichtlich des Vorgangs aus 2018 durchzuführen.

### 4.3.1 Allgemeines zur Datenübermittlung

Datenübermittlungen an Europol finden vornehmlich über die in Erwägungsgrund 24 der Europol-VO erwähnte *Secure Information Exchange Network Application* oder kurz *SIENA* statt. Hierbei handelt es sich um ein spezielles Kommunikationstool, das dem schnellen, sicheren und anwenderfreundlichen Austausch operativer und strategischer kriminalitätsbezogener Erkenntnisse dienen soll. Das BKA tritt dabei als *National Contact Point / Europol National Unit / nationale Zugangsstelle* auf: Entweder fungiert das BKA selbst im Auftrag der nationalen Teilnehmerbehörden als Übermittler und Empfänger von Informationen beim Kontakt mit Europol oder aber es mittelt in technischer Hinsicht eine „direkte" Kommunikation der nationalen Teilnehmerbehörden mit der Zentraleinheit bei Europol („SIENA-Direktverkehr").

Die Rahmenbedingungen für den Informationsaustausch im Zuge des SIENA-Direktverkehrs werden für die deutschen Teilnehmerbehörden im sogenannten *„Rahmenkonzept SIENA-Roll-out in Deutschland"* festgehalten. Zudem hat Europol selbst (als Betreiber von SIENA) bestimmte Vorgaben für die Aufbewahrungsmodalitäten in der *„SIENA Data Retention Policy"* vorgeschrieben. Hierzu gehört beispielsweise eine Löschfrist von zwei Jahren, gemessen ab dem Zeitpunkt der letzten Aktivität oder des Vorgangsabschlusses. Nach Ablauf dieser Zeitspanne wird der jeweilige SIENA-Nachrichtenverlauf automatisiert gelöscht.

### 4.3.2 Erkenntnisse aus der Einzelfallkontrolle

Gerade diese automatisierte Löschfrist stellte sich jedoch im diesjährigen Prüfverfahren als erhebliches Hindernis für die Einzelfallkontrolle heraus. Da die fragliche Datenübermittlung an Europol aus dem Saarland bereits 2018 stattgefunden hatte, war der als Anhaltspunkt dienende SIENA-Nachrichtenverlauf bereits entsprechend den Vorgaben der *„SIENA Data Retention Policy"* gelöscht worden. Nur mithilfe des BKA, das aufgrund einer gewissen Zentralstellenrelevanz einzelne Informationen der Kommunikation in einen eigenen Vorgang übernommen hatte, konnten letztlich noch anhand eines vermerkten staatsanwaltschaftlichen Aktenzeichens bestimmte Grundinformationen zum betroffenen Sachverhalt ermittelt werden. Hierzu gehörte der Tatzeitpunkt, das konkret betroffene Delikt und das Geburtsdatum der betroffenen Person sowie der genaue Übermittlungszeitpunkt. Zudem existierten Anhaltspunkte dafür, welche Rolle der Minderjährige in dem Verfahren eingenommen hatte. Darüber hinausgehende Sachverhaltsinformationen waren nicht mehr rekonstruierbar.

Demnach betraf die Datenübermittlung einen zum Tatzeitpunkt 13-Jährigen, der als einer von insgesamt fünf Personen als etwaiger Beschuldigter im Rahmen einer Strafanzeige (Wohnungseinbruchsdiebstahl, § 244 Abs. 1 Nr. 3 des Strafgesetzbuchs – StGB) erfasst worden war. Im Zeitpunkt der Datenübermittlung an Europol hatte die betroffene Person bereits das 14. Lebensjahr erreicht. Der letztlich bei Europol angelegte Datensatz wies ihn als „suspect" („Verdächtiger") aus.

Anhand dieser relativ knappen Informationen konnten derweil einige für die Einzelfallkontrolle essentielle Feststellungen getroffen werden. Nach § 3 Abs. 1 S. 1 EuropolG ist eine Datenübermittlung an Europol dann zulässig, wenn die Informationen den Zwecken nach Art. 18 Abs. 2 lit. a bis lit. c Europol-VO (i.V.m. Art. 3 Abs. 1 Europol-VO und den Anhängen 1 und 2) dienen. Als Anknüpfungspunkt dient hier eine *Europol-relevante Straftat*, welche den Bereichen der *schweren Krimina-*

*lität*, des *Terrorismus* oder *sonstiger Kriminalitätsformen, die ein gemeinsames Interesse der Union verletzen,* zuzuordnen ist. Letztere werden durch eine umfangreiche Liste der in Betracht kommenden Delikte in Anhang 1 der Europol-VO näher konkretisiert. Zu diesen gehört insbesondere gem. Spiegelstrich 13 *„Raub und schwerer Diebstahl"*, sodass der im konkreten Fall angegebene Wohnungseinbruchdiebstahl (§ 244 Abs. 1 Nr. 3 StGB) als ausreichend anzusehen war.

Problematischer war dagegen die Bewertung der betroffenen Personengruppe. Denn die Datenverarbeitungsvorschriften der Europol-VO sehen hier grundsätzlich nur zwei mögliche Kategorien vor: *„Suspects"* (Verdächtige) und *„potential future criminals"* (Künftige potenzielle Straftäter). Gerade die Minderjährigkeit der betroffenen Person zum Zeitpunkt der Tatbegehung erwies sich deswegen als zentrale Frage. So war der bei Europol ermittelte Datensatz zwar als „suspect" gekennzeichnet; gleichwohl kam eine solche Stellung als Verdächtiger hier eigentlich nicht in Betracht, da eine strafbewehrte Täterschaft nach deutschem Recht erst nach Ende der Strafunmündigkeit, also mit Vollendung des 14. Lebensjahres, eintreten kann. Aufgrund der fehlenden Sachverhaltsinformationen und der unklaren technischen Ausgestaltung der Europol-Datenbank konnte nicht ausgeschlossen werden, dass die Übermittlung möglicherweise auch auf eine Stellung als „potential future criminal" gestützt worden war. Diese kommt theoretisch auch bei minderjährigen Personen in Betracht, soweit faktische Anhaltspunkte für eine künftige, verfolgbare Begehung von Straftaten sprechen. Diese Negativprognose muss dann aber erhöhtes Augenmerk auf die Begründung möglicher Entwicklungstendenzen legen. Dies gilt umso mehr bei sehr jungen Betroffenen, deren Werdegang bis zum Eintritt der Strafmündigkeit nur sehr schwer mit Sicherheit vorhergesagt werden kann.

### 4.3.3 Ergebnisse der Prüfung

Da somit im konkreten Prüfverfahren zwar hinreichende Anknüpfungstatsachen in Bezug auf das relevante Delikt vorla-

gen, eine sichere Einordnung als „suspect" oder als „potential future criminal" aber dagegen nicht möglich war, konnte auch keine abschließende Bewertung des polizeilichen Vorgehens erfolgen. Soweit die Person als Verdächtiger übermittelt wurde, wäre das Vorgehen als unzulässig zu bewerten gewesen. Eine Einstufung als künftiger potentieller Straftäter war dagegen wohl möglich – eine Kontrolle des Einzelfalls dahingehend, ob dies als Grundlage der Übermittlung in Betracht kam, konnte jedoch aufgrund fehlender Sachverhaltsinformationen nicht weiter durchgeführt werden.

Vor diesem Hintergrund regten wir beim LPP eine Evaluation der internen Abläufe in Bezug auf Europol-Übermittlungen an. Auf Basis der Feststellungen im Prüfverfahren sollte insbesondere die Arbeitspraxis im Hinblick auf die Einordnung zu den möglichen Personengruppen nach Europol-VO näher betrachtet werden. Da die Kontrolle der Übermittlung von Daten Minderjähriger an Europol nach den derzeitigen Bestrebungen des EDSB in regelmäßigen Zeitabständen wiederkehren soll, ist auch zu erwarten, dass unsere Behörde künftig Prüfungen zu diesem Themenbereich beim LPP durchführen wird. Es ist davon auszugehen, dass bei diesen Untersuchungen die betroffenen Datenbestände dann noch vorhanden und somit umfangreichere und detailliertere Bewertungen möglich sein werden.

## 4.4 Prüfungen zur Fingerabdruckdatenbank Eurodac

*„Eine gemeinsame Asylpolitik, einschließlich eines Gemeinsamen Europäischen Asylsystems [GEAS], ist wesentlicher Bestandteil des Ziels der Europäischen Union, schrittweise einen Raum der Freiheit, der Sicherheit und des Rechts aufzubauen, der allen offensteht, die wegen besonderer Umstände in der Union um internationalen Schutz nachsuchen."*[20]

[20] Jeweils Erwägungsgrund 2 der Verordnungen (EU) 603/2013 und (EU) 604/2013 vom 26. Juni 2013.

Die Verordnung (EU) 603/2013 (Eurodac-VO) verfolgt die effektive Anwendung des Dubliner Übereinkommens bzw. dessen Nachfolgeregelung (VO (EU) 604/2013 – Dublin-III-Verordnung) i.V.m. der einschlägigen Durchführungsverordnung (VO (EU) 118/2014), indem sie den dafür notwendigen Informationsaustausch durch Schaffung einer europäischen Fingerabdruckdatenbank ermöglicht. Zweck des Dublin-Verfahrens ist es, dass jeder Asylantrag im Hoheitsgebiet der europäischen Mitgliedstaaten stets nur einmal geprüft wird und somit auch eine „Sekundärwanderung" innerhalb Europas gesteuert bzw. begrenzt wird.[21]

In Deutschland ist die Arbeit mit der Eurodac-Datenbank in den Prozess der Erstregistrierung von Drittstaatsangehörigen fest implementiert und betrifft somit sowohl Mitarbeitende von Bundes- oder Länderpolizei als auch solche des Bundesamtes für Migration und Flüchtlinge (BAMF) oder der Länder in Aufnahmeeinrichtungen, Ausländerbehörden und Ankunfts- oder AnkER-Zentren. Zudem ist es seit der Reform des Eurodac-Systems im Jahr 2013 möglich, die ursprünglich zum Zwecke des Asylverfahrens in Eurodac gespeicherten Daten unter bestimmten Bedingungen auch für einen Datenabgleich zu Zwecken der Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten heranzuziehen – die Fingerabdruckdatenbank wurde so für die Gefahrenabwehr- und Strafverfolgungsbehörden geöffnet (vgl. Erwägungsgrund 8 Eurodac-VO).

Zur Gewährleistung der Einhaltung datenschutzrechtlicher Vorgaben sieht die Eurodac-VO eine turnusmäßige (jährlich) durchzuführende Prüfung der Verarbeitung personenbezogener Daten im Rahmen des europäischen Fingerabdrucksystems zu Zwecken der Gefahrenabwehr und Strafverfolgung vor (Artt. 30 Abs. 1, 32 Abs. 2, 33 Abs. 2 Eurodac-VO). Sonstige

[21] Bundesamt für Migration und Flüchtlinge (BAMF), https://www.bamf.de/DE/Themen/AsylFluechtlingsschutz/AblaufAsylverfahrens/DublinVerfahren/Streptococcus mitits dublinverfahren-node.html (letzter Abruf: 15.12.2023).

Kontrollen sollen regelmäßig, aber ohne festen Prüfturnus, erfolgen. Die Kontrollen in diesem Bereich finden somit grundsätzlich anlassunabhängig statt. Saarländische Stellen, die mit dem Eurodac-System arbeiten, fallen hierbei in den Zuständigkeitsbereich unserer Behörde.

### 4.4.1 Kontrolle bei der Landesaufnahmestelle

Im Jahr 2022 wurde mit einer Kontrolle der Datenverarbeitungsvorgänge im Zusammenhang mit Eurodac bei der Zentralen Ausländerbehörde (ZAB) des Saarländischen Landesverwaltungsamts (LaVA) begonnen, welche ihren Abschluss im Jahr 2023 fand. Eurodac-relevante Handlungen fanden im Zeitraum des Prüfverfahrens nur im Rahmen der Erstregistrierung von Asylsuchenden (durchgeführt bei der Landesaufnahmestelle (LASt) in Lebach) statt. Bei einem Prüfbesuch vor Ort wurde die Arbeit an eigens zu diesem Zweck besonders eingerichteten Computerarbeitsplätzen (sog. Personalisierungs- und Infrastrukturkomponenten, „PIK-Stationen") präsentiert und Einsicht in mehrere Akten gewährt.

Während der Kontrolle fiel auf, dass Eurodac für die Arbeit der Ausländerbehörde auf Landesebene nur eine eher untergeordnete Rolle spielt. So nimmt die LASt zwar den Ankömmlingen bei der Erstregistratur die Fingerabdrücke ab und leitet diese über die PIK-Station an die zentrale europäische Fingerabdruckdatenbank weiter. Allerdings findet dieser Zulieferprozess rein automatisiert durch die von der Bundesdruckerei bereitgestellte Infrastruktur statt. Zudem werden die Fingerabdruckdaten zwar an Eurodac zum Zwecke eines Abgleichs mit den dort hinterlegten Informationen übersandt (Feststellung, ob ein Asylantrag zuvor bereits in einem anderen europäischen Staat gestellt wurde); das Ergebnis dieses Abgleichs erhält jedoch nicht die LASt, sondern das für die Durchführung des Asylverfahrens zuständige BAMF.

Einfluss hat die LASt somit nur auf die rechtliche und technische Schulung der dort tätigen Mitarbeiter mit Blick auf deren

Arbeit an den PIK-Stationen. Gerade diese weist aber wohl keinen großen Schwierigkeitsgrad auf, da das installierte Fachverfahren Schritt für Schritt durch den Vorgang leitet und insbesondere Qualitätsdefizite bei der Abnahme der Fingerabdrücke automatisch signalisiert. Auf weiteres Schulungs- und Informationsmaterial der Agentur der europäischen Union für Grundrechte (FRA) wurde durch unsere Behörde hingewiesen.[22] Auch kommen der LASt teilweise Informations- und Belehrungspflichten zu, welchen bereits in erheblichem Umfang nachgekommen wird. Verbesserungspotential wurde dennoch erkannt und im Rahmen des erstellten Prüfberichts aufgezeigt. Hierzu gehört insbesondere die Auslage einer Informationsbroschüre der für den Betrieb von Eurodac zuständigen Agentur.[23]

Weitere für die LASt relevante rechtliche Fragestellungen bezogen sich vor allem auf die zeitlichen Vorgaben für die Anlieferung von Fingerabdruckdaten an Eurodac und die Handhabung bei der Abnahme von Fingerabdrücken bei Minderjährigen / Kindern.

So verlangt Art. 9 Abs. 1 UA 2 der Eurodac-VO, dass erhobene Fingerabdruckdaten innerhalb von 72 Stunden nach Stellung des Asylantrags an das Zentralsystem übermittelt werden. Die LASt konnte im Prüfverfahren glaubhaft darlegen, dass durch den konkreten organisatorischen Ablauf, bei dem die Registratur an den PIK-Stationen an vorderster Stelle steht, im Saarland grundsätzlich keine Überschreitung dieser zeitlichen Vorgaben eintreten wird.

Darüber hinaus war beachtlich, dass Art. 9 Abs. 1 UA 1 Eurodac-VO eine Anlieferung von Fingerabdruckdaten aller zu registrierender Personen *ab 14 Jahren* vorschreibt, die korres-

[22] Abrufbar über die Website des EDSB unter: https://edps.europa.eu/system/files/2021-12/eurodac_right_to_information_guide_de.pdf (letzter Abruf: 15.12.2023).
[23] Abrufbar über die Website der Agentur eu-LISA unter: https://www.eulisa.europa.eu/Publications/Information%20Material/Leaflet%20Eurodac.pdf (letzter Abruf: 15.12.2023).

pondierende Vorschrift in § 16 Abs. 1 Satz 1 u. 2 des deutschen Asylgesetzes (AsylG) aber dagegen eine *Altersgrenze von sechs Jahren* vorsieht. Diese Divergenz ist auf einen „Vorgriff" des nationalen Gesetzgebers zurückzuführen, denn während bis zum 01.04.2021 auch in Deutschland eine Altersgrenze von 14 Jahren für die in diesem Kontext erfolgende Abnahme von Fingerabdrücken bestand, wurde die Altersgrenze durch das 2. Datenaustauschverbesserungsgesetz in Erwartung einer baldigen Reform der Eurodac-VO auf das vollendete sechste Lebensjahr herabgesetzt.[24] Die avisierten Änderungen auf europäischer Ebene sind jedoch bislang nicht erfolgt; das Gesetzgebungsverfahren ist noch nicht abgeschlossen.[25] Da damit jedoch an den PIK-Stationen alle Minderjährigen ab sechs Jahren unterschiedslos erkennungsdienstlich behandelt werden, interessierte sich unsere Behörde dafür, wie die unterschiedlichen Vorgaben aus AsylG und Eurodac-VO letztlich beachtet werden. Zwar stellte sich die Ermittlung der konkreten Infrastruktur bei der Übermittlung an Eurodac wegen mehrerer im Hintergrund beteiligter Akteure als eher schwierig heraus; dennoch konnten wir letztlich feststellen, dass systemtechnisch sichergestellt wird, dass nur Daten von über 14-jährigen Personen an Eurodac weitergeleitet werden.

Insgesamt war die Prüfung bei der LASt somit sehr zufriedenstellend und offenbarte keine besonderen datenschutzrechtlichen Bedenken.

### 4.4.2 Kontrolle beim Landespolizeipräsidium

Im Gegensatz zu der im vorstehenden Abschnitt beschriebenen Kontrolle bei der LASt bezog sich die Prüfung beim LPP im

[24] Bis zum Jahr 2016 war in diesem Kontext sogar jegliche erkennungsdienstliche Maßnahme gegenüber Minderjährigen unzulässig; erst mit dem Inkrafttreten des Datenaustauschverbesserungsgesetzes vom 02.02.2016 (BGBl. I 2016, 130) wurde dies in Deutschland ermöglicht. Siehe hierzu Houben, in: BeckOK Ausländerrecht, Kluth/Heusch [37. Edition, Stand: 01.01.2023], § 16 AsylG, Rn. 9b.1.

[25] Siehe: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM:2016:272:FIN (letzter Abruf: 15.12.2023).

Jahr 2023 vornehmlich auf die Zulässigkeit von Zugriffen auf die in Eurodac gespeicherten Fingerabdruckdaten.

Für die Polizei bilden Fingerabdrücke aufgrund ihrer grundsätzlich unveränderlichen Papillarstrukturen und Minutien einen zuverlässigen Ansatz für die Identifikation von menschlichen Individuen,[26] und gehören deswegen seit geraumer Zeit zu den wichtigsten Sachbeweisen und Anknüpfungstatsachen in Bezug auf Straf- und Gefahrenabwehrverfahren. Als Standardmaßnahme in der polizeilichen Aufgabenwahrnehmung dient die erkennungsdienstliche Behandlung in Form der Abnahme von Fingerabdrücken deswegen der Sicherstellung von Informationen, die die Aufklärung von relevanten Zusammenhängen fördern soll.

Fingerabdruckdaten werden hierbei entweder als Personenrecherche (= es liegt ein vollständiger Fingerabdruckdatensatz einer unbekannten Person aus bspw. einer erkennungsdienstlichen Behandlung vor) oder als Spurenrecherche (= es wurden bspw. bei der forensischen Untersuchung eines Tatorts Fingerabdruckspuren sichergestellt) durchgeführt. Die neu erlangten Daten werden hierbei mit bereits vorhandenen Informationen abgeglichen. Hierzu dient vornehmlich das automatisierte Fingerabdruckidentifizierungssystem der deutschen Polizei (AFIS+).

Werden die Polizeibeamten hierin nicht fündig, stehen jedoch noch weitere Datenbanken für einen Abgleich zur Verfügung, zu denen auch Eurodac gehört. Die Eurodac-VO lässt einen solchen Zugriff jedoch nur unter relativ strengen Voraussetzungen zu.

So schreibt Art. 19 Eurodac-VO unter anderem vor, dass Zugriffe nur durch besonders benannte Behörden erfolgen dür-

[26] Salzer, Einzigartiger Nachweis, Magazin Öffentliche Sicherheit (Bundesministerium für Inneres Österreich), Jahrgang 2019, Heft 7/8, S. 42 ff.; Wagner, Der Daktyloskop am Tatort, in: Das Kriminalpolizeiliche Ermittlungsverfahren (Sicherung des objektiven und subjektiven Tatbefundes), Hrsg.: Bundeskriminalamt, Wiesbaden 1957, S. 81.

fen, deren Anträge von einer eigens hierfür eingerichteten Prüfstelle zu überprüfen und zu bearbeiten sind. Erst dann erfolgt ein Zugriff auf die Eurodac-Datenbank über eine einzelne nationale Zugangsstelle (eingerichtet beim Bundeskriminalamt).

Daneben sieht Art. 20 Eurodac-VO mehrere materielle Voraussetzungen vor. Hierzu gehören insbesondere und vor allem zwingend durchzuführende Vorrecherchen in anderen Datenbanken. Darüber hinaus darf nicht aus jeglichem Anlass ein Abgleich initiiert werden – die benannten Behörden dürfen nur zum Zwecke der Gefahrenabwehr oder Strafverfolgung tätig werden, um terroristische oder sonstige schwere Straftaten zu verhüten, aufzudecken oder zu untersuchen.

In dem von uns durchgeführten Prüfverfahren befassten wir uns näher mit diesen Anforderungen – sowohl mit Blick auf das allgemeine Vorgehen beim LPP als auch im Rahmen einer Einzelfallkontrolle. So stellten wir zunächst fest, dass eine aktuelle Liste der zugriffsberechtigten benannten Behörden sowie der Prüf- und operativen Dienststellen, wie sie in Art. 43 Abs. 1, Abs. 3 Eurodac-VO gefordert wird, wohl nicht existiert. Dies bemängelten wir und forderten eine Aktualisierung. Gegen die tatsächlich vorhandenen Organisationsstrukturen beim LPP (eingerichtete Prüfstelle und antragsbefugte operative Dienststellen) bestanden allerdings grundsätzlich keine datenschutzrechtlichen Bedenken. Lediglich den durch die Prüfstelle wahrgenommenen Prüfumfang sahen wir als zu gering an. Unsere Behörde geht davon aus, dass die in Art. 19 Abs. 1 S. 2 Eurodac-VO angelegte Prüftätigkeit keine reine Plausibilitätsprüfung umfasst, sondern eine detailliertere Kontrolle der Voraussetzungen für einen Abgleich intendiert. Wir baten das LPP deswegen die Beteiligung der Prüfstelle neu zu evaluieren. Um dieser eine umfassende Kontrolle zu ermöglichen, schlugen wir zudem Anpassungen an den derzeit in Verwendung befindlichen Antragsformularen für Eurodac-Recherchen vor.

Die zu berücksichtigenden Voraussetzungen für einen Abgleich nach Art. 20 Eurodac-VO spiegelten sich dabei grundsätzlich in dem vorgehaltenen Antragsformular wider. Unsere Behörde äußerte lediglich Zweifel mit Blick auf die Durchführung der verpflichtenden Vorrecherchen. So verlangt die Eurodac-VO ihrem Wortlaut nach vor einer Eurodac-Recherche nicht nur eine Suche nach passenden Treffern im nationalen AFIS+, sondern auch in den automatisierten Fingerabdruckidentifizierungssystemen der anderen europäischen PRÜM-Staaten[27] und im Visa-Informationssystem[28]. Aufgrund der eigentlich strengen Zweckbindung der Eurodac-Daten (für die Durchführung des Asylverfahrens) müssten diese Vorrecherchen eigentlich *vollumfänglich* durchzuführen sein – beim derzeitigen Vorgehen des LPP existieren jedoch gewisse Erleichterungen, die vor diesem Hintergrund kritisch erscheinen. Es ist davon auszugehen, dass wir zur Klärung dieser Frage noch weiter mit dem LPP in Austausch treten werden.

Letztlich stellte sich die durchgeführte Einzelfallkontrolle als sehr übersichtlich heraus. So war in den vergangenen fünf bis sechs Jahren (2018 bis Anfang 2023) in lediglich einem einzigen Ermittlungsverfahren auf Eurodac-Daten zugegriffen worden. Sowohl die formellen als auch die materiellen Voraussetzungen (mit Ausnahme der vorstehend kritisch bezeichneten Vorrecherchen) waren hier aber gegeben, sodass wir den Abgleich in diesem Einzelfall nicht weiter beanstandeten.

---

[27] Aden, in: Lisken/Denninger, Handbuch des Polizeirechts (7. Auflage 2021), Kapitel M, Rn. 56 ff.: Die Prüm-Kooperation basiert auf einem 2005 unterzeichneten multilateralen Vertrag („Prümer Vertrag"; Ratifizierung Deutschland 2006), der der „Vertiefung grenzüberschreitender Zusammenarbeit, insbesondere bei der Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration" dienen soll. Mit Ratsbeschluss von 2008 wurde das Abkommen in den europäischen Rechtsrahmen überführt (2008/615/JI). Die Zusammenarbeit findet insb. bzgl. daktyloskopischer Daten statt.

[28] Das Visa-Informationssystem (VIS) dient dem Austausch von Visa-Daten zwischen den Schengenstaaten, um die gemeinsame Visumspolitik der europäischen Union zu gewährleisten.

## 4.5 Gerichtsentscheidungen aus dem Bereich der öffentlichen Sicherheit

Im Berichtszeitraum ergingen zwei Entscheidungen des Bundesverfassungsgerichts (BVerfG) zu Rechtsnormen die Datenverarbeitung der Polizei betreffend, die auch für das Saarland von nicht zu unterschätzender Bedeutung sind.

### 4.5.1 Polizeiliche Eingriffsbefugnisse nach dem SOG MV

Hierbei handelt es sich zunächst um die Entscheidung des BVerfG in der Rechtssache 1 BvR 1345/21.[29] Thematisch befasste sich das Gericht hierin mit der Verfassungsmäßigkeit mehrerer Normen aus dem Sicherheits- und Ordnungsgesetz des Landes Mecklenburg-Vorpommern (SOG MV), die den Einsatz bestimmter, besonderer Mittel der Datenerhebung betrafen.

Das BVerfG äußerte sich in diesem Zusammenhang nicht nur zu den verfassungsrechtlich allgemein zu fordernden Eingriffsschwellen für solche Maßnahmen, die nicht zu weit in das Vorfeld einer konkretisierten Gefahr verlagert werden dürfen. Das Gericht ging auch vertieft auf die spezifischen Regelungen zum Einsatz verdeckter Ermittler und Vertrauenspersonen, zur Online-Durchsuchung, zur Telekommunikationsüberwachung (TKÜ), zur Ausschreibung zwecks polizeilicher Beobachtung und zur Rasterfahndung ein.

Zudem wurde darauf hingewiesen, dass das Gebot der Normenklarheit nicht zwangsläufig der Verwendung von Verweisungsketten entgegensteht (z.B. Verweis von Gesetz 1 auf Gesetz 2, welches auf Gesetz 3 rekurriert) – allerdings können unübersichtliche oder kontextvernichtende „Verweisungskaskaden" durchaus problematisch sein.

Im Saarländischen Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG) existieren teilweise

[29] BVerfG, Urt. v. 09.12.2022 – 1 BvR 1345/21, ZD 2023, 346.

Regelungen, die den Normen des SOG MV ähneln. Vor diesem Hintergrund sind die gesetzlichen Festlegungen in den §§ 29, 31, 34, 35, 40 und 41 SPolDVG entsprechend zu evaluieren. Insbesondere finden sich auch hier Verweisungen auf größere Paragrafenlisten (z.B. in § 100b der Strafprozessordnung – StPO), die mit Blick auf Verweisungskaskaden und Vorfeldstraftaten näher untersucht werden sollten.

Bislang wurde unsere Behörde seitens des Saarländischen Ministeriums für Inneres, Bauen und Sport (MIBS) zu etwaigen, aus dem BVerfG-Urteil resultierenden Fragen noch nicht beteiligt. Die Landesregierung berichtete jedoch bereits im Innenausschuss des Landtages und wies auf einen gewissen Änderungsbedarf (insbesondere zu den Regelungen der Vertrauenspersonen und verdeckten Ermittler) hin. Auch wir sehen in einigen Konstellationen teilweise Anpassungsspielraum. Gerne stehen wir deswegen bei Bedarf auch schon vor einer formellen Befassung im parlamentarischen Verfahren beratend zur Verfügung.

### 4.5.2 Ermächtigungen der Polizei zur automatisierten Datenanalyse

Bei der zweiten überaus relevanten Entscheidung handelt es sich um das Urteil des BVerfG in der Rechtssache 1 BvR 1547/19, 1 BvR 2634/20.[30] Mit Verfassungsbeschwerden wurden hier die landesrechtlichen Ermächtigungen der Polizei zur automatisierten Datenanalyse und -auswertung in Hessen und in Hamburg angegriffen.

In Hessen betrifft dies die Verwendung des Programms „Gotham" des Software-Unternehmens Palantir (bekannt unter dem Namen „hessenDATA"). In Hamburg befand sich bislang keine solche Software im Einsatz – die Verfassungsbeschwerde betraf hier Normen, die in Vorbereitung eines solchen Einsat-

[30] BVerfG, Urt. v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196.

zes seitens der Hamburgischen Bürgerschaft geschaffen worden waren.

Auch in Nordrhein-Westfalen wird bereits seit einiger Zeit die Software Gotham der Firma Palantir genutzt. Gegen die diesbezügliche Rechtsgrundlage in § 23 des Polizeigesetzes des Landes Nordrhein-Westfalen (PolG NRW) erhob die Gesellschaft für Freiheitsrechte (GFF) bereits im Jahr 2022 Verfassungsbeschwerde vor dem BVerfG[31]. Zudem hat Bayern im Jahr 2023 mit dem besagten Unternehmen Palantir einen Rahmenvertrag für den Einsatz der Auswertungs- und Analysesoftware VERA abgeschlossen – diesem Rahmenvertrag könnten sich andere Bundesländer unproblematisch anschließen.

Das BVerfG erklärte derweil in der zitierten Entscheidung die angegriffenen Rechtsgrundlagen in Hessen für mit der Verfassung unvereinbar bzw. in Hamburg für verfassungswidrig und nichtig. Das Urteil basiert hierbei auf der Feststellung des Gerichts, dass auch der automatisierten Datenanalyse und -auswertung von *bestehenden* Datenbeständen ein erhebliches Eigengewicht zugestanden werden muss. Eine Rechtsgrundlage, die einen solchen Eingriff gestattet, hat deswegen weitergehende Rechtfertigungsanforderungen zu erfüllen. Welche Voraussetzungen genau zu beachten sind, ist unter Beachtung der Grundsätze der Zweckbindung und Zweckänderung vor allem daran zu beurteilen, welche Auswertungsmethode gestattet werden soll und welche Art sowie welcher Umfang an Daten betroffen sein wird. Je schwerwiegender die Maßnahmen in das Recht auf informationelle Selbstbestimmung eingreifen, desto strenger müssen die in den jeweiligen Ermächtigungsgrundlagen niedergelegten Eingriffsschwellen definiert werden. Diesen Anforderungen genügten die Regelungen in Hessen und Hamburg nach Ansicht des BVerfG nicht.

[31] Siehe hierzu den veröffentlichten Schriftsatz der GFF: https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Polizeigesetz-NRW/2022-10-05-PolG_NRW_Palantir_Website_geschwaerzt_Punkte.pdf.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) hat sich im Jahr 2023 anlässlich dieses Urteils in Form einer Entschließung zu den verfassungsrechtlichen Anforderungen bei automatisierten Datenanalysen durch Polizei und Nachrichtendienste geäußert.[32] Sie appellierte an die politisch Verantwortlichen, sollte der Einsatz komplexer Datenanalysemethoden für erforderlich gehalten werden, klare Rechtsgrundlagen unter Beachtung geeigneter Rahmenbedingungen im Sinne der beschriebenen Verfassungsrechtsprechung zu schaffen.

Bislang hat uns weder das Saarländische Landespolizeipräsidium noch das MIBS signalisiert, in den Rahmenvertrag für VERA eintreten oder eine sonstige übergreifende Auswertungs- und Analysesoftware beziehen zu wollen. Auf bundespolitischer Ebene wurden zwischenzeitlich Forderungen geäußert, den entsprechenden Einsatz solcher „Data Mining"-Lösungen weiter zu verfolgen.[33] Aus Sicht des UDZ ist bei solchen Bestrebungen aus den vorgenannten Gründen äußerste Vorsicht walten zu lassen.

## 4.6 Datenübermittlung durch die Jagdbehörde

Wer in Deutschland der Jagd nachgehen möchte, der ist vor deren Ausübung – egal ob als Hobby oder als Beruf – mit diversen Zugangsvoraussetzungen konfrontiert. Nicht nur hat der ambitionierte Waidmann eine umfangreiche und anspruchsvolle Jagdprüfung abzulegen. Daneben muss er auch einen befristeten Jagdschein erwerben und in Bezug auf die unweigerlich benötigte Jagdwaffe samt Munition diverse waf-

[32] Abrufbar über den Webauftritt der DSK: https://www.datenschutzkonferenz-online.de/media/en/2023-05-11_DSK-Entschliessung_Datenanalyse-Polizei.pdf.
[33] Antrag der Fraktion der CDU/CSU, Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren, BT-Drs. 20/9495; Plenarprotokoll, Deutscher Bundestag – 20. Wahlperiode – 142. Sitzung, Berlin, Freitag, den 1. Dezember 2023 (Plenarprotokoll 20/142), S. 18052 ff.

fenrechtliche Erlaubnisse – wenn auch unter teilweise erleichterten Bedingungen („Jägerprivileg") – einholen.

Im Fokus der die jeweiligen Genehmigungen ausstellenden Behörden stehen hier insbesondere zwei konkrete Fragen: *„Besitzt der Antragsteller die erforderliche Zuverlässigkeit?"* und *„Ist der Antragsteller persönlich geeignet?"*. Während die Bewertung der „Zuverlässigkeit" nach § 5 des Waffengesetzes (WaffG) an verantwortbares und vorwerfbares Verhalten einer Person in der Vergangenheit anknüpft (z.B. rechtskräftige Verurteilungen), erfasst die „persönliche Eignung" nach § 6 WaffG solche Mängel, die in der Person des Antragstellers liegen und auf die diese selbst nur begrenzt oder gar keinen Einfluss nehmen kann (z.B. Geschäftsunfähigkeit oder Drogenabhängigkeit).[34] Werden die vorgenannten Fragen verneint, so sind die Erlaubnisse zu versagen oder – falls sie bereits ausgesprochen wurden – im Nachhinein zu widerrufen.

Zur umfassenden Bewertung dieser Aspekte benötigen die beteiligten Behörden umfangreiche Informationen, wobei insbesondere bei deren Erhebung, Nutzung und ggf. Übermittlung der datenschutzrechtliche Rahmen nicht außer Acht gelassen werden darf.

### 4.6.1 Datenschutzrechtliche Beschwerde

In diesem Zusammenhang wandte sich im Berichtszeitraum ein Beschwerdeführer an das Unabhängige Datenschutzzentrum und bat um Überprüfung der Datenverarbeitung durch die Jagd- und Waffenbehörde einer saarländischen Gebietskörperschaft. Diese hatte einen Antrag des langjährigen Jägers auf Verlängerung seines Jagdscheines abgelehnt und dies mit einem Wegfall der erforderlichen Zuverlässigkeit begründet. Der Beschwerdeführer bezweifelte hier nicht nur, dass die für diese Entscheidung herangezogenen Informationen daten-

[34] Gade, in: Gade, Waffengesetz [3. Auflage 2022], § 5 WaffG, Rn. 1 mit Verweis auf BT-Drs. 14/7758, S. 54.

schutzrechtlich korrekt erhoben und aufbewahrt wurden, sondern ging auch davon aus, dass die Behörde seine jagd- und waffenbehördliche Akte in unzulässiger Weise außenstehenden Dritten offengelegt bzw. an diese übersandt hatte.

Im Rahmen des Beschwerdeverfahrens baten wir die Gebietskörperschaft um Stellungnahme und führten einen Vor-Ort-Termin zur Einsicht in die relevanten Akten des Beschwerdeführers durch. Die geäußerten datenschutzrechtlichen Bedenken konnten im Zuge dessen jedoch nicht bestätigt werden.

### 4.6.2 Erhebung und Aufbewahrung verfahrensrelevanter Daten

Zunächst war die Ermittlung der entscheidungsrelevanten Informationen durch die Waffen- und Jagdbehörde im konkreten Fall als datenschutzkonform zu bewerten.

So zeigte unsere Untersuchung auf, dass der Beschwerdeführer bereits im Jahr 2020 einen Antrag auf Verlängerung seines Jagdscheins gestellt hatte. Die Waffen- und Jagdbehörde zog daraufhin zur Bewertung seiner Zuverlässigkeit Informationen aus dem Bundeszentralregister (BZR) und dem Zentralen Staatsanwaltschaftlichen Verfahrensregister (ZStV) heran. Die so erlangten Daten zeigten auf, dass gegen den Antragsteller in den Jahren zuvor mehrere Strafverfahren wegen Beleidigungs- und Körperverletzungsdelikten eingeleitet worden waren. Die in den Strafanzeigen vorgebrachten Anschuldigungen konnten dem Beschuldigten zwar von der Staatsanwaltschaft letztlich nicht nachgewiesen werden, sodass die Strafverfahren einzustellen waren. Dennoch wurde von der Waffen- und Jagdbehörde aufgrund der Vorfälle und der ermittelten Sachverhalte auf eine gewisse „aggressive Grundhaltung" des Betroffenen geschlossen, was dessen Zuverlässigkeit in gewissem Umfang in Zweifel zog. Indessen reichten die Anhaltspunkte aus Sicht der zuständigen Stelle für eine Versagung der beantragten Erlaubnis im Jahr 2020 noch nicht aus. Die Verlängerung des Jagdscheins wurde deswegen nochmals genehmigt, wobei der Antragsteller aber explizit darauf hinge-

wiesen wurde, dass künftige Auffälligkeiten eine Versagung des Jagdscheins zur Folge haben würden. Hierzu kam es dann letztendlich im Jahr 2022, als der Beschwerdeführer erneut eine Verlängerung seines Jagdscheins beantragte und diese aufgrund zwischenzeitlich erlangter, neuer Erkenntnisse negativ beschieden wurde.

Zur Ermittlung der Zuverlässigkeit des Antragstellers stehen der Waffen- und Jagdbehörde diverse Erkenntnisquellen zur Verfügung. Hierzu gehören insbesondere auch die besagten zentralen Register: BZR und ZStV. Wie sich aus § 5 Abs. 5 S. 1 Nr. 1 und Nr. 2 WaffG ergibt, sind diese Datensammlungen durch die Behörde im Rahmen der Bewertung sogar verpflichtend heranzuziehen. Entsprechende Übermittlungsregelungen existieren in der Verordnung über den Betrieb des Zentralen Staatsanwaltschaftlichen Verfahrensregisters (ZStVBetrV) und im Gesetz über das Zentralregister und das Erziehungsregister (BZRG). Als Datenverarbeitungen, die im Rahmen der Wahrnehmung öffentlicher Aufgaben stattfanden und hierfür auch erforderlich waren, waren die beschwerdegegenständlichen Abfragen somit über Art. 6 Abs. 1 lit. e, Abs. 3 DSGVO gerechtfertigt.

Auch das vorübergehende Vorhalten und Nutzen der im Jahr 2020 erlangten Erkenntnisse stieß im Zuge unserer Befassung auf keine datenschutzrechtlichen Bedenken. Die darin gesehenen Anhaltspunkte für eine etwaige künftige Relevanz der Daten im Zusammenhang mit einer möglichen Versagung waffen- und jagdrechtlicher Erlaubnisse rechtfertigten eine entsprechende Aufbewahrung, insbesondere mit Blick auf die in § 44a Satz 2 WaffG genannten Speicherfristen, wonach die zuständige Behörde alle Unterlagen, aus denen sich die Versagung einer waffenrechtlichen Erlaubnis ergibt, zehn Jahre aufzubewahren hat.

### 4.6.3 Datenübermittlung an Dritte

Daneben konnte im Rahmen der durchgeführten Akteneinsicht eine Übermittlung von Informationen an Dritte, namentlich an die *„Vereinigung der Jäger des Saarlandes"* (VJS) bestätigt werden. Auch diese Datenverarbeitung war im konkreten Fall aber nicht zu beanstanden.

Bei der VJS handelt es sich um eine Körperschaft des öffentlichen Rechts, der insbesondere Aufgaben der Jägerausbildung und -prüfung obliegt. Gleichzeitig besteht eine Beteiligungspflicht der VJS in solchen Fällen, in denen die Versagung oder Einziehung eines Jagdscheins in Rede steht – die Vereinigung ist hier vorab zu hören (§ 48 Abs. 5 S. 1 Saarländisches Jagdgesetz – SJG).

Im Beschwerdefall hatte die Waffen- und Jagdbehörde der VJS ein Anhörungsschreiben übersandt, in dem unter anderem der Anlass (Anhörung aufgrund intendierter Versagung eines Jagdscheins) und die Gründe für die geplante Entscheidung unter Auseinandersetzung mit den rechtlichen Bewertungsmaßstäben dargelegt wurden. Eine Übersendung der gesamten Akten fand nicht statt. Da es im Rahmen einer solchen Anhörung für eine umfangreiche Bewertung des Sachverhalts – sowohl für als auch wider die betroffene Person – notwendig erscheint, die Gründe der intendierten Entscheidung in ausreichendem Umfang mitzuteilen, sahen wir die Übermittlung diesbezüglicher, personenbezogener Daten im Beschwerdefall als unbedenklich an.

Die Verarbeitung der Waffen- und Jagdbehörde war hier als für die öffentliche Aufgabenwahrnehmung erforderlich anzusehen und konnte sich somit auf § 4 Abs. 2 des Saarländischen Datenschutzgesetzes (SDSG) stützen.

### 4.6.4 Aufbewahrungsmodalitäten in waffen- und jagdbehördlichen Akten

Für den Kern des konkreten Beschwerdeverfahrens waren allgemeine Aufbewahrungsmodalitäten zwar nicht relevant. Den-

noch fiel im Rahmen der Prüfung letztlich auf, dass konkrete gesetzliche Vorgaben für die allgemeine Speicherdauer von Informationen in waffenrechtlichen Akten nicht existieren. Das WaffG sieht nur für zwei Sonderfälle konkrete Speicherdauern vor: in § 44a Satz 1 eine 30-jährige Speicherdauer für solche Informationen, die für die Feststellung der gegenwärtigen und früheren Besitzverhältnisse sowie für die Rückverfolgung von Verkaufswegen in Bezug auf Waffen relevant sind, und in § 44a Satz 2 eine 10-jährige Aufbewahrungszeit in Bezug auf solche Daten, aus denen sich die Gründe für eine Versagung waffenrechtlicher Erlaubnisse in Bezug auf Zuverlässigkeit und persönliche Eignung ergeben.

Da sich die Aufbewahrungsfristen für alle sonstigen waffenrechtlichen Informationen aus Sicht unserer Behörde damit nach den allgemeinen Regelungen des SDSG und somit nach dem zu konkretisierenden Erforderlichkeitsprinzip richten, werden wir diesbezüglich mit dem Ministerium für Inneres, Bauen und Sport in Kontakt treten und auf eine möglichst einheitliche Behandlung bei allen Waffenbehörden im Saarland hinwirken.

5.1 Entwurf eines Saarländischen Kinderschutzgesetzes

# V.

# Rechtsetzungsverfahren

# 5 Rechtsetzungsverfahren

## 5.1 Entwurf eines Saarländischen Kinderschutzgesetzes

Im Berichtszeitraum hat die saarländische Landesregierung einen Entwurf für ein Kinderschutzgesetz (SKG) auf den Weg gebracht. Ziel des Gesetzesvorhabens war es, den Kinderschutz als gesamtgesellschaftliche Aufgabe weiter voranzutreiben, indem Schutzlücken geschlossen und die zuständigen Stellen, insbesondere die Jugendämter, bei ihrer Arbeit unterstützt werden.

Kerninhalte des Gesetzentwurfs waren dabei Vorschriften zur Stärkung der Rechte von Kindern und Jugendlichen, die Einrichtung des Amtes eines saarländischen Kinderschutzbeauftragten und die bessere Vernetzung der am Kinderschutz beteiligten Akteure.

Durch das federführende Ministerium für Arbeit, Soziales, Frauen und Gesundheit (MASFG) wurden wir frühzeitig gem. § 19 Abs. 2 SDSG in das Vorhaben eingebunden und um Beratung aus datenschutzrechtlicher Sicht gebeten.

### Einrichtung des Amtes eines Kinderschutzbeauftragten

Im Fokus des Austauschs mit dem Ministerium stand zunächst die Rolle des Kinderschutzbeauftragten.

Der Gesetzentwurf sah vor, dass dieses Amt vom MASFG mit einer geeigneten Person, die ihre Tätigkeit unabhängig und weisungsfrei ausübt, besetzt werden soll.

Aus der ersten Entwurfsfassung des SKG ging indes nicht klar hervor, in welcher Form die Aufgabenwahrnehmung in dem neu geschaffenen Amt konkret ausgestaltet sein soll. Eine möglichst konkrete Aufgabenzuweisung ist jedoch mit entscheidend für die Beurteilung der Zulässigkeit der jeweils erfolgenden Verarbeitung personenbezogener Daten.

Im Austausch mit dem Ministerium konnte herausgearbeitet werden, dass der Kinderschutzbeauftragte in erster Linie eine Beratungs- und Lotsenfunktion innehaben soll. Ein Tätigwerden in konkreten Einzelfällen war nicht vorgesehen. Dies war zur Abgrenzung gegenüber der bereits existierenden „Ombudsstelle in der Kinder- und Jugendhilfe im Saarland" klarzustellen, die durch § 39 des Ersten Gesetzes zur Ausführung des Kinder- und Jugendhilfegesetzes (AG KJHG) geschaffen wurde und in Konfliktfällen zwischen Jugendämtern und Betroffenen vermitteln soll. Der Kinderschutzbeauftragte soll dagegen als allgemeiner Ansprechpartner dienen, bestehende Hilfsangebote koordinieren sowie beratend tätig werden.

Die Verarbeitung personenbezogener Daten von Hilfesuchenden beschränkt sich insoweit auf Informationen, die die Betroffenen selbst mitteilen, wenn sie sich an ihn wenden. Die mit der Aufgabenwahrnehmung einhergehende Datenverarbeitung kann vor diesem Hintergrund auf bereits existierende datenschutzrechtliche Regelungen, insbesondere auf die Generalklausel des § 4 Abs. 1 SDSG, gestützt werden. Danach ist die Verarbeitung personenbezogener Daten zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der oder des Verantwortlichen liegenden Aufgabe erforderlich ist.

Im Hinblick auf die laut Gesetzentwurf zu bildenden lokalen „Netzwerke Kinderschutz" zur interdisziplinären Kooperation zwischen verschiedenen Trägern und Einrichtungen wurde auf Grund unseres Hinweises klargestellt, dass bei dem Austausch unter den Beteiligten keine personenbezogenen Daten verarbeitet werden. Soweit konkrete Sachverhalte besprochen werden sollen, hat dies in anonymisierter Form zu erfolgen.

### Einrichtung einer Ansprech- und Beschwerdestelle „sexualisierte Gewalt in Schulen"

Gemeinsam mit dem Entwurf für ein saarländisches Kinderschutzgesetz hat die Landesregierung eine Änderung des Schulordnungsgesetzes (SchoG) vorgeschlagen.

Demnach sollte das SchoG insbesondere um eine Regelung ergänzt werden, die die Einrichtung einer zentralen Ansprech- und Beschwerdestelle „sexualisierte Gewalt in Schulen" beim Ministerium für Bildung und Kultur (MBK) vorsieht. Eine solche „Ombudsstelle für Opfer sexualisierter Gewalt in Schulen" hatte das Ministerium eingerichtet, nachdem im Jahr 2023 bekannt wurde, dass ein verstorbener Priester, der zu Lebzeiten unter anderem auch an saarländischen Schulen als Lehrkraft für das Fach katholische Religion eingesetzt war, jahrzehntelang sexuellen Missbrauch gegenüber Jugendlichen begangen haben soll. Die Ombudsstelle sollte es Betroffenen ermöglichen, sowohl aktuelle als auch in der Vergangenheit liegende Vorfälle, die mögliche sexuelle Übergriffe im schulischen Umfeld betreffen, zu melden.

Im Rahmen einer datenschutzrechtlichen Beratung wies unsere Behörde das Ministerium darauf hin, dass es für die Datenverarbeitung durch eine solche Ombudsstelle zwingend einer bereichsspezifischen Rechtsgrundlage bedarf.

Aus den daraufhin beabsichtigten Regelungen des Gesetzentwurfs konnten jedoch die Datenverarbeitungsbefugnisse der Ansprech- und Beschwerdestelle nicht abgeleitet werden, da Art und Umfang der Aufgaben und Befugnisse dieser Stelle nicht schon in dem Gesetz, sondern erst in einer noch zu erlassenden Rechtsverordnung des Ministeriums geregelt werden sollten.

Hiergegen haben wir verfassungsrechtliche Bedenken erhoben. Denn nach Art. 104 Abs. 1 Satz 2 der Saarländischen Verfassung (SVerf) hat der Gesetzgeber Inhalt, Zweck und Ausmaß der dem Verordnungsgeber erteilten Ermächtigung zu bestimmen und damit eine vorprägende Regelungsentscheidung zu treffen, aus der mögliche Inhalte und Grenzen der zu erlassenden Verordnung deutlich werden müssen. Dies war nach unserer Auffassung vorliegend nicht der Fall.

Kritisiert haben wir auch die im Gesetzentwurf vorgesehene generalklauselartige Datenverarbeitungsbefugnis. Zwar ist

weitgehend anerkannt, dass solche Generalklauseln zumindest für Datenverarbeitungen mit geringer Eingriffstiefe oder bei nicht vorhersehbaren und daher vom Gesetzgeber nicht typisierbaren Fällen als Ermächtigungsgrundlage in Betracht kommen können. Diese Voraussetzungen lagen hier jedoch unseres Erachtens nicht vor. Denn bereits in der Entgegennahme und Dokumentation des Vorwurfs von Fehlverhalten im Kontext sexualisierter Gewalt, der sich gegen Lehr- und Aufsichtspersonen richtet, liegt ein schwerwiegender Grundrechtseingriff, der den Rückgriff auf datenschutzrechtliche Generalklauseln verbietet. Vertieft wird dieser Grundrechtseingriff im Falle von eigenen Ermittlungen der Ansprech- und Beschwerdestelle bzw. dann, wenn diese etwaige Vorwürfe an die für die Verfolgung und Ahndung zuständigen Stellen weitergibt. Diese Eingriffe in das Grundrecht auf Schutz der personenbezogenen Daten bedürfen daher in der Regel einer förmlichen, parlamentarischen Ermächtigung, die die zu erhebenden personenbezogenen Daten als solche, den Anlass und den spezifischen Zweck der Erhebung, die Art und Dauer der Aufbewahrung sowie ihre Löschung normenklar und bestimmt regelt und den Grundsatz der Verhältnismäßigkeit wahrt. Zu den essentialia einer solchen gesetzlichen Regelung gehören daher unter anderem auch abstrakt generelle Vorgaben, unter welchen Voraussetzungen eingegangene Beschwerden an welche Stellen weitergegeben werden dürfen, während die Details dann in einer Rechtsverordnung präzisiert werden können.

Weiter haben wir darauf hingewiesen, dass die im Gesetzentwurf vorgesehene Befugnis zur Verarbeitung von besonderen Kategorien personenbezogener Daten in der geplanten Form mit europarechtlichen Vorgaben nicht zu vereinbaren ist. Im Rahmen der Öffnungsklausel des Art. 9 Abs. 2 lit. g DSGVO kann eine Verarbeitung besonderer Kategorien personenbezogener Daten ausnahmsweise zulässig sein, wenn das mitgliedstaatliche Recht eine solche Verarbeitung vorsieht und gleichzeitig im mitgliedstaatlichen Recht angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und

Interessen der betroffenen Personen vorgesehen sind. Dabei darf allerdings nicht – wie es im Gesetzentwurf vorgesehen war – die Pflicht zur Umsetzung entsprechender Schutzmaßnahmen auf die verantwortliche Stelle delegiert werden, sondern der Gesetzgeber selbst muss die von ihm als geeignet angesehenen Garantien vorgeben und die hierfür konkret zu treffenden Maßnahmen festlegen.

Unsere Hinweise wurden in der Folge weitgehend aufgegriffen und der Gesetzentwurf wurde entsprechend angepasst.

### Interkollegialer Ärzteaustausch

Im nachfolgenden parlamentarischen Verfahren zu dem Gesetzentwurf sollte das Kinderschutzgesetz zudem um eine Regelung zum sogenannten interkollegialen Ärzteaustausch erweitert werden soll.

Hierdurch soll es insbesondere Kinderärzten ermöglicht werden, sich untereinander auszutauschen und personenbezogene Daten zu übermitteln, wenn sich Anhaltspunkte für einen möglichen Kindesmissbrauch ergeben. Damit soll dem Phänomen des „Ärzte-Hoppings" begegnet werden, bei dem durch häufige Wechsel des behandelnden Arztes Kindesmissbrauch verschleiert wird.

Diesbezüglich ist anzumerken, dass bereits eine gesetzliche Befugnis zur Datenübermittlung existiert, die es Ärzten ermöglicht, bei Anhaltspunkten für eine Gefährdung des Kindeswohls die notwendigen Informationen weiterzugeben. So sieht § 4 Abs. 3 des Gesetzes zur Kooperation und Information im Kinderschutz (KKG) vor, dass Behandelnde befugt sind, das Jugendamt einzubinden und personenbezogene Daten dorthin zu übermitteln, wenn ihnen gewichtige Anhaltspunkte für die Gefährdung des Wohls eines Kindes oder eines Jugendlichen bekannt werden.

Darüber hinaus ist ein fachlicher Austausch mit Kollegen in anonymisierter Form jederzeit möglich.

Der Gesetzgeber hält es jedoch für notwendig, als Vorstufe zur Einbindung des Jugendamtes einen Austausch unter Ärzten ohne Bruch der ärztlichen Schweigepflicht zu ermöglichen, um diesen die Entscheidung über die Information der Behörde zu erleichtern.

Aus datenschutzrechtlicher Sicht zu begrüßen ist, dass letztlich Einigkeit darüber bestand, den personenbezogenen Austausch auf Ärzte zu begrenzen, zu denen das jeweilige Kind in einem Behandlungsverhältnis steht oder stand.

Ergänzungen bzw. Klarstellungen zu der beabsichtigten Regelung haben wir bezüglich der Aufbewahrungsfristen sowie der Informationspflichten gegenüber den betroffenen Personen angeregt. Dies wurde vom Landtag auch entsprechend aufgegriffen.

Die Verabschiedung des SKG durch den Landtag erfolgte am 15. November 2023.

### Fazit

Das SKG leistet einen wichtigen Beitrag zur Stärkung der Rechte von Kindern und Jugendlichen im Saarland. Das Unabhängige Datenschutzzentrum wird die praktische Umsetzung der neu geschaffenen Regelungen, insbesondere derer zum interkollegialen Ärzteaustausch, aus datenschutzrechtlicher Sicht begleiten.

# VI.

# Gesundheit und Soziales

# 6 Gesundheit und Soziales

## 6.1 Datenpannenmeldungen aus dem Gesundheitswesen

Viele Meldungen von Datenschutzverletzungen, die beim Unabhängigen Datenschutzzentrum Saarland eingehen, stammen aus dem Gesundheitssektor. Dies lässt sich dadurch erklären, dass Gesundheitsdaten zu den besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO gehören und als sehr sensibel gelten. Daher ist bei Datenschutzverletzungen in diesem Bereich regelmäßig von einem Risiko für die Rechte und Freiheiten natürlicher Personen und damit von einer Meldepflicht gegenüber der Aufsichtsbehörde nach Art. 33 DSGVO auszugehen, vor allem dann, wenn Unberechtigte Kenntnis von Gesundheitsdaten erlangt haben. Bei den verantwortlichen Stellen aus dem Gesundheitssektor, die Datenpannen melden, handelt es sich vor allem um Arztpraxen, Krankenhäuser und externe Abrechnungsunternehmen. Letztere sollen im Folgenden näher betrachtet werden.

Nutzt eine Gesundheitseinrichtung (meist Arztpraxis oder Krankenhaus) eine externe Abrechnungsstelle zur Erstellung ihrer Rechnungen, werden die hierfür erforderlichen Patientendaten an die Abrechnungsstelle übermittelt. Das Abrechnungsunternehmen verarbeitet die Daten dann in der Regel in eigener Verantwortung, ist also Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Daher ist für die Datenübermittlung von der Gesundheitseinrichtung an das Abrechnungsunternehmen aus datenschutzrechtlicher Sicht eine Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) des jeweiligen Patienten erforderlich. Es handelt sich beim Einholen der Einwilligung um eine Verpflichtung der Gesundheitseinrichtung als Kunde des Abrechnungsunternehmens, worauf auch in den vertraglichen Regelungen zwischen den beiden Parteien hingewiesen wird.

Vor diesem Hintergrund werden unserer Behörde durch eine Abrechnungsstelle immer wieder Fälle als Datenpanne gemel-

det, in denen sich nachträglich herausstellt, dass eine Einwilligung in die Datenübermittlung nicht vorlag. In diesen Fällen hätte die Gesundheitseinrichtung die Daten nicht übermitteln und das Abrechnungsunternehmen sie nicht verarbeiten dürfen. Die Meldung an uns erfolgt hierbei durch die Abrechnungsstelle als Verantwortliche; die Ursache für den Datenschutzverstoß liegt jedoch auf der Seite des Kunden, der Patientendaten ohne die erforderliche Einwilligung und somit unzulässig übermittelt hat. In solchen Fällen ist auch die jeweils betroffene Gesundheitseinrichtung verpflichtet, eine Meldung nach Art. 33 DSGVO an die für sie zuständige Aufsichtsbehörde vorzunehmen.

Nach unserer Auffassung darf sich die Abrechnungsstelle grundsätzlich darauf verlassen, dass Kunden ihrer Verpflichtung nachkommen und Patientendaten nur mit Einwilligung übermittelt werden. Ergeben sich diesbezüglich aber Zweifel, ist eine Überprüfung, ggf. gefolgt von einer Löschung zu Unrecht übermittelter Daten, angezeigt.

Bei der Einbindung von Abrechnungsstellen kommt es daneben auch zu Fehlversendungen von Rechnungen, die häufig darauf beruhen, dass die Gesundheitseinrichtung unzutreffende Rechnungsempfängerdaten an das Abrechnungsunternehmen übermittelt hat. Auch hier erfolgt eine Meldung durch das Unternehmen, in dessen Verantwortungsbereich die Fehlversendung erfolgt ist, wobei die Ursache wiederum beim Kunden zu suchen ist.

Dies zeigt, wie wichtig es ist, dass Gesundheitseinrichtungen auf die Aktualität ihres Datenbestandes achten.

## 6.2 Diskretion in der Arztpraxis

Im Gesundheitsbereich werden naturgemäß sehr sensible personenbezogene Daten verarbeitet, und verständlicherweise legen Patientinnen und Patienten besonderen Wert auf einen vertraulichen Umgang mit Informationen, die ihren Gesundheitszustand betreffen. Vor diesem Hintergrund erreichen das

Unabhängige Datenschutzzentrum Saarland immer wieder Hinweise und Beschwerden bezüglich mangelnder Diskretion in Arztpraxen und Krankenhäusern.

Im Rahmen einer solchen Beschwerde wurden wir auf eine aus datenschutzrechtlicher Sicht fragwürdige Vorgehensweise einer Arztpraxis aufmerksam gemacht.

Die betroffene Person schilderte, dass im Vorfeld einer anstehenden Untersuchung ein Aufklärungsgespräch gemeinsam mit anderen Patientinnen und Patienten der Praxis durchgeführt worden sei. Die Namen der Anwesenden und die Art der anstehenden Behandlung seien dadurch den übrigen anwesenden Personen bekannt geworden; zudem sei bei dem Gespräch auch nach (Vor-)Erkrankungen gefragt worden, die bei der Untersuchung ggf. zu berücksichtigen wären. Eine ausdrückliche Einwilligung in diese Vorgehensweise sei nicht eingeholt, vielmehr sei man damit „überrumpelt" worden.

Wird ein medizinisches Aufklärungsgespräch mit mehreren Personen geführt und werden hierbei Informationen über mögliche Erkrankungen der Anwesenden abgefragt, geht dies mit einer Offenlegung von Gesundheitsdaten einher und stellt aus datenschutzrechtlicher Sicht eine Übermittlung der Daten an Dritte, nämlich an die anderen Patientinnen und Patienten, dar. Eine gesetzliche Grundlage für eine solche Übermittlung ist nicht ersichtlich, so dass lediglich eine Einwilligung als Rechtsgrundlage in Betracht kommt. Diese muss bei Gesundheitsdaten, die zu den besonderen Kategorien von Daten im Sinne von Art. 9 Abs. 1 DSGVO zählen, ausdrücklich erfolgen und den allgemeinen Anforderungen an eine Einwilligung nach Art. 7 DSGVO genügen, also unter anderem freiwillig erfolgen. Aus Gründen der Nachweisbarkeit (Art. 5 Abs. 2 DSGVO) empfiehlt sich die Einholung einer schriftlichen Einwilligungserklärung.

In ihrer Stellungnahme hat die betroffene Praxis ausgeführt, es handele sich bei dem Gespräch mit mehreren Patientinnen und Patienten lediglich um die Vermittlung von allgemeinen Informationen, nicht um die individuelle Patientenaufklärung.

Letztere finde im Rahmen eines gesonderten Vier-Augen-Gesprächs zwischen Arzt und Patient statt. Auf Wunsch würden auch die allgemeinen Informationen in einem Einzelgespräch übermittelt. Beschwerden aus dem Patientenkreis über das Procedere habe es bislang nicht gegeben.

Dennoch hat die Praxis angekündigt, ihre Vorgehensweise dahingehend umzustellen, dass zukünftig alle Patientinnen und Patienten vorab über den geplanten Ablauf informiert und um schriftliche Zustimmung gebeten werden. Alternativ werden Einzelaufklärungsgespräche angeboten.

Dies ist aus datenschutzrechtlicher Sicht auch erforderlich. Denn bereits die Information darüber, welcher Untersuchung sich eine Person unterziehen wird, ist als Gesundheitsdatum im Sinne von Art. 4 Nr. 15 DSGVO zu werten. Hierauf wurde die Praxis hingewiesen und außerdem dazu aufgefordert, im Vorfeld des Gesprächs ausdrücklich klarzustellen, dass individuelle Fragen gesondert unter vier Augen erörtert werden können, so dass sich niemand gezwungen sieht, im Beisein anderer Patientinnen und Patienten Angaben über den eigenen Gesundheitszustand machen zu müssen. Die Einwilligung in ein gemeinsames Aufklärungsgespräch ist zudem nur dann freiwillig, wenn die Betroffenen sich nicht unter Druck gesetzt fühlen, dem zuzustimmen, um beispielsweise den Ablauf nicht zu verzögern.

Wir gehen davon aus, dass durch die Anpassung der Vorgehensweise ein datenschutzkonformer Zustand erreicht werden kann.

### Fazit

Arztpraxen müssen ihre Abläufe grundsätzlich so ausgestalten, dass Gesundheitsdaten von Patientinnen und Patienten nicht gegenüber Dritten offengelegt werden. Ausnahmen sind nur auf Grundlage einer informierten Einwilligung der betroffenen Person denkbar.

## 6.3 Auskunftsanspruch im Behandlungsverhältnis

Das Auskunftsrecht aus Art. 15 DSGVO ist das datenschutzrechtliche Betroffenenrecht, mit dem die Aufsichtsbehörden wohl am häufigsten befasst sind. Dieses Recht gewährt einen Anspruch auf umfassende Informationen hinsichtlich der Verarbeitung personenbezogener Daten der betroffenen Person sowie spezifischer Umstände der Datenverarbeitung.

Im Gesundheitsbereich hat sich in der Vergangenheit diesbezüglich die Frage nach dem Verhältnis zwischen Art. 15 DSGVO und § 630g Bürgerliches Gesetzbuch (BGB), der im Behandlungsverhältnis ein Recht auf Einsicht in die Patientenakte und Erhalt einer Kopie normiert, gestellt. Die beiden Regelungen unterscheiden sich insbesondere im Hinblick auf die Möglichkeit des Verantwortlichen, für eine Kopie Kosten geltend zu machen. Im 28.[35] und im 29.[36] Tätigkeitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit wurde dies bereits näher beleuchtet.

Der Europäische Gerichtshof (EuGH) hat sich nun in seinem Urteil vom 26.10.2023[37] zu mehreren Vorlagefragen in diesem Kontext geäußert.

So wurde zunächst generell festgestellt, dass es dem Auskunftsanspruch nach Art. 15 DSGVO nicht entgegensteht, wenn die betroffene Person hiermit datenschutzfremde Zwecke verfolgt. Art. 12 Abs. 5 sowie Art. 15 Abs. 1 und 3 DSGVO sind demnach dahin auszulegen, dass die Verpflichtung des Verantwortlichen, der betroffenen Person unentgeltlich eine erste Kopie ihrer personenbezogenen Daten, die Gegenstand einer Verarbeitung sind, zur Verfügung zu stellen, auch dann gilt, wenn der betreffende Antrag mit anderen als den in Satz 1 des 63. Erwägungsgrundes der DSGVO genannten Zwecken begründet wird. Dies ergibt sich daraus, dass weder nach dem

[35] Vgl. 28. Tätigkeitsbericht 2019, Kapitel 4.21, S. 119 ff.
[36] Vgl. 29. Tätigkeitsbericht 2020, Kapitel 3.22, S. 113 f.
[37] EuGH, Urteil vom 26.10.2023, C-307/22, Celex-Nr. 62022CJ0307

Wortlaut von Art. 12 Abs. 5 noch dem von Art. 15 Abs. 1 und 3 DSGVO eine Begründung für das Auskunftsersuchen durch die betroffene Person erfolgen muss. Ist ein Auskunftsersuchen ohne Nennung eines Zwecks zulässig, muss dies auch gelten, wenn ein datenschutzfremder Zweck angegeben wird.

Die zweite Vorlagefrage betraf konkret die Vorschrift des § 630g Abs. 2 Satz 2 BGB, welche bereits vor Inkrafttreten der DSGVO existiert hat und anders als Art. 15 Abs. 3 DSGVO vorsieht, dass der Behandler des Patienten die Erstattung seiner Kosten für Abschriften von der Patientenakte verlangen kann. Hierzu hat der EuGH festgestellt, dass eine nationale Reglung, die bereits vor dem Inkrafttreten der DSGVO erlassen wurde, grundsätzlich die Betroffenenrechte nach Art. 12 ff. DSGVO beschränken kann. Art. 23 Abs. 1 DSGVO schließt dies nicht aus.

Allerdings muss die durch die nationale Regelung vorgenommene Beschränkung notwendig und verhältnismäßig sein und die Rechte und Freiheiten anderer Personen sicherstellen (Art. 23 Abs. 1 lit. I 2. Var. DSGVO). Letzteres trifft nach Auffassung des EuGH hier nicht zu.

So ist – wie das vorlegende Gericht es dargestellt hat – Sinn und Zweck des § 630g Abs. 2 Satz 2 BGB in erster Linie, die wirtschaftlichen Interessen von Ärzten zu schützen, indem Patienten davon abgehalten werden, unnötig Kopien ihrer Akte anzufordern. Derartige Erwägungen fallen laut EuGH nicht unter die Rechte und Freiheiten anderer Personen im Sinne oben genannter Vorschrift. Begründet wird dies damit, dass eine solche Regelung zum einen dazu führt, dass nicht nur unnötigen, sondern auch berechtigten Anträgen auf Kopie entgegengewirkt wird. Zum anderen sei nicht zu erkennen, dass die von der nationalen Regelung geschützten Interessen über rein administrative oder wirtschaftliche Erwägungen hinausgehen. Daneben führt der EuGH aus, dass in Art. 12 Abs. 5 und Art. 15 Abs. 3 Satz 2 DSGVO festgelegt wird, unter welchen Umständen Verantwortliche ein Entgelt für die Kosten der Überlassung einer Kopie personenbezogener Daten ver-

langen können und insoweit wirtschaftliche Interessen bereits Berücksichtigung in der DSGVO finden. Dies sind die Fälle, in denen die Anträge der betroffenen Personen als missbräuchlich anzusehen sind oder sie weitere als die bereits zur Verfügung gestellten Kopien verlangt.

In der dritten Vorlagefrage ging es darum, ob das Recht auf Kopie gem. Art. 15 Abs. 3 Satz 1 DSGVO im Rahmen eines Arzt-Patienten-Verhältnisses dahin auszulegen ist, dass der betroffenen Person eine vollständige Kopie der in ihrer Patientenakte enthaltenen Dokumente mit ihren personenbezogenen Daten zu überlassen ist, oder ob nur eine Kopie der Daten als solche beansprucht werden kann.

Hierzu verweist der EuGH zunächst auf sein Urteil vom 04.05. 2023[38] zum Auskunftsrecht. Danach ist Art. 15 Abs. 3 Satz 1 DSGVO so auszulegen, dass das Recht, von dem für die Verarbeitung Verantwortlichen eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zu erhalten, bedeutet, dass der betroffenen Person eine originalgetreue und verständliche Reproduktion aller dieser Daten ausgefolgt wird. Dies setzt das Recht voraus, eine Kopie von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die u. a. diese Daten enthalten, zu erlangen, wenn die Zurverfügungstellung einer solchen Kopie unerlässlich ist, um der betroffenen Person die wirksame Ausübung der ihr durch die DSGVO verliehenen Rechte zu ermöglichen. Dabei kann sich die Reproduktion ganzer Dokumente, die personenbezogene Daten enthalten, als unerlässlich erweisen, wenn die Kontextualisierung der verarbeiteten Daten zur Verständlichkeit erforderlich ist.

Im Hinblick auf Gesundheitsdaten ist dabei Erwägungsgrund 63 der DSGVO zu berücksichtigen, wonach das Recht auf Auskunft Daten in der Patientenakte, die Informationen wie z. B. Diagnosen, Untersuchungsergebnisse, Befunde und Angaben

[38] EuGH, Urteil vom 4. Mai 2023 – C-487/21 –, juris.

zu Behandlungen oder Eingriffen enthalten, einschließt. Nach Auffassung des EuGH besteht bei solchen Daten die Gefahr, dass durch die Zurverfügungstellung einer einfachen Zusammenfassung oder Zusammenstellung der Informationen etwas ausgelassen oder unrichtig wiedergegeben wird oder dass jedenfalls die Überprüfung von Richtigkeit und Vollständigkeit durch den Patienten erschwert wird.

Im Ergebnis hält der EuGH – anschließend an seine bisherige Rechtsprechung – fest, dass Art. 15 Abs. 3 Satz 1 DSGVO dahin auszulegen ist, dass im Rahmen eines Arzt-Patienten-Verhältnisses das Recht auf Erhalt einer Kopie der personenbezogenen Daten, die Gegenstand einer Verarbeitung sind, umfasst, dass der betroffenen Person eine originalgetreue und verständliche Reproduktion all dieser Daten überlassen wird. Dieses Recht kann eine vollständige Kopie aller Dokumente einer Patientenakte beinhalten, wenn die Zurverfügungstellung einer solchen Kopie erforderlich ist, um der betroffenen Person die Überprüfung der Richtigkeit und Vollständigkeit der Daten zu ermöglichen und die Verständlichkeit der Daten zu gewährleisten. In Bezug auf die Gesundheitsdaten der betroffenen Person schließt dieses Recht jedenfalls das Recht ein, eine Kopie der Dokumente aus ihrer Patientenakte zu erhalten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu an ihr vorgenommenen Behandlungen oder Eingriffen umfasst.

Der Anspruch auf eine Kopie von einzelnen Dokumenten bzw. allen in der Patientenakte enthaltenen Dokumenten wird somit davon abhängig gemacht, ob diese zum Verständnis erforderlich sind, wobei der EuGH offenbar davon ausgeht, dass dies zumindest bei den genannten Informationen in der Regel der Fall ist.

Im Umkehrschluss bedeutet dies, dass nur solche Dokumente aus der Patientenakte nicht zur Verfügung gestellt werden müssen, die entweder keine personenbezogenen Daten ent-

halten oder die nicht zum Verständnis der Daten und deren Verarbeitung erforderlich sind.

### Fazit

Zusammengefasst lässt sich für den Umgang mit Art. 15 DSGVO im Behandlungskontext festhalten, dass eine erste Kopie der Patientenakte kostenlos zur Verfügung zu stellen ist und ein datenschutzfremder Zweck dem Anspruch der betroffenen Person dabei nicht entgegensteht. Hinsichtlich des Umfangs der zur Verfügung zu stellenden Kopie ist zu prüfen, welche Dokumente nach den vom EuGH aufgestellten Kriterien herauszugeben sind. Hier dürfte sich für Ärzte allerdings die Frage stellen, ob eine solche Prüfung nicht aufwändiger ist als dem Patienten einfach eine vollständige Kopie der gesamten Akte zu überlassen.

# VII.

# Schule und Bildung

# 7 Schule und Bildung

## 7.1 Veröffentlichung von Lehrerkontaktdaten im Internet

Immer wieder werden wir mit der Frage konfrontiert, ob die Kontaktdaten von Lehrkräften im Internet, beispielsweise auf der Schulhomepage, veröffentlicht werden dürfen. Zunächst ist dabei klarzustellen, dass es sich hierbei nur um dienstliche Kontaktdaten, wie die vom Saarland für Lehrkräfte zur Verfügung gestellte dienstliche E-Mail-Adresse (Nachname@schule.saarland) oder eine dienstlich zur Verfügung gestellte Telefonnummer handeln kann. Die Veröffentlichung der dienstlich zur Verfügung gestellten E-Mail-Adresse auf der Schulhomepage kann dabei gem. § 22 Abs. 6 SDSG legitimiert werden, soweit die dortigen Voraussetzungen vorliegen. Zu diesen gehört zum einen, dass die Veröffentlichung zum Zweck der Information der Allgemeinheit oder der anderen Beschäftigten erforderlich sein muss und zum anderen, dass der Veröffentlichung keine schutzwürdigen Interessen der betroffenen Person entgegenstehen dürfen. Lehrkräfte sind in der Regel als Beschäftigte mit Außenkontakt anzusehen, da sie den Eltern ihrer Schüler als Ansprechpartner bei Problemen im jeweiligen Schulfach zur Verfügung stehen sollen. Um eine Kontaktaufnahme zu den Lehrkräften zu ermöglichen, ist daher die Veröffentlichung der dienstlichen Kontaktdaten gem. § 22 Abs. 6 SDSG grundsätzlich möglich.

Möchte eine Schule die dienstlichen Kontaktdaten aller Lehrkräfte veröffentlichen, empfehlen wir, im Vorfeld das Kollegium über diese Absicht zu informieren. Sollte eine Lehrerin oder ein Lehrer schutzwürdige Interessen vortragen, die einer Veröffentlichung entgegenstehen, kann nach Prüfung der vorgetragenen schutzwürdigen Interessen von einer Veröffentlichung abgesehen werden. Dieses Vorgehen entspricht auch einem Urteil des OVG Rheinland-Pfalz[39], das die Veröffentlichung

[39] Urteil vom 10.09.2007, 2 A 10413/07.

einer dienstlichen, namensbezogenen E-Mail-Adresse im Interesse einer transparenten, bürgernahen öffentlichen Verwaltung sieht, der sich einzelne Beamte, die hierdurch nicht als Privatperson, sondern aufgrund der Stellung als Teil der Beschäftigungsbehörde betroffen sind, nicht generell verschließen können.

**Fazit**

Vor der Veröffentlichung von dienstlichen personenbezogenen Kontaktdaten sollten die Betroffenen entsprechend informiert werden und ihnen die Möglichkeit eingeräumt werden, schutzwürdige Interessen vorzutragen, die einer möglichen Veröffentlichung entgegenstehen könnten. Erst nach abgeschlossener Prüfung aller Einwände kann eine Veröffentlichung der dienstlichen Kontaktdaten erfolgen.

## 7.2 Auskunfts- und Löschansprüche in der Online-Schule-Saar

Die Betroffenenrechte aus den Art. 12 ff. DSGVO stehen zweifellos auch Schülern und Lehrkräften zu. So haben sie unter anderem das Recht, gem. Art. 15 DSGVO Auskunft über ihre in der Online-Schule-Saar hinterlegten personenbezogenen Daten zu erhalten oder diese Daten gem. Art. 17 DSGVO löschen zu lassen, sobald sie nicht mehr zur Aufgabenerfüllung erforderlich sind und keine gesetzliche Aufbewahrungspflicht der Löschung entgegensteht. Die erforderlichen Informationen sind den Betroffenen gem. Art. 12 Abs. 3 DSGVO unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang eines entsprechenden Antrags zur Verfügung zu stellen. Im Berichtszeitraum ließ das Ministerium für Bildung und Kultur diese gesetzlich vorgegebene Frist in mehreren Fällen verstreichen, ohne den Betroffenen entsprechende Informationen zukommen zu lassen. Das führte zu Beschwerden gem. Art. 77 DSGVO bei unserer Behörde. Nach Kontaktaufnahme durch unsere

Behörde bemühte sich das Ministerium um eine schnellstmögliche Beantwortung der Anträge.

Zum Löschantrag eines ehemaligen Schülers für seine in der Online-Schule-Saar hinterlegten Daten berief sich das Ministerium auf die Regelung aus § 6 Abs. 3 Nr. 4 der Verordnung über die Verarbeitung personenbezogener Daten in den Schulen (PersDatSchulV), wonach sonstige personenbezogene Schulunterlagen mindestens 5 Jahre nach dem Ausscheiden des Schülers aufzubewahren sind. Diese Verordnung wurde vor 2008 bezogen auf schriftliche Unterlagen in der Schule erstellt und die heutige Digitalisierung in der Schule war zum Zeitpunkt der Erstellung der Verordnung nicht abzusehen. Da es fraglich bleibt, ob auch ein Account in der Online-Schule-Saar unter den Begriff der sonstigen Schulunterlagen zu subsumieren ist, wäre es sinnvoll, diese Regelungen den neuen Gegebenheiten zur Digitalisierung im Schulalltag anzupassen und damit einhergehend auch die Aufbewahrungsfristen für digital gespeicherte Daten zu überdenken. Im Hinblick auf die Erforderlichkeit der weiteren Aufbewahrung der in der Online-Schule-Saar gespeicherten Daten von ausgeschiedenen Schülern, die sich bereits in einer Berufsausbildung oder im Studium befinden, wäre es aus unserer Sicht ausreichend, die Daten maximal noch bis zum Ende des Jahres des Ausscheidens aufzubewahren.

# VIII.

# Wirtschaft

# 8 Wirtschaft

## 8.1 E-Mails am Arbeitsplatz

Immer wieder erreichen uns Anfragen bzw. Beschwerden im Zusammenhang mit der Nutzung von E-Mails am Arbeitsplatz. Die Anfragen kommen dabei sowohl von Arbeitgebern als auch von Arbeitnehmern. Ist die Natur der Anfragen auch vielfältig, so drehen sie sich im Kern doch um ein und dasselbe Problem: Was ist hinsichtlich der Nutzung von E-Mails am Arbeitsplatz erlaubt und welche Rechte haben Arbeitgeber bezüglich Einsicht und Kontrolle?

In einem konkreten Fall erhielten wir eine Beschwerde eines ausgeschiedenen Mitarbeiters eines Unternehmens, welches nach dessen Ausscheiden auf seinen E-Mail-Account zugriff und die gesamte E-Mail-Korrespondenz archivierte, um gesetzlichen Aufbewahrungspflichten nachzukommen. Hierbei wurden E-Mails privater Natur aufgefunden und gesichtet, die nach Angaben des Verantwortlichen Geschäftsgeheimnisse des Unternehmens beinhalteten und an unbefugte Dritte offenbart worden waren. In dem Unternehmen existierte eine IT-Vereinbarung, in welcher die private Nutzung des E-Mail-Accounts ausgeschlossen war. Der Beschwerdeführer rügte dennoch, dass die Sichtung der E-Mails privater Natur nicht rechtmäßig erfolgt sei.

Gemäß § 26 Abs. 1 Satz 1 BDSG darf der Arbeitgeber personenbezogene Daten des Arbeitnehmers verarbeiten, wenn dies zur Begründung, Durchführung oder Beendigung eines Arbeitsverhältnisses erforderlich ist. Diese Rechtsgrundlage ist auch im Zusammenhang mit dem Zugriff auf E-Mails eines Arbeitnehmers einschlägig. Entsprechend der hier erforderlichen Interessenabwägung müssen die Interessen des Arbeitgebers gegenüber den Interessen des Arbeitnehmers überwiegen, um einen Zugriff zu rechtfertigen. Erster entscheidender Punkt für diese Interessenabwägung ist die Frage, ob eine Privatnutzung ausgeschlossen oder erlaubt ist. Im Falle des

Ausschlusses der privaten Nutzung fällt die Interessenabwägung sodann regelmäßig zugunsten des Arbeitgebers aus. E-Mails dürfen jedoch grundsätzlich auch bei Ausschluss der Privatnutzung von dem Arbeitgeber dann nicht weiter inhaltlich zur Kenntnis genommen werden, sobald ihr privater Charakter erkannt wurde.

In einem parallel zu dem vorliegenden Beschwerdeverfahren laufenden arbeitsgerichtlichen Rechtsstreit war jedoch die unzulässige Weitergabe von Betriebsinterna in den privat versendeten E-Mails Gegenstand der Einsichtnahme, so dass aufgrund dieser Sachlage im Einzelfall letztlich von einer rechtmäßigen Einsichtnahme in die E-Mails auszugehen war.

Dieser Fall zeigt, wie kompliziert der Umgang mit E-Mails am Arbeitsplatz aus datenschutzrechtlicher Sicht werden kann, wenn seitens des Arbeitgebers nicht entsprechend vorgesorgt wurde. Grundsätzlich empfehlen wir daher dringend, in schriftlichen Dienst- oder Betriebsvereinbarungen Regelungen zum Umgang mit E-Mails am Arbeitsplatz zu treffen, um bereits vorab datenschutzrechtlichen Streitigkeiten oder Problemen vorzubeugen.

Dabei gilt: Je ausführlicher die Einzelfälle geschildert und geregelt sind, desto besser.

Hierbei ist im Grundsatz zunächst zu klären, ob eine private Nutzung erlaubt oder ausgeschlossen ist. Wird die private Nutzung ausgeschlossen, sind die Möglichkeiten eines Zugriffs auf das E-Mail-Postfach umfassender. Aus datenschutzrechtlicher Sicht ist eine rein dienstliche Nutzung grundsätzlich vorzugswürdig.

Darüber hinaus sollten auch spezifische Regelungen zur Vorgehensweise bei Ausscheiden eines Arbeitnehmers getroffen werden. Hier kommt etwa die Verpflichtung des Arbeitnehmers in Betracht, bei Verlassen eines Unternehmens abschließend sein Postfach zu sichten und gegebenenfalls E-Mails zu

löschen, bevor diese archiviert und dabei eventuell auch gesichtet werden können.

Auch die unerwartete Abwesenheit oder der Tod von Arbeitnehmern sowie die damit zusammenhängende Frage eines Zugriffs bei diesen Ereignissen sollte klar geregelt werden.

Ebenso sollten Anforderungen und Vorgehensweise bei möglichen Zugriffsszenarien auf einen dienstlichen E-Mail-Account festgehalten werden.

Seit 2016 existiert zu der Thematik die Orientierungshilfe der Datenschutzkonferenz „E-Mail und Internet am Arbeitsplatz" der Datenschutzkonferenz (DSK). Diese Orientierungshilfe befindet sich zwar derzeit in Überarbeitung und ist noch nicht an die gegenwärtige Rechtslage angepasst, die Grundsätze darin sind aber nach wie vor aktuell.

**Fazit**

Der Umgang mit E-Mail am Arbeitsplatz sollte im Detail schriftlich geregelt werden. Hierbei bieten sich insbesondere Betriebs- oder Dienstvereinbarungen an.

## 8.2 Ausschluss des Auskunftsanspruchs im arbeitsgerichtlichen Vergleich

Auch im Beschäftigungsverhältnis zwischen Arbeitnehmer und Arbeitgeber stellt der Auskunftsanspruch aus Art. 15 DSGVO ein nicht zu unterschätzendes Informationsrecht dar, denn ungeachtet des arbeitsrechtlichen Schwerpunkts dieses Rechtsverhältnisses, steht es natürlich jedem Beschäftigten zu, seine datenschutzrechtlichen Betroffenenrechte auch gegenüber seinem derzeitigen oder ehemaligen Arbeitgeber geltend zu machen, insbesondere dann, wenn er die auf seine Person bezogene Datenverarbeitung auf ihre Rechtmäßigkeit hin überprüfen möchte.

Im Falle bereits längere Zeit bestehender Beschäftigungsverhältnisse können jedoch derart große Datenmengen mit einem Personenbezug zu dem Arbeitnehmer entstanden sein, dass eine Beauskunftung dieser Daten für den Arbeitgeber mit einem erheblichen Verwaltungsaufwand verbunden sein kann. Insbesondere im Zusammenhang mit der Beendigung eines Arbeitsverhältnisses kann es daher im Interesse des Arbeitgebers liegen, Rechtssicherheit dergestalt zu erhalten, dass er sich von möglichen künftigen datenschutzrechtlichen Ansprüchen seines Arbeitnehmers frei macht. Dies gilt erst recht für den Fall eines arbeitsgerichtlichen Verfahrens bei dem es darum geht, ein Arbeitsverhältnis zur weitgehenden Zufriedenheit aller Parteien einvernehmlich zu beenden und dabei auch sämtliche mögliche gegenseitige Ansprüche aus der Vergangenheit, im Sinne eines endgültigen Auseinandergehens, ein für allemal aufzulösen.

Hierbei stellt sich zum einen jedoch die Frage, inwieweit die Betroffenenrechte der Art. 12 ff. DSGVO und hierbei insbesondere von Art. 15 DSGVO überhaupt der Privatautonomie zwischen den Parteien zugänglich sind, und zum anderen, ob diese durch einen gerichtlichen Vergleich abbedungen werden können und welchen Inhalt ein solcher Vergleich aufweisen muss. Zu dieser Frage vertritt unsere Behörde die folgende Rechtsauffassung:

Das europäische Datenschutzrecht ist Ausfluss des Grundrechts aus Art. 8 der Charta der Grundrechte der Europäischen Union (GRCh). Selbiges ist zweifelsohne ein herausragendes, jedoch gerade kein Grundrecht unabdingbarer Natur, wie etwa die Menschenwürde aus Art. 1 GRCh. Das Datenschutzrecht wird vielmehr von dem Gedanken der Selbstbestimmtheit des Betroffenen getragen, was es vor allem durch das Institut der Einwilligung aus Art. 6 Abs. 1 lit. a, Art. 7 DSGVO unmissverständlich zum Ausdruck bringt. Kann der Betroffene durch eine Einwilligung zur Verarbeitung seiner personenbezogenen Daten seine Zustimmung erteilen und dieser Verarbeitung dadurch eine rechtliche Grundlage verleihen, so muss er auch

eine Entscheidungsbefugnis dahingehend haben, ob und inwieweit er seine hierzu im Annex stehenden Betroffenenrechte ausübt bzw. auf diese verzichtet.

Selbst wenn man in einer Verarbeitungssituation im Beschäftigungsverhältnis den Arbeitnehmer und Betroffenen einer Datenverarbeitung als strukturell unterlegen erachtet und, gewissermaßen um diesen vor sich selbst zu schützen, die Disponibilität aufgrund der Notwendigkeit einer damit einhergehenden effektiven Rechtsdurchsetzung verneint,[40] so wird man jedenfalls einen Ausschluss betreffend zurückliegender Datenverarbeitungen des Arbeitsverhältnisses bejahen müssen.[41]

Dass die Formulierungen in einem arbeitsgerichtlichen Vergleich hinreichend klar und bestimmt sein müssen, um ein datenschutzrechtliches Betroffenenrecht einvernehmlich auszuschließen, liegt auf der Hand. Bestandteil eines solchen Vergleichs ist in der Regel jedoch auch eine salvatorische Abgeltungsklausel, welche jegliche Ansprüche aus dem Arbeitsverhältnis und dessen Beendigung, *gleich ob bekannt oder unbekannt und gleich aus welchem Rechtsgrund,* abgelten soll.

Enthält ein Vergleich eine solche Abgeltungsklausel, so genügt dies aus hiesiger Sicht dem Bestimmtheitserfordernis. Auch wenn sich der Vergleich seinem Wortlaut nach „nur" auf Ansprüche „aus dem Arbeitsverhältnis" beziehen sollte, ist dies unschädlich, da das Arbeitsverhältnis gerade Grundlage der Datenverarbeitung ist. Umfasst sind demnach nicht nur arbeitsrechtliche Ansprüche im engeren Sinne, sondern auch solche datenschutzrechtlicher Art, welche mit dem Arbeitsverhältnis in Verbindung stehen und für welche das Arbeitsverhältnis Verarbeitungsgrundlage war.

Die in einem arbeitsgerichtlichen Streit zwischen dem Arbeitnehmer und dem Arbeitgeber zugrunde liegenden Umstände

[40] Fuhlrott/Garden: Vergleichsweise Erledigung des datenschutzrechtlichen Auskunftsanspruchs, NZA 2021, S. 530 (534)
[41] Fuhlrott/Garden, a.a.O, S. 535 f.

sollen durch einen Vergleich im Wege des gegenseitigen Nachgebens abschließend geklärt werden. Diese abschließende Klärung würde nicht erreicht werden, wenn der Verantwortliche (Arbeitgeber) befürchten müsste, weiterhin Auskünfte über zurückliegende Sachverhalte und Datenverarbeitungen erteilen zu müssen.

Jedoch ist eine solche Abdingbarkeit nicht in unbeschränkter Form möglich. Dem Betroffenen (Arbeitnehmer) muss insbesondere für noch nicht absehbare Datenverarbeitungen der Zukunft die Möglichkeit der Auskunft bei dem Verantwortlichen (Arbeitgeber) erhalten bleiben. Auskunftsansprüche über Datenverarbeitungen der Vergangenheit, genauer über solche Verarbeitungen, welche aus zeitlich vor dem hierauf gerichteten Vertragsschluss (Vergleichsschluss) resultierenden Datenerhebungen stammen, stehen indes grundsätzlich zur Disposition der Vertragsparteien.

**Fazit**

Sollte im arbeitsgerichtlichen Vergleich der Auskunftsanspruch des Arbeitnehmers ausgeschlossen werden, empfiehlt es sich der Klarheit und Eindeutigkeit wegen, den Ausschluss des Auskunftsanspruchs aus Art. 15 DSGVO und evtl. weiterer datenschutzrechtlicher Betroffenenrechte explizit, d. h. unter Verweis auf die jeweilige Rechtsgrundlage des Anspruchs, zu benennen und für erledigt zu erklären.

## 8.3 Zugriffsberechtigungen bei Versicherungen

Unklare und intransparente Zugriffe auf bei einem Versicherungsunternehmen gespeicherte Kundendaten waren im Berichtszeitraum Anlass für eine Beschwerde. Die Beschwerdeführerin trug vor, in der Vergangenheit bei einem Versicherungsunternehmen einen Vertrag über eine Riester-Rentenversicherung abgeschlossen und diesen vor Jahren auf ein anderes Versicherungsunternehmen übertragen zu haben.

Als Zeugin eines Verkehrsunfalls wurde die Beschwerdeführerin von einer Schadenssachbearbeiterin ihres früheren Versicherers, bei der das Unfallopfer Versicherungsnehmer war, im Rahmen der Schadensabwicklung kontaktiert. Dabei stellte sich heraus, dass die Schadenssachbearbeiterin Zugriff auf die im Rahmen des früheren Rentenversicherungsvertrags gespeicherten personenbezogenen Daten nehmen konnte, da diese auf eine Namensabweichung gegenüber den hinterlegten personenbezogenen Daten der Beschwerdeführerin hinwies. Die Beschwerdeführerin war sich darüber im Klaren, dass personenbezogene Daten im Rahmen der Durchführung und Abwicklung des Rentenversicherungsvertrags noch aufzubewahren waren, allerdings zeigte sie sich erschrocken darüber, dass offenbar diverse Abteilungen – ohne nachvollziehbare Zwecke zu verfolgen – Zugriff auf ihre personenbezogenen Daten haben und bat daher die Aufsichtsbehörde um Einleitung eines Prüfverfahrens.

Das Versicherungsunternehmen teilte auf aufsichtsbehördliche Nachfrage im Wesentlichen mit, dass die personenbezogenen Daten der Beschwerdeführerin trotz der in der Vergangenheit liegenden Kündigung des Rentenversicherungsvertrags und dessen Übertragung auf einen anderen Anbieter aufgrund gesetzlicher Aufbewahrungs- und Meldepflichten gemäß Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit fachspezifischem Recht[42] aufzubewahren waren. Die noch ausschließlich auf der Grundlage von Art. 6 Abs. 1 lit. c DSGVO verarbeiteten personenbezogenen Daten würden in den Datenbanken und Fachanwendungen gesperrt und damit dem Zugriff der Sachbearbeitung entzogen; ausschließlich zur Erfüllung gesetzlicher Mitteilungspflichten würden die Daten der Beschwerdeführerin kurzzeitig entsperrt, um dem neuen Anbieter der Riester-Rentenversicherung die in § 92 Einkommensteuergesetz (EStG)

[42] Nach § 19 Abs. 3 Altersvorsorge-Durchführungsverordnung (AltvDV) sind Versicherungsunternehmer verpflichtet, vertragsrelevante Unterlagen spätestens am Ende des zehnten Kalenderjahres zu löschen oder zu vernichten, das auf die Mitteilung nach § 22 Nr. 5 Satz 7 Einkommensteuergesetz (EStG) folgt.

genannten Daten[43] einschließlich der auf den Zeitpunkt der Übertragung fortgeschriebenen Beträge mitteilen zu können (§ 11 Altersvorsorge-Durchführungsverordnung - AltvDV).

Während der Stammdatensatz der Beschwerdeführerin, bestehend u.a. aus dem Namen und der Anschrift sowie laufenden Geschäftsobjekten, hier Angaben über den Rentenversicherungsvertrag, im Fall der Sperrung in den Fachanwendungen und Datenbanken weder angezeigt wurde noch bearbeitet werden konnte, galt für den Zeitraum der Entsperrung etwas anderes; so war zum Zeitpunkt der Kontaktaufnahme der Schadenssachbearbeiterin mit der Beschwerdeführerin die Sperre zur Erfüllung gesetzlicher Mitteilungspflichten zeitweilig aufgehoben, mit der Folge, dass der Stammdatensatz der Beschwerdeführerin auch in der Fachanwendung für die Schadenssachbearbeiterin abruf- und bearbeitbar war.

Ergänzend teilte das Versicherungsunternehmen hierzu mit, dass die während des Entsperrzyklus mögliche, zeitweilige Datenabrufbarkeit in den Fachanwendungen zur Erfüllung der gesetzlichen Meldepflichten erforderlich sei und nur so für die zu übermittelnden Daten eine Aktualität im Sinne der Datenrichtigkeit nach Art. 5 Abs. 1 lit. d DSGVO gewährleistet werden könne.

Sowohl die zum Zweck der Erfüllung gesetzlicher Mitteilungspflichten nach § 11 Abs. 1 und § 19 Abs. 1 und 2 AltvDV erfolgende Datenübermittlung an den neuen Anbieter als auch die Datenabrufbarkeit in den Fachanwendungen für die Sachbearbeitung während des Entsperrzyklus ist als Datenverarbeitung in Form der Offenlegung im Sinne des Art. 4 Nr. 2 DSGVO zu qualifizieren. Für die Erforderlichkeit dieser Datenoffenlegung zur Erfüllung der gesetzlichen Meldepflichten ist unter anderem auf den sich aus der maßgeblichen rechtlichen Verpflichtung ergebenden Verarbeitungszweck abzustellen. Angesichts der konkreten Vorgaben zur Datenoffenlegungspflicht gegen-

[43] U.a. die Höhe der jährlichen Altersvorsorgebeiträge.

über dem neuen Anbieter nach der AltvDV ist der Verarbeitungszweck und das Verarbeitungshandeln präzise vorgegeben und somit nach Art. 6 Abs. 1 lit. c DSGVO legitimiert. Dies ist für die verfahrensgegenständliche Datenabrufbarkeit in den internen Fachanwendungen und Datenbanken des Versicherungsunternehmens während des Entsperrzyklus keineswegs ersichtlich; die gesetzliche Mitteilungspflicht wurde durch die situative Datenabrufbarkeit in den Fachanwendungen erkennbar weder direkt verfolgt noch entscheidend gefördert.

Daneben gilt das Gebot der Datenrichtigkeit im Sinne des Art. 5 Abs. 1 lit. d DSGVO in Ausprägung der Datenaktualität nicht absolut, sondern ist anhand des Verarbeitungszwecks zu beurteilen. Wie der Wortlaut der Vorschrift verdeutlicht („erforderlichenfalls auf dem neuesten Stand", „im Hinblick auf ihre Zwecke ihrer Verarbeitung"), sieht sie die Gewährleistung einer dem jeweiligen Verarbeitungszweck abgeleiteten, zeitlich kontextualisierten[44] Datenrichtigkeit vor. Für das datenempfangende Versicherungsunternehmen sollte vor dem Hintergrund einer dort vorliegenden Meldehistorie, die bspw. Vertragsnummer und -datum umfasst,[45] auch für den Fall zwischenzeitlich geänderter Namens- oder Adressdaten ein Abgleich mit dem dort vorliegenden Datenbestand möglich sein. Folglich ergibt sich für die zum letzten Geschäftskontakt aktuellen Daten der betroffenen Personen eine zeitlich-kontextualisierte Datenrichtigkeit, die ausdrücklich nicht von einem zwingenden Aktualitätserfordernis („erforderlichenfalls") durchbrochen wird. Zudem wäre eine nur zeitweilige Datenabrufbarkeit während des Entsperrzyklus ohnehin nicht geeignet, die Datenaktualität dann konsequent zu gewährleisten, wenn ein Datenabgleich – wie beschwerdegegenständlich – allenfalls rein zufällig erfolgen kann.

[44] OVG Hamburg, Beschl. v. 27.5.2019 – 5 Bf 225/18.Z, NVwZ 2019, 1532 Rn. 22.
[45] § 11 Abs. 1 S. 3 AltvDV.

Das Unternehmen wurde schließlich aufgefordert, technische und organisatorische Maßnahmen im Sinne der Artt. 25 und 32 DSGVO zu implementieren, um revisionssicher zu gewährleisten, dass auch im Falle der Entsperrung die jeweiligen personenbezogenen Datensätze nicht in den Fachanwendungen für andere Zwecke (bspw. zur Schadensabwicklung, zur Gewährleistung der Datenrichtigkeit o.ä.) – soweit sich hierfür keine Legitimationsgrundlage nach Art. 6 Abs. 1 DSGVO ergibt – verarbeitet werden.

## 8.4 Cyberangriff auf Dienstleister im Bereich Wohnungswirtschaft

Ein Dienstleister im Bereich Wohnungswirtschaft wurde bereits im Juli 2022 Ziel eines Cyberangriffs, in dessen Zusammenhang Angreifer Zugriff auf bei dem Unternehmen gespeicherte personenbezogene Daten – u. a. Abrechnungsdaten aus den Jahren 2006 bis 2012, Namen und Anschriften, Größe der Wohneinheiten – erlangt und diese im Darknet veröffentlicht haben. Das Unternehmen, das bundesweit in der Regel als Auftragsverarbeiter für Heizkostenabrechnung im Auftrag von Wohnungsunternehmen, Hausverwaltungen und Einzelvermietern tätig ist, hat seine Auftraggeber im August 2022 über die stattgefundene Verletzung des Schutzes personenbezogener Daten nach Art. 33 Abs. 2 Datenschutz-Grundverordnung benachrichtigt und dabei sachverhaltsbezogene Begleitinformationen, wie betroffene Datenkategorien und die Anzahl der betroffenen Personen, zur Verfügung gestellt. Während der Dienstleister aus datenschutzrechtlicher Sicht als Auftragsverarbeiter im Sinne des Art. 28 DSGVO agiert, werden die von dem Cybersicherheitsvorfall tangierten personenbezogenen Daten von den jeweiligen Auftraggebern als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO verarbeitet. Obschon der Dienstleister die für ihn zuständige Datenschutzaufsichtsbehörde über den Cybersicherheitsvorfall informierte bzw. diesen an die bundesweit betroffenen Auftraggeber nach Art. 33 Abs. 2 DSGVO

meldete, erreichte unsere Behörde keine Meldung nach Art. 33 Abs. 1 DSGVO von saarländischen Verantwortlichen.

Die für den Dienstleister zuständige Aufsichtsbehörde stellte uns auf Nachfrage eine Liste von saarländischen Auftraggebern zur Verfügung, so dass durch unsere Behörde eine Anzahl von Wohnungsunternehmen mittels Fragenkatalog um Stellungnahme gebeten wurden, welche Maßnahmen diese nach Eingang der Information des Dienstleisters über den stattgefundenen Cybersicherheitsvorfall im Einzelnen ergriffen haben und wie der Prozess zum Umgang mit Datenschutzverletzungen operationalisiert wurde. Die diesbezüglichen Rückmeldungen der befragten Unternehmen ließen zumindest erkennen, dass unternehmensinterne Verfahren für den Fall von festgestellten Datenschutzverletzungen zwar implementiert waren, aber diese unternehmensinternen Prozesse im Zusammenhang mit dem stattgefundenen Cybersicherheitsvorfall gerade nicht dazu geführt haben, dass adäquate Maßnahmen ergriffen wurden. Da der Dienstleister in seiner Information über den Vorfall an die Auftraggeber mitgeteilt hat, dass keine besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO betroffen sind und dementsprechend durch die Datenoffenlegung ein „Schadenseintritt" für betroffene Personen nicht wahrscheinlich sei, haben sich nahezu alle der befragten Wohnungsunternehmen auf diese Aussagen unkritisch verlassen und nach Dokumentation der erteilten Information des Dienstleisters im Sinne des Art. 33 Abs. 5 DSGVO keine weiteren Maßnahmen ergriffen.

Zur Klärung der Frage, ob die mit dem Cybersicherheitsvorfall verbundene Datenschutzverletzung der Aufsichtsbehörde nach Art. 33 Abs. 1 DSGVO zu melden und eine Benachrichtigung der betroffenen Personen nach Art. 34 Abs. 1 DSGVO erforderlich gewesen wäre, hätten die Wohnungsunternehmen das Risiko für Rechte und Freiheiten der von der Datenschutzverletzung betroffenen Personen prognostisch bewerten werden müssen. Für die Ermittlung der Eintrittswahrscheinlichkeit und Schwere von Nachteilen für die von der Datenschutzverletzung

betroffenen Personen hätten dabei bspw. die Faktoren spezifischer Schutzbedarf der offengelegten Daten, Anzahl und besondere Eigenschaften der betroffenen Personen, Verarbeitungskontext und ggf. weitere sachverhaltsbezogene Parameter Berücksichtigung finden müssen. Um eine ausreichende Beurteilungsgrundlage herzustellen, hätten die befragten Wohnungsunternehmen somit bei dem Auftragsverarbeiter weitere Informationen einholen und weitere Erkenntnismittel in Betracht ziehen müssen; nur auf diese Weise wäre es den Unternehmen möglich gewesen, die Aussagen zur Unwahrscheinlichkeit eines Schadenseintritts durch eigene Prüfung zu validieren und darauf gestützt eine objektiv überprüfbare Prognoseentscheidung zu treffen. Allein die Mitteilung des Dienstleisters mit den darin getroffenen Aussagen zur vermeintlichen Unwahrscheinlichkeit eines „Schadenseintritts" war als Beurteilungsgrundlage für die nach Art. 33 Abs. 1 und Art. 34 Abs. 1 DSGVO zu fordernde Risikoprognose jedenfalls unzureichend.

Den Wohnungsunternehmen wurde im Wege des Hinweises nach Art. 58 Abs. 1 lit. d DSGVO mitgeteilt, dass die entsprechenden unternehmensinternen Prozesse als defizitär anzusehen waren und das Ergreifen geeigneter Erkenntnismittel zur Schaffung einer hinreichenden Beurteilungsgrundlage für die Risikobewertung operationalisiert werden müsse. Im Nachgang meldete die überwiegende Anzahl der befragten Wohnungsunternehmen den Cybersicherheitsvorfall als Datenschutzverletzung. Das Ergreifen von Sanktionen nach Art. 58 Abs. 2 DSGVO gegenüber den untersuchten Wohnungsunternehmen war dabei nicht opportun.

# IX.

# Videoüberwachung

# 9 Videoüberwachung

## 9.1 Verwaltungsvorschrift zum Umgang mit Beschwerden

Bereits seit Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) ist insbesondere im Bereich der nachbarschaftlichen Videoüberwachung aufgrund des hohen Beschwerdeaufkommens und der begrenzten personellen Ressourcen eine Bearbeitung der Anliegen von Bürgerinnen und Bürger nicht mehr in einem Umfang gewährleistet, der dem Grundrecht auf Schutz der personenbezogenen Daten angemessen Rechnung trägt. Komplexen datenschutzrechtlichen Zulässigkeitsvoraussetzungen, die Privatpersonen als Kamerabetreiber häufig überfordern, stehen fehlende effektive Untersuchungsbefugnisse im räumlichen Zusammenhang mit Privatwohnungen und eine knappe aufsichtsbehördliche Personalausstattung gegenüber, mit der Folge einer erheblichen Ausdehnung der jeweiligen Verfahrensdauer.

Um diesem Vollzugsdefizit bei der aufsichtsrechtlichen Aufgabenwahrnehmung, das sowohl dem unionsrechtlichen Effektivitätsgrundsatz[46] als auch dem für Verwaltungsverfahren geltenden Effizienzgebot[47] entgegenläuft, begegnen zu können, wurde die für die Mitarbeitenden unserer Behörde geltende „*Verwaltungsvorschrift zum Umgang mit Beschwerden nach Art. 77 DSGVO im Kontext der von Privatpersonen betriebenen Videoüberwachungsmaßnahmen*" erlassen. Mit dieser ermessenslenkenden Verwaltungsvorschrift wurde dabei das Ziel verfolgt, durch eine standardisierte Vorgabe zur Bearbeitung von Fällen der nachbarschaftlichen Videoüberwachung dem Anspruch der Beschwerdeführenden auf ermessensfehlerfreie, angemessene Befassung mit ihren Anliegen zu genügen und

[46] Art. 4 Vertrag über die Europäische Union (EUV).
[47] § 10 S. 2 Saarländisches Verwaltungsverfahrensgesetz (SVwVfG).

gleichzeitig ein effektiviertes, ressourcenschonendes Verwaltungsverfahren zu gewährleisten.

Soweit sich nach Würdigung eines beschwerdegegenständlichen Vorbringens bloße Anhaltspunkte für einen datenschutzrechtlichen Verstoß in Form einer nicht ausschließlich auf das selbstgenutzte Grundstück eines Kamerabetreibers beschränkten Überwachungsmaßnahme ergeben, ist zunächst die Einleitung von Untersuchungsbefugnissen nach Art. 58 Abs. 1 DSGVO erforderlich. Eine wesentliche Effektivierung des Verwaltungsverfahrens wird dabei gerade nicht mit einer an den Kamerabetreiber adressierten Aufforderung zur Bereitstellung von Informationen nach Art. 58 Abs. 1 lit. a DSGVO oder der Durchführung von Vorortkontrollen nach Art. 58 Abs. 1 lit. f DSGVO, sondern vielmehr durch einen das Verfahren bereits an dieser Stelle abschließenden Hinweis nach Art. 58 Abs. 1 lit. d DSGVO erreicht.

Gibt es laut Beschwerdevortrag keine greifbaren Anhaltspunkte für eine Überwachung öffentlicher Bereiche und damit einhergehend ein eng begrenzter Personenkreis, der von dem Kameraeinsatz betroffen ist, sprechen in typisierender Betrachtung ein mit der Beschwerdebefassung verbundener regelmäßiger Untersuchungsaufwand und die diesbezügliche Bindung aufsichtsbehördlicher Ressourcen sowie die betroffenen Individualrechtsgüter und das Beziehungsgefüge zwischen Kamerabetreiber und betroffener Person im Regelfall gegen ein über die Maßnahme nach Art. 58 Abs. 1 it. d DSGVO hinausgehendes aufsichtsbehördliches Tätigwerden.

In den vorstehenden Fällen sieht die Verwaltungsvorschrift folgendes vor:

Der vermeintlich eine Videoüberwachungsmaßnahme betreibenden Person wird mittels eines standardisierten Schreibens mitgeteilt, dass der Aufsichtsbehörde diesbezüglich ein potenzieller datenschutzrechtlicher Verstoß im Rahmen einer Beschwerde vorgetragen wurde. In diesem Schreiben werden ferner die Anforderungen für einen datenschutzkonformen

Betrieb einer Videoüberwachungsmaßnahme dargelegt und anhand von Beispielen für unzulässige Überwachungsszenarien erläutert sowie Gelegenheit gegeben, eine gegebenenfalls bestehende Rechtswidrigkeit der Überwachungsmaßnahme zu beseitigen.

Die beschwerdeführende Person wird im Rahmen einer standardisierten Abschlussmitteilung darüber unterrichtet, dass der Anlagenbetreiber auf Grundlage der Verwaltungsvorschrift auf einen gegebenenfalls bestehenden Verstoß und die Bedingungen für einen datenschutzkonformen Betrieb der Überwachungsanlage hingewiesen wurde. Darüber hinaus wird aufgrund des mit der Kamera verbundenen Eingriffs in das allgemeine Persönlichkeitsrecht und des im Fall einer Attrappe fortbestehenden Überwachungsanscheins auf die Möglichkeit der Geltendmachung eines Abwehr- und Beseitigungsanspruchs auf dem Zivilrechtsweg hingewiesen.

Nach zweijähriger Erfahrung mit dem Einsatz der Hinweisschreiben kann ein durchweg positives Fazit gezogen werden. In der überwiegenden Mehrzahl der Fälle war eine datenschutzwidrige Videoüberwachung von Privatpersonen nicht intendiert, sondern schlicht auf Unachtsamkeit und Unkenntnis datenschutzrechtlicher Vorgaben zurückzuführen; nach den bisherigen Rückmeldungen war für die Adressatinnen und Adressaten der Hinweis nach Art. 58 Abs. 1 lit. d DSGVO überhaupt erst Anlass, sich mit rechtlichen Voraussetzungen zu privaten Kameraeinsätzen zu befassen und diese sodann umzusetzen. Bei Verfahren, die nach den Vorgaben der Verwaltungsvorschrift bearbeitet wurden, kam es zudem bislang nicht zu Folgebeschwerden, was aus hiesiger Sicht für die Effektivität und Zweckmäßigkeit ebendieses aufsichtsrechtlichen Vorgehens spricht.

## 9.2 Videoüberwachung im privaten Umfeld

Trotz der Effektivierung der Beschwerdebefassung durch die beschriebene Verwaltungsvorschrift nahmen in den vergangenen Berichtszeiträumen die durch Privatpersonen betriebenen

Videoüberwachungsmaßnahmen in quantitativer Hinsicht einen erheblichen Anteil der hier eingegangenen Beschwerden ein und banden aufsichtsbehördliche Ressourcen. Das Bedürfnis, das subjektive Sicherheitsgefühl im privaten Umfeld zu erhöhen, und ein signifikanter Preisverfall von Überwachungstechnik, führen zu einem Umsichgreifen von Überwachungssystemen im nachbarschaftlichen Kontext. Das Einsatzspektrum ist dabei breit gefächert: neben klassischen Überwachungskameras werden vermehrt elektronische Türspione installiert, Tierbeobachtungskameras werden im heimischen Garten aufgestellt, und Dashcams zeichnen permanent das Verkehrsgeschehen auf.

Der aufsichtsbehördliche Prüfauftrag, die datenschutzrechtliche Zulässigkeit von Kameraeinsätzen zu beurteilen und ggf. Maßnahmen zur Herstellung datenschutzkonformer Zustände zu ergreifen, beginnt grundsätzlich mit der Aufklärung des zugrundeliegenden Sachverhalts. Nach Art. 58 Abs. 1 lit. a DSGVO sind Anlagenbetreiber verpflichtet, der Aufsichtsbehörde die zur Aufgabenerfüllung erforderlichen Informationen zur Verfügung zu stellen. Wird dieser Pflicht nicht nachgekommen, kann die Auskunftserteilung durch Bescheid angeordnet werden. Werden die Auskünfte ungeachtet dessen nicht erteilt, kann die den Verwaltungsakt erlassende Behörde nach dem Saarländischen Verwaltungsvollstreckungsgesetzes (SVwVG) Zwangsmittel anwenden. In einem ersten Schritt können gemäß § 21 SVwVG Zwangsgelder festgesetzt werden. Sofern auch die Festsetzung von Zwangsgeldern nicht den angestrebten Erfolg herbeiführt, kann auch ein Antrag auf Erzwingungshaft gemäß § 28 SVwVG beim Verwaltungsgericht des Saarlandes gestellt werden. Andere Zwangsmittel wie die Ersatzvornahme oder unmittelbarer Zwang kommen nicht in Betracht, da die Erteilung der Auskünfte zur Videoüberwachung eine Pflicht begründet, die regelmäßig nur der Verwaltungsaktadressat selbst erbringen kann.

Sobald alle entscheidungserheblichen Informationen bzw. Unterlagen vorliegen, obliegt es der Aufsichtsbehörde zu be-

urteilen, ob die Anlage den datenschutzrechtlichen Anforderungen genügt oder bestimmte Anpassungsmaßnahmen vorzunehmen sind. Im letztgenannten Falle kann die Aufsichtsbehörde eine Beschränkung oder auch ein Verbot der Videoüberwachungsmaßnahme gemäß Art. 58 Abs. 2 lit. f DSGVO anordnen, sofern der Anlagenbetreiber dem nicht ohnehin nachkommt.

Von ihren Anordnungsbefugnissen nach Art. 58 DSGVO hat die Aufsichtsbehörde im Berichtszeitraum in etlichen Fällen Gebrauch gemacht. In einigen Fällen hat sich das Verwaltungsgericht des Saarlandes aufgrund eingelegter Rechtsbehelfe mit der Rechtmäßigkeit der diesbezüglichen Anordnungen befasst.

### 9.2.1 Auskunftsverweigerungsrecht des Betroffenen

Im Rahmen eines Beschwerdeverfahrens verweigerte der Anlagenbetreiber neben der Erteilung diverser Auskünfte zur Videoüberwachung auch die Zurverfügungstellung von Bildaufnahmen, die der Feststellung der konkreten Erfassungsbereiche der angebrachten Überwachungskameras dienen sollten. Hiesiges, per einfachem Brief übersandte Aufforderungsschreiben war mit einem Hinweis versehen, dass der Auskunftspflichtige gemäß § 40 Abs. 4 Satz 2 Bundesdatenschutzgesetz (BDSG) die Auskunft auf solche Fragen verweigern kann, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

Bevor die Bereitstellung der erforderlichen Informationen angeordnet werden konnte, wurde der Anlagenbetreiber gemäß § 28 Saarländisches Verwaltungsverfahrensgesetz (SVwVfG) angehört. Weder das Anhörungsschreiben noch die im Nachgang dazu ausgesprochene und förmlich zugestellte Anordnung enthielten allerdings einen Hinweis auf das Auskunftsverweigerungsrecht. Daneben wurde die sofortige Vollziehung

des Bescheids gemäß § 80 Abs. 2 Nr. 4 Verwaltungsgerichtsordnung (VwGO) angeordnet.

Der Verantwortliche erhob Klage beim Verwaltungsgericht des Saarlandes gegen den Auskunftsheranziehungsbescheid und beantragte gemäß § 80 Abs. 5 VwGO die Wiederherstellung der aufschiebenden Wirkung seiner Klage; er war der Auffassung, dass er ausschließlich sein eigenes Grundstück überwache und der Betrieb der Überwachungskameras nach Art. 2 Abs. 2 Nr. 3 DSGVO als eine „*Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten*" nicht in den Anwendungsbereich der Verordnung falle. Darüber hinaus teilte er mit, er habe das ursprüngliche Aufforderungsschreiben, das den Hinweis nach § 40 Abs. 4 Satz 2 BDSG enthielt, nicht erhalten.

Das Gericht führte in seiner Entscheidung aus, dass die Anordnung der sofortigen Vollziehung den formalen Erfordernissen des § 80 Abs. 3 Satz 1 VwGO entsprechen würde. So spreche die Intention des Art. 58 Abs. 1 lit. a DSGVO dafür, dass der Antragsteller sich nicht durch Einlegung eines Rechtsbehelfs auf unbestimmte Zeit der aufsichtsbehördlichen Kontrolle entziehen können dürfe, da die zeitnahe Erteilung der Auskünfte notwendig sei, um dem öffentlichen Interesse an der Überprüfung der Einhaltung der datenschutzrechtlichen Vorschriften schnellstmöglich gerecht zu werden. Da durch den Beschwerdeführer Bildaufnahmen der Überwachungskameras vorgelegt wurden und aufgrund der erkennbaren Ausrichtung eine Erfassung von Bereichen außerhalb seines selbstgenutzten Grundstücks wahrscheinlich war, bestanden nach Ansicht der Kammer zudem ausreichende Anhaltspunkte dafür, dass deren Betrieb nicht ausschließlich zu persönlich-familiären Zwecken erfolgte.[48]

Allerdings falle die im Rahmen der nach § 80 Abs. 5 VwGO vorzunehmende Abwägung mangels nachweislich erfolgter Belehrung des Antragstellers über sein Auskunftsverweige-

[48] Vgl. EuGH, Urteil vom 11.12.2014, Reynes (C-212/13).

rungsrecht zu dessen Gunsten aus, weshalb dem Antrag stattzugeben sei. § 40 Abs. 4 S. 2 BDSG trage dem Grundsatz der Selbstbelastungsfreiheit Rechnung. Eine fehlende Belehrung führe zu einem Verwertungsverbot erteilter Auskünfte in einem etwaigen Bußgeld- und Strafverfahren und könne behördlichen Auskunftsbegehren entgegenstehen.

Der Antragsteller sei daher berechtigt gewesen, die Auskunft auf solche Fragen zu verweigern, die ihn der Gefahr eines Ordnungswidrigkeitsverfahrens aussetzen würden. Das Gericht bejahte dies für wesentliche Teile des Fragenkatalogs sowie im Hinblick auf die Übersendung der Musterbilder der Erfassungsbereiche, da ein möglicher Datenschutzverstoß im Raum stand, und dieser potentiell bußgeldbewehrt ist. Ob ein Berufen auf das Auskunftsverweigerungsrecht bei ordnungsgemäßer Belehrung dazu geführt hätte, dass der Antragsteller die Auskünfte nicht hätte erteilen müssen, wurde in dem Verfahren nicht abschließend geklärt.

Hiesige Prüfpraxis wurde in der Folge dergestalt angepasst, dass Beschwerdegegner nunmehr in sämtlichen aufsichtsbehördlichen Schreiben auf ihr gesetzliches Auskunftsverweigerungsrecht hingewiesen werden. Dies insbesondere auch im Rahmen des per Postzustellungsurkunde übermittelten Auskunftsheranziehungsbescheides. So wurde auch der Verantwortliche im Nachgang in entsprechender Anwendung nochmals zur Stellungnahme hinsichtlich des Betriebs der Videoüberwachungsmaßnahme aufgefordert. Umso erstaunlicher war, dass er nunmehr alle entscheidungserheblichen Informationen ohne größeren Widerstand zur Verfügung stellte – und diese auch keinen Anlass für ein weiteres aufsichtsbehördliches Tätigwerden gaben.

### 9.2.2 Verweigerung der Auskunftserteilung

In einem weiteren Verfahren weigerte sich ein Anlagenbetreiber auf aufsichtsbehördliche Schreiben zu antworten; auch mittels Zwangsgelder konnte der Anlagenbetreiber nicht zu den geforderten Auskünften veranlasst werden, da diese man-

gels wirtschaftlicher Leistungsfähigkeit nicht eingetrieben werden konnten. Aus diesem Grund wurde ihm durch Bescheid angedroht, beim Verwaltungsgericht des Saarlandes einen Antrag auf Anordnung der Erzwingungshaft gemäß § 28 SVwVG zu stellen, soweit die begehrten Informationen weiterhin nicht zur Verfügung gestellt werden.

Gegen diese Androhung klagte der Anlagenbetreiber beim Verwaltungsgericht des Saarlandes. Er trug vor, die verfahrensgegenständlichen Kameras seien bereits abgebaut, so dass sich die begehrte Auskunftserteilung über Art und Umfang der Videoüberwachung erledigt habe. Dass der behauptete Kameraabbau unzutreffend war, ergab ein unangekündigter Vorortttermin am Privathaus des Klägers. Diese Erkenntnis wurde dem Gericht mitgeteilt.

Nach Auffassung des Verwaltungsgerichts hatte sich der Verwaltungsakt aber dennoch durch die im Rahmen der Klagebegründung erfolgte Mitteilung des Anlagenbetreibers, dass er die Kameras abgebaut habe, erledigt. Damit seien weitere Erläuterungen zur Modalität der Kamera überflüssig und das behördliche Auskunftsersuchen obsolet. Das Gericht statuierte in der Entscheidung, dass der Aufsichtsbehörde kein Anspruch auf Erteilung einer bestimmten Auskunft zustehe und sie sich daher mit der erfolgten Mitteilung des Klägers, er habe die Kameras abgebaut, zufriedengeben müsse; dass im Rahmen des Vorortttermins ein weiteres Vorhandensein der verfahrensgegenständlichen Kameras dokumentiert wurde und der behauptete Kameraabbau damit objektiv wahrheitswidrig war, war nach Wertung des Gerichts unerheblich.

Diesseits wurde nach § 124 Abs. 2 Nr. 1 Verwaltungsgerichtsordnung (VwGO) mit Blick auf ernstliche Zweifel an der Richtigkeit der Entscheidung ein Antrag auf Zulassung der Berufung gestellt. Soweit das Verwaltungsgericht die Auffassung vertritt, es sei unbeachtlich, inwiefern die getätigten Auskünfte zum Kameraabbau zutreffen oder falsch sind, wird nach hiesiger Auffassung der Zweck und die Reichweite von

Art. 58 Abs. 1 lit. a DSGVO konterkariert. Der hierin geregelte Informationsanspruch der Aufsichtsbehörde, welcher auf Seiten des Verantwortlichen mit einer Auskunftsverpflichtung einhergeht, kann nach seinem Sinn und Zweck nur dahingehend ausgelegt werden, dass der Aufsichtsbehörde zutreffende, d. h. aus Sicht des Verantwortlichen wahre Informationen übermittelt werden. Ein Auskunftsverlangen ist hiernach vollständig, richtig, zeitlich aktuell und nachvollziehbar zu beantworten.[49] Gesetzessystematisch korrespondiert dies mit dem Auskunftsverweigerungsrecht in Art. 58 Abs. 4 DSGVO i.V.m. § 40 Abs. 4 S. 2 BDSG; hiernach wird die Auskunftspflicht in den dort normierten Tatbeständen zwar eingeschränkt, allerdings mit der Folge, dass der Verantwortliche lediglich zur Verweigerung von Auskünften und gerade nicht zur unwahren, unvollständigen oder irreführenden Auskunftserteilung berechtigt ist.

Über den Zulassungsantrag wurde bisher noch nicht entschieden.

### 9.2.3 Überwachung privater Zuwegungen

Videoüberwachungsmaßnahmen im nachbarschaftlichen Kontext bergen häufig erhebliches Konfliktpotential. So auch im Falle einer Videoüberwachung im Umfeld eines landwirtschaftlichen Betriebs, bei der der Landwirt sein Grundstück mit Überwachungskameras gesichert hatte. Allerdings führte über sein Grundstück eine Zuwegung, die dem benachbarten Hof als einziger Zugang zum Gelände diente. Die Betreiber und Besucher des benachbarten Hofs waren demnach gezwungen, den mit Videokameras überwachten Bereich zu durchqueren, um überhaupt zu dem Hofgelände zu gelangen bzw. diesen wieder verlassen zu können. Das Bestehen eines Wegerechts war dabei bereits Gegenstand einer zivilgerichtlichen Auseinandersetzung. Den Betreibern des benachbarten Hofs wurde

[49] Thüringer OVG, Beschluss vom 19. März 2021 – 3 EO 423/20, Rn. 40, juris; Selmayr, in Ehmann/Selmayr, DSGVO 2. Aufl. 2018, Art. 58 Rn. 12.

dabei die Inanspruchnahme der Zuwegung im Wege eines Notwegerechts gerichtlich zugesichert, nachdem der Landwirt ebendiese Zuwegung über einen längeren Zeitraum mithilfe von Bauzäunen blockiert hatte.

Im Rahmen der datenschutzrechtlichen Prüfung wurde die Einstellung der Videoüberwachung im Bereich der Zuwegung wegen eines Verstoßes gegen Art. 6 Abs. 1 lit. f DSGVO angeordnet. Gegen den Bescheid klagte der Anlagenbetreiber vor dem Verwaltungsgericht des Saarlandes.

### Haushaltsausnahme nach Art. 2 Abs. 2 lit. c DSGVO

Das Verwaltungsgericht des Saarlandes sah den Anwendungsbereich der DSGVO gemäß Art. 2 Abs. 2 lit. c DSGVO nicht als eröffnet an. Danach unterfallen solche Verarbeitungen nicht dem datenschutzrechtlichen Regelungsregime, die durch eine natürliche Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgen (sog. Haushaltsausnahme). Nach Ansicht des Verwaltungsgerichts seien räumliche und soziale Gesichtspunkte sowie der Zweck der Datenverarbeitung bei der Abgrenzung zwischen privaten und nicht-(nur)-privaten Tätigkeiten heranzuziehen. In räumlicher Sicht sei entscheidend, ob öffentliche Bereiche oder der Privatbereich des Verarbeiters betroffen seien. In sozialer Hinsicht komme es auf die Beziehung des Verarbeiters zu den betroffenen Personen an und welcher Personenkreis Zugriff auf die verarbeiteten Daten erhalten soll.

Nach der Rechtsprechung des europäischen Gerichtshofs könne sich eine Privatperson zwar dann nicht auf das Haushaltsprivileg berufen, soweit durch die Überwachungskameras auch Teile des öffentlichen Verkehrsraums erfasst werden,[50] vorliegend habe der Anlagenbetreiber aber keine öffentlichen Bereiche erfasst, sondern ausschließlich sein eigenes Grundstück. Die Überwachung des eigenen Grundstücks zum Selbst-

[50] Vgl. EuGH, Urteil vom 11.12.2014, Reynes (C-212/13).

schutz unterfalle der Haushaltsausnahme, so dass die DSGVO für die verfahrensgegenständliche Kamera keine Anwendung finden könne. Das Notwegerecht führe nicht dazu, dass der Bereich der Zuwegung als öffentlich zugänglich zu qualifizieren sei.

Unsere Behörde trat dieser Einschätzung entgegen, da bereits in räumlich-sozialer Sicht einiges gegen die Haushaltsausnahme sprach. Denn der von der Videoüberwachung betroffene Personenkreis, die Inhaber des benachbarten Landwirtschaftsbetriebs und deren zahlreiche Besucher, war gerade nicht dem familiären Umfeld des Anlagenbetreibers zuzurechnen. Auch war der vom Anlagenbetreiber im Rahmen des Verwaltungsverfahrens kommunizierte Zweck der Überwachungsmaßnahme ein starkes Indiz gegen eine ausschließlich persönlich-familiäre Tätigkeit. Die Überwachung des von den Beschwerdeführern und deren Besuchern täglich genutzten Überwegs sollte gerade auch der Beweissicherung bei eingetretenen Schadenshandlungen dienen und deren Ahndung ermöglichen. Im Bedarfsfalle sollten die Aufzeichnungen den Strafverfolgungsbehörden übergeben werden. Zudem wurden die Kameras nicht im unmittelbaren Wohnumfeld des Betreibers, sondern auf einem landwirtschaftlichen Betriebsgelände eingesetzt.

Das Gericht hob indes den Bescheid in weiten Teilen mangels Anwendbarkeit der DSGVO mit der Begründung auf, dass lediglich eine private Zuwegung überwacht wurde und insoweit die privilegierende Wirkung der Haushaltsausnahme zum Tragen komme.

### Datenschutzrechtliche Zulässigkeit nach Art. 6 Abs. 1 lit. f DSGVO

Auch für den Fall der Anwendbarkeit der DSGVO sah das Gericht die konkrete Videoüberwachungsmaßnahme auf der Grundlage des Art. 6 Abs. 1 lit. f DSGVO als legitimiert an. Nach dieser Vorschrift ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn diese zur Wahrung der berechtigten

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

Auch wenn durch den Anlagenbetreiber im Verwaltungsverfahren einige Vorkommnisse, wie Beschädigungen von Bauzäunen belegt werden konnten, war unter Berücksichtigung der im Raum stehenden Überwachungsinteressen die Kameraerfassung des mit dem Wegerecht belasteten Teil des Grundstücks aus Sicht unserer Behörde nicht legitimiert. Insbesondere war zu berücksichtigen, dass aufgrund des Überwachungskontextes tagtäglich eine Vielzahl von Personen anlasslos erfasst wurden und gerade auch Kinder regelmäßig von der Videoüberwachung betroffen waren, deren personenbezogene Daten besonders schützenswert sind.

In der mündlichen Verhandlung führte der Anlagenbetreiber sein Überwachungsinteresse untermauernde und im aufsichtsbehördlichen Verfahren nicht vorgelegte Videoaufnahmen als Beweismittel ein. Unter dem Eindruck des Inhalts der vorgelegten Videoaufnahmen und der mangelnden Möglichkeit der Aufsichtsbehörde, die Aufzeichnung auch unter Berücksichtigung der Perspektive der Beschwerdeführer situativ kontextualisieren zu können, stellte sich das Überwachungsinteresse des Anlagenbetreibers für das Gericht als überwiegend dar.

Eine Beiladung der Beschwerdeführer wurde zwar gemäß § 65 VwGO angeregt, allerdings sah die Kammer davon ab. Eine solche Beiladung von Beschwerdeführern könnte gerade in solchen Konstellationen, in denen die Behörde letztlich nicht über sämtliche tatsächlichen und für die Entscheidung maßgeblichen Informationen verfügt, der Wahrung der Interessen der Beschwerdeführer dienen und zudem dem Gericht die erforderliche Sachverhaltsaufklärung erleichtern.

### Ausblick

Durch die Rechtsprechung des Verwaltungsgerichts werden die aufsichtbehördlichen Maßnahmen im Bereich von durch Privatpersonen betriebenen Videoüberwachungsmaßnahmen deutlich eingeschränkt. Betrifft eine Videoüberwachung ausschließlich das Grundstück des Anlagenbetreibers, kann die Aufsichtsbehörde aufgrund der Haushaltsausnahme nicht tätig werden, selbst wenn Dritte das Grundstück zulässigerweise aufgrund eines eingeräumten Wegerechts betreten dürfen. Ungeachtet dessen, dass die gerichtlichen Feststellungen zur Anwendung der Haushaltsausnahme aufgrund der besonderen Umstände im entschiedenen Fall unsererseits nicht vollumfänglich geteilt werden, wird die aufsichtsbehördliche Befassung mit Fällen der Überwachung von mit Wegerechten belasteten Grundstücken zukünftig eher von Zurückhaltung geprägt sein.

## 9.3 KFZ-Kennzeichenerfassung bei Parkraumbewirtschaftung

Die Parkplatzsituation ist in vielen Städten angespannt. Kostenlose Parkplätze sind Mangelware und die Preise in innerstädtischen Parkhäusern können das Einkaufsvergnügen recht schnell trüben. Nicht selten werden daher die Parkflächen von verkehrsgünstig gelegenen Läden und Supermärkten in Anspruch genommen, um Erledigungen ohne zusätzliche Parkkosten machen zu können. Dies sehr zum Ärgernis der Parkplatzinhaber, die in Spitzenzeiten kaum genügend freie Parkfläche für ihre eigenen Kundinnen und Kunden zur Verfügung stellen können.

Um dem Problem des Fremd- und Dauerparkens begegnen zu können, stehen den Betreibern unterschiedliche Möglichkeiten zur Verfügung. Neben manuellen Schrankensystemen, die allerdings wartungsanfällig sind und auch zu Stoßzeiten zu Staus an den Ausfahrten führen können, kann durch Auslegen einer Parkscheibe die Standzeit nachgewiesen oder durch Bodensensoren die zulässige Parkdauer überprüft werden.

Als vergleichsweise neuartiges Instrument wird von Handelsunternehmen zur Kontrolle der Kundenparkplätze zunehmend die automatisierte Kennzeichenerfassung herangezogen. Dabei wird sowohl beim Befahren als auch beim Verlassen der Parkfläche das Kfz-Kennzeichen erfasst, um erkennen zu können, ob die im Vorfeld definierte Parkhöchstdauer überschritten wurde und um gegebenenfalls auch Kosten für die Parkraumnutzung geltend zu machen können.

Die datenschutzrechtliche Zulässigkeit ist dabei grundsätzlich nach Art. 6 Abs. 1 lit.f Datenschutz-Grundverordnung (DSGVO) zu beurteilen. Danach ist die Verarbeitung zulässig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und keine schutzwürdigen Interessen der betroffenen Personen überwiegen. Die Betreiber von Parkflächen haben ein grundsätzlich berechtigtes Interesse daran, dass ihre Parkflächen nicht durch Fremdparker und Dauerparker blockiert werden. In datenschutzrechtlich zulässiger Weise können solche Systeme dann betrieben werden, soweit ausschließlich das Kfz-Kennzeichen erfasst wird, transparent im Sinne der Art. 12 ff. DSGVO durch eine Hinweisbeschilderung zum Zeitpunkt des Befahrens des erfassten Bereichs auf den Einsatz derartiger Systeme hingewiesen wird und die gespeicherten Daten umgehend gelöscht werden, soweit keine Vertragsstrafe aufgrund einer Überschreitung der zulässigen Parkhöchstdauer geltend gemacht werden soll.

In einem im Berichtszeitraum untersuchten Sachverhalt wurden mehrere den jeweiligen Märkten zugehörigen Parkflächen eines Handelsunternehmens auf Grundlage eines Parkraumbewirtschaftungsvertrags durch einen auf den Betrieb einer Kennzeichenerfassung spezialisierten Dienstleister überwacht. Bei Überschreitung der Parkhöchstdauer wurde durch den Dienstleister eine – in solchen Fällen grundsätzlich zulässige – Halterermittlung durchgeführt und eine Vertragsstrafe in eigenem Namen geltend gemacht. Im Rahmen der Befassung mit der Parkraumüberwachung war letztlich fraglich, welcher Grad an datenschutzrechtlicher Verantwortlichkeit im Sinne des

Art. 4 Nr. 7 DSGVO dem Handelsunternehmen und dem Parkraum überwachenden Dienstleister zuzuschreiben war.

Wir sind dabei zu dem vorläufigen Ergebnis gelangt, dass die im Rahmen der im Wesentlichen als datenschutzrechtlich zulässigen Kennzeichenerfassung erfolgende Kooperation zwischen dem Handelsunternehmen und dem den Parkraum überwachenden Dienstleister als gemeinsame Verantwortlichkeit im Sinne des Art. 26 Abs. 1 Satz 1 DSGVO zu qualifizieren war. Entscheidend für das Vorliegen einer gemeinsamen Verantwortlichkeit ist nach dem Wortlaut des Art. 26 Abs. 1 Satz 1 DSGVO, dass mindestens zwei Verantwortliche gemeinsam die Zwecke und die Mittel der Datenverarbeitung festlegen. Als Zweck der Verarbeitung ist dabei das erwartete Ergebnis, das beabsichtigt ist oder die geplante Aktion leitet, anzusehen, mithin „warum" und „mit welchem Ziel" eine Verarbeitung erfolgt.[51] Das Fehlen eines tatsächlichen Zugangs zu den verarbeiteten Daten schließt dabei eine (Mit-)Verantwortlichkeit nicht aus.[52]

Mit der Beauftragung der Kfz-Kennzeichenerfassung verfolgte das Handelsunternehmen das Ziel, eine Blockade der Parkflächen durch unberechtigte Fremd- und Dauerparker einzuschränken, um hierdurch eine ausreichende Anzahl an Parkplätzen für die eigene Kundschaft zur Verfügung stellen zu können. Vor diesem Hintergrund kann somit im Rahmen der Auftragserteilung eine Zweckentscheidung des Handelsunternehmens im Sinne des Art. 4 Nr. 7 DSGVO unterstellt werden, die notwendigerweise eine Verarbeitung personenbezogener Daten im Zusammenhang mit der Parkraumüberwachung bedingt. Gleichermaßen setzt der vom Dienstleister verfolgte Zweck, Vertragsstrafen bei einer Überschreitung der Parkhöchstdauer in eigenem Namen geltend zu machen, die Verarbeitung ebendieser personenbezogenen Daten voraus.

[51] EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, Rn. 35.
[52] EuGH, Urteil vom 5. Juni 2018 – C-201/16, Rn. 38.

Eine gemeinsame Verantwortlichkeit verlangt gerade nicht, dass die von den beteiligten Akteuren verfolgten Zwecke identisch sind; vielmehr ist es bereits ausreichend, dass sich die Zwecke gegenseitig ergänzen bzw. die Verfolgung des einen Zwecks die Verwirklichung des anderen Zwecks fördert.[53] Auch wenn scheinbar unterschiedliche wirtschaftliche Interessen verfolgt werden, sind die der parkraumbezogenen Kennzeichenerfassung zugrundeliegenden Zwecke der Akteure eng verknüpft; das vom Handelsunternehmen verfolgte Ziel der Bereitstellung einer ausreichenden Anzahl an Kundenparkplätzen und das von dem Parkraum überwachenden Unternehmen verfolgte Interesse der Geltendmachung von Vertragsstrafen im Zusammenhang mit Parkverstößen, stehen dabei im vorliegenden Kontext der Kfz-Kennzeichenerfassung nicht losgelöst nebeneinander, sondern sind als sich bedingend und von beiderseitigem Nutzen geleitet anzusehen. So fördert die kontinuierliche Durchsetzung von Vertragsstrafen bei Überschreitung der Höchstparkdauer das vom Handelsunternehmen verfolgte Ziel, Fremd- oder Dauerparker durch Abschreckung von der Parkfläche fernzuhalten. Das Handelsunternehmen hat als Grundstückseigentümer an der Datenverarbeitung insoweit ein originäres Interesse und die Parkraumüberwachung als solche initiiert.

Das Handelsunternehmen hatte über den Parkraumbewirtschaftungsvertrag und ergänzende Vereinbarungen Einfluss auf die Mittel der Datenverarbeitung, da von diesem mittelbar grundlegende Vorgaben zur zweckspezifischen Datenverarbeitung gemacht und damit Entscheidungen über „wesentliche" Mittel[54] getroffen wurden. Während bereits durch die Entscheidung für die Ausgestaltung des Auftrags als „Kennzeichenerfassungstechnologie" die Art der durch den Dienstleister zu verarbeitenden Daten – Kfz-Kennzeichen des Halters bzw. Fahrzeugführers – determiniert wird, spricht darüber hin-

[53] EuGH, Urteil vom 29. Juli 2019 – C-40/17, Rn. 80 ff.
[54] EDSA, a. a. O., Rn. 40

aus die durch das Handelsunternehmen für die jeweiligen Märkte erfolgte unterschiedliche Festlegung der Parkhöchstdauer sowie die individuelle Einräumung einer zeitunabhängigen Nutzung der Parkflächen für bestimmte Personen („Whitelists") für eine entscheidende Parametrierung der Datenverarbeitung des Dienstleisters.

Mit Blick auf die vollständige Bereitstellung der Überwachungsinfrastruktur durch den Dienstleister und der von dem Handelsunternehmen getroffenen Entscheidung diese Mittel zu nutzen, kann grundsätzlich auch eine gemeinsame Mittelentscheidung unterstellt werden.[55] Da seitens des Handelsunternehmens keinerlei Einfluss auf die im Zusammenhang mit der Geltendmachung von Vertragsstrafen erfolgende Datenverarbeitung des Dienstleisters genommen wurde, waren die der Kennzeichenerfassung zugrundeliegenden Verarbeitungsvorgänge differenzierend zu betrachten mit der Folge, dass eine gemeinsame Verantwortlichkeit auch nur für Teile des diesbezüglichen Verarbeitungshandelns angenommen werden konnte. Zumindest für die Erhebung und zeitweilige Speicherung der Kfz-Kennzeichen sowie für deren Abgleich mit den zur Verfügung gestellten Whitelists war eine gemeinsame Verantwortlichkeit zu unterstellen; dahingegen erfolgte die Halterermittlung und die Geltendmachung der Vertragsstrafe in eigener datenschutzrechtlicher Verantwortlichkeit des Dienstleisters.

Das Vorliegen einer gemeinsamen Verantwortlichkeit bedingt zwingend den Abschluss einer Vereinbarung zwischen den beteiligten Stellen. Diese Vereinbarung dient gemäß Art. 26 Abs. 1 S. 1 DSGVO u.a. der Festlegung, welcher der Beteiligten welcher Verpflichtung gemäß der DSGVO nachzukommen hat. Dies betrifft insbesondere die Erfüllung der Betroffenenrechte nach Art. 15 ff. DSGVO sowie der Informationspflichten nach Art. 13 DSGVO. Den von der Datenverarbeitung betroffenen Personen muss demnach in transparenter

[55] EDSA, a. a. O. Rn. 60

Form durch eine angemessene Hinweisbeschilderung dargestellt werden, welche Stellen an der Kfz-Kennzeichenerfassung datenschutzrechtlich verantwortlich mitwirken.

Die im Rahmen der Parkraumbewirtschaftung betriebene Kennzeichenerfassung wird von dem in Erscheinung getretenen Dienstleister deutschlandweit angeboten, so dass eine einheitliche Auslegung der skizzierten rechtlichen Fragestellung unter den Datenschutzaufsichtsbehörden des Bundes und der Länder angestrebt wird. Wir befinden uns insoweit in einem regen Austausch mit den anderen Aufsichtsbehörden und vertreten die hier dargestellte Auffassung gegenüber den in unserem Zuständigkeitsbereich ansässigen Handelsunternehmen.

# X.

# Künstliche Intelligenz

# 10 Künstliche Intelligenz

Das Thema künstliche Intelligenz (KI) hatte im Berichtsjahr nicht nur in der öffentlichen Debatte einen großen Stellenwert, sondern erreicht zunehmend auch die breite Masse der Unternehmen. Die aktuellen Fortschritte in der Entwicklung neuer KI-gestützter Anwendungen führen dazu, dass zunehmend auch Unternehmen, die selbst nicht die nötigen Ressourcen zur Entwicklung eigener KI-gestützter Lösungen besitzen, auf am Markt befindliche Angebote von Dienstleistern zurückgreifen können, die die neuen Technologien auch für den individuellen Einsatzzweck nutzbar machen.

Gerade dann, wenn durch KI-gestützte Anwendungen auch personenbezogene Daten, wie beispielsweise die von Endkunden eines Unternehmens, verarbeitet werden sollen, geht im Zuge der nachvollziehbaren Begeisterung für die neuen Möglichkeiten leider oftmals auch das Bewusstsein für etwaige datenschutzrechtliche Risiken derartiger Verarbeitungsvorgänge verloren.

Während auf EU-Ebene bis zum Ende des Berichtsjahrs über den Inhalt einer neuen KI-Verordnung debattiert wurde, wird häufig vergessen, dass auch die Datenschutz-Grundverordnung (DSGVO) mit ihrem bewusst technologieneutralen Ansatz für den Bereich der Künstlichen Intelligenz etliche Vorgaben statuiert. Diese sind zwar nicht geeignet, sämtliche im gesamtgesellschaftlichen Interesse regulierungsbedürftigen Aspekte von KI zu adressieren, sie können aber negative Auswirkungen auf unmittelbar Betroffene verhindern und Risiken für Betroffene in einen angemessenen Ausgleich mit den unternehmerischen Vorteilen des KI-Einsatzes bringen.

Unternehmen, die KI-gestützte Anwendungen einsetzen wollen, müssen sich dabei insbesondere der nachfolgenden datenschutzrechtlichen Anforderungen bewusst sein, um auch im Fall der aufsichtsbehördlichen Prüfung hierzu im Rahmen der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO die Einhaltung

der datenschutzrechtlichen Rahmenbedingungen substantiiert vortragen zu können.

## 10.1 Bestimmung der datenschutzrechtlichen Verantwortlichkeit

In den von uns betriebenen Prüfverfahren ließen die Unternehmen oftmals bereits eine tiefgehende Auseinandersetzung mit der Verteilung der datenschutzrechtlichen Verantwortlichkeiten vermissen, obwohl für die Beteiligten ohne diesbezügliche Feststellungen bereits unklar bleibt, ob und ggf. welche datenschutzrechtlichen Pflichten einzuhalten sind. Beim Einsatz eines KI-gestützten Dienstes zur Verarbeitung personenbezogener Daten sind in der Regel nämlich mehrere Verarbeitungsschritte bei mehreren beteiligten Stellen zu unterscheiden und gesondert datenschutzrechtlich zu prüfen.[56] Gesondert zu prüfen sind beim Einsatz eines KI-gestützten Dienstes etwa das Training der KI auf Basis personenbezogener Daten oder ggf. auch die Anonymisierung von personenbezogenen Daten zum Zwecke des Trainings der KI sowie die Nutzung der KI an sich.

Während die datenschutzrechtliche Verantwortlichkeit bei der Nutzung der KI an sich regelmäßig allein der Stelle zukommt, die diese für ihre unternehmerischen Zwecke einsetzt, ist bei der Verwendung personenbezogener Daten für das Training der KI eine Einzelfallbetrachtung erforderlich. In diesem Zusammenhang ist maßgeblich, inwieweit nur der Dienstleister ein wirtschaftliches Eigeninteresse am Training hat oder ob auch das die KI einsetzende Unternehmen ein Interesse an der aufgabenbezogenen (Fort-)Entwicklung der KI geltend macht. Es muss daher durch alle Beteiligten in tatsächlicher Hinsicht trennscharf bestimmt werden, welche Einflussmöglichkeiten und Interessenlagen bzgl. des Trainings der KI bestehen. Ab-

[56] Vgl. EuGH, Urteil v. 29.07.2019, C-40/17, Rn. 74, der für die Bestimmung des Umfangs der Verantwortlichkeit von mehreren Beteiligten zwischen verschiedenen, ggf. auch vor- bzw. nachgelagerten Vorgängen einer Verarbeitungskette differenziert.

hängig von den Interessenlagen der Beteiligten kann ggf. auch eine gemeinsame Verantwortlichkeit i. S. d. Art. 26 DSGVO vorliegen.

Gehört es zum konkreten Leistungsspektrum des Dienstleisters, dass die KI entsprechend den spezifischen Anforderungen des Auftraggebers fortlaufend modifiziert und fortentwickelt wird, diese Fortentwicklung durch den Dienstleister aber nicht auch für dessen übrige Kunden nutzbar gemacht wird, erfolgt das Training der KI auf Basis personenbezogener Daten allein im Interesse des Auftraggebers. In derartigen Fällen kann es in Betracht kommen, dass auch für das Training ausnahmsweise allein das KI-nutzende Unternehmen als Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO einzuordnen ist.

In vielen Fällen werden Unternehmen aber KI-gestützte Dienste einsetzen, bei denen der Dienstleister das Training für den konkreten Einsatzzweck bereits abgeschlossen hat. Wurden in diesen Fällen (auch) personenbezogene Daten für deren Training verwendet, ist der Dienstleister hierfür i. S. d. Art. 4 Nr. 7 DSGVO verantwortlich und muss bzgl. der durch ihn verwendeten personenbezogenen Daten alle Anforderungen der DSGVO einhalten. Im Verhältnis zu seinen Kunden, die personenbezogene Daten mittels der KI-Anwendung verarbeiten, nimmt er dann die Rolle eines Auftragsverarbeiters ein, wenn er die technische Infrastruktur des Dienstes betreibt.

Bereits die Bestimmung der datenschutzrechtlichen Verantwortlichkeiten beim Einsatz von KI-gestützten Diensten ist somit im Einzelfall alles andere als trivial, so dass alle Beteiligten hierauf ein besonderes Augenmerk legen müssen.

## 10.2 Datenschutz-Folgenabschätzung

In der überwiegenden Zahl der Fälle ist vor dem Einsatz eines KI-gestützten Dienstes zudem eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen, da dies in der Regel voraussichtlich ein hohes Risiko für die Rechte und Freiheiten von Betroffenen zur Folge hat. Denn beim Einsatz eines solchen

Dienstes handelt es sich in der Regel um eine „Verwendung neuer Technologien" i. S. d. Art. 35 Abs. 1 DSGVO, die insbesondere deshalb ein erhöhtes Risiko für Betroffene mit sich bringen kann, da die persönlichen und gesellschaftlichen Folgen des Einsatzes neuer Technologien im Einzelfall nur schwer absehbar sind.[57] Zudem wurde in den uns bislang bekannt gewordenen Anwendungsfällen üblicherweise eine große Zahl an Datensätzen von einer Vielzahl betroffener Personen mit dem KI-gestützten Dienst verarbeitet, weshalb zudem eine für ein großes Risiko sprechende „umfangreiche" Verarbeitung vorlag. Je nach konkretem Zweck des KI-Einsatzes sind auch noch weitere Kriterien in die Risikobewertung einzustellen. Maßgeblich für die Risikobewertung ist außerdem, ob mittels der KI-Anwendung eine automatisierte Entscheidungsfindung gem. Art. 22 DSGVO erfolgt, die für Betroffene Rechtswirkungen entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Außerdem steigt das Risiko der Verarbeitung, sofern vertrauliche oder höchst persönliche Daten durch den KI-gestützten Dienst verarbeitet werden sollen, wozu nicht nur, aber auch, besondere Kategorien personenbezogener Daten i. S. d. Art. 9 DSGVO, wie bspw. Gesundheitsdaten, gehören.

Auch auf Seiten des Dienstleisters, der den Dienst zur Verfügung stellt und in dessen Verantwortungsbereich ein Training der KI erfolgt, wird im Hinblick auf dieselben Kriterien üblicherweise eine DSFA durchzuführen sein.

Die DSFA des Dienstleisters und des KI-nutzenden Unternehmens sind dabei oft nicht deckungsgleich, da sie sich – zumindest teilweise – mit unterschiedlichen Risikolagen auseinanderzusetzen haben. Auf der einen Seite sind Risiken für Betroffene zu berücksichtigen, die daraus entstehen, dass ein Training der KI unter Verwendung ihrer personenbezogenen Daten erfolgt, während auf der anderen Seite die Risiken für

[57] Vgl. auch Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", WP 248 Rev. 01, III., B., a), 8.

Betroffene in ihrer Rolle als Endkundinnen und -kunden, deren personenbezogene Daten mittels der KI verarbeitet werden, maßgeblich sind. Es wird daher unzureichend sein, wenn ein KI-nutzendes Unternehmen der Aufsichtsbehörde eine DSFA vorlegt, die von seinem Dienstleister angefertigt wurde, und die sich lediglich mit den abstrakten Risiken des KI-gestützten Dienstes auseinandersetzt, ohne die spezifischen Risiken beim KI-nutzenden Unternehmen zu berücksichtigen.

Andererseits wird ein KI-nutzendes Unternehmen die eigene DSFA nicht erstellen können, ohne auch die technischen Rahmenbedingungen des Dienstes mit einzustellen, wofür aber weitere Informationen des Dienstleisters erforderlich sind; sofern diesem die Rolle eines Auftragsverarbeiters zukommt, hat der Dienstleister im Rahmen des Vertrags nach Art. 28 Abs. 3 DSGVO diese dabei ohnehin zur Verfügung zu stellen.[58]

Alle Beteiligten müssen beim Anfertigen der DSFA die inhaltlichen Mindestanforderungen erfüllen, wie sie in Art. 35 Abs. 7 DSGVO festgelegt sind. Unzureichend waren uns vorgelegte DSFA oft schon im Hinblick auf Art. 35 Abs. 7 lit. a DSGVO, wonach unter anderem eine „systematische Beschreibung der geplanten Verarbeitungsvorgänge" erforderlich ist. Diese systematische Beschreibung ist zwingende Voraussetzung für die sich hieran anschließende Risikobewertung, da sie hierfür erst die nötige Tatsachengrundlage schafft. Eine DSFA, die keine substantiierte (technische) Beschreibung des KI-Systems und eine Darstellung der spezifischen Art und Weise des Einsatzes bzw. des Trainings der KI enthält, genügt diesen Anforderungen nicht und zieht Zweifel an einer ordnungsgemäßen Risikoabschätzung nach sich.

[58] vgl. Art. 28 Abs. 3 lit. f DSGVO, wonach der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung der Pflichten aus Art. 35 DSGVO zu unterstützen hat, insbesondere indem er die hierfür nötigen Informationen zur Verfügung stellt.

## 10.3 Rechtsgrundlagen

Wurden die Verantwortungsbereiche aller Beteiligten bestimmt, ist zu prüfen, ob für die Verarbeitungsschritte in der Verantwortlichkeit i. S. d. Art. 4 Nr. 7 DSGVO des jeweiligen Akteurs auch eine Legitimationsgrundlage nach Art. 6 DSGVO herangezogen werden kann. Auch dies betrifft im Einzelnen das Training der KI auf Basis personenbezogener Daten, ggf. die Anonymisierung von personenbezogenen Daten zum Zwecke des Trainings der KI, die Nutzung der KI an sich sowie ggf. die Übermittlung personenbezogener Daten an einen Dienstleister für dessen Zweck eines eigenverantwortlichen Trainings der KI.

Problematisch kann hierbei vor allem sein, wenn der Dienstleister die im Rahmen des Auftragsverhältnisses verarbeiteten personenbezogenen Daten zudem für das Training und die Fortentwicklung seines KI-gestützten Dienstes nutzen möchte und er damit beabsichtigt, personenbezogene Daten aus der Sphäre seiner Kunden (KI-nutzendes Unternehmen) für eigene Zwecke zu verarbeiten. In diesem Fall können insbesondere auch die Vorgaben des Art. 6 Abs. 4 DSGVO relevant werden, mit der Folge, dass im Rahmen eines sog. Kompatibilitätstests geprüft werden muss, ob die Weiterverarbeitung mit dem Zweck vereinbar ist, für den die Daten ursprünglich erhoben wurden. Ferner muss gegenüber den betroffenen Personen hinsichtlich der Datenweiterverarbeitung nach Art. 13 Abs. 3 oder Art. 14 Abs. 4 DSGVO hinreichende Transparenz hergestellt werden.

## 10.4 Anonymisierung für Trainingszwecke

Vor allem im Bereich des Trainings einer KI hat das Thema Anonymisierung von personenbezogenen Daten einen hohen Stellenwert, da für ein Training mittels anonymer Daten einerseits die Vorgaben der DSGVO nicht (mehr) anwendbar sind und dadurch gleichzeitig keine Risiken für zuvor Betroffene zu berücksichtigen sind.

Auf den ersten Blick scheint die Anonymisierung von personenbezogenen Daten daher für alle Beteiligten, sowohl auf Seiten der Betroffenen, als auch auf Seiten der datenverarbeitenden Stelle, ausschließlich Vorteile zu bringen; problematisch scheint aus hiesiger Perspektive jedoch, dass datenverarbeitende Stellen oftmals vorschnell von einer Anonymisierung ausgehen und dabei verkannt wird, dass die Wirksamkeit der Anonymisierung der Aufsichtsbehörde im Falle eines Prüfverfahrens auch in der nötigen Tiefe darzulegen ist.

Nach Erwägungsgrund 26 S. 5 DSGVO sollen die „Grundsätze des Datenschutzes (...) nicht für anonyme Informationen gelten, d.h. für Informationen, (...) die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann". Voraussetzung für eine Anonymisierung ist also, dass die Daten über keinerlei Personenbezug mehr verfügen. Das ist dann der Fall, wenn „eine Re-Identifizierung praktisch nicht durchführbar ist, weil der Personenbezug nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden kann".[59]

Da bei einer großen Zahl zu anonymisierender Datensätze auch die Anonymisierung in der Regel durch ein automatisiertes Verfahren erfolgt, ist eine fortlaufende Evaluierung des Verfahrens erforderlich, die sicherstellt, dass dieses für die Erreichung des verfolgten Zwecks geeignet und eine wirksame Entfernung des Personenbezugs sichergestellt ist.

Es kann daher zu überprüfen sein, wie hoch die Fehlerquote im Rahmen des Verfahrens ist, mithin in welchem Umfang personenbezogene Daten ggf. falsch-negativ nicht als personenbezogen annotiert werden. Soweit Fehleinordnungen nicht mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden können, steigt mit der Anzahl der zu anonymisierenden Daten zwangsläufig in einem absehbaren, der Fehlerquote entsprechenden Umfang auch die Anzahl der Datensätze, für

[59] BeckOK DatenschutzR/Schild DS-GVO Art. 4 Rn. 15a.

die eine Personenbeziehbarkeit nicht ausgeschlossen werden kann.

Zudem kann ein Datensatz weiterhin als personenbezogen einzuordnen sein, wenn entsprechend obiger Definition dem Verantwortlichen weitere Informationen vorliegen, die eine Re-Identifizierung der Betroffenen ermöglichen. Das kann etwa dann der Fall sein, wenn der den KI-gestützten Dienst anbietende Dienstleister das Training seiner KI zwar nur mit aus der Sphäre des Kunden stammenden Datensätzen durchführt, die das „Anonymisierungsverfahren" durchlaufen haben, er aber in seiner Rolle als Auftragsverarbeiter zudem gleichzeitig eben diese personenbezogenen Datensätze für seine Kunden verarbeitet. Er verfügt in dieser Konstellation über Mittel, die ihm eine Rückzuordnung der Daten zu identifizierbaren Personen durch eine Rekombination der Datensätze potenziell ermöglicht.

In derartigen Fällen kann eine wertende Betrachtung des verwendeten Verfahrens und seiner Rahmenbedingungen zum Ergebnis haben, dass die personenbezogenen Datensätze nicht wirksam „anonymisiert", sondern allenfalls pseudonymisiert i. S. d. Art. 4 Nr. 5 DSGVO wurden.

Abhängig vom spezifischen Anwendungsfall wird daher auch bei der Etablierung eines Anonymisierungsverfahrens in der Mehrheit der Anwendungsszenarien eine DSFA durchzuführen sein, die sich insbesondere mit der Wirksamkeit des Verfahrens auseinandersetzt. Geht eine verantwortliche Stelle fälschlicherweise davon aus, dass verarbeitete Datensätze anonymisiert sind und wird deren Verarbeitung nicht mehr an den datenschutzrechtlichen Vorgaben ausgerichtet, kommt ihnen nicht mehr der Schutz zu, der nach der DSGVO geboten ist. Wenngleich ein wirksames Anonymisierungsverfahren auch für Betroffene einen zusätzlichen Schutz bietet, können aus einem mangelhaften Anonymisierungsverfahren zusätzliche Risiken für Betroffene entstehen, die es zu vermeiden gilt.

## 10.5 Einzelfall: KI-gestützte Videoüberwachung im Schwimmbad

Beim Einsatz von künstlicher Intelligenz können im Einzelfall auch die Vorgaben des Art. 22 DSGVO zu berücksichtigen sein. Dies wurde im nachfolgenden Fall, mit dem unsere Dienststelle befasst war, deutlich:

Die Videoüberwachung öffentlicher und privater Badeanstalten stellt einen datenschutzrechtlich besonders sensiblen Bereich dar. Waren hier bislang vor allem Überwachungsmaßnahmen im Außenbereich und/oder Foyer der Schwimmbäder, in einzelnen Fällen auch von Umkleide- und Spindbereichen, Gegenstand unserer Befassung, so rückte in diesem Jahr erstmals auch die Videoüberwachung des Beckenbereichs in den Fokus unserer aufsichtsbehördlichen Tätigkeit. Grund hierfür dürfte die in technischer Sicht mittlerweile gegebene Möglichkeit sein, mittels künstlicher Intelligenz die Bewegungsmuster von Personen während des Aufenthalts im Schwimmbecken zu analysieren und dabei in Not geratene oder ertrinkende Personen zu erkennen. Die Systeme setzen in diesen Fällen einen Alarm an das Aufsichtspersonal des Schwimmbades ab, welcher in der Regel auch bereits den ungefähren Ort der in Not geratenen Person, etwa unter Anzeige des jeweiligen Beckenbereichs, mitteilt. Die am Markt verfügbaren Systeme lassen sich dabei grob in zwei Kategorien einteilen. Bei der einen erfolgt die Überwachung mittels eines Kamerasystems, welches außerhalb des Schwimmbeckens, z. B an der Deckenhalle, angebracht ist. Bei der anderen findet die Überwachung durch eine Art Bullauge unter Wasser mittels in den Beckenrand eingebauter Kameras statt.

Dass eine solche Datenverarbeitung den allgemeinen Anforderungen an eine Videoüberwachung entsprechen muss, mehr noch, aufgrund der besonderen Situation der Erfassung von lediglich in Bademode gekleidete Personen, nur in besonders engen Grenzen erfolgen darf, liegt auf der Hand. So erweist sich der Zweck dieser Überwachungsform von vornherein nur

dann als legitim, wenn er ausschließlich auf die Abwehr von Gefahren für besonders wichtige Rechtsgüter, konkret auf die Abwehr einer Lebensgefahr für Badegäste, gerichtet ist. Zwar mag die Möglichkeit der Rekonstruktion von Badeunfällen in strafrechtlicher und/oder zivilrechtlicher Sicht ein ebenfalls legitimer Nebenzweck sein, im Fokus steht jedoch die Prävention, d. h. die Rettung von Menschenleben.[60] Diese Differenzierung der Zwecke der Videoüberwachung ist relevant, folgt doch hieraus, dass eine Aufzeichnung (Speicherung) des Videosignals grundsätzlich nicht erfolgen darf. Nur anlassbezogen, d. h. im Fall eines Unfalls (Alarms) kann eine Speicherung für kurze Zeiträume (wenige Minuten) zulässig sein, um nachträglich Rückschlüsse auf das Unfallgeschehen ziehen zu können.

Für den Betrieb eines solchen Systems ist aus hiesiger Sicht entsprechend den obigen Ausführungen eine Datenschutzfolgenabschätzung gemäß Art 35 DSGVO[61] sowie die Bestellung eines Datenschutzbeauftragten erforderlich (vgl. § 38 Abs. 1 Satz 2 BDSG). Diese, auf die Sicherheit der Datenverarbeitung gerichteten Maßnahmen des Verantwortlichen sind obligatorisch und vor allem der im vorliegenden Sachverhalt bereits erwähnten Sensibilität der Videoüberwachung sowie dem Einsatz neuer Technologien geschuldet.

Im Rahmen einer KI-gestützten Videoüberwachung von Schwimmbecken, welche ein Ertrinken badender Personen verhindern soll, muss darüber hinaus Art. 22 DSGVO in Bezug genommen werden. Nach dieser Vorschrift hat die betroffene Person das Recht, *„(...) nicht einer ausschließlichen auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise*

---

[60] Die Möglichkeit durch entsprechendes Videomaterial evtl. einen Entlastungsbeweis zu führen, stellt demnach keinen isolierten legitimen Verarbeitungszweck dar.

[61] Vgl. DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist (Version 1.1), elektronisch abrufbar unter: https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/Download/dsfa_muss_liste_dsk_de.pdf.

*erheblich beeinträchtigt."* Der Mensch soll nicht zum bloßen Objekt einer computergestützten Auswertung und Entscheidung gemacht werden. Insbesondere aufgrund des Umstands, dass maschinelle Entscheidungsprozesse auf immer komplexeren und intransparenteren Algorithmen basieren, ist sicherzustellen, dass der maschinell erzeugte Entscheidungsprozess stets nur eine Vorstufe, ein Vorschlag ist. Es ist sicherzustellen, dass das Ergebnis dieses Entscheidungsprozesses immer einem menschlichen Entscheidungsträger zur Ausführung zugeführt werden muss.[62]

Es wäre hiernach ein untragbares Ergebnis, wenn ein Algorithmus allein aufgrund KI-basierter Berechnungsmethoden darüber befinden würde, wann eine Notlage vorliegt und wann nicht. Die diesbezügliche Kontrolle und Aufsicht muss nach wie vor einem Menschen, sprich dem Badepersonal vorbehalten bleiben. Der Schwimmbadbetreiber muss sich dessen bewusst sein und darf die Videoüberwachung daher nur als zusätzliche Unterstützung für das Badepersonal begreifen. Zur Absicherung muss er organisatorische Maßnahmen treffen, welche verhindern, dass sich das Badepersonal in nicht oder nicht mehr verantwortbarem Maße auf die Funktionalität der Überwachung verlässt oder dieser gar blind vertraut. Vor allem mittels schriftlicher Dienstanweisungen und Kontrollen ist sicherzustellen, dass das Badepersonal sich nicht in falscher Sicherheit wiegt und die Beckenkontrolle in gleichem Maße und in der gleichen Intensität durchführt, wie dies vor der Inbetriebnahme der Videoüberwachung der Fall war. Zusammenfassend bedeutet dies, dass der menschliche Beitrag zur Gewährleistung der Badesicherheit nicht reduziert werden darf. Diese Feststellung erscheint gerade in den Fällen wichtig, in welchen die Videoüberwachung besonders zuverlässig funktioniert und damit womöglich auch dem Badepersonal ein Gefühl großer Sicherheit vermittelt.

[62] *Buchner*, in: Kühling/Buchner, DS-GVO, Art. 22, Rn. 1.

Diese und weitere Maßnahmen des Verantwortlichen zur Steigerung der Sicherheit in diesem Bereich sind derzeit Gegenstand unserer Befassung. Allgemeinverbindliche Lösungen und Vorgaben kann es hierbei nicht geben, da die Mechanismen und Verfahren der Badesicherheit und damit auch die hierauf gerichteten Datenverarbeitungen, in den Schwimmbädern unterschiedlich ausgestaltet sein können und daher die jeweilige Situation vor Ort in den Fokus zu nehmen ist.

Die vorgenannten Ausführungen verdeutlichen jedoch, dass es im Anwendungsbereich der DSGVO nicht nur um den bloßen Schutz von Daten geht. Die DSGVO zielt vielmehr darauf ab, Gefahren und Schäden für die hinter diesen Daten stehenden Personen abzuwenden. Wie der vorliegende Sachverhalt und der Bezug auf Art. 22 DSGVO zeigt, können die Gefahren, welche von einer Datenverarbeitung ausgehen dabei sogar lebenswichtige Interessen der Betroffenen tangieren. Dies verleiht dem Datenschutz in diesem Bereich nochmals eine gesteigerte Bedeutung.

# XI.

# Internet und Werbung

# 11 Internet und Werbung

## 11.1 Veröffentlichung von Event-Fotos auf Instagram

Zu Beginn des Berichtsjahres wurde die Aufsichtsbehörde aufgrund mehrerer Anfragen der Presse und von Betroffenen darauf aufmerksam, dass über ein Instagram-Profil mehrere hundert Fotos von Besuchern diverser Club-Events veröffentlicht wurden. Diese Bildaufnahmen entstammten einer in den 2000ern betriebenen, insbesondere im Saarland etablierten Webcommunity, auf der damals im Nachgang zu diversen Feiern und Veranstaltungen in Diskotheken Fotos der Gäste veröffentlicht wurden.

Wenngleich die Veröffentlichung der Fotos auf Instagram teilweise mit nostalgischem Interesse aufgenommen wurde, gingen bei hiesiger Dienststelle Anfragen potenziell betroffener Personen ein, die befürchteten, dass unter den Fotos, die fortlaufend und teils täglich neu auf Instagram hochgeladen wurden, auch solche von ihnen vorhanden sein könnten.

Im Ergebnis verstieß die Veröffentlichung der Fotos in weiten Teilen gegen die Vorgaben aus Art. 5 Abs. 1 lit. a 1. Alt i.V.m. Art. 6 Abs. 1 DSGVO, da hierfür keine datenschutzrechtliche Legitimationsgrundlage herangezogen werden konnte. Denn weder existierten wirksame Einwilligungen der betroffenen Personen zur Veröffentlichung der Fotos noch konnte sich die verantwortliche Stelle insoweit auf ein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 lit. f DSGVO berufen.

Nach Art. 4 Nr. 11 ist eine Einwilligung „*jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist*". Erwägungsgrund 32 DSGVO spezifiziert

insoweit, dass die Erklärung auch „*durch eine (...) Verhaltensweise geschehen [kann], mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert*".

Ausgehend hiervon kann ein Posieren oder Lächeln in die Kamera je nach situativem Kontext als konkludente Einwilligung dafür betrachtet werden, dass ein Foto angefertigt wird. Auch vorliegend handelte es sich bei der Mehrzahl der veröffentlichten Bilder um solche, bei denen die Abgebildeten sich offensichtlich proaktiv für eine Aufnahme zur Verfügung gestellt hatten. Zumindest bezüglich des Anfertigens der Aufnahmen lag demnach nach damaliger Rechtslage, aber auch nach den Maßstäben der DSGVO, eine konkludente Einwilligung der Abgebildeten vor. Zu differenzieren war jedoch einerseits zwischen dem Anfertigen der Fotos zum damaligen Zeitpunkt und andererseits der (Neu-)Veröffentlichung der Fotos auf Instagram, die als eigenständiger Verarbeitungsvorgang i. S. d. Art. 4 Nr. 2 DSGVO einer datenschutzrechtlichen Beurteilung zu unterziehen war.

Auch wenn die Fotos ursprünglich zwar angefertigt werden durften, lagen für deren erneute Veröffentlichung keine nachweisbaren Einwilligungen der Betroffenen vor. Grundvoraussetzung für die Wirksamkeit einer Einwilligung ist es, dass diese „in informierter Weise" i.S.d. Art. 4 Nr. 11 DSGVO erfolgt ist. Eine Einwilligung ist daher nur wirksam, wenn sie in voller Kenntnis der Sachlage erteilt wird und die betroffene Person hierdurch in die Lage versetzt wird, „*die Konsequenzen einer etwaigen von ihr erteilten Einwilligung leicht zu bestimmen*".[63] Auch eine konkludente Einwilligung konnte sich denklogisch damit nur auf solche Verarbeitungsvorgänge beziehen, über die die Betroffenen im Zeitpunkt der Bildaufnahme ohne jeden Zweifel hinreichende Informationen erhalten hatten. Denn nur dann konnten sie auch zum Gegenstand ihrer Willensbildung

[63] EuGH, Urteil vom 11.11.2020 – C-61/19 – Orange România/ANSPDCP, Rn. 40.

werden. Maßgeblich sind hierfür die Gesamtumstände der Aufnahmesituation, die aufsichtsrechtlich einer wertenden Betrachtung zu unterziehen war.

In den 2000ern war die Webcommunity, für die die Fotos ursprünglich angefertigt wurden, allgemein unter den Besuchern entsprechender Events bekannt. Auch gaben sich die Fotografen auf den Veranstaltungen regelmäßig bereits dadurch als solche der Webcommunity zu erkennen, dass sie T-Shirts mit einem Aufdruck der Webadresse bzw. des Logos der Webcommunity trugen. Wenngleich daher nahe liegt, dass Betroffene zum damaligen Zeitpunkt mit einer Veröffentlichung der Fotos einverstanden waren, bezog sich diese Einwilligung allenfalls auf eine Veröffentlichung im unmittelbaren zeitlichen Zusammenhang zur Veranstaltung und zudem lediglich auf eine Veröffentlichung auf ebendieser Plattform. Weder konnten die ursprünglichen Einwilligungen den Upload von Fotos auf einem damals noch nicht existierenden Sozialen Netzwerk wie Instagram rechtfertigen noch konnte ein Lächeln in die Kamera dahingehend ausgelegt werden, dass Betroffene mit einer Neuveröffentlichung der Fotos auch noch nach Jahrzehnten einverstanden waren.

Auch Art. 6 Abs. 1 lit. f DSGVO kam vorliegend nicht als Legitimationsgrundlage für die Veröffentlichung der Fotos auf Instagram in Betracht. Danach kann eine Verarbeitung rechtmäßig sein, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Als berechtigte Interessen der Verantwortlichen können dabei grundsätzlich rechtliche, wirtschaftliche, aber auch ideelle Interessen zu berücksichtigen sein. Nach dem Wortlaut der Regelung sind dabei ausdrücklich auch Interessen Dritter zu berücksichtigen. Die verantwortliche Stelle kann insoweit ein berechtigtes Interesse an einer Veröffentlichung der Fotos für sich in Anspruch nehmen, welches darin bestand, die Marke der da-

maligen Webcommunity mit ihrem Markenkern, der Eventfotografie, zu bewahren. Auch ein Interesse der Öffentlichkeit, die Fotos aus nostalgischem Interesse zugänglich zu halten, kann Eingang in diese Interessenabwägung finden; Selbiges mag abstrakt auch für die Interessen von einigen der so abgebildeten Personen gelten, die einer Neuveröffentlichung positiv gegenüberstehen.

Diesen Interessen an einer Veröffentlichung der Fotos standen jedoch die Interessen und Grundrechte der Betroffenen entgegen.

Gerade bei Veröffentlichungen von Fotos Betroffener im Internet und insbesondere auf Sozialen Netzwerken ist zu berücksichtigen, dass „*eine solche Veröffentlichung aufgrund bestehender Missbrauchsmöglichkeiten sowie aufgrund der großen Reichweite derartiger Netzwerke mit erheblichen Risiken verbunden ist*".[64] Dies insbesondere auch, weil es für Betroffene schwierig ist, einen Überblick über sämtliche über sie veröffentliche Daten zu behalten.[65] Soweit der verantwortliche Accountbetreiber darauf verwies, dass es doch in der Natur des Internets läge, dass Inhalte, die einmal im Internet auffindbar seien, nie wieder komplett aus dem Netz verschwänden, war dem entgegenzutreten, dass genau darin eine der Kernproblematiken liegt, die das europäische Datenschutzrecht mit seinen Vorgaben zu adressieren beabsichtigt. Denn die betroffene Person soll gerade befähigt bleiben, eine Kontrolle über ihre personenbezogenen Daten in einem Umfang zu behalten, die ihrer Persönlichkeit und ihrem Interesse an Privatheit ausreichend Rechnung trägt. Sie soll gerade nicht zum Objekt einer für sie nicht mehr kontrollierbaren Weiterverbreitung ihrer personenbezogenen Daten im Internet gemacht werden.

[64] OVG Lüneburg, Beschluss vom 19. Januar 2021 – 11 LA 16/20.
[65] OVG Lüneburg, aaO, Rn. 26.

Nach Erwägungsgrund 47 DSGVO sind bei der Abwägung der widerstreitenden Interessen außerdem die vernünftigen Erwartungen der betroffenen Personen in objektiver Weise zu berücksichtigen. Dabei hat auch der zeitliche Abstand zwischen Aufnahme und Veröffentlichung des Fotos Einfluss darauf, ob eine (Neu-)Veröffentlichung vernünftigerweise durch Betroffene zu erwarten ist. Die Erwartungshaltung der Abgebildeten im Zeitpunkt der Aufnahme richtete sich allein darauf, dass die Fotos auf der damals betriebenen Plattform zeitnah im Zusammenhang mit dem konkreten Event veröffentlicht würden. Die Abgebildeten mussten hingegen nicht damit rechnen, dass Fotos viele Jahre später auf dem Social-Media-Account eines Drittanbieters erneut veröffentlicht würden.

Zudem waren den ursprünglichen Einwilligungen zur Veröffentlichung der Fotos keine abwägungsrelevanten Anhaltspunkte dafür zu entnehmen, dass Betroffene grundsätzlich auch mit einer fortgesetzten oder etliche Jahre später erneut stattfindenden Veröffentlichung der Fotos einverstanden gewesen wären. Denn es ist ebenso denkbar, dass die betroffene Person zum damaligen Zeitpunkt allein deshalb bereit war ein Foto anfertigen zu lassen, da sie davon ausging, dass eine Veröffentlichung ohnehin nur in unmittelbarem zeitlichem Zusammenhang mit der Veranstaltung auf der ihr bekannten Webcommunity erfolgen würde und daher eine Kontrolle über die Veröffentlichung, gerade auch in Form einer Löschmöglichkeit, fortbesteht. Da aber der spezifische Wille des Einzelnen über den Inhalt seiner Erklärung hinaus nicht bekannt ist, können etwaige Annahmen hierüber auch nicht im Rahmen der Abwägung der widerstreitenden Interessen maßgeblich sein.

Zudem sprach gegen eine Veröffentlichung der Fotos, dass Betroffene, die ggf. keine Kenntnis von der Neuveröffentlichung hatten, ihre Betroffenenrechte nach Kapitel III der DSGVO nicht ordnungsgemäß ausüben konnten. Denn es konnte nicht zwangsläufig davon ausgegangen werden, dass jede der betroffenen Personen einen eigenen Account bei Instagram besitzt. Auch bei Instagram-Nutzern war nicht sichergestellt,

dass diese den Upload ihres Fotos zur Kenntnis nehmen. Dadurch blieb vielen Betroffenen die Möglichkeit verwehrt, etwa ihr Recht auf Löschung eines Fotos geltend zu machen, soweit sie einer Veröffentlichung kritisch gegenüberstehen. Auch dieser Umstand erhöhte die Eingriffsintensität in die Rechtsposition der Betroffenen in nicht unerheblichem Maße.

Unter Beachtung der hiesigen Rechtsauffassung wurden Fotos, für deren Veröffentlichung keine Legitimationsgrundlage herangezogen werden konnte, von der verantwortlichen Stelle entfernt. Es wurde eine Verwarnung nach Art. 58 Abs. 2 lit. b DSGVO ausgesprochen.

## 11.2 Datenschutzrechtliche Pflichten für Entwickler

Unternehmen entwickeln in der überwiegenden Zahl der Fälle keine eigenen Anwendungen, sondern greifen regelmäßig auf am Markt etablierte Anwendungen zurück. Dies führt zu einer Grundproblematik, die das europäische Datenschutzrecht nicht im erforderlichen Maße adressiert.

Die Ausgestaltung der jeweiligen Anwendung determiniert in vielen Fällen in nicht unerheblichem Maße, auf welche Art und Weise personenbezogene Daten beim jeweiligen Unternehmen verarbeitet werden. Adressat der datenschutzrechtlichen Pflichten ist jedoch regelmäßig allein das Unternehmen, das als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO personenbezogene Daten für eigene Zwecke verarbeitet und sich dafür einer extern entwickelten Anwendung bedient. Für Unternehmen bedeutet dies, dass mit Blick auf die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO die Datenschutzkonformität der Verarbeitung personenbezogener Daten auch im Zusammenhang mit den eingesetzten Anwendungen nachgewiesen werden können muss. Daher kommt gerade beim Betrieb komplexerer IT-Anwendungen der Vorschrift des Art. 25 DSGVO eine zentrale Bedeutung zu, die vorsieht, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen dafür treffen muss, dass sämtliche Datenschutzgrundsätze aus Art. 5

DSGVO wirksam umgesetzt werden („Datenschutz durch Technikgestaltung" oder „privacy by design"). Da Unternehmen aber in vielen Fällen keinen tatsächlichen Einfluss auf die technische Ausgestaltung der Anwendung des Dienstleisters haben, sind sie beim Einsatz der Anwendung darauf angewiesen, dass der Entwickler der Anwendung bereits bei deren Konzeption datenschutzrechtliche Anforderungen im Detail identifiziert und operationalisiert. Aus hiesiger Erfahrung werben zwar viele Entwickler mit dem Schlagwort „DSGVO-konform", antizipieren jedoch teilweise nicht in der nötigen fachlichen Tiefe, welche datenschutzrechtlichen Anforderungen die Unternehmen beim Einsatz der Anwendung einhalten müssen.

Schon bei der Konzeption und Planung einer Anwendung muss daher auf Seiten des Entwicklers soweit wie möglich sichergestellt werden, dass personenbezogene Daten innerhalb der Anwendung nur auf rechtmäßige Weise und in einer für betroffene Personen nachvollziehbaren Weise verarbeitet werden (Art. 5 Abs. 1 lit. a DSGVO). Auch den Grundsätzen der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO), der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO), der Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO), der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) sowie der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO) muss dabei entsprochen werden. Soll der Einsatz einer Anwendung durch ein Unternehmen datenschutzkonform möglich sein, muss das Unternehmen geprüft haben, ob und wie die Anwendung allen obigen Grundsätzen hinreichend Rechnung trägt (vgl. Art. 5 Abs. 2 DSGVO) und dies durch eine entsprechende Dokumentation darlegen können. Dies wird aber ohne entsprechende Vorarbeit des Entwicklers der Anwendung, beispielsweise in Gestalt entsprechender Dokumentationen, die er den Verwendern der Anwendung zur Verfügung stellt, in den meisten Fällen kaum möglich sein.

Es wird demnach deutlich, dass Anwendungsentwicklern eine zentrale Rolle dabei zukommt, dass datenschutzrechtliche Vorgaben in der Praxis von Unternehmen eingehalten werden können. Trotz ihres Stellenwerts bei der Implementierung da-

tenschutzkonformer Prozesse bei verantwortlichen Stellen sind die Entwickler jedoch üblicherweise nicht unmittelbar Adressat datenschutzrechtlicher Pflichten. Aus diesem Grund hatte die Datenschutzkonferenz bereits darauf hingewiesen, dass es hierdurch *„zu einer Potenzierung von technischem und bürokratischem Aufwand bei dem Versuch [kommt], dezentral Mängel zu beseitigen, die zentral verursacht werden*“[66] und insoweit eine Ergänzung der DSGVO um Pflichten für „Hersteller“ von Diensten und Anwendungen gefordert.

Die hiesige Aufsichtspraxis hat den Bedarf für eine entsprechende gesetzliche Ergänzung in einer Vielzahl von untersuchten Fällen verdeutlicht. Zwar treten wir regelmäßig auch in einen kooperativen Dialog mit Herstellern und Entwicklern von Anwendungen, sofern diese im Saarland ansässig sind. Unsere Aufsichtsbehörde besitzt jedoch keine aufsichtsbehördlichen Befugnisse, mittels derer wir eine Ausrichtung etwaiger Anwendungsentwicklungen an den Vorgaben des Art. 25 DSGVO im Bedarfsfall auch durchsetzen können. Daher verbleibt nur die Möglichkeit, über eine Prüfung der verantwortlichen Stellen mittelbar auf die Entwickler einzuwirken, was sowohl aus Sicht der Aufsichtsbehörde als auch vieler Unternehmen in der praktischen aufsichtsbehördlichen Tätigkeit unbefriedigend ist.

## 11.3 Direktwerbung

Auch im zurückliegenden Berichtszeitraum war die im Zusammenhang mit Werbemaßnahmen stattfindende Verarbeitung personenbezogener Daten häufiger Gegenstand von Beschwerden und Beratungsanfragen. Bei dem Großteil der an das Datenschutzzentrum adressierten Anliegen handelte es sich dabei um die Verarbeitung personenbezogener Daten im Kontext von E-Mail– und telefongestützten Marketings, während postalische Werbemaßnahmen kaum noch beschwerdegegenständlich vorgetragen werden.

[66] Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO, November 2019, S. 16.

### 11.3.1 Telefonmarketing B2B

Kein Sachverhalt begleitet die zuständigen Mitarbeitenden des Datenschutzzentrums so lange, wie die gerichtliche Klärung der Frage, unter welchen Bedingungen die Daten von Einzelzahnärztinnen und -ärzten für Zwecke der telefonischen Direktwerbung in zulässiger Weise verarbeitet werden können. Dem bisherigen Verfahrensgang lag im Wesentlichen folgendes Geschehen zugrunde:

Noch vor Geltungseintritt der Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018 wurde gegen einen Werbetreibenden, der – ohne vorherigen Geschäftskontakt – die Daten von Einzelzahnärztinnen und -ärzten aus öffentlichen Rufnummernverzeichnissen erhoben hatte, eine Anordnung erlassen und die diesbezügliche Datenverarbeitung untersagt. Die gegen diesen Bescheid des Datenschutzzentrums gerichtete Klage des Werbetreibenden und der Antrag auf Zulassung der Berufung wurden abgewiesen.[67] Nach gerichtlichem Hinweis in dem Beschluss zur Abweisung der Berufungszulassung hat der Werbetreibende mit Blick auf die zwischenzeitlich anwendbaren Regelungen der DSGVO einen Antrag auf Wiederaufgreifen des Verfahrens an uns gerichtet, welcher mit Bescheid abgewiesen wurde. Auch die anschließende Klage des Werbetreibenden gegen diesen Bescheid hatte vor dem Verwaltungsgericht keinen Erfolg.[68]

Das Oberverwaltungsgericht des Saarlandes (OVG) hat im Berichtszeitraum nunmehr auch über die diesbezügliche Berufung des Werbetreibenden entschieden und im Urteil vom 2. Mai 2023 – 2 A 111/22 – die Rechtsauffassung des Datenschutzzentrums bestätigt. Unter Berücksichtigung seiner bisherigen Rechtsprechung[69] zur datenschutzrechtlichen Zulässig-

[67] Vgl. 27. Tätigkeitsbericht Datenschutz 2017/2018, Kapitel 14.3., S. 132 ff.
[68] Vgl. 30. Tätigkeitsbericht Datenschutz 2021, Kapitel 4.22., S. 112 ff.
[69] OVG des Saarlandes, Beschluss vom 16. Februar 2021 – 2 A 355/19 Rn. 30, juris, hinsichtlich der datenschutzrechtlichen Zulässigkeit der telefonischen Werbeansprache gegenüber Verbrauchern.

keit von telefonischen Werbeansprachen gegenüber Verbrauchern statuiert der entscheidende Senat, dass Werbemaßnahmen, die nach § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) als unzumutbare Belästigung und somit als wettbewerbswidrig zu qualifizieren sind, kein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit. f DSGVO darstellen können. Das Gericht begründet dies damit, dass § 7 Abs. 2 Nr. 1 UWG einen gemeinschaftsrechtlichen Ursprung in Art. 13 Abs. 3 und 5 der Richtlinie 2002/58/EG hat und das vollharmonisierte Datenschutzrecht die Verfolgung unionsrechtskonformer Ziele der Datenverarbeitung bedingt. Die telefonische Werbeansprache war im zu entscheidenden Fall daher auch nach Geltungseintritt der DSGVO datenschutzrechtlich nicht legitimiert, soweit weder eine ausdrückliche noch eine mutmaßliche Einwilligung der Werbeadressaten im Sinne des § 7 Abs. 2 Nr. 1 UWG gegeben war.

Bemerkenswert sind dabei die leider in der Entscheidung nicht vertieften Ausführungen zur Frage, ob bei den Einzelzahnärztinnen und -ärzten auf das Vorliegen einer ausdrücklichen Einwilligung im Sinne des § 7 Abs. 2 Nr. 1 1. Alternative UWG abgestellt werden muss oder eine mutmaßliche Einwilligung nach der 2. Alternative der Vorschrift ausreichen kann; denn während § 7 Abs. 2 Nr. 1 UWG begrifflich zwischen Verbrauchern und sonstigen Marktteilnehmern unterscheidet und für Letztgenannte eine mutmaßliche Einwilligung ausreichen lässt, differenziert die der Vorschrift zugrundeliegende Regelung des Art. 13 Abs. 3 und 5 Richtlinie 2002/58/EG nur zwischen natürlichen und juristischen Personen.

Da natürliche Personen allerdings nach dem Wortlaut von § 7 Abs. 2 Nr. 1 UWG sowohl als Verbraucher als auch in ihrer beruflichen Sphäre als sonstige Marktteilnehmer im Sinne des § 2 Abs. 1 Nr. 3 UWG agieren können, steht die durch den Bundesgesetzgeber gewählte Differenzierung nicht mit dem Wortlaut der Richtlinie in Einklang.[70] Das OVG qualifiziert dabei

[70] Köhler/Bornkamm/Feddersen/Köhler, 42. Aufl. 2024, UWG § 7 Rn. 134.

die Praxisinhaberinnen und -inhaber im Zusammenhang mit ihrer beruflichen Betätigung als natürliche Personen im Sinne des Art. 1 Abs. 1 und 2 DSGVO[71] und Art. 13 Abs. 3 und 5 Richtlinie 2002/58/EG und hält – zur Gewährleistung eines einheitlichen Schutzes natürlicher Personen – eine richtlinienkonforme Auslegung von § 7 Abs. 2 Nr. 1 UWG für geboten.[72] Da der Senat im zu entscheidenden Sachverhalt allerdings weder das Vorliegen einer ausdrücklichen noch mutmaßlichen Einwilligung der Werbeadressaten angenommen und die streitgegenständlichen Werbeanrufe daher als unzumutbare Belästigung qualifiziert hat, vertieft er in dem Urteil letztlich diesen Standpunkt und die daraus folgenden Implikationen nicht.

Da das OVG die Revision zugelassen hat, diese von dem Werbetreibenden eingelegt wurde und gerade auch der Aspekt der richtlinienkonformen Auslegung von § 7 Abs. 2 Nr. 1 UWG Gegenstand der Revision ist, wird diese Frage – soweit diese letztlich für die Urteilsfindung überhaupt relevant ist – eventuell durch das Bundesverwaltungsgericht erörtert.

### 11.3.2 Werbe-E-Mails an Bestandskunden

Da im Onlinehandel die Einholung von Einwilligungen zur werblichen Nutzung von Kontaktinformationen wohl überwiegend wenig Feedback von Kundinnen und Kunden nach sich zieht, wird von Werbetreibenden häufig auf die Möglichkeit der Nutzung von E-Mail-Adressen nach § 7 Abs. 3 UWG zurückgegriffen. Die Vorschrift ermöglicht eine Verwendung der E-Mail-Adresse für werbliche Kommunikation auch ohne Einwilligung der Werbeadressaten unter den Voraussetzungen, dass der Werbetreibende

[71] In diesem Sinne auch BGH, Urteil vom 12. Oktober 2021 – VI ZR 488/19.
[72] OVG des Saarlandes, Urteil vom 2. Mai 2023 – 2 A 111/22 Rn. 35, juris.

a) die E-Mail-Adresse im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden erhalten hat,
b) diese ausschließlich zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,
c) der Kunde der Verwendung nicht widersprochen hat und
d) bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann.

Sofern nicht sämtliche in der Vorschrift genannten Voraussetzungen erfüllt sind, stellt die E-Mail-Ansprache von Bestandskunden eine unzumutbare Belästigung dar und ist damit als wettbewerbswidrig zu qualifizieren. Da der Bundesgesetzgeber mit der Vorschrift des § 7 Abs. 3 UWG die unionsrechtliche Regelung aus Art. 13 Abs. 2 Richtlinie 2002/58/EG im deutschen Recht umsetzt, kann – wie beim Telefonmarketing – eine Werbemaßnahme, die gegen wettbewerbsrechtliche Vorgaben verstößt, aus datenschutzrechtlicher Sicht kein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit. f DSGVO und damit auch keine zulässige Datenverarbeitung darstellen.[73]

Die Erfüllung aller Vorgaben der Vorschrift gelang der überwiegenden Mehrzahl der werbetreibenden Unternehmen, deren dahingehende E-Mail-gestützte Werbetätigkeit im Berichtszeitraum Gegenstand von Beschwerden war, oftmals nicht.

zu a)

So wurden entgegen der Vorgabe „*im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung*" in mehreren untersuchten Fällen oftmals reine Interessentenanfragen von betroffenen Personen zum Anlass genommen, um an Empfän-

[73] OVG des Saarlandes, Beschluss vom 16. Februar 2021 – 2 A 355/19 Rn. 30, juris.

ger E-Mail-Newsletter zu adressieren; maßgeblich für die Zulässigkeit der Bestandskundenwerbung ist jedoch, dass es zwischen werbetreibendem Unternehmen und Adressat der Werbebotschaft zu einem Vertragsschluss gekommen ist.

zu b)

Auch die *„Direktwerbung für eigene ähnliche Waren oder Dienstleitungen"* wurde als Zulässigkeitsvoraussetzung von werbetreibenden Unternehmen weit überwiegend zu extensiv ausgelegt.

Obschon die Vorschrift zunächst bei eigenen Produkten des werbenden Unternehmens ansetzt, wurden im Berichtszeitraum wiederholt Beschwerden zu Unternehmen vorgetragen, die im Rahmen ihres Bestandskundenmailings neben eigenen auch Produkte von Partnerunternehmen beworben haben. Von den Werbetreibenden wurde in den diesbezüglichen Verfahren oftmals vorgetragen, dass der Fremdanteil der Werbung im Vergleich zu dem eigenen Werbeanteil allenfalls marginal sei und dementsprechend nicht ins Gewicht falle. Da die Vorschrift jedoch ausdrücklich nur Eigenwerbung privilegiert, kommt es somit nicht auf eine Bagatellgrenze der Werbung für Produkte Dritter an.

Die tatbestandliche Ähnlichkeit zwischen erworbenen und beworbenen Produkten war allerdings als häufigste Fehlerquelle zu identifizieren. Das Merkmal der Ähnlichkeit ist dabei individuell anhand der bereits erworbenen Waren und Dienstleistungen unter Berücksichtigung eines typischen Verwendungszwecks oder Bedarfs des Kunden zu betrachten. Dies setzt nicht voraus, dass erworbenes und beworbenes Produkt identisch sein müssen; die zu fordernde enge Auslegung des Ähnlichkeitsbegriffs gestattet allerdings keine beliebige Ausdehnung auf ein ganzes Produktsortiment eines Unternehmens, sondern stellt im Einzelfall auf die Funktionsähnlichkeit oder die Zubehör-/Ergänzungseigenschaft des beworbenen Produkts ab. Die Bandbreite an Werbemöglichkeiten kann sich somit im Rahmen eines Bestandskundenverhältnisses abhän-

gig von Art und Umfang der getätigten Einkäufe erheblich vergrößern.

Das Ähnlichkeitsmerkmal wurde in den im Berichtszeitraum untersuchten beschwerdegegenständlichen Werbeansprachen nahezu durchgehend überstrapaziert. Regelmäßig standen einmaligen Einkäufen eines oder weniger Produkte ein Strauß von Werbe-E-Mails gegenüber, in denen Unternehmen undifferenziert für vielgestaltige Produktsortimente warben. Dass Werbetreibende geeignete Maßnahmen operationalisiert hätten, um kundenindividuell einen Konnex zwischen erworbenen und zu bewerbenden Produkten herstellen und dadurch die zu fordernde Ähnlichkeit gewährleisteten zu können, war in keinem Verfahren ersichtlich.

zu c)

Dass der *Kunde bei der Verwendung der E-Mail-Adresse nicht widersprochen haben darf*, ist einleuchtend und dieser wettbewerbsrechtliche Widerspruch, der seine datenschutzrechtliche Entsprechung in Art. 21 Abs. 2 DSGVO hat, konnte in den von uns untersuchten Fällen regelmäßig von dem Werbetreibenden ohne Schwierigkeiten berücksichtigt und dokumentiert werden.

zu d)

Die Pflicht, *Kundinnen und Kunden bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hinzuweisen, dass sie der Verwendung jederzeit widersprechen können,* wurde in den beschwerdegegenständlichen Verfahren zumeist dergestalt umgesetzt, dass innerhalb eines Bestellprozesses bei Abfrage einer E-Mail-Adresse eine dahingehende Belehrung erfolgt und in den versandten Werbe-E-Mails ohne weiteren Hinweis ein Abmeldelink eingebunden war. Auch wenn wettbewerbsrechtlich eine Belehrung über das Widerspruchsrecht notwendig ist, geht die Kommentarliteratur davon aus, dass diese alternativ durch Bereitstellung einer unmittelbaren Möglichkeit der Widerspruchseinlegung (Opt-out) – wie bspw.

durch einen Abmeldelink in einer Werbe-E-Mail – als erfüllt gelten kann.[74] Ein ausdrücklicher Hinweis auf das Widerspruchsrecht – bspw. zum Zeitpunkt der Datenerhebung im Bestellprozess – bleibt allerdings datenschutzrechtlich nach dem unmissverständlichen Wortlaut von Art. 21 Abs. 4 DSGVO geboten.

Ungeachtet dessen sollten Unternehmen, die von der Ausnahmeregelung des § 7 Abs. 3 UWG wirksam Gebrauch machen wollen, sowohl im Bestellprozess als auch in den versandten Werbe-E-Mails auch eine wirksame Opt-out-Möglichkeit vorsehen.

In § 7 Abs. 3 UWG hat der Bundesgesetzgeber die europarechtliche Regelung des Art. 13 Abs. 2 Richtlinie 2002/58/EG, nach der eine Nutzung der elektronischen Kontaktinformation dann gestattet ist, wenn Kundinnen und Kunden zum Zeitpunkt der Datenerhebung und der nachfolgenden Werbeansprache die Möglichkeit der Ablehnung der werblichen Datennutzung gegeben wurde, in nationales Recht umgesetzt. Während der Richtliniengeber somit Kundinnen und Kunden ausdrücklich die konkrete Handlungsmöglichkeit der Ablehnung der Datenverwendung bereits zum Zeitpunkt der Datenerhebung einräumt, bleibt der Bundesgesetzgeber mit der Regelung einer reinen Belehrung über das Widerspruchsrecht erkennbar hinter der Vorgabe der EU-Richtlinie zurück.

Die im deutschen Recht geregelte Hinweispflicht gewährleistet somit ausdrücklich nicht, dass Kundinnen und Kunden bereits zum Zeitpunkt der Datenerhebung in einem Bestellprozess eine aktive Möglichkeit der Ablehnung der werblichen Datenverwendung – bspw. durch Abwahl einer vorausgefüllten Checkbox – eingeräumt wird. Um dem europäischen Recht effektiv Geltung zu verschaffen, ist eine Auslegung von § 7 Abs. 3 Nr. 4 UWG im Sinne des Wortlauts von Art. 13 Abs. 2

[74] GRUR 2006, 285, beck-online; Spindler/Schuster/Micklitz/Schirmbacher, 4. Aufl. 2019, UWG § 7 Rn. 222; Fezer/Büscher/Obergfell/Mankowski, 3. Aufl. 2016, UWG § 7 Rn. 276.

Richtlinie 2002/58/EG geboten, mit der Folge, dass die reine Widerrufsbelehrung zum Zeitpunkt der Datenerhebung und erst die Möglichkeit der Einlegung eines Widerspruchs durch Abmeldelink in den erhaltenen Werbe-E-Mails nicht als unionsrechtskonform zu qualifizieren ist.

Auch ohne Rückgriff auf eine richtlinienkonforme Auslegung von § 7 Abs. 3 Nr. 4 UWG ist im datenschutzrechtlichen Kontext des Werbewiderspruchs nach Art. 21 Abs. 2 DSGVO das Erleichterungsgebot bei der Geltendmachung von Betroffenenrechten nach Art. 12 Abs. 2 Satz 1 DSGVO zu berücksichtigen. Das Erleichterungsgebot eröffnet dem datenschutzrechtlich Verantwortlichen zwar einen weiten Gestaltungsspielraum, ist als programmatischer Ansatz aber auch konsequent zu operationalisieren; soweit ein werbetreibendes Unternehmen im Rahmen der Aussendung von Werbe-E-Mails eine proaktive Opt-out-Möglichkeit durch Abmeldelink technisch realisiert hat, ist zur einheitlichen Umsetzung des Erleichterungsgebots somit die Gewährleistung einer vergleichbar einfachen Möglichkeit zur Widerspruchseinlegung – bspw. durch Checkbox – bereits im Bestellprozess vorzusehen.

Zusammengefasst ist es aufgrund der Komplexität der in § 7 Abs. 3 UWG geregelten Vorgaben zur werblichen Verwendung von E-Mail-Adressen im Rahmen der Bestandskundenwerbung für Werbetreibende mindestens herausfordernd, hiervon in wettbewerbsrechtlich zulässiger Weise Gebrauch zu machen. Folge einer Wettbewerbswidrigkeit ist ein Datenschutzverstoß, da die der Werbeansprache zugrundeliegende Datenverarbeitung nicht nach Art. 6 Abs. 1 lit. f DSGVO legitimiert sein kann.

Will ein Werbetreibender die Vorgaben zur tatbestandlichen Produktähnlichkeit effektiv operationalisieren, setzt dies eine stetige kundenindividuelle Analyse der Einkäufe[75] und eine

[75] Diese kundenindividuelle Analyse der Einkaufshistorie stellt dabei für sich genommen eine eigenständige Verarbeitung personenbezogener Daten dar,

damit korrespondierende feingranulare Kategorisierung des Produktsortiments voraus, da nur hierdurch ein hinreichender Zusammenhang zwischen erworbener und zu bewerbender Ware und Dienstleistung hergestellt werden kann. Ferner sollte eine einheitliche Gewährleistung des Widerspruchsrechts durch Implementierung der Möglichkeit des Opt-outs zum Zeitpunkt der Datenerhebung und -nutzung umgesetzt werden.[76]

Die im Berichtszeitraum untersuchten Sachverhalte waren nahezu ausschließlich als wettbewerbswidrige Bestandskundenwerbung zu qualifizieren, die somit letztlich auch nicht nach Art. 6 Abs. 1 lit. f DSGVO datenschutzrechtlich legitimiert waren; neben Hinweisen nach Art. 58 Abs. 1 lit. b DSGVO und Verwarnungen nach Art. 58 Abs. 2 lit. b DSGVO wurde in einem Fall die Bußgeldstelle mit dem Sachverhalt befasst.

### 11.3.3 Bonusprogramme und Gewinnspiele

Mit Bonusprogrammen und Gewinnspielen verfolgen Unternehmen überwiegend keine altruistischen Zwecke, sondern das legitime Ziel, personenbezogene Daten von (potenziellen) Kundinnen und Kunden für zielgerichtete Maßnahmen der Direktwerbung zu gewinnen und dadurch den Absatz von Produkten oder Dienstleistungen zu fördern.

Da sich die Teilnahme an einem Bonusprogramm oder Gewinnspiel regelmäßig als eine zwischen der teilnehmenden Person und dem anbietenden Unternehmen geschlossene vertragliche Vereinbarung darstellt, kann die Verarbeitung der Daten der teilnehmenden Person zur Vertragserfüllung auf Grundlage von Art. 6 Abs. 1 lit. b DSGVO datenschutzrechtlich legitimiert sein. Soweit bspw. in Teilnahmebedingungen festgehalten ist, dass Rabatte oder Boni nur anhand individueller

---

die einer Legitimationsgrundlage nach Art. 6 Abs. 1 DSGVO bedarf und über die transparent informiert werden muss.

[76] Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO), Ziffer 5.3.

Umsätze gewährt werden, ist die Verarbeitung von einkaufsbezogenen Daten von Kundinnen und Kunden im Kontext der vertraglichen Beziehung zur Erreichung dieses Vertragszwecks erforderlich.

Das Tatbestandsmerkmal der *„Erforderlichkeit zur Vertragserfüllung"* kann allerdings nicht beliebig für jedwedes Element von Teilnahmebedingungen unterstellt werden, sondern ist mit objektivem Blick auf eine konkrete vertragliche Hauptleistungspflicht eng auszulegen.[77] Das anbietende Unternehmen muss vor diesem Hintergrund den Nachweis führen können, dass ohne die auf die Teilnahmebedingungen gestützte Verarbeitung personenbezogener Daten der Hauptgegenstand des Vertrages nicht erreicht werden kann. Allein die Erwähnung einer Datenverarbeitung in einem Vertragstext oder deren mögliche Nützlichkeit für die Erreichung eines Vertragszwecks reicht nicht aus, um von einer Erforderlichkeit im Sinne des Art. 6 Abs. 1 lit. b DSGVO auszugehen.[78]

Im Berichtszeitraum wurde aufgrund einer Beschwerde das Vorgehen eines Handelsunternehmens, das in den Teilnahmebedingungen eines angebotenen Bonusprogramms die Verarbeitung der Kundendaten für Zwecke der telefonischen und E-Mail-gestützten Direktwerbung einseitig vorgab und diese Datenverarbeitung als im Sinne des Art. 6 Abs. 1 lit. b DSGVO erforderlich zur Vertragserfüllung qualifizierte, untersucht. Da nach den Teilnahmebedingungen des Bonusprogramms der Hauptgegenstand dieses Vertrags die Gewährung von umsatzbezogenen Rabatten war, konnte das Unternehmen gerade nicht glaubhaft machen, dass dieser Hauptgegenstand ohne die Verarbeitung der Daten der betroffenen Kundinnen und Kunden für Zwecke der Direktwerbung nicht erfüllt werden kann. Die dementsprechend von dem Unternehmen als

---

[77] Europäischer Datenschutzausschuss, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Art. 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten, Version 2.0, Rn. 30 ff.

[78] EuGH, Urteil vom 4. Juli 2023 in der Rechtssache Meta Platforms Inc. gegen Bundeskartellamt, C-252/21, EU:C:2022:704, Rn. 98 ff.

Legitimationsgrundlage für die werbliche Datenverwendung der Kundinnen und Kunden in Anspruch genommene Vorschrift Art. 6 Abs. 1 lit. b DSGVO konnte dafür nicht herangezogen werden.

Unter Berücksichtigung des wettbewerbsrechtlichen Einwilligungsvorbehalts aus § 7 Abs. 2 Nr. 1 und 2 UWG für die werbliche Nutzung der Kommunikationskanäle Telefon und E-Mail war somit auch für die Datenverarbeitung der Kundinnen und Kunden für Zwecke der Direktwerbung ausschließlich auf die Einwilligung nach Art. 4 Nr. 11 in Verbindung mit Art. 6 Abs. 1 lit. a DSGVO abzustellen. Dass die Teilnahme an einem Bonusprogramm oder – wie in weiteren Beschwerden im Berichtszeitraum vorgetragen – an einem Gewinnspiel eines Handelsunternehmens von einer obligatorischen Werbeeinwilligung abhängig gemacht wird, stellt dabei keinen Verstoß gegen die Wirksamkeitsbedingungen aus Art. 7 Abs. 4 DSGVO (sog. Koppelungsverbot) dar.

Für die Beantwortung der Frage, ob eine neben einem Vertrag verpflichtend abzugebende Einwilligung freiwillig i. S. d. Art. 7 Abs. 4 DSGVO erteilt wird, ist im Wesentlichen darauf abzustellen, inwiefern diese Erklärung durch die betroffene Person ohne jeden Druck oder Zwang abgegeben werden kann. Die Freiwilligkeit kann typischerweise dann bestritten werden, wenn der Verarbeitungssituation ein rechtliches Abhängigkeitsverhältnis, wie es typischerweise im Zusammenhang mit einem Beschäftigungs- oder Mietverhältnis anzunehmen ist, zugrunde liegt; auch kann die Monopolstellung eines Unternehmens und die Angewiesenheit des Erklärenden auf eine spezifische Ware oder Dienstleistung bzw. deren Alternativlosigkeit durchgreifende Zweifel an der Freiwilligkeit einer Einwilligung begründen. Grundsätzlich ist unter Beachtung des Erwägungsgrunds 42 DSGVO von einer wirksamen, da freiwilligen Einwilligung der betroffenen Person auszugehen, sofern sich für diese nach Verweigerung oder Widerruf der Einwilligung keine Nachteile ergeben oder zu befürchten sind.

Für die im Berichtszeitraum untersuchten Fälle der Kopplung einer Werbeeinwilligung an die Teilnahme an einem Bonusprogramm oder Gewinnspiel ergaben sich keine Anhaltspunkte, dass diese Verbindung nicht freiwillig und damit datenschutzrechtlich unzulässig gewesen wäre; regelmäßig konnte weder ein asymmetrisches Machtgefälle oder eine Monopolstellung im Verhältnis zwischen Kundinnen und Kunden und Handelsunternehmen angenommen werden noch führte eine Verweigerung der Werbeeinwilligung und damit verbunden der Ausschluss an der Teilnahme an Rabattprogrammen oder Gewinnspielen zu einem Nachteil im Sinne des Erwägungsgrunds 42. Dabei ist der Begriff des Nachteils restriktiv auszulegen, so dass hiervon lediglich schwerwiegende Folgen – wie bspw. eine missbräuchliche Übervorteilung der betroffenen Person – und nicht nur hinnehmbare Unannehmlichkeiten erfasst sind.

# XII.

# Ordnungswidrigkeiten- und Bußgeldverfahren

# 12 Ordnungswidrigkeiten- und Bußgeldverfahren

## 12.1 Leitlinien zur Bußgeldbemessung

### 12.1.1 Hintergrund und Zielsetzung

Eine der zentralen Aufgaben der Bußgeldstellen der Datenschutzaufsichtsbehörden ist die konkrete Berechnung der Höhe der festzusetzenden Bußgelder. Diese können, insbesondere bei Unternehmen als Betroffene eines Bußgeldverfahrens, erheblich divergieren, da der europäische Gesetzgeber den Bußgeldbehörden bezüglich der Bußgeldhöhe bei Datenschutzverstößen nach der Datenschutz-Grundverordnung (DSGVO) gemäß Art. 83 Abs. 4, 5 und 6 DSGVO einen erheblichen Ermessensspielraum eingeräumt hat.

Als Bußgeldrahmen bei Verstößen gegen die in Art. 83 Abs. 4 DSGVO genannten Bestimmungen ist eine Geldbuße von bis zu 10 Mio. € beziehungsweise im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des der behördlichen Entscheidung vorangegangenen Geschäftsjahres vorgesehen. Bei Verstößen i. S. d. Art. 83 Abs. 5, 6 DSGVO kann im Höchstmaß sogar eine Geldbuße von bis zu 20 Mio. € beziehungsweise von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des der behördlichen Entscheidung vorangegangenen Geschäftsjahres festgesetzt werden.

Da die Höhe der Bußgelder gemäß Art. 83 Abs. 1 DSGVO jeweils so festzusetzen ist, dass das Bußgeld im Einzelfall wirksam, verhältnismäßig und abschreckend ist, handelt es sich bei der Schwere des Verstoßes und dem Jahresumsatz des Unternehmens um die für die Bußgeldberechnung maßgeblichen Parameter. Des Weiteren regelt Art. 83 Abs. 2 DSGVO, welche weiteren Umstände bei der Festsetzung einer Geldbuße zu berücksichtigen sind. Dennoch blieb in Bezug auf die konkrete Bußgeldhöhe, insbesondere auf Grund des weiten Bußgeld-

rahmens und der Berücksichtigung des Jahresumsatzes der Unternehmen, gerade bei Unternehmen mit hohen Jahresumsätzen, eine erhebliche Unsicherheit sowohl für die Anwender der Bußgeldbestimmungen der DSGVO, die diese nach den Vorstellungen des europäischen Gesetzgebers möglichst einheitlich anwenden sollen, als auch für die jeweiligen Betroffenen.

Aus diesem Grund hat der Europäische Datenschutzausschuss (EDSA) zunächst im Mai 2022 und dann als überarbeitete Version im Mai 2023 die sogenannten „Leitlinien 04/2022 zur Berechnung von Bußgeldern nach der Datenschutz-Grundverordnung" („guidelines 04/2022 on the calculation of administrative fines under the GDPR") entwickelt und veröffentlicht. Diese sollen eine klare und transparente Grundlage für die Festsetzung von Geldbußen bei Datenschutzverstößen, die durch Unternehmen begangen werden, schaffen und eine länderübergreifende, einheitliche Rechtsanwendung ermöglichen. Gleichzeitig sollen die Behörden allerdings weiterhin befugt und verpflichtet sein, jeweils eine Einzelfallbetrachtung vorzunehmen. Im Vordergrund der Leitlinien steht daher die Harmonisierung der Methodik der Bußgeldberechnung, nicht aber des Ergebnisses.

### 12.1.2 Funktionsweise

Die Leitlinien des EDSA sehen eine mehrstufige Berechnung der Geldbuße in insgesamt fünf Schritten mit teilweise integrierten Zwischenschritten vor. Diese sollen nach den Leitlinien des EDSA zwar grundsätzlich befolgt werden, allerdings liegt die Festsetzung der Höhe der Geldbuße, ungeachtet der Anwendung der Leitlinien, weiterhin im Ermessen der Behörde, sodass die Behörde unter Beachtung ihrer europäischen Kooperations- und Kohärenzpflichten auch einzelne Schritte ganz oder teilweise auslassen kann, sofern sie diese im Einzelfall für unanwendbar hält.

Im Folgenden werden die fünf Schritte der Bußgeldberechnung nach den Leitlinien des EDSA grob skizziert:

*Schritt 1:* In einem ersten Schritt ist das der Verhängung der Geldbuße zu Grunde liegende tatsächliche Verhalten des betroffenen Unternehmens zu ermitteln. Dabei ist zunächst festzustellen, ob es sich nach den Gesamtumständen um ein und dasselbe oder um getrennt sanktionierbare Verhaltensweisen handelt, und ob ein und dasselbe Verhalten zu einer Reihe verschiedener Zuwiderhandlungen geführt hat. Wurden durch ein einheitliches Verhalten mehrere Zuwiderhandlungen begangen, ist weiterhin zu untersuchen, ob einzelne Verstöße durch die Anwendung der auf europäischer Ebene anerkannten Konkurrenzregelungen wiederum ausgeschlossen werden.

*Schritt 2:* In einem zweiten Schritt erfolgt die Ermittlung des sog. Ausgangswertes, d.h. eine erste Bezifferung der Bußgeldhöhe anhand des Schweregrades des ermittelten Verstoßes sowie die Anpassung des Ausgangsbetrages anhand des Jahresumsatzes des der Bußgeldentscheidung vorausgegangenen Geschäftsjahres.

Als Orientierungshilfe für die Berechnung des Ausgangswertes wurde den Datenschutzaufsichtsbehörden in den Leitlinien eine Tabelle an die Hand gegeben, durch deren Anwendung eine möglichst einheitliche und nachvollziehbare Ermittlung des Ausgangswertes ermöglicht wird. Die Höhe des Ausgangswertes bestimmt sich nach dieser Tabelle anhand von drei Kriterien, nämlich danach, ob es sich um einen Verstoß nach Art. 83 Abs. 4 DSGVO oder nach Art. 83 Abs. 5 oder 6 DSGVO handelt, ob es sich bei dem betroffenen Unternehmen um ein solches mit einem Jahresumsatz von unter oder über 500 Mio. € handelt und welcher Schweregrad bezüglich der einzelnen Verstöße anzunehmen ist. Gemäß den Leitlinien sind Verstöße gegen die DSGVO in die drei Schweregrade leicht (low level of seriousness), mittel (medium level of seriousness) und schwer (high level of seriousness) einzuordnen. Welcher Schweregrad konkret vorliegt, ergibt sich im Wesentlichen aus der Art des Verstoßes, dem Umfang, der Art und dem Zweck

der Verarbeitung, der Anzahl der konkret betroffenen Personen, der Höhe des Schadens, der Dauer des Verstoßes und danach, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde.

Der konkrete Ausgangsbetrag wird durch den Anwender anschließend innerhalb des zuvor ermittelten Rahmens festgesetzt, wobei der Ausgangswert mit zunehmender Schwere des Verstoßes höher anzusetzen ist.

Der Ausgangsbetrag ist sodann an die Unternehmensgröße und damit an die individuelle Leistungsfähigkeit des betroffenen Unternehmens anzupassen. Maßgeblich hierfür ist der Jahresumsatz des der behördlichen Entscheidung vorausgegangenen Geschäftsjahres. Der Unternehmensbegriff umfasst dabei, wie durch den Gerichtshof der Europäischen Union erneut definiert wurde,[79] jede eine wirtschaftliche Tätigkeit ausübende Einheit, auch wenn diese aus rechtlicher Sicht aus mehreren natürlichen oder juristischen Personen besteht. Diese wirtschaftliche Einheit muss dabei in einer einheitlichen Organisation persönlicher, materieller und immaterieller Mittel, die dauerhaft einen bestimmten wirtschaftlichen Zweck verfolgt, bestehen. Je nach Unternehmensgröße sehen die Leitlinien eine Anpassung des zuvor ermittelten Ausgangswertes auf eine Summe von bis zu 0,2 % des Ausgangsbetrages vor. Während in der Regel bei Unternehmen mit einem Jahresumsatz von etwa 500 Mio. € eine Reduzierung des Ausgangswertes ausscheidet, dient eine Kürzung des Ausgangsbetrags in der vorgenannten Größenordnung insbesondere der Berücksichtigung der Belange von Unternehmen mit sehr geringen Jahresumsätzen.

*Schritt 3:* Anschließend ist der dem Bußgeldverfahren zu Grunde liegende Sachverhalt auf mildernde und erschwerende Umstände zu überprüfen und der angepasste Ausgangsbetrag bei Bedarf entsprechend herabzusetzen oder zu erhöhen. Als erhö-

[79] EuGH, Urteil vom 05.12.2023, C-807/21.

hende oder mildernde Umstände kommen alle in Art. 83 Abs. 2 DSGVO geregelten Umstände in Betracht, deren Vorliegen nicht bereits in die Berechnung des Ausgangsbetrages eingeflossen ist. Mindernd können sich gemäß Art. 83 Abs. 2 lit. c) DSGVO beispielsweise Maßnahmen des betroffenen Unternehmens auswirken, die dieses zur Schadensbegrenzung trifft. Bußgelderhöhend wirken sich hingegen gemäß Art. 83 Abs. 2 lit. e) DSGVO in der Regel einschlägige frühere Verstöße des betroffenen Unternehmens aus.

*Schritt 4:* Sodann ist sicherzustellen, dass die errechnete Geldbuße die gesetzlichen Höchstbeträge des Art. 83 Abs. 4 bzw. der Art. 83 Abs. 5 oder 6 DSGVO nicht übersteigt.

*Schritt 5:* In einem letzten Schritt erfolgt schließlich eine abschließende Kontrolle, ob die zuvor berechnete Geldbuße ihrer Höhe nach den in Art. 83 Abs. 1 DSGVO gestellten Anforderungen an Wirksamkeit, Verhältnismäßigkeit und Abschreckung entspricht. Anschließend ist gegebenenfalls eine finale Anpassung der Höhe der Geldbuße vorzunehmen, sofern sich eine solche nach dem Ergebnis der zuvor vorgenommenen abschließenden Kontrolle als erforderlich herausstellt.

### Fazit

Die durch den EDSA entwickelten Leitlinien zur Berechnung von Bußgeldern nach der Datenschutz-Grundverordnung stellen ein wichtiges Hilfsmittel für die Datenschutzaufsichtsbehörden bei der Berechnung von Bußgeldern dar und können auch für die betroffenen Unternehmen eine Möglichkeit bieten, behördliche Bußgeldentscheidungen absehbarer zu machen. Dennoch muss es sich bei allen Bußgeldentscheidungen um das Ergebnis einer Einzelfallbetrachtung handeln, die auf Grundlage einer wertenden Betrachtung aller Gesamtumstände getroffen wurde.

## 12.2 Die Nichtverfolgungszusicherung im Bußgeldverfahren

Unsere Dienststelle hat sich im Laufe des vergangenen Jahres vertieft mit dem Thema der Nichtverfolgungszusicherung/Nichtverfolgungszusage im Rahmen von Bußgeldverfahren beschäftigt. Eine solche Nichtverfolgungszusicherung kann für Datenschutzaufsichtsbehörden im Einzelfall ein wichtiges Instrument zur Aufklärung von Sachverhalten und zur Beweisgewinnung darstellen.

Gerade bei der Aufklärung und Verfolgung erheblicher und teilweise systematischer Datenschutzverstöße, die durch Unternehmen begangen werden, können Verfahrensverläufe maßgeblich von den Aussagen einzelner Zeugen abhängen, die auf Grund spezifischer Kenntnisse über interne Vorgänge in den jeweiligen Unternehmen von entscheidendem Gewicht für die Behörden im Bußgeldverfahren sind. In Betracht kommen insoweit beispielsweise Aussagen von Mitarbeitern der betroffenen Unternehmen oder von Geschäftspartnern.

Vorgenannte Zeugen haben allerdings in einigen Fällen auf Grund einer möglichen Beteiligung an den Datenschutzverstößen ein Aussageverweigerungsrecht nach § 41 Abs. 2 Bundesdatenschutzgesetz (BDSG) i.V.m. §§ 46 Abs. 1 Ordnungswidrigkeitengesetz (OWiG), 55 Strafprozessordnung (StPO). Gemäß § 55 StPO kann jeder Zeuge die Auskunft auf solche Fragen verweigern, durch deren Beantwortung für ihn selbst oder für einen der in § 52 Abs. 1 StPO bezeichneten Angehörigen die Gefahr entstehen würde, wegen einer Straftat oder einer Ordnungswidrigkeit verfolgt zu werden. Voraussetzung für die Entstehung eines Aussageverweigerungsrechts ist daher das tatsächliche Bestehen einer Verfolgungsgefahr. Eine solche Verfolgungsgefahr besteht für den Zeugen allerdings dann nicht mehr, wenn offenkundig ist, dass er nicht mehr für eine etwaige Tat verfolgt werden kann.[80]

[80] KK-StPO/Bader, 9. Aufl. 2023, StPO § 55 Rn. 4-5a.

Insbesondere bei grundsätzlich aussagewilligen Zeugen ergibt sich daher die Problematik, dass diese lediglich deswegen von ihrem Aussageverweigerungsrecht Gebrauch machen, um nicht selbst wegen eines möglichen Datenschutzverstoßes verfolgt zu werden, sodass dadurch die Aufklärung und Verfolgung des Datenschutzverstoßes gänzlich verhindert oder jedenfalls wesentlich erschwert wird.

Nach dem Ergebnis unserer rechtlichen Bewertung kann im Einzelfall durch den Erlass einer Nichtverfolgungszusicherung bezüglich dieser Problematik Abhilfe geschaffen werden.

Durch den Erlass einer wirksamen Nichtverfolgungszusicherung, die im Kartellrecht als gängige Praxis gilt, kann die Behörde die Voraussetzungen für das Bestehen eines Aussageverweigerungsrechts nach § 55 StPO und damit die Verfolgungsgefahr für den Zeugen ausschließen.

Die Behörde erklärt in dieser Fallkonstellation mittels ihrer Zusicherung gegenüber dem Zeugen verbindlich, dass ihm wegen der Verstöße, wegen derer die Aussage des Zeugen erfolgen soll, kein Bußgeldverfahren durch die Behörde droht. Voraussetzung ist, dass die Verfolgung des Zeugen wegen einer Straftat bezüglich der Verstöße, wegen derer er vernommen werden soll, ausgeschlossen ist und dass es sich bei den zu verfolgenden Ordnungswidrigkeiten ausschließlich um Verstöße gegen datenschutzrechtliche Bestimmungen handelt, bezüglich derer auf die Verfolgung des Zeugen verzichtet werden kann. Liegen diese Voraussetzungen vor, kann die Behörde von ihrem Verfolgungsermessen nach § 47 Abs. 1 OWiG Gebrauch machen und eine Nichtverfolgungszusicherung erlassen.

Da eine Behörde die Verfolgung durch andere Stellen allerdings nicht ausschließen kann, kommt der Erlass einer Nichtverfolgungszusicherung, wie bereits erläutert, lediglich dann in Betracht, wenn die Verfolgung des Zeugen wegen einer Straftat ausgeschlossen ist und es sich bei den zu verfolgenden Ordnungswidrigkeiten ausschließlich um Verstöße gegen datenschutzrechtliche Bestimmungen handelt. Durch die behörd-

liche Zusicherung wird ein Vertrauenstatbestand gegenüber dem Zeugen geschaffen, der nach den Grundsätzen des fairen Verfahrens und dem Verbot widersprüchlichen Verhaltens eine Selbstbindung der Behörde bewirkt, sodass die Behörde, solange die zulässigen Grenzen des Ermessens nicht überschritten sind und die Behörde daher nicht zu einer Rücknahme der Zusicherung verpflichtet ist, nicht wieder von der Zusicherung abweichen darf.[81]

Im Falle einer Nichtverfolgungszusicherung besteht in dem Moment der behördlichen Entscheidung daher die Verfolgungsgefahr für den Zeugen nicht mehr und sein Aussageverweigerungsrecht erlischt automatisch. In der Folge ist es der Behörde möglich, den Zeugen vollumfänglich zu vernehmen.

**Fazit**

Die Nichtverfolgungszusicherung kann nach dem Ergebnis unserer rechtlichen Bewertung ein wichtiges Instrument bei der Verfolgung datenschutzrechtlicher Verstöße darstellen und bietet insbesondere Vorteile für die Vernehmung aussagewilliger Zeugen, die ihre Aussage lediglich wegen der Befürchtung, sich auf Grund ihrer eigenen Aussage einer Verfolgung im Rahmen eines Straf-oder Bußgeldverfahrens auszusetzen, verweigern.

## 12.3 Durchführung eines Beschlagnahmeverfahrens

Das Unabhängige Datenschutzzentrum Saarland nimmt im Rahmen datenschutzrechtlicher Ordnungswidrigkeitenverfahren nach Art. 83 Datenschutz-Grundverordnung (DSGVO) die gleiche Stellung wie die Staatsanwaltschaft in strafrechtlichen Ermittlungsverfahren ein. Gemäß § 46 Abs. 1 Ordnungswidrigkeitengesetz (OWiG) gelten für das Bußgeldverfahren sinngemäß die Vorschriften der allgemeinen Gesetze über das Straf-

[81] BT-Drucksache 19/2349, Seite 117 zu § 59 Abs. 4 GWB.

verfahren, namentlich der Strafprozessordnung (StPO). Für die Durchführung eines Bußgeldverfahrens wegen des Verdachts eines Datenschutzverstoßes stehen unserer Behörde nach § 46 Abs. 2 OWiG grundsätzlich dieselben Rechte und Pflichten wie der Staatsanwaltschaft bei der Verfolgung von Straftaten zu. Hierzu zählen auch die allgemeinen Befugnisse im Rahmen durchzuführender Ermittlungen zur Aufklärung des Sachverhalts.

So können während eines Ermittlungsverfahrens beispielsweise Zeugen vernommen, Sachverständige herangezogen oder im Rahmen einer Durchsuchung Gegenstände zu Beweiszwecken sichergestellt und beschlagnahmt werden.

In einem konkreten Fall beobachtete ein Betroffener mehr als ein Jahr lang mit einer in seinem Kraftfahrzeug dauerhaft angebrachten Dashcam ununterbrochen und ohne konkreten Anlass während des Fahrzeugbetriebs den öffentlichen Verkehrsraum, zeichnete diesen permanent auf und speicherte die so entstandenen Videosequenzen dauerhaft ab. Dabei wurde eine Vielzahl von Kraftfahrzeugen mit erkennbaren Kennzeichen, deren Fahrzeugführer sowie teilweise weitere Fahrzeuginsassen, andere Verkehrsteilnehmer oder Fußgänger erfasst. Für eine solch permanente sowie umfassende Beobachtung und Aufzeichnung des öffentlichen Verkehrsraums, die noch dazu anlasslos und für die sich in der Öffentlichkeit bewegenden Personen intransparent erfolgt, existiert keine Verarbeitungsbefugnis nach Art. 5 Abs. 1 lit. a und Art. 6 Abs. 1 DSGVO; sie ist somit datenschutzrechtlich unzulässig.[182] Zudem stellt ein vorsätzlicher oder fahrlässiger Verstoß gegen die Grundsätze der Verarbeitung gemäß den Artikeln 5, 6, 7 und 9 DSGVO nach Art. 83 Abs. 5 lit. a DSGVO eine Ordnungswidrigkeit dar.

Im Rahmen des insoweit eingeleiteten Ermittlungsverfahrens ergab sich, dass für die vollständige Aufklärung des Sachverhalts, sowohl hinsichtlich der Verifizierung des tatsächlichen

[82] BGH, Urteil vom 15.05.2018 - VI ZR 233/17.

Ausmaßes der Ordnungswidrigkeit als auch zur gerichtsverwertbaren Beweiserhebung, eine Durchsuchung und Sicherstellung von Speichermedien geboten schien. Da eine solche Maßnahme einen erheblichen Grundrechtseingriff für den Betroffenen darstellt, unterliegt sie dem Richtervorbehalt und ist daher bei Gericht zu beantragen. Auf unseren Antrag auf Erlass eines Durchsuchungs- und Beschlagnahmebeschlusses wurde durch das zuständige Amtsgericht die Durchsuchung der Wohnung, der Garage und des Kraftfahrzeugs des Betroffenen sowie die Beschlagnahme der dort aufgefundenen installierten Videokameras, sonstigen Aufzeichnungs- und Verarbeitungsgeräten sowie Speichermedien nach § 46 Abs. 1 OWiG i.V.m. §§ 94, 98, 102 und 105 StPO angeordnet.

Aufgrund der Regelung von § 46 Abs. 2 OWiG i.V.m. § 161 Abs. 1 Satz 1 und 2 StPO ist die Verfolgungsbehörde befugt, zum Zweck der Sachverhaltsaufklärung Ermittlungen selbst durchzuführen oder durch die Behörden oder Beamten des Polizeidienstes durchführen zu lassen. Die Behörden und Beamten des Polizeidienstes sind verpflichtet, einem entsprechenden Ersuchen der Verwaltungsbehörde auf Durchführung der Ermittlungsmaßnahme zu genügen.[83]

Gerade mit Blick auf eine Maßnahme mit einer sehr hohen Eingriffsintensität, wie der Durchsuchung einer Wohnung, bei deren Durchführung möglicherweise weitere, unmittelbare Maßnahmen erforderlich werden können, bedarf es besonders geschulter und mit hoheitlichen Befugnissen ausgestatteter Beamter. Nicht zuletzt hängt auch der Ermittlungserfolg bei der Durchführung von Durchsuchungen maßgeblich von der umfangreichen kriminalistischen Erfahrung polizeilicher Mitarbeiter ab. Wir haben daher zur Aufklärung des Sachverhalts, dem Beschluss des Amtsgerichts entsprechend, das Landespolizeipräsidium im Rahmen der Ermittlungshilfe gebeten, die

[83] *Vgl. Bäcker*, in: Lisken/Denninger PolR-HdB, D. Polizeiaufgaben und Regelungsmuster des polizeilichen Eingriffsrechts, Rn. 34, beck-online.

Durchsuchung und ggf. Beschlagnahme im Beisein zweier Bediensteter unserer Dienststelle durchzuführen.

Im Ergebnis konnte im konkreten Fall hierdurch weiteres Beweismaterial sichergestellt werden, das nicht nur die permanente Überwachung des öffentlichen Verkehrsraumes durch den Betroffenen belegte, sondern auch die auf Dauer angelegte Speicherung der erhobenen Videosequenzen auf externen Speichermedien und den damit verbunden erheblichen Eingriff in die Persönlichkeitsrechte der Verkehrsteilnehmer ohne deren Wissen.

Nach Auswertung und Analyse des umfangreichen Beweismaterials konnte der Betroffene zu den ihm zur Last gelegten Datenschutzverstößen angehört und das Bußgeldverfahren fortgeführt werden.

# Anlagenverzeichnis

AsylG – Asylgesetz vom 2. September 2008 (BGBl. I S. 1798), zuletzt geändert durch Artikel 1 des Gesetzes vom 21. Dezember 2022 (BGBl. I S. 2817).

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

BGB – Bürgerliches Gesetzbuch neugefasst durch Bek. v. 2.1.2002 I 42, 2909; 2003, 738; zuletzt geändert durch Art. 4 G v. 25.10.2023 I Nr. 294

BKAG – Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz) vom 1. Juni 2017 (BGBl. I S. 1354; 2019 I S. 400), zuletzt geändert durch Artikel 3 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2632; 2023 I Nr. 60).

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

Europol-VO – Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (ABl. L 135 vom 24.05.2016, S. 53 - 114).

EuropolG – Gesetz zur Anwendung der Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates: Vom 16. Dezember 1997 (BGBl. 1997 II S. 2150), zuletzt geändert durch Artikel 8 des Gesetzes vom 25. Juni 2021 (BGBl. I S. 2083).

PsychKHG – Psychisch-Kranken-Hilfe-Gesetz vom 16. März 2022

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

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

SJG – Gesetz Nr. 1407 zur Jagd und zum Wildtiermanagement (Saarländisches Jagdgesetz) vom 27. Mai 1998 (Amtsbl. S. 638), zuletzt geändert durch Artikel 164 des Gesetzes vom 8. Dezember 2021 (Amtsbl. I S. 2629).

SKHG – Saarländisches Krankenhausgesetz vom 13. Juli 2005 in der Fassung der Bekanntmachung vom 6. November 2015; letzte berücksichtigte Änderung: mehrfach geändert, neuer Fünfter Abschnitt und §§ 5a, 15a, 15b eingefügt, Fünfter bis Neunter Abschnitt (alt) werden Sechter bis Zehnter Abschnitt (neu) durch Gesetz vom 16. März 2022 (Amtsbl. I S. 629)

SKRG – Saarländisches Krebsregistergesetz vom 11. Februar 2015; letzte berücksichtigte Änderung: mehrfach geändert, §§ 7a, 13c und 13d neu eingefügt durch Gesetz vom 14. April 2021 (Amtsbl. I S. 1484)

SPolDVG – Saarländisches Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei vom 6. Oktober 2020 (Amtsbl. I S. 1133), zuletzt geändert durch Artikel 2 des Gesetzes vom 8. Dezember 2021 (Amtsbl. I S. 52).

StGB – Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 1 des Gesetzes vom 26. Juli 2023 (BGBl. 2023 I Nr. 203).

StPO – Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, ber. S. 1319), zuletzt geändert durch Art. 2 G zur Überarbeitung des Sanktionenrechts – Ersatzfreiheitsstrafe, Strafzumessung, Auflagen und Weisungen sowie Unterbringung in einer Entziehungsanstalt vom 26.7.2023 (BGBl. 2023 I Nr. 203)

OWiG – Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 1. Februar vom 19. Februar 1987 (BGBl. I S. 602), zuletzt geändert durch Art. 5 Zweites Gesetz zur Änd. schifffahrtsrechtlicher Vorschriften vom 14.3.2023 (BGBl. 2023 I Nr.73)

UWG – Gesetz gegen den unlauteren Wettbewerb vom 3. Juli 2004 (BGBl. I S. 1414), zuletzt geändert durch Gesetz vom 8. Oktober 2023 (BGBl. I S. 272)

WaffG – Waffengesetz vom 11. Oktober 2002 (BGBl. I S. 3970, 4592), 2003 I 1957), zuletzt geändert durch Artikel 228 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328).