Die Landesbeauftragte für
Datenschutz und Informationsfreiheit

31. Tätigkeitsbericht Datenschutz

UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

2022

31. Tätigkeitsbericht

der Landesbeauftragten für Datenschutz und Informationsfreiheit

Berichtszeitraum: 2022

Dem Landtag und der Landesregierung
vorgelegt am 21. Juni 2023
(Landtagsdrucksache 17/402)

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 europäische Datenschutzrecht gewinnt im fünften Jahr nach Geltungseintritt weiter an Profilschärfe. Die stetige Konturierung des materiellen Rechts durch den Europäischen Gerichtshof und die Intensivierung der Zusammenarbeit europäischer und deutscher Aufsichtsbehörden effektiveren den Vollzug datenschutzrechtlicher Vorgaben.

Die Kooperation auf innerdeutscher und europäischer Ebene ist dabei unabdingbare Voraussetzung um den wachsenden Herausforderungen für die Aufsichtstätigkeit begegnen zu können; angesichts transnationaler Geschäftsmodelle, datenintensiver Schlüsseltechnologien und der Dynamik des Unionsgesetzgebers bei der Schaffung weiterer regulatorischer Vorgaben können Antworten auf die drängenden datenschutzrechtlichen Fragen von den Aufsichtsbehörden nur gemeinsam gefunden werden. Allein dies entspricht auch dem Wesenskern des Datenschutzrechts als genuin europäischem und seit Geltungseintritt der DSGVO vollständig harmonisiertem Recht, das nationale Sonderwege ausschließlich in engen Grenzen zulässt.

Der im Unionsrecht angelegte Auftrag zur Zusammenarbeit der europäischen und auch nationalen Aufsichtsbehörden kollidiert dabei allerdings mit der haushälterischen Realität eines Haushaltsnotlagelandes. Soweit ich im Vorwort zum letztjährigen Tätigkeitsbericht noch die Hoffnung geäußert habe, dass die Wahrnehmung der Kernaufgaben meiner Behörde unter Berücksichtigung sich verändernder Rahmenbedingungen durch eine angemessene Ausstattung mit personellen Ressourcen gewährleistet werden kann, hat sich diese zunächst zerschlagen. Unter fiskalischen Gesichtspunkten kann die Entscheidung des Haushaltsgesetzgebers, für meine Behörde keine weiteren Stellen vorzusehen, zwar durchaus als vertretbar erachtet

werden, allerdings ergeben sich daraus auch nachteilige Auswirkungen hinsichtlich des aufsichtsbehördlichen Aufgabenvollzugs und damit letztlich für den Schutz der Daten der saarländischen Bürgerinnen und Bürger. Um meinem gesetzlichen Schutzauftrag und der Rolle meiner Behörde bei der Zusammenarbeit der Aufsichtsbehörden nachhaltig gerecht werden zu können, werde ich mich auch weiterhin für einen angemessenen Stellenzuwachs einsetzen.

Der nun vorgelegte 31. Tätigkeitsbericht Datenschutz für den Berichtszeitraum 2022 ist der erste Bericht nach meiner Wiederwahl als saarländische Landesbeauftragte für Datenschutz und Informationsfreiheit im Februar 2022. An dieser Stelle möchte ich mich bei den Abgeordneten des saarländischen Landtags für das in mich gesetzte Vertrauen bedanken. Auch meine zweite Amtszeit soll vorrangig von dem Leitgedanken einer kritischen, aber vor allem lösungsorientierten Zusammenarbeit mit Entscheidungsträgern in Politik, Verwaltung und Wirtschaft geprägt sein.

Schließlich gilt mein Dank insbesondere den Mitarbeiterinnen und Mitarbeitern meiner Behörde für ihren Einsatz.

Saarbrücken, im Juni 2023

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. Entsprechend dieser Vereinbarung werden im Folgenden die wesentlichen Kategorien von Verfahren, mit denen sich das Unabhängige Datenschutzzentrum Saarland (UDZ) im Berichtszeitraum zu befassen hatte, aufgeführt, wobei landesspezifische Aufgaben und Tätigkeiten nicht erfasst werden.

1.1 Beschwerden

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

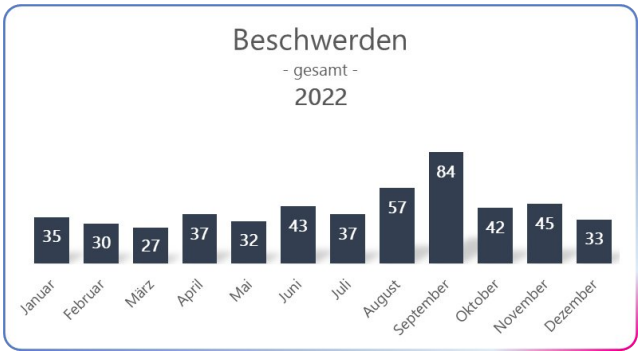

Abb. 1: Beschwerden (gesamt) 2022

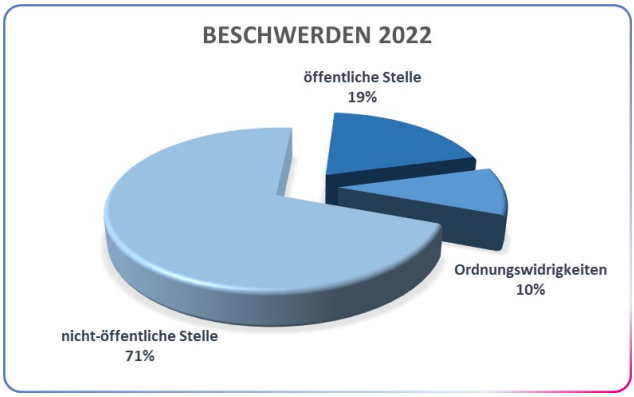

Abb. 2: Beschwerden (Aufteilung) 2022

1.2 Beratungen

Hier wird eine Übersicht über die Anzahl von schriftlichen Beratungen gegeben. Dies umfasst Beratungen von Verantwortlichen, betroffenen Personen und der Landesregierung. Ausschließlich (fern-)mündliche Beratungen werden statistisch nicht erfasst, obwohl diese einen sehr hohen

Anteil der an unsere Behörde gerichteten Anfragen darstellen und einen hohen zeitlichen Aufwand erfordern.

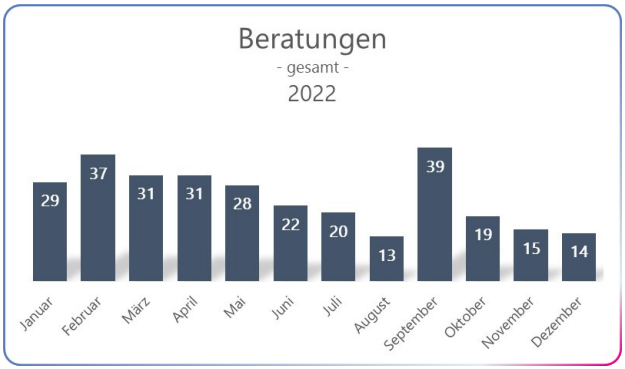

Abb. 3: Beratungen (gesamt) 2022

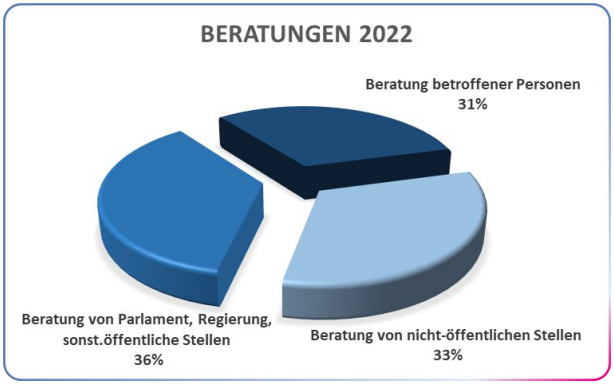

Abb. 4 Beratungen (Aufteilung) 2022

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.

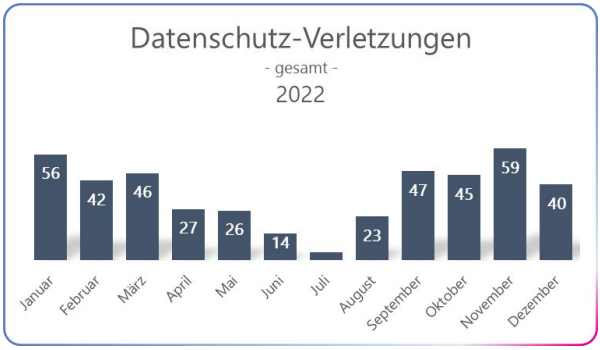

Abb. 5: Datenschutzverletzungen 2022

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.

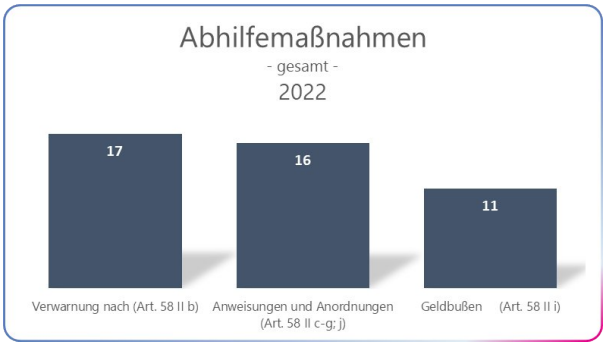

Abb. 5: Abhilfemaßnahmen (gesamt) 2022

1.5 Europäische Verfahren

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

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

Ein Teilaspekt dieser Verfahren besteht darin, dass nationale Datenschutzaufsichtsbehörden die Möglichkeit erhalten, auf

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

	Bundesrepublik Deutschland	Saarland
Verfahren mit Betroffenheit Art. 56 Abs. 1	362	3
Verfahren mit Federführung Art. 56 Abs. 2	33	0
Verfahren gem. Kapitel VII DSGVO	2060	858

Abb. 6: Europäische Verfahren (gesamt) 2022

Zu diesem Zweck hatte auch das UDZ im Jahr 2022 in insgesamt 362 Fällen zu beurteilen, inwieweit es als „betroffene Aufsichtsbehörde“ im Sinne des Art. 4 Nr. 22 DSGVO gem. Art. 56 Abs. 1 DSGVO an diesen grenzüberschreitenden Verfahren zu beteiligen war, weil bspw. eine Niederlassung der verarbeitenden Stelle im Saarland existiert oder weil auch saarländische Bürger von einer konkreten Verarbeitung erheblich betroffen sein könnten.
In 3 Fällen wurde diese Betroffenheit für das UDZ bejaht.
Eine federführende Zuständigkeit i. S. v. Art. 56 Abs. 2 DSGVO lag im Berichtsjahr nicht beim UDZ.
Im gleichen Zeitraum hatte das UDZ zudem in insgesamt 2060 Fällen zu beurteilen, inwiefern eine Beteiligung an Verfahren gem. Kapitel VII (Zusammenarbeit und Kohärenz) vorlagen. In insgesamt 858 Fällen traf dies zu. Hierzu zählen u.a. an das

UDZ i. S. v. Art. 61 DSGVO gerichtete freiwillige Amtshilfeersuchen europäischer Aufsichtsbehörden, im Rahmen derer ein allgemeiner Austausch über diverse datenschutzrechtliche Fragestellungen erfolgte.

1.6 Förmliche Begleitung von Rechtsetzungsvorhaben

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

Im Berichtzeitraum wurde das Unabhängige Datenschutzzentrum Saarland (UDZ) hiernach in 6 Rechtsetzungsvorhaben verfahrensbegleitend tätig.

1.7 Gerichts- und Bußgeldverfahren

In 2022 führte das Unabhängige Datenschutzzentrum insgesamt 42 Gerichts- und Bußgeldverfahren.

1.8 Presseanfragen

In 2022 wurden insgesamt 49 Presseanfragen an hiesige Dienststelle gerichtet.

II.

Erwartungen an die Landesregierung

2 Erwartungen an die Landesregierung

Neben der Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften bei den öffentlichen und nicht-öffentlichen Stellen im Saarland gehört es auch zu den Aufgaben der Landesbeauftragten für Datenschutz und Informationsfreiheit, den Landtag, die Landesregierung und sonstige öffentlichen Stellen in Fragen des Datenschutzes zu beraten und Empfehlungen zur Verbesserung des Datenschutzes zu geben. Wir haben daher den Regierungswechsel im Berichtsjahr zum Anlass genommen, um gegenüber dem neu gewählten Landtag und der Landesregierung auf datenschutzrechtliche Handlungsbedarfe hinzuweisen und für den Datenschutz als Treiber und Faktor einer erfolgreichen, weil nachhaltigen Digitalisierung zu werben.

Die Digitalisierung der Wirtschafts- und Verwaltungsprozesse, und damit einhergehend auch die Nutzung personenbezogener Daten, wird bei der Bewältigung der Herausforderungen, die mit der Transformation des Saarlandes von einem klassischen Automobil- und Stahlstandort zu einem Zentrum für innovative Technologien, für zukünftige nachhaltige Mobilität und „grünen“ Stahl eine wichtige Rolle einnehmen und zugleich den auch durch den demographischen Wandel bedingten Mangel an qualifizierten Arbeitskräften in Wirtschaft und Verwaltung dämpfen können.

Nachhaltige Digitalisierung bedeutet, Digitalisierung so zu gestalten, dass Wirtschaft und Gesellschaft langfristig von ihr profitieren (IW-Policy-Paper 3/2022). Datenschutz trägt zu einer nachhaltigen Digitalisierung bei, indem er aufzeigt, wie wichtig es ist, auch im digitalen Bereich verantwortlich zu handeln und Risiken für die Rechte und Freiheiten der Betroffenen zu minimieren. Zugleich stärkt Datenschutz das Vertrauen der Nutzerinnen und Nutzer in die entsprechenden Verfahren und Prozesse, sorgt somit für Akzeptanz in die digitale Transformation und maximiert so letztlich die Chancen der Digitalisierung.

Übertragen auf das Saarland erfordert dies zunächst eine Evaluierung und Anpassung der rechtlichen Rahmenbedingungen. Vier Jahre Aufsichtspraxis unter der Datenschutz-Grundverordnung (DSGVO) und dem neu gefassten Saarländischen Datenschutzgesetz (SDSG) zeigen, dass der regulatorische Rahmen des SDSG einer Nachschärfung und Präzisierung bedarf. Insbesondere fordern wir die datenschutzrechtliche Zertifizierung zu einem Standard bei der Einführung neuer IT-Verfahren in der öffentlichen Verwaltung zu machen und hierfür auch die Überlegungen zur Schaffung einer saarländischen Zertifizierungsstelle anzustellen.

Mit Blick auf die zunehmende Abhängigkeit von externen, privaten IT-Anbietern haben wir eine Diversifizierung der in der öffentlichen Verwaltung zum Einsatz kommenden Hard- und Software angemahnt. Der konsequente Einsatz von quelloffener Software und offenen Standards sind nach hiesiger Auffassung tragende Säulen einer solchen Diversifizierungsstrategie.

Neben der im Wahlprogramm der neuen Landesregierung angekündigten Neuordnung des Saarländischen Polizeigesetzes und des Saarländischen Gesetzes zur Verarbeitung personenbezogener Daten durch die Polizei, die auch wir für erforderlich halten und daher ausdrücklich unterstützen, sehen wir auch im Bildungsbereich Handlungsbedarf bei der datenschutzfreundlichen Umsetzung der dortigen Digitalisierungsanstrengungen. Insbesondere sind wir der Auffassung, dass der Anpassung aller schulrechtlich relevanten Vorschriften an die DSGVO eine besondere Priorität einzuräumen ist, um auch die geplanten Digitalisierungsvorhaben im Bildungsbereich rechtssicher umsetzen zu können.

Im Bereich der Informationsfreiheit hat der Landtag mit der Einführung eines Lobbyregisters schon einen wichtigen Beitrag zur Schaffung von Transparenz im politischen

Entscheidungsprozess geleistet. Der logische nächste Schritt muss nun darin bestehen, auch der Zivilgesellschaft die Informationsgrundlagen zur Verfügung zu stellen, um staatliche Entscheidungen nachvollziehbar zu machen. Die in der öffentlichen Verwaltung vorhandenen Daten ohne Personenbezug können zudem eine wichtige Ressource für Wissenschaft, Forschung und Wirtschaft sein. Dementsprechend fordern wir die Weiterentwicklung des aus dem Jahre 2006 stammenden Saarländischen Informationsfreiheitsgesetzes zu einem Transparenzgesetz und die Schaffung eines Transparenzregisters nach dem Vorbild anderer Bundesländer.

Das vollständige Dokument mit detaillierten Ausführungen zu unseren Erwartungen an den neuen Landtag und die neue Landesregierung im Saarland, das wir im April 2022 an die Landtagsfraktionen und die einzelnen Ministerien versandt haben, ist auf unserer Webseite unter https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/datenschutz/stellungnahmen/2204-Erwartungen-an-LT-und-LR.pdf abrufbar.

III.

Ausgewählte Prüfungen

3 Ausgewählte Prüfungen

3.1 Prüfung der Videoüberwachungsanlage am Standort Johanneskirche

Der Einsatz von Videoüberwachungstechnik ist immer wieder Anlass für eine Befassung der Aufsichtsbehörden. Zwar betreffen die meisten Bürgeranfragen privat betriebene Kameras, allerdings sind in bestimmten Situationen auch öffentliche Stellen dazu befugt, optisch-elektronische Maßnahmen zu diversen Zwecken einzusetzen.[1] Hierzu gehört auch die saarländische Vollzugspolizei.

Bereits vor vier Jahren[2] berichteten wir in diesem Zusammenhang von einem Vorhaben, auf dem Vorplatz des Saarbrücker Hauptbahnhofs sowie im näheren Umfeld der Johanneskirche in Saarbrücken jeweils stationäre Videoüberwachungsanlagen zu installieren. Ausgangspunkt des Projekts war ein konkreter Auftrag des damaligen Ministeriums für Inneres und Sport an die saarländische Landespolizei (2016). In den Folgejahren wurden wir hinsichtlich des Gesamtvorhabens regelmäßig beteiligt. Der symbolische Spatenstich erfolgte im August 2019 – die offizielle Inbetriebnahme fand ab Januar 2020 in mehreren Ausbaustufen statt.

3.1.1 Ablauf der Prüfung

Da sich die bisherige Beteiligung unserer Behörde auf die Planungs- und Umsetzungsphase beschränkt hatte, leiteten wir im Herbst des Jahres 2021 eine Prüfung der Videoüberwachungsanlage im Wirkbetrieb ein. Weiteren

[1] Leitfaden für saarländische öffentliche Stellen – abrufbar unter: https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/themen/Leitfaden_Videoueberwachung_durch_oeffentliche_Stellen_Stand_2020-08-10.pdf.

[2] Vgl. 27. Tätigkeitsbericht, 2017/2018, Kapitel 3.1, S. 40 – 41, elektronisch abrufbar unter: https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/berichte/tb27_1718.pdf

Anlass boten verwaltungsgerichtliche Entscheidungen aus Nordrhein-Westfalen, die sich mit dem Einsatz von Überwachungstechnik im öffentlichen Raum durch die Vollzugspolizei beschäftigten[3], sowie die Änderung des rechtlichen Rahmens durch das seit Ende des Jahres 2020 geltende Saarländische Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG).

Für die diesmalige Kontrolle wählten wir zwei Schwerpunkte: Zum einen überprüften wir die technische Ausgestaltung des Gesamtsystems. Zum anderen nahmen wir die konkreten Begebenheiten am Standort Johanneskirche in Augenschein.

Unsere Prüfankündigung Anfang August 2021 wurde seitens des Landespolizeipräsidiums (LPP) mit einer Einladung zur Vor-Ort-Besichtigung der Kamera- und Technikstandorte beantwortet. Bei dem vereinbarten Termin konnten wir die Örtlichkeiten umfassend begehen und die eingesetzten Netzwerkkomponenten begutachten. Um weitere Detailfragen zu klären, fand einen Monat später ein zweites Treffen in den Räumlichkeiten des LPP statt, wo auch Einblicke in die Führungsleitzentrale (FLZ) und auf die dortigen Videobeobachter-Arbeitsplätze ermöglicht wurden.

Besonders hervorzuheben ist, dass bei der Durchführung der Prüftermine die von uns im Vorfeld geäußerten Wünschen für deren Ablauf in Gänze erfüllt wurden. Hierdurch konnte eine sehr zielorientierte sowie ergebnisfördernde Arbeitsatmosphäre geschaffen werden.

Auch im Nachgang der Arbeitstreffen standen wir weiterhin in engem Austausch mit dem LPP. Die finale Klärung aller Detailfragen nahm dabei einen Großteil der ersten Jahreshälfte 2022 in Anspruch, sodass das Prüfverfahren erst im Juni 2022 abgeschlossen werden konnte.

---

[3] Siehe hierzu die verwaltungsgerichtlichen Entscheidungen des VG Köln und des OVG Nordrhein-Westfalen: 20 L 2340/19, 20 L 2343/20, 20 L 2344/20, 5 B 137/21 und 5 B 1289/21, juris.

3.1.2 Feststellungen im Rahmen der Prüfung

Zunächst befassten wir uns mit der technischen Infrastruktur, indem wir die vorhandenen Sicherheitsstandards und die im Einsatz befindlichen Netzwerkkomponenten anhand verschiedener Angriffsszenarien untersuchten. Schwerpunkte lagen hierbei auf Fragen des Datentransports (von der Kamerahardware zum Videoserver), der Verschlüsselung und der Gewährleistung der Datenintegrität.

Ebenfalls betrachteten wir die Zugriffsmöglichkeiten auf das Gesamtsystem und überprüften hier das bestehende Rechte-Rollen-Konzept (das sich an den „Common Criteria“ für Videoüberwachungssoftware des Bundesamtes für Sicherheit in der Informationstechnik orientiert), das Vorgehen bei Systemwartungen sowie die bestehenden technischen Sicherheitsschranken, um das Dazwischentreten Dritter zu erkennen und zu verhindern.

Die Einsichtnahme in die vorhandenen Protokolldaten zeigte zudem auf, dass eine umfangreiche, übersichtliche und nach bestimmten Kategorien auswertbare Dokumentation stattfindet, die sowohl die Handhabung des Videostreams als auch die nachträgliche Verwaltung der Bildaufzeichnungen umfasst. So kann bspw. für jede Aufnahmeeinheit isoliert nachvollzogen werden, wann und wie sie im Vollbild betrachtet wurde und ggf. ob eine konkrete Steuerung / Ausrichtung der Kamera erfolgte. Jegliches Auslesen (Exportieren) von Bilddaten wird ebenfalls unter Angabe des handelnden Benutzers protokolliert. Das Vorgehen der Polizei kann in diesem Zusammenhang deswegen als mustergültig bezeichnet werden.

Als Maßnahme, die einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt, bedarf es für den Einsatz von Videoüberwachungstechnik einer entsprechenden Ermächtigungsgrundlage. Das LPP stützt sich hierbei auf § 32 Abs. 2 Satz 1 Nr. 1 SPolDVG, der Bildaufzeichnungen an öffentlich zugänglichen Kriminalitätsschwerpunkten erlaubt. Da sich tatsächliche

Begebenheiten stetig ändern können, handelt es sich bei der Klassifizierung als Kriminalitäts-Hotspot lediglich um eine Momentaufnahme. Korrekterweise führt das LPP deswegen (trotz fehlender gesetzlicher Normierung) eine halbjährliche Evaluierung der Dauermaßnahme „Videoüberwachung“ durch. Diese wird u. a. auf das Brennpunktkonzept Saarbrücken gestützt. Im ersten Halbjahr 2021 ergab sich für den Kontrollbereich Johanneskirche eine wesentlich erhöhte Kriminalitätsbelastung im Vergleich zum übrigen Innenstadtbereich, weswegen die Annahme eines „Schwerpunkts“ im Sinne der Norm weiterhin gegeben ist.

Ebenfalls Teil der Kontrolle war die konkrete Ausgestaltung der Videoüberwachungsanlage am Standort Johanneskirche. Hierzu gehörte insbesondere die Frage, ob tatsächlich nur solche Areale erfasst werden, die die Voraussetzungen des § 32 Abs. 2 Satz 1 Nr. 1 SPolDVG erfüllen. Bereiche, die wegen ihrer Grundrechtsrelevanz als besonders schützenswert zu klassifizieren sind, müssen entweder durch eine entsprechende Ausrichtung der Kameras gar nicht erst erfasst oder aber durch sonstige technische Vorkehrungen hinreichend unkenntlich gemacht werden (z. B. durch sog. Privatzonenmaskierung).

Unsere Überprüfung ergab, dass eine solche Maskierung seitens der Polizei bereits weitgehend eingesetzt wird. In vielen Fällen reichte jedoch bereits die gewählte spitze Sichtachse der Kamera aus, um einen Einblick in grundrechtlich geschützte Räumlichkeiten zu verhindern. Fenster und Glasfronten werden größtenteils durch technische Graufelder verdeckt; nur vereinzelt hielten wir eine Ausweitung auf weitere Bereiche für erforderlich. Der Eingangsbereich der Johanneskirche stellte im Hinblick auf die ebenfalls tangierte Religionsfreiheit einen Sonderfall dar. Zwar werden bereits jetzt Einblicke in das Innere der Kirche effektiv verhindert. Ein Beobachten beim Betreten und Verlassen der Glaubensstätte ist derzeit aber möglich. Um die Schwere des an sich zulässigen Grundrechtseingriffs so

gering wie möglich zu halten, schlugen wir hier verschiedene Anpassungsmöglichkeiten vor.

Zwar verläuft durch den Erfassbereich auch die viel befahrene Stephansstraße, sodass von der Kameraanlage unweigerlich auch Kfz-Kennzeichen erfasst werden. Ein automatisiertes Erkennen und Auslesen von Buchstaben- und Ziffernfolgen sowie ein darauf aufbauender Abgleich mit vorhandenen Datenbeständen wird durch die eingesetzten Kameratypen jedoch bereits auf technischer Ebene nicht unterstützt. Eine besondere Eingriffstiefe ist mit dem Erfassen dieser Daten nach hiesiger Ansicht deswegen grundsätzlich nicht verbunden, sodass die allgemeine Videoüberwachungsnorm hier ausreichend erscheint. Eine Verpixelung von Kfz-Kennzeichen, wie es das VG Köln in ähnlicher Sache zunächst verlangte[4], sahen wir insbesondere deswegen als nicht erforderlich an.

Letztlich verlangen datenschutzrechtliche Grundsätze eine ausreichende Information von Betroffenen. Diesem Umstand trägt auch § 32 Abs. 5 SPolDVG Rechnung, indem er Vorgaben für die Ausgestaltung von Transparenzräumen normiert und insbesondere eine ausreichende Hinweisbeschilderung verlangt. Zwar befinden sich bereits jetzt entsprechende Hinweistafeln rund um die S-Bahn-Haltestelle Johanneskirche. Diese reichen unserer Ansicht jedoch nicht aus, um Passanten eine eindeutige Identifikation des videoüberwachten Bereichs zu ermöglichen. Wir schlugen deswegen die Anbringung weiterer Informationsschilder vor.

Jede der Hinweisplaketten enthält zudem einen QR-Code, der auf die Website „Polizeilicher Videoschutz“ der saarländischen Polizei[5] verweist. Die dort ergänzend aufgeführten Informationen zur Videoüberwachungsanlage waren jedoch

[4] VG Köln, Beschluss vom 28. Juli 2021 – 20 L 2343/20, BeckRS 2021, 32440.

[5] Elektronisch abrufbar unter: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/videoueberwachung/videoueberwachung_node.html

teilweise veraltet, sodass wir um entsprechende Aktualisierung und ggf. Ergänzung baten.

3.1.3 Ergebnis

Eine erste Rückmeldung des LPP ging uns bereits kurz nach Übersendung des Prüfberichts zu. Eine umfassende Auswertung der aufgeführten Feststellungen wurde uns darin durch die für die Videoüberwachung verantwortliche Stelle angekündigt. An diese sei unser Bericht weitergeleitet worden.

Eine ausführliche Stellungnahme des LPP steht zum Zeitpunkt des Redaktionsschlusses jedoch noch aus.

3.2 Kontrolle des Schengener Informationssystems (SIS II)

In einem weiteren Prüfverfahren beschäftigten wir uns mit dem „Schengener Informationssystem der zweiten Generation (SIS II)“[6]. Seit Abbau der europäischen Binnengrenzen und der damit weitgehend entfallenen Grenzkontrollen im Schengen-Raum dient diese Datenbank den Sicherheitsbehörden der Mitgliedstaaten als Mittel zur schengenweiten Personen- und Sachfahndung. In den das SIS II statuierenden Rechtsakten der Europäischen Union[7] sind turnusmäßige Prüfverpflichtungen normiert, denen sich die zuständigen Aufsichtsbehörden in den Jahren 2021 / 2022 annahmen.

3.2.1 Prüfungsagenda und Verfahrensgang

Schwerpunktmäßig konzentrierte sich die diesmalige Prüfung auf Personenausschreibungen nach Art. 36 des SIS-II-Beschlusses. Dieser gestattet die Eintragung von Personen im SIS II zur „polizeilichen Beobachtung“ bzw. „verdeckten

[6] Mehr Informationen zum Schengener Informationssystem auf der Website des Europäischen Datenschutzbeauftragten, elektronisch abrufbar unter: https://edps.europa.eu/data-protection/european-it-systems/schengen-information-system_de

[7] Beschluss 2007/533/JI (SIS-II-Beschluss), Verordnung (EG) 1987/2006 und Verordnung (EG) 1986/2006, Stand November 2022.

Kontrolle“. Hierunter ist ein Vorgehen zu verstehen, bei dem im Falle des Antreffens einer gesuchten Person im Rahmen eines anderen Anlasses (z. B. bei einer allgemeinen Verkehrskontrolle) unauffällig Informationen erhoben werden, um diese Erkenntnisse sodann der ausschreibenden Sicherheitsbehörde weiterzuleiten. Die Wahl des Prüfungsschwerpunkts fiel auf Art. 36 SIS-II-Beschluss, da in diesem Bereich relativ hohe Ausschreibungszahlen zu verzeichnen waren.[8]

Die Prüfung orientierte sich an einem Fragenkatalog (Questionnaire), den ursprünglich die auf europäischer Ebene tätige SIS II Supervision Coordination Group entworfen hatte. Da SIS-II-Ausschreibungen in Deutschland zentral über das polizeiliche Informationssystem (INPOL) verwaltet werden, wandten wir uns mit unserem Anliegen zunächst an das Saarländische Landespolizeipräsidium (LPP). Von dort sollte uns zu einem bestimmten Stichtag der Bestand an solchen Ausschreibungsfällen mitgeteilt werden, die auf Ersuchen saarländischer Stellen in die Datenbank eingetragen wurden.

Daraufhin übersandte uns das LPP die bei der dortigen Eingabestelle vorhandenen Fallakten. Eine umfassende Überprüfung der Einzelfälle erschien jedoch aufgrund der in den Fallakten nur begrenzt enthaltenen Informationen zum zugrundeliegenden Sachverhalt nicht möglich. Deshalb fanden zusätzlich Vor-Ort-Termine beim LPP und dem in mehreren Fällen als Führungsaufsichtsstelle beteiligten Kompetenzzentrum der Justiz für ambulante Resozialisierung und Opferhilfe (KARO) statt. Durch Einsicht in die Verfahrensakten und der in INPOL abrufbaren Datensätze sowie durch persönliche Gespräche mit den zuständigen Mitarbeitern konnten dabei alle offenen Fragen geklärt werden.

[8] Statistik der Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen (eu-LISA), elektronisch abrufbar unter: https://www.eulisa.europa.eu/Publications/Reports/2017%20SIS%20II%20Statistics.pdf

3.2.2 Feststellungen im Rahmen der Prüfung

Unsere Prüfung befasste sich zunächst mit den rechtlichen Voraussetzungen einer Ausschreibung zur polizeilichen Beobachtung. Eine solche kann entweder rein national in INPOL oder schengenweit über das SIS II erfolgen. Auf nationaler Ebene finden sich die entsprechenden Ermächtigungsgrundlagen entweder für den repressiven Bereich der Strafverfolgung in den §§ 163e und 463a der Strafprozessordnung (StPO) oder für den präventiven Bereich der Gefahrenabwehr in § 40 des Saarländischen Gesetzes über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG). Eine Ausschreibung auf Ebene aller Schengenstaaten im SIS II setzt zusätzlich das Vorliegen einer „Schengenrelevanz“ voraus, die anhand von Art. 36 Abs. 2 SIS-II-Beschluss zu bewerten ist. Unsere Kontrolle der Einzelfälle kam hier zu dem Ergebnis, dass gegen keine der im Saarland initiierten Ausschreibungen datenschutzrechtliche Bedenken bestanden – die erfolgten Eintragungen basierten alle auf hinreichend legitimierenden Sachverhalten.

Auch das Vorgehen bei Eingabe und Abruf von SIS-II-Daten war in technisch-organisatorischer Hinsicht nicht zu beanstanden. Zudem entsprach der eingespeicherte Datenkranz in den überprüften Einzelfällen stets den Anforderungen, die Art. 20 ff. SIS-II-Beschluss aufstellt.

Die Überprüfung der Speicherfristen wies dagegen gemischte Resultate auf. Bei einer europarechtlich angeordneten (verlängerbaren) Speicherfrist von einem Jahr (Art. 44 SIS-II-Beschluss) sind Verlängerungsanordnungen sowohl rechtzeitig als auch von der hierzu befugten Organisationseinheit vorzunehmen. Da in den überprüften Einzelfällen beide Aspekte nicht immer hinreichend beachtet wurden, rieten wir zu einer Evaluierung der derzeitigen Verfahrensabläufe. Des Weiteren ist bei bestimmten Ausschreibungen in turnusmäßigen Abständen bereits vor Ablauf der Höchstspeicherfrist zu überprüfen, ob das Beibehalten der Personenausschreibung

auch tatsächlich erforderlich ist. Auch hier stellten wir teilweise Mängel fest und verlangten, dass künftig auf eine fristgemäße Initiierung und detaillierte Dokumentation solcher Überprüfungen geachtet wird.

Die Anordnungen der Ausschreibungen selbst haben neben einer behördenleitenden auch eine dokumentierende Funktion. Bezüglich letzterer stellten wir in einzelnen Fallakten Defizite fest. Wir wiesen die Verantwortlichen auf diese hin und unterbreiteten Vorschläge, wie der aus unserer Sicht erforderliche Detailgrad bei der Dokumentation erreicht werden kann. Insbesondere muss unseres Erachtens in Ausschreibungsfällen entweder in der Anordnung selbst oder aber zumindest in einem in Bezug genommenen und ggf. heranziehbaren Vermerk oder Gutachten eine Begründung zur ersuchten Eintragung in INPOL / SIS II enthalten sein.

Gleichzeitig befassten wir uns mit der Aktenführung als solche. Diese dient grundsätzlich der Transparenz staatlichen Handelns und muss eine Nachvollziehbarkeit und Überprüfbarkeit der jeweiligen Einzelfälle ermöglichen. Bei der Ausschreibung zur polizeilichen Beobachtung ergibt sich aufgrund der systemimmanenten Beteiligung mehrerer Akteure (Staatsanwaltschaft, Gerichte, LPP, KARO), dass Akten nicht vollständig an einer einzigen Stelle vorgehalten werden. Dies führte in der vorliegenden Prüfung zu anfänglichen Problemen bei der Zusammenstellung der erforderlichen Datengrundlage. Um dies für künftige Kontrollen zu verbessern, schlugen wir bestimmte Standardisierungen hinsichtlich des Aktenaufbaus (insbesondere bei der Eingabestelle des LPP) vor und baten um klare Verweisungen, falls sich Aktenteile oder notwendige Informationen an anderer Stelle befinden.

Zwischenzeitlich hat bereits das KARO bestätigt, unseren Prüfbericht gesichtet und ausgewertet sowie die erforderlichen. Handlungsbedarfe ermittelt und umgesetzt zu haben. Eine Stellungnahme des LPP ging bis zum Redaktionsschluss des vorliegenden Tätigkeitsberichts noch nicht bei uns ein.

3.2.3 Ausblick

Wie in vielen anderen Bereichen ebenfalls, schreitet auch auf europäischer Ebene die Modernisierung, Optimierung und Erweiterung bestehender Datenstrukturen immer weiter voran. Mit mehreren neuen EU-Verordnungen[9] wird deswegen das bisher betriebene Schengener Informationssystem mit anderen großen europäischen IT-Systemen interoperabel werden – das SIS II entwickelt sich hierdurch zum SIS 3.0. Die Aufnahme des operativen Betriebs steht zum Zeitpunkt des Redaktionsschlusses zwar weiterhin aus, soll aber perspektivisch im ersten Quartal 2023 erfolgen.

Die neuen Verordnungen sehen derweil ebenfalls turnusmäßige Prüfverpflichtungen seitens der zuständigen Aufsichtsbehörden vor. Wir werden uns also auch künftig mit der Datenverarbeitung im Schengener Informationssystem befassen und bei Durchführung weiterer Prüfungen erneut darüber berichten.

3.3 Prüfung der Datenverarbeitung in einem Hochschulinstitut

Im Berichtszeitraum haben wir aufgrund eines Hinweises eine Datenschutzprüfung in einem Institut der Universität des Saarlandes durchgeführt. Dabei wurden gleich mehrere Mängel beim technischen und organisatorischen Datenschutz festgestellt. Die größten Mängel ergaben sich dabei aus fehlenden Löschkonzepten und der unzulässigen Nutzung externer Speichermedien.

3.3.1 Fehlende Löschkonzepte

Es stellte sich zunächst heraus, dass innerhalb des Instituts zur Ablage und Bearbeitung aller Fälle eine elektronische Aktenstruktur unter Windows 7 angelegt wurde. Diese elektronische Aktenablage war bis zur erstmaligen Erstellung

[9] VO (EU) 2018/1860, VO (EU) 2018/1861 und VO (EU) 2018/1862.

im Jahr 2011 nachvollziehbar, ein entsprechendes Löschkonzept war nicht vorhanden.

Die parallel laufende schriftliche Aktenführung reicht laut Institutsleitung bis in die 1990er Jahre zurück. Auch für die Papierakten existierte kein Löschkonzept.

Um aber eine datenschutzkonforme Umsetzung des Grundsatzes der „Speicherbegrenzung“ aus Art. 5 Abs. 1 lit. e DSGVO zu gewährleisten, darf bei der Speicherung personenbezogener Daten die Identifizierung der betroffenen Personen nur so lange möglich sein, wie es für die Verarbeitungszwecke erforderlich ist. Dementsprechend ist durch den Verantwortlichen sicherzustellen, dass Fristen für die regelmäßige Überprüfung und Löschung personenbezogenen Daten festgelegt werden. Die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien sind zudem gem. Art. 30 Abs. 1 lit. f DSGVO in einem Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren.

Da sowohl die Festlegung von Löschfristen als auch eine entsprechende Löschung von Daten durch das Institut versäumt wurde, führte dies zu einer unzulässigen Speicherung personenbezogener Daten auch über den zur Aufgabenerfüllung erforderlichen Zeitraum hinaus.

Es wurde daher vereinbart, schnellstmöglich ein entsprechendes Löschkonzept im Institut zu implementieren und dieses unserer Behörde zur Prüfung vorzulegen.

3.3.2 Nutzung externer Speichermedien

Laut Aussage der Institutsleitung war es in der Vergangenheit bspw. zur Erstellung von Gutachten üblich, dienstliche Daten unverschlüsselt zunächst auf einen USB-Stick und anschließend zur weiteren Bearbeitung auf privaten Computern zu speichern. Auch wurden bei der weiteren Speicherung unter anderem private Cloud-Dienste eingesetzt, die nicht den datenschutzrechtlichen Vorgaben der DSGVO entsprachen.

Erst im Jahr 2022 sei im Rahmen der Corona-Pandemie eine Möglichkeit geschaffen worden, über eine VPN-Lösung auf dienstliche Daten von zu Hause aus über einen dienstlich zur Verfügung gestellten Laptop zugreifen zu können.

Gem. Art. 32 DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau der personenbezogenen Daten zu gewährleisten. Dies wurde in der Vergangenheit durch die unverschlüsselte Speicherung und Übermittlung dienstlicher Daten, die auch besondere Kategorien von Daten im Sinne des Art. 9 DSGVO enthalten haben, per USB-Stick und privaten Cloud-Diensten missachtet und somit gegen die Vorgaben der DSGVO verstoßen.

Es wurde vereinbart, die bestehenden Regelungen der Universität des Saarlandes zur IT-Sicherheit und zum Datenschutz im Rahmen einer Schulungsmaßnahme für alle Beschäftigten des Instituts aufzufrischen und die Beschäftigten für einen datenschutzkonformen Umgang, gerade auch mit besonderen Kategorien von Daten, zu sensibilisieren.

Fazit/ Empfehlung:

Eine automatisierte Verarbeitung personenbezogener Daten muss jederzeit den datenschutzrechtlichen Anforderungen genügen. Daher bedarf es neben einer ständigen Überprüfung der Einhaltung der gesetzlichen Vorgaben auch einer regelmäßigen Schulung der Beschäftigten.

IV.

Justiz

4 Justiz

4.1 Unzureichende Anonymisierung von veröffentlichten Gerichtsentscheidungen

Die Veröffentlichung von Gerichtsentscheidungen stellt einen wesentlichen Beitrag zur Rechtspflege und Rechtsfortbildung dar und dient zugleich der Gerichtsöffentlichkeit. Aus dem Rechtsstaatsprinzip ergibt sich die verfassungsrechtliche Pflicht, veröffentlichungswürdige Entscheidungen der Allgemeinheit zugänglich zu machen. Begrenzt wird diese Pflicht gleichwohl durch die Persönlichkeitsrechte der Verfahrensbeteiligten. Enthält eine veröffentlichte Entscheidung personenbezogene Daten, berührt sie hierdurch das allgemeine Persönlichkeitsrecht in Form des Rechts auf informationelle Selbstbestimmung.

Dem Unabhängigen Datenschutzzentrum Saarland wurde im Berichtszeitraum im Wege einer Beschwerde zur Kenntnis gebracht, dass auf einer für jedermann zugänglichen Datenbank im Internet eine unzureichend anonymisierte Entscheidung eines saarländischen Gerichts veröffentlicht wurde. In dieser Entscheidung waren das Geburtsdatum, der Ausbildungsberuf und -zeitraum sowie Angaben über die Busstrecke eines der Verfahrensbeteiligten enthalten. Zudem wurden Ortsangaben nur teilweise durch einen Platzhalter ersetzt. Der Beschwerdeführer teilte mit, dass aufgrund dieser Angaben bereits einer der Verfahrensbeteiligten durch Dritte identifiziert worden sei. Er bat um Prüfung, ob eine Veröffentlichung der Entscheidung in dieser Form datenschutzrechtlich zulässig sei.

4.1.1 Der Rechtsrahmen bei der Urteilsveröffentlichung

Die Rechtsgrundlage für die Veröffentlichung von Gerichtsentscheidungen durch saarländische Gerichte findet sich in Art. 6 Abs. 1 lit. e, Abs. 3 lit. b DSGVO i. V. m § 4 Abs. 1 SDSG i. V. m dem Rechtsstaats- und Demokratieprinzip (Art. 20

Abs. 1, Art. 28 Abs. 1 GG). Die datenschutzrechtlichen Vorgaben sehen aber gleichwohl vor, dass nur solche personenbezogenen Daten in die Veröffentlichung Eingang finden dürfen, die für die Entscheidungsfindung und das Verständnis der Entscheidung erforderlich sind. Sonstige personenbezogene Daten müssen entfernt oder hinreichend unkenntlich gemacht werden.

Eine Anonymisierung im Sinne des Erwägungsgrundes 26 zur DSGVO, die einen vollständigen Wegfall des Personenbezugs zur Folge hat und dadurch keinerlei Rückschlüsse auf die Verfahrensbeteiligten zulässt, ist praktisch aber nicht durchführbar. Eine Identifizierung der Verfahrensbeteiligten ist häufig schon anhand des entscheidenden Gerichts, des Entscheidungsdatums oder der Sachverhaltsdarstellung möglich. Zudem dürfen die Verständlichkeit und Lesbarkeit einer Entscheidung durch die Neutralisierung von Daten nicht unzumutbar beeinträchtigt werden. Das Ziel kann daher nicht die vollständige Anonymität sein, sondern vielmehr nur ein möglichst hoher Grad, der den Informationsgehalt der Entscheidung nicht zu stark abschwächt. Maßgeblicher Anknüpfungspunkt für eine solche zureichende „Neutralisierung“ ist, ob nach den ergriffenen Maßnahmen ein durchschnittlicher Leser die Verfahrensbeteiligten noch identifizieren kann oder nicht.

4.1.2 Die „Neutralisierung“ einer Gerichtsentscheidung

Die konkreten Anforderungen hierfür richten sich deshalb stets nach dem jeweiligen Einzelfall.

So sind bspw. Vor- und Zunamen natürlicher Personen nach Auffassung hiesiger Behörde vollständig aus einer Entscheidungsveröffentlichung zu entfernen. Die Bezeichnung bloß mit dem Anfangsbuchstaben des Namens genügt nicht den Anforderungen an eine Neutralisierung, da sich hierdurch der Personenbezug bei vorhandenem Spezialwissen auch durch Dritte sehr einfach wieder herstellen lässt. Gleiches gilt für (Adels-)Titel, Namenszusätze und konkrete Geburtsdaten,

sofern diese für die Entscheidung nicht von maßgebender Bedeutung sind.

Die Angabe von Berufsbezeichnungen und Tätigkeiten ist unbedenklich, sofern sie entscheidungserheblich ist. Eine Neutralisierung ist demgegenüber in solchen Fällen geboten, in denen der Beruf an sich bereits als Alleinstellungsmerkmal in Betracht kommt und für den Inhalt der Entscheidung keine Rolle spielt. Zu differenzieren ist hier insbesondere bei der Benennung von Institutionen und Behörden: Diese reicht im Regelfall gerade nicht aus, um einen Personenbezug zu einem Verfahrensbeteiligten herzustellen, weswegen eine Neutralisierung nicht zwingend geboten ist. Anderes gilt jedoch hinsichtlich der Angabe konkreter Amts- oder Funktionsbezeichnungen in Verbindung mit Organisationseinheiten (z. B. „Die Leiterin der Vergabestelle der Stadt X“). Diese ermöglichen die Zuordnung zu einer individualisierbaren Person und sind, sofern sie nicht entscheidungserheblich sind, zu neutralisieren.

Auch konkrete Orts- und Zeitangaben haben sich an den vorgenannten Erfordernissen zu bemessen und werden regelmäßig zu entfernen sein. Eine generalisierende Bewertung ist dabei nicht möglich; auch hier kommt es jeweils auf die Umstände des Einzelfalls an. In Betracht kommen Fällen, in denen ein Ort einzigartige Wesenszüge aufweist, mehrere Orte – bspw. Fahrtwege – einander gegenüber gestellt werden oder zeitliche Abfolgen Einzug in die Entscheidung finden, obwohl deren Beschreibungen für die Entscheidung von keinerlei Relevanz sind. Zu beachten ist hier, dass eingesetzte Platzhalter nicht lediglich aus dem korrekten Anfangsbuchstaben der Örtlichkeit bestehen sollten, da Rückschlüsse auf die konkrete Lokalität so sehr einfach möglich wären.

Nicht zu neutralisieren ist die Nennung gesetzlicher Vorschriften, selbst wenn sie auf einen bestimmten Personenkreis bezogen sind. Bei gesetzlichen Vorschriften

handelt es sich um abstrakt-generelle Regelungen, die keinen hinreichenden Personenbezug aufweisen und für die Verständlichkeit der Entscheidung regelmäßig von erheblicher Relevanz sind.

4.1.3 Neuveröffentlichung und Sensibilisierung

In der vorliegenden Angelegenheit waren nach Auffassung hiesiger Behörde die Nennung des Geburtsdatums und des Ausbildungsberufs sowie der konkreten Busstrecke eines Verfahrensbeteiligten für das Verständnis der Entscheidung nicht erforderlich. Wir wandten uns deswegen mit unserem Anliegen an das zuständige Gericht und wiesen – unter Hinweis auf die vorstehend beschriebenen Grundsätze – auf die unzureichende Anonymisierung im konkreten Beschwerdefall hin. Während die Herstellung einer neutralisierten Entscheidungsfassung im Regelfall durch den jeweiligen Spruchkörper des Gerichts erfolgt und somit als „justizielle Tätigkeit“ (Art. 55 Abs. 3 DSGVO) unserer Zuständigkeit entzogen ist, stellt die Entscheidung über die Veröffentlichung eines so bearbeiteten Gerichtsurteils eine unserer Aufsicht unterliegende Verwaltungstätigkeit des Gerichts dar. Es wurde deswegen darum gebeten, bei dem Betreiber der betroffenen Datenbank auf die Veröffentlichung einer nachträglich hinreichend neutralisierten Entscheidung hinzuwirken.

Auf unseren Hinweis hin, teilte uns der Datenschutzbeauftragte des Gerichts mit, dass die Anonymisierung der fraglichen Gerichtsentscheidung dort nochmals überarbeitet würde. Zur Unterstützung neuer Richterinnen und Richter sei des Weiteren ohnehin die Erarbeitung einer Handreichung zur hier relevanten Thematik ins Auge gefasst. Auf Nachfrage stellten wir deswegen gerne unsere Ausführungen für die Erstellung interner Hinweise zur Verfügung; ein entsprechendes Informationsschreiben wurde zwischenzeitlich gerichtsintern verbreitet.

Auch in dem Ausgangsfall wurde die fragliche Entscheidung des Gerichts nachträglich neutralisiert und letztlich in dieser Form neu veröffentlicht.

Fazit/ Empfehlung:

Bei der Veröffentlichung von Gerichtsentscheidungen muss darauf geachtet werden, möglichst alle personenbezogenen Daten, die für das Verständnis und die Lesbarkeit der Entscheidung nicht zwingend erforderlich sind, zu entfernen oder zu verfremden. Dies gilt insbesondere für Namen, Geburtsdaten sowie Orts- und Zeitangaben.

4.2 Datenverarbeitung bei der Beantragung des „kleinen Waffenscheins“

Nicht nur in den USA ist das Waffenrecht ein heikles Thema und immer wieder Gegenstand politischer Debatten. Der Ruf nach mehr Kontrolle ist vor dem Hintergrund der potentiellen Gefahren, die von Waffen wesenstypisch ausgehen, natürlich nachvollziehbar. Eine mit Sicherheitsaspekten begründete, überschießende Datenerhebungspraxis darf damit jedoch nicht einhergehen. Die Verarbeitung personenbezogener Informationen durch öffentliche Stellen muss sich auch in diesem Zusammenhang stets am Grundsatz der Erforderlichkeit orientieren (Art. 5 Abs. 1 lit. c, Art. 6 Abs. 1 Satz 1 lit. e DSGVO; § 4 Abs. 1 SDSG). So dürfen bspw. für die Bearbeitung eines waffenrechtlichen Antrags nur solche Daten vom Antragsteller verpflichtend abgefragt werden, die für das konkrete Verfahren auch tatsächlich benötigt werden bzw. für die Bearbeitung des Antrags von Bedeutung sind.

Unserer Behörde fiel bei Betrachtung der Antragsformulare für den sog. „kleinen Waffenschein“ der insgesamt sieben saarländischen Waffenbehörden auf[10], dass diese sehr

[10] Es handelt sich hierbei um die Waffenbehörden der Landkreise Merzig-Wadern, Neunkirchen, Saarlouis und St. Wendel, des Saarpfalz-Kreises, des Regionalverbands Saarbrücken und der Landeshauptstadt Saarbrücken.

unterschiedlich ausgestaltet sind und in diesen teilweise Informationen abgefragt werden, die für die gesetzlich normierten Gewährleistungsvoraussetzungen keinerlei Bewandtnis haben. Bereits seit geraumer Zeit stehen wir diesbezüglich mit dem Saarländischen Ministerium für Inneres, Bauen und Sport (MIBS) in Kontakt. Dieses war als Fachaufsicht für den waffenrechtlichen Bereich im Saarland auf das Unabhängige Datenschutzzentrum zugegangen, um eine zentrale Zusammenarbeit mit den zuständigen Landkreisen zu ermöglichen.

Der kleine Waffenschein berechtigt zum Führen von Schreckschuss-, Reizstoff- und Signalwaffen, die als PTB-Waffe[11] gekennzeichnet sind. Der Erwerb und Besitz solcher Waffen ist dagegen grundsätzlich erlaubnisfrei.

Im Gegensatz zum „(großen) Waffenschein“ werden geringere Anforderungen an den Antragsteller gestellt. Dieser muss weder eine bestehende Sachkunde noch das zugrundeliegende Bedürfnis oder das Bestehen einer Haftpflichtversicherung nachweisen. Es reicht die Vollendung des 18. Lebensjahres sowie der Nachweis der erforderlichen Zuverlässigkeit und der persönlichen Eignung aus.

Vor diesem Hintergrund erschienen bestimmte Datenfelder in den untersuchten Antragsformularen, die verpflichtend den Familienstand (ledig, verheiratet), die Personalien von Familienangehörigen (Ehepartner) oder den ausgeübten Beruf des Antragstellers abfragten, nicht erforderlich. Gleiches galt für Angaben zu bereits früher erteilten waffenrechtlichen Erlaubnissen.

In einem Arbeitstreffen mit dem für Waffenrecht zuständigen Referat des MIBS im September 2022 konnte die Erforderlichkeit dieser und weiterer Datenabfragen für die Arbeit der Waffenbehörden erörtert werden. Als Ergebnis der

[11] PTB steht für „Phsyikalisch-Technische-Bundesanstalt“; entsprechende Waffen erhalten ein Prüfsiegel (Aufschrift PTB und Prüfnummer im Kreis).

Unterredung hielten wir eine Überarbeitung der in Verwendung befindlichen Antragsformulare anhand eines gemeinsam erstellten Musters fest. Dieses sollte außerdem eine umfängliche Datenschutzerklärung und ein Informationsblatt zu Fragen der rechtlichen Zusammenhänge mit PTB-Waffen und kleinem Waffenschein erhalten. Eine baldige Umsetzung der Anpassungsbemühungen wurde von Seiten des Ministeriums zugesagt. Aufgrund personeller Einspannungen der zuständigen Mitarbeiter des MIBS in priorisierten Verfahren kam es jedoch zu zeitlichen Verzögerungen. Eine Finalisierung des Musters und die anschließende Verteilung an die Waffenbehörden zur weiteren Umsetzung steht zum Zeitpunkt des Redaktionsschlusses weiterhin aus.

4.3 Kontrolle des Schriftverkehrs in den Justizvollzugsanstalten

Im Berichtzeitraum erreichte uns auch eine Beschwerde aus einer Justizvollzugsanstalt (JVA). Da der Grundrechtsschutz nicht an den Mauern der Einrichtung endet, können sich natürlich auch Strafgefangene jederzeit an das Unabhängige Datenschutzzentrum wenden, wenn sie einen nicht korrekten Umgang mit ihren personenbezogenen Daten und somit einen Verstoß gegen ihr Recht auf informationelle Selbstbestimmung vermuten.

Im hier erwähnten Fall wandte sich der Beschwerdeführer mit dem Verdacht an uns, dass Bedienstete der betroffenen saarländischen JVA in ungerechtfertigter Weise an ihn adressierte Briefe öffneten, die darin enthaltenen Informationen zur Kenntnis nähmen und diese sodann in unrechtmäßiger Weise verwendeten und offenlegten. Die Bedenken stützte der Gefangene auf die Beobachtung, dass ihm ein Schreiben in einem geöffneten Umschlag präsentiert und bestimmte inhaltliche und durchaus sensible Zusatzinformationen in Gegenwart Dritter mündlich mitgeteilt wurden.

4.3.1 Grundrechtlicher Rahmen

Um den Gesamtvorgang umfänglich in datenschutzrechtlicher Hinsicht bewerten zu können, bedurfte es somit nicht nur einer Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG), sondern auch einer Befassung mit den in engem Zusammenhang stehenden Grundrechten aus Art. 10 GG.

Die darin verankerten Freiheitsrechte des Brief-, Post- und Fernmeldegeheimnisses sind als besondere Garantien der Privatheit zu verstehen.[12] Sie bieten einen Raum, in dem die private Fernkommunikation weitgehend vor staatlichen Eingriffen geschützt und somit der „Neugierde“ bzw. den „Fahndungs- und Ermittlungsinteressen“ des Staates entzogen wird.[13] Beschränkungen dieser Grundrechte sind nur auf Grundlage eines Gesetzes möglich.

Gerade beim Justizvollzug bestehen besondere Begebenheiten und Anforderungen (etwa: die Sicherung der Anstalt oder die Gewährleistung des Vollzugsziels), die das Bedürfnis nach gerade solchen Beschränkungen mit sich bringen. Deshalb existieren in diesem Bereich einige Normen, die bestimmte Eingriffe in die beschriebene Schutzsphäre zulassen. Einen solchen Eingriff stellt die Kontrolle des Schriftverkehrs dar.

4.3.2 Der Schriftverkehr in saarländischen JVA

Die Regelungen hierzu finden sich in den §§ 33 und 34 des Saarländischen Strafvollzugsgesetzes (SLStVollzG) bzw. in § 37 des Saarländischen Untersuchungshaftvollzugsgesetzes (SUVollzG). So steht den Gefangenen zwar grundsätzlich das Recht zu, Schreiben abzusenden und zu empfangen. Eine Überwachung des Schriftverkehrs durch die JVA ist jedoch (soweit der Schriftverkehr nicht bereits aufgrund richterlicher

[12] BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03, 2357/04, 603/05, BVerfGE 118, 168 [184].

[13] vgl. Ogorek, in: BeckOK Grundgesetz, Epping/Hillgruber (52. Edition, Stand: 15.08.2022), Art. 10 GG – Vor. Rn. 1.

Anordnung einem Gericht vorzulegen ist) in unterschiedlicher Weise möglich.

So kann der Postinhalt auf verbotene Gegenstände und auf „grobe“ Unstimmigkeiten überprüft werden, etwa hinsichtlich fehlender Briefköpfe bei Rechtsanwalts- und Behördenpost oder eines auffälligen Schriftbilds (sog. Sichtkontrolle). In Fällen, in denen die Leitung der JVA bei einzelnen Gefangenen eine besondere Situation erkennt, kann auch eine Kenntnisnahme des gedanklichen Inhalts des Schriftverkehrs angeordnet werden (sog. Inhaltskontrolle). Eine solche Kontrolle ist jedoch stets nur dann zulässig, wenn diese aus Gründen der Anstaltssicherheit oder aufgrund einer sonst zu befürchtenden Gefährdung des Vollzugszieles erforderlich ist.

Gegenüber bestimmten Absendern / Empfängern (soweit deren Identität zweifelsfrei feststeht) findet derweil eine Überwachung des Schriftverkehrs nicht statt. Hierbei handelt es sich um solche, bei denen die Kommunikation in erheblichem Maße vertraulich ist. Hierzu gehören zum Beispiel die Volksvertretungen des Bundes und der Länder, die konsularischen Vertretungen des Heimatlandes und grundsätzlich auch die Verteidigerinnen und Verteidiger des Inhaftierten. Auch die Datenschutzbeauftragten des Bundes und der Länder sind von dem Ausnahmetatbestand erfasst (§ 34 Abs. 3 SLStVollzG und § 37 Abs. 3 SUVollzG).

4.3.3 Konkreter Fall im Berichtszeitraum

In dem konkret von uns überprüften Fall konnten die Bedenken des Beschwerdeführers nicht bestätigt werden. Es stellte sich heraus, dass die in der JVA eingegangene Postsendung nicht persönlich an den Gefangenen adressiert war, sondern die JVA als Empfängerin auswies. Dieses Schreiben enthielt neben der Bitte, ein unverschlossen beiliegendes Dokument an den Gefangenen zu übergeben, auch bereits selbst sensible Informationen zu dem Gefangenen.

Aufgrund dieser Begebenheiten konnte von unserer Behörde kein datenschutzrechtlicher Verstoß der Einrichtung festgestellt werden. Weder das Öffnen des Briefs noch die Kenntnisnahme der Informationen aus dem an die JVA adressierten Begleitschreiben konnten der Einrichtung angelastet werden.

Die Wahl und Ausgestaltung der konkreten Postsendung (offenlegende Inhalte im Begleitschreiben und unverschlossen beiliegende Dokumente) wirft dennoch Fragen auf. Inwiefern sich der Absender des Schreibens datenschutzkonform verhalten hat, war jedoch durch eine andere Aufsichtsbehörde festzustellen. Das Verfahren haben wir deswegen diesbezüglich mit Zustimmung des Petenten an die zuständigen Kollegen zur Prüfung abgegeben.

Fazit/ Empfehlung:

Für die Kontrolle des Schriftverkehrs in Saarländischen Justizvollzugsanstalten bestehen diverse Voraussetzungen. Sicht- und Inhaltskontrolle unterscheiden sich hierbei in ihrer Eingriffstiefe. Insbesondere für letztere bestehen deswegen enge Regelungen in SLStVollzG und SUVollzG. Zudem existieren diverse Kommunikationspartner, bei denen eine Kontrolle grundsätzlich nicht stattfinden darf.

Bei Verdacht eines Verstoßes in diesem Zusammenhang, bietet sich zunächst ein klärendes Gespräch mit der JVA-Leitung an. Daneben besteht aber stets auch die Möglichkeit, sich mit einer Datenschutzbeschwerde an unsere Behörde zu wenden.

4.4 Datenübermittlungen durch eine Justizvollzugsanstalt

Eine Justizvollzugsanstalt (JVA) war auch in einem weiteren Beschwerdeverfahren zentraler Akteur. Im Mittelpunkt standen hier Fragen des Auskunftsanspruchs hinsichtlich der konkreten Empfänger einer Datenübermittlung. Da die Datenweitergabe

nicht im Zusammenhang mit dem Strafvollzug als solchem stattfand und auch sonst keine personenbezogenen Daten Inhaftierter betroffen waren, hatten wir uns nicht mit den §§ 54 ff. des Justizvollzugsdatenschutzgesetzes (JVollzDSG), sondern mit Art. 15 DSGVO zu befassen.

4.4.1 Das Ausgangsverfahren

Die uns zugegangene Beschwerde hatte dabei ihren Ursprung in einer Informationsfreiheitsanfrage. Der Antragsteller hatte durch diese in Erfahrung bringen wollen, welche konkreten Unternehmen bei der fraglichen JVA als sogenannte „Partnerfirmen“ regelmäßig Aufträge zur Gefangenenarbeit erteilen und somit Arbeiten durch Inhaftierte verrichten lassen.

Zwei der Betriebe baten im Rahmen des vorgeschalteten Beteiligungsverfahrens (§§ 6, 8 Informationsfreiheitsgesetz, IFG)[14] – zur Prüfung etwaiger entgegenstehender Betriebs- und Geschäftsgeheimnisse – um Mitteilung des Namens des Antragstellers und begründeten dies damit, ausschließen zu wollen, dass es sich bei diesem um einen potentiellen Konkurrenten und Mitwettbewerber handelte. Der daraufhin kontaktierte Antragsteller stimmte einer Übermittlung seines Namens zu, wies gleichzeitig aber bereits auf etwaige Ansprüche aus Art. 15 DSGVO hin.

Nach Erhalt dieser Informationen und interner Prüfung verweigerten die beiden betroffenen Unternehmen jedoch die Zustimmung zur Offenlegung der begehrten Angaben durch die JVA. Auf den negativen Bescheid der Anstalt hin machte der Antragsteller gegenüber der JVA sodann seinen Auskunftsanspruch nach Art. 15 DSGVO geltend und verlangte insbesondere Mitteilung dahingehend, an welche Empfänger seine personenbezogenen Daten übermittelt wurden (Art. 15 Abs. 1 lit. c DSGVO). Die Auskunft diene dazu, seine Rechte aus der DSGVO gegenüber diesen geltend machen zu können. Die JVA verweigerte die Auskunft mit Verweis auf Art. 15 Abs. 4

[14] IFG anwendbar über § 1 Saarländisches Informationsfreiheitsgesetz (SIFG).

DSGVO; Betriebs- und Geschäftsgeheimnisse Dritter (der Partnerfirmen) stünden dem Anspruch entgegen. Zudem sei die Geltendmachung rechtsmissbräuchlich; es gehe dem Antragsteller tatsächlich nur um Komplettierung seiner Informationsfreiheitsanfrage und keineswegs um Verwirklichung seiner Datenschutzrechte.

Im Rahmen der daraufhin bei uns eingereichten Beschwerde befassten wir uns folglich mit mehreren Problemfeldern:

4.4.2 Die Reichweite der möglichen Auskunftsbeschränkung in Art. 15 Abs. 4 DSGVO

Zunächst beschäftigten wir uns mit der Reichweite der Auskunftsbeschränkung in Art. 15 Abs. 4 DSGVO. Dieser verweist seinem Wortlaut nach nämlich lediglich auf Art. 15 Abs. 3 DSGVO und das dort verbriefte „Recht auf Kopie". Ob Abs. 4 daneben auch auf das in Abs. 1 grundsätzlich aufgeführte Auskunftsrecht als solches Anwendung finden kann, ist in der deutschen Rechtsliteratur zwar umstritten,[15] es ist aber kein entscheidender Grund ersichtlich, warum sich die dortige Interessenabwägung nur auf die Erteilung von Auskünften in Form einer Kopie beschränken sollte. Unserer Meinung nach spielt es keine Rolle, ob die Auskunft über personenbezogene Daten im Wege einer Kopie oder in sonstiger Art und Weise erfolgt. Erwägungsgrund 63 zur DSGVO sieht die Beschränkungsmöglichkeit allgemein und nicht nur in Bezug auf eine etwaige Kopie vor.

Die von der gewählten Auskunftsform unabhängige Geltung der möglichen Auskunftsbeschränkung bedeutet indes nicht automatisch, dass die Norm auch jegliche Art von inhaltlicher

[15] Bejahend: DIX, in: Simitis/Hornung/Spiecker gen. Döhmann [1. Auflage 2019], Art. 15 Rn. 34; DSK-Kurzpapier Nr. 6 „Auskunftsrecht der betroffenen Person, Art. 15 DSGVO", S. 3; Paal, in: Paal/Pauly, DS-GVO BDSG [3. Auflage 2021], Art. 15 Rn. 41; Schmidt-Wudy, in: BeckOK Datenschutzrecht Wolff/Brink [38. Edition, 01.11.2021], Art. 15 Rn. 96 f.; verneinend: Bäcker in: Kühling/Buchner, DS-GVO BDSG [3. Auflage 2020], Art. 15 Rn. 33; Kremer, CR 2018, 560 [564].

Information erfasst. So gehen wir davon aus, dass die Auskunft der in Art. 15 Abs. 1 HS. 2 lit a) bis h) genannten „Metainformationen“ gerade nicht durch Art. 15 Abs. 4 DSGVO beschränkt werden kann.

Bei den in den Buchstaben a) bis h) genannten Informationen handelt es sich um entscheidende Angaben, die der Aufklärung des Individuums über die Rechtslage dienen und sowohl eine Nachvollziehbarkeit des Verfahrens fördern als auch die weiterführende Durchsetzung von Betroffenenrechten ermöglichen sollen. Würde über diese nicht informiert, so wäre die Weiterverfolgung etwaiger Eingriffe in die herausragende Rechtsposition nach Art. 8 Grundrechte-Charta und Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz durch die betroffene Person stark beeinträchtigt. Entgegenstehende Rechte Dritter (i. S. d. Art. 15 Abs. 4 DSGVO) wären ohnehin nur bei Buchstabe c (Empfänger) und Buchstabe g (Herkunft, Quelle) denkbar. Gegen eine Ausweitung auf diese spricht aber das Verhältnis zwischen Art. 15 DSGVO und den Art. 13, 14 DSGVO. Denn der Auskunftsanspruch ist quasi als nachgelagertes Äquivalent zur bereits bei Datenerhebung existierenden Informationspflicht des Verantwortlichen zu sehen. Dort müssen Herkunft und Empfänger mitgeteilt werden, ohne dass eine mit Art. 15 Abs. 4 DSGVO vergleichbare Ausnahmeregelung geschaffen wurde. Diese Wertung des europäischen Verordnungsgebers muss deswegen in gleichem Umfang auch auf die identischen Nennungen in Art. 15 Abs. 1 HS 1 lit. c) und g) DSGVO erstreckt werden.

Nicht ausgeschlossen wäre eine Beschränkung durch nationale Regelungen im Sinne von Art. 23 DSGVO. Eine solche war im vorliegenden Verfahren aber nicht ersichtlich.

4.4.3 Anforderungen an Betriebs- und Geschäftsgeheimnisse

Unabhängig davon waren nach unserem Dafürhalten aber auch die Voraussetzungen des Art 15 Abs. 4 DSGVO – nämlich entgegenstehende Rechte Dritter – nicht gegeben. Zwar

können Betriebs- und Geschäftsgeheimnisse eine Position im Sinne der Norm begründen. Im vorliegenden Fall gingen wir jedoch davon aus, dass die Offenlegung der Identität der Partnerfirmen und somit deren Geschäftsbeziehung mit der JVA nicht unter die genannten Begriffe zu fassen sind.

Die Auslegung von „Geschäftsgeheimnis“ im Datenschutzrecht hat sich am gewachsenen Verständnis des Wettbewerbsrechts zu orientieren. Deswegen zogen wir für unsere Bewertung sowohl die von der Rechtsprechung entwickelten, klassischen Merkmale,[16] als auch die Voraussetzungen des relativ neuen Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) in § 2 Nr. 1 heran. Auch nach näherer Befassung konnten uns die JVA und die betroffenen Partnerfirmen nicht hinreichend darlegen, dass zum Schutz der konkreten fraglichen Information relevante Geheimhaltungsmaßnahmen i. S .d. § 2 Nr. 1 lit. b GeschGehG ergriffen wurden. Da uns somit Anhaltspunkte für das Vorliegen schützenswerter Geheimnisse fehlten, sahen wir auch in dieser Hinsicht keine Veranlassung, Art. 15 Abs. 4 DSGVO Anwendung finden zu lassen.

4.4.4 Der Einwand des Rechtsmissbrauchs

Auch konnten wir im Handeln des Beschwerdeführers kein rechtsmissbräuchliches Verhalten erblicken. Die Rechtsansicht, dass in bestimmten Situationen der abweichenden Zweckrichtung eines Auskunftsanspruchs der Einwand des Rechtsmissbrauchs Anwendung finden kann, ist in der jüngeren Rechtsprechung zwar anzutreffen, wurde bislang aber noch keiner verbindlichen und harmonisierten Klärung zugeführt. Dies könnte sich durch eine Vorlagefrage des BGH an den EuGH aus dem März 2022 künftig ändern.[17] Die Ausführungen des BGH deuten zumindest an, dass dieser

[16] statt vieler: BGH, Urteil vom 10. Mai 1995 – 1 StR 764/94, BGHSt 41, 140 [142].

[17] BGH, Beschluss vom 29. März 2022 – VI ZR 1352/20, GRUR-RS 2022, 9584.

von engen Voraussetzungen für die Einwendung ausgeht. Ein Rechtsmissbrauch könne nach Senatsauffassung nämlich nicht bereits bejaht werden, wenn ein vom datenschutzrechtlichen Zweck des Auskunftsanspruchs nicht ausdrücklich gedecktes Ziel verfolgt wird, sondern nur dann in Betracht kommen, „wenn der Betroffene mit seinem Begehren von der Rechtsordnung missbilligte Ziele verfolgt, arglistig oder schikanös handelt“.[18] In dem hier berichteten Fall konnten wir keine dieser Merkmale feststellen. Zwar war nicht auszuschließen, dass der Beschwerdeführer eine „Komplettierung“ seines IFG-Antrags verfolgte; als Ziel seines Auskunftsverlangens berief er sich jedoch stets und ohne inhaltliche Widersprüche auf die effektive Durchsetzung seiner Datenschutzrechte gegenüber den Empfängern (Partnerunternehmen). Es fehlten eindeutige objektive Anhaltspunkte, die eine überwiegende, abweichende Willensrichtung belegten. Zudem hatte der Beschwerdeführer schon im Vorfeld der Datenübermittlung durch die JVA die Geltendmachung des datenschutzrechtlichen Auskunftsrechts avisiert; insbesondere Arglist und Schikane waren somit ebenfalls auszuschließen.

Wir legten der JVA deswegen in diesem Verfahren nahe, dem Auskunftsbegehren des Beschwerdeführers nachzukommen. Die Anstalt konsultierte daraufhin nochmals die beiden betroffenen Firmen, folgte letztlich aber unseren Ausführungen und beantwortete das Auskunftsersuchen des Petenten zeitnah unter Übersendung der gewünschten Firmennamen.

Fazit/ Empfehlung:

Das Auskunftsrecht der DSGVO war und ist weiterhin Gegenstand erheblicher Diskussion in Rechtsprechung und Literatur. Als zentrales Betroffenenrecht sollten Beschränkungen jedoch eher restriktiv gehandhabt werden. Art. 15 Abs. 4 DSGVO gilt zwar für jede Art der Auskunftsgewährung, insbesondere die in Art. 15 Abs. 1 HS 2

[18] BGH, Beschluss vom 29. März 2022 – VI ZR 1352/20, GRUR-RS 2022, 9584, Rn. 19.

lit. a) bis h) genannten Metainformationen können aber durch diesen nicht beschränkt werden. Rechtsnormen, die auf der Öffnungsklausel des Art. 23 DSGVO basieren, bleiben hiervon unberührt. Auch der Einwand des Rechtsmissbrauchs hat unserer Ansicht nach hohe Hürden – von der Rechtsordnung missbilligte Ziele, Schikane oder Arglist sind hier Voraussetzung und müssen objektiv belegbar sein. Konkretere Erkenntnisse zu diesem Thema wird hoffentlich das Vorabentscheidungsverfahren beim EuGH mit sich bringen.

4.5 Online-Zeugenvernehmung in Ordnungswidrigkeitenverfahren

Im Bereich der Ordnungswidrigkeiten belasten Massenverfahren schon seit jeher die mit deren Verfolgung befassten Behörden. So etwa und besonders im Zusammenhang mit Verkehrsverstößen. Aus diesem Grund ist es nicht verwunderlich, wenn gerade in diesem Bereich immer wieder neue Verfahren und Tools zur Arbeitserleichterung vorgeschlagen werden. Im Berichtzeitraum wurden wir in diesem Kontext (erneut) zu Rate gezogen.

4.5.1 Bisherige Beteiligung des Unabhängigen Datenschutzzentrums

Bereits 2017 hatte sich die beim Landesverwaltungsamt (LaVA) eingerichtete Zentrale Bußgeldbehörde des Saarlandes (ZBB) mit einem Vorhaben der „Online-Anhörung“ an uns gewandt. Das Projekt sah vor, Betroffenen einer Ordnungswidrigkeit, die gem. § 55 des Gesetzes über Ordnungswidrigkeiten (OWiG) zu dem vorgeworfenen Verstoß anzuhören sind, künftig auch die Einreichung von Stellungnahmen direkt über ein Online-Portal – unter Verzicht auf die Papierform – zu ermöglichen. Über unsere erste Einschätzung des Verfahrens berichteten wir in unserem 27. Tätigkeitsbericht.[19]

[19] Vgl. 27. Tätigkeitsbericht, 2017/2018, Kapitel 2.2, S. 32 - 33, elektronisch

Im Rahmen unserer weiteren Beteiligung erreichten wir, dass technische Anpassungen der geplanten Abläufe vorgenommen wurden. Zudem konnten offene Fragen einer Klärung zugeführt werden, sodass aus datenschutzrechtlicher Sicht einer Einführung in Bezug auf die Betroffenenanhörung keine grundsätzlichen Bedenken im Wege standen.

Zu einer perspektivisch avisierten Anwendung des Verfahrens auf die Online-Vernehmung von Zeugen äußerten wir uns zum damaligen Zeitpunkt jedoch kritisch. Wir argumentierten unter Verweis auf vorhandene Kommentarliteratur, dass in Schrift fixierte Zeugenvernehmungen der Schriftform unterlägen und somit auch die in § 32a Abs. 3 der Strafprozessordnung (StPO)[20] aufgeführten Vorgaben für den elektronischen Rechtsverkehr zu beachten wären. Hierzu zählt insbesondere die Verwendung einer qualifizierten elektronischen Signatur. Die Implementierung einer solchen Lösung wurde von der ZBB allerdings als unpraktikabel verworfen.

Das Online-Portal wird laut Information der ZBB seit Juni 2021 für die Anhörung Betroffener produktiv genutzt.

4.5.2 Online-Zeugenvernehmung 2.0 (2022)

Aufgrund der seither gemachten positiven Erfahrungen im Wirkbetrieb der Online-Anhörung, wandte sich die ZBB im Berichtsjahr erneut an unsere Behörde und bat um Prüfung, ob das Verfahren nicht doch auch für die Vernehmung von Zeugen genutzt werden könne. Unsere Argumentation zur Schriftform wurde in diesem Zusammenhang in Frage gestellt.

Bei der Bearbeitung der Anfrage setzten wir uns kritisch mit unserer eigenen Argumentation aus dem zurückliegenden Verfahren auseinander. Tatsächlich finden sich zu der Frage, ob niedergeschriebene Zeugenaussagen einer bestimmten

---

abrufbar unter: https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/berichte/tb27_1718.pdf

Form (Schriftform) unterliegen, keine belastbaren Nachweise in der Rechtsprechung oder der Kommentarliteratur. Grund hierfür ist wohl das im strafprozessualen Kontext vorherrschende Primat der Unmittelbarkeit; der Zeugenbeweis wird grundsätzlich durch persönliche Vernehmung im Rahmen einer mündlichen Verhandlung geführt (vgl. § 250 ff. StPO). Eine schriftliche Beantwortung von Beweisfragen, wie sie in § 377 Abs. 3 der Zivilprozessordnung (ZPO) oder über den Verweis in § 98 der Verwaltungsgerichtsordnung (VwGO) normiert wurde, ist nicht vorgesehen. Hinsichtlich des Ermittlungsverfahrens sieht zumindest Nr. 67 der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) vor, dass Zeugen sich in bestimmten Fällen über bestimmte Fragen zunächst nur in einem schriftlichen Verfahren äußern können.

Allen diesen Vorschriften lässt sich jedoch kein gesetzlich normiertes, prozessuales Schriftformerfordernis (vgl. BT-Drs. 18/9416, S. 45) entnehmen, weswegen wir nicht mehr an unserem ursprünglichen Argument festhielten.

Dennoch erachten wir die Verwendung eines Online-Formulars für die Vernehmung von Zeugen als problematischer als bei der Anhörung von Betroffenen. Während die in § 55 OWiG angelegte Anhörung ein Recht des Betroffenen darstellt, ist die Vernehmung eines Zeugen mit einer Pflicht verbunden (vgl. § 49 StPO; soweit kein Zeugnisverweigerungsrecht vorliegt). Bei der Person des Zeugen handelt es sich außerdem um ein Beweismittel, das erheblichen Einfluss auf das Verfahren gegen den Betroffenen haben kann. Wir vertreten deswegen die Auffassung, dass sich sowohl daraus als auch aus einer Gesamtschau der Regelungen in den §§ 32a ff. StPO, §§ 110 ff. OWiG und aus Art. 29 Abs. 1 der JI-RL erhöhte Anforderungen an die Gewährleistung von Authentizität und Integrität der eingegebenen Datensätze ergeben. So kann etwa § 32c Satz 4 StPO bzw. § 110b Satz 4 OWiG der Gedanke des Gesetzgebers entnommen werden, dass bei der Verwendung elektronischer Formulare Maßnahmen zu ergreifen sind, die die Identifikation des Formularverwenders sicherstellen und

nachweisbar machen. Auch Art. 29 Abs. 2 lit. g JI-RL verlangt, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in Verarbeitungssysteme eingegeben worden sind.

Schriftlichen Aussagen kommt bei der Bewertung eines Sachverhalts zudem große Bedeutung zu.[21] Dies gilt insbesondere für den Bereich ordnungswidrigkeitsrechtlicher Massenverfahren, in denen schriftliche Zeugenaussagen die persönliche Vernehmung meist vollkommen ersetzen. Solche finden häufig erst und nur dann statt, wenn in Folge eines Einspruchs gegen einen Bußgeldbescheid doch noch eine mündliche Verhandlung vor Gericht anberaumt wird (vgl. §§ 67 ff. OWiG). Da Verfolgungsbehörden dem Rechtmäßigkeitsprinzip verpflichtet sind und sich aus einem fehlenden Nachweis der Authentizität von Zeugenaussagen oder einer unzureichenden Sicherung der Integrität von Datensätzen ein stark reduzierter Beweiswert mit entsprechenden Folgen für das Gesamtverfahren ergeben kann, empfahlen wir der ZBB, höhere Anforderungen an die Identifikation der Nutzer zu stellen. Statt der geplanten postalischen Übersendung einer Zugangskennung samt Passwort wiesen wir auf die Verwendung der eID-Funktion des neuen Bundespersonalausweises hin. Wenn auch die Implementierung eines solchen Verfahrens mit Kosten für die Behörde verbunden ist, bietet die Nutzung der eID-Funktion jedoch (insbesondere aufgrund der mittlerweile umfangreichen Verbreitung der Smartphone-Technologie) einen für den Bürger einfach handhabbaren, praxistauglichen und vor allem sicheren Authentifizierungsmechanismus. Wir erachten dieses weiterhin viel zu selten genutzte Instrument für den dargestellten Bereich als ein effektives, zweckmäßiges und vor allem auch datenschutzkonformes Mittel.

Ob und ggf. wie eine Online-Zeugenvernehmung bei Ordnungswidrigkeitenverfahren der ZBB künftig zum Einsatz

[21] Sommer, Signatur-Renitenz, StraFo 2018, 451 [insb. 455 f.].

kommen wird, ist uns zum Zeitpunkt des Redaktionsschlusses noch nicht bekannt. Wir gehen davon aus, dass wir die Thematik im Frühjahr 2023 erneut mit Vertretern des LaVA erörtern werden. Eine datenschutzfreundliche Ausgestaltung durch Verwendung der vorbeschriebenen Instrumente wäre natürlich erfreulich.

Bei datenschutzrechtlichen Fragen zu geeigneten technischen und organisatorischen Sicherungsmaßnahmen, wie dem Einsatz sicherer Authentifizierungsmethoden (z. B. im Kontext der eID-Funktion des Bundespersonalausweises), steht unsere Behörde allen Interessierten gerne zur Verfügung.

V.

Sicherheit

5 Sicherheit

5.1 PoC Datenkonsolidierung

Unter der Bezeichnung „Polizei 20/20“ (oder mittlerweile schlicht „P20“) betreiben das Bundesinnenministerium und die Polizeibehörden von Bund und Ländern derzeit ein weitreichendes Vorhaben zur Modernisierung der deutschen Polizei-IT-Landschaft. Das Gesamtprojekt soll der Realisierung eines völlig neuen digitalen Arbeitens bei der deutschen Polizei dienen und gliedert sich hierbei in diverse Teilprojekte auf.

5.1.1 Teilprojekt: PoC Datenkonsolidierung

Eines dieser Teilprojekte ist der sogenannte „Proof of Concept (PoC)[22] – Datenkonsolidierung“ (im Folgenden: PoC), der in einer Kooperation der Landeskriminalämter der Länder Nordrhein-Westfalen und Rheinland-Pfalz sowie des Landespolizeipräsidiums des Saarlandes als Projektverantwortliche entwickelt und begleitet wird.

Die Studie betrifft hierbei die Realisierbarkeit eines Informationssystems, das abseits des bundesweit abrufbaren polizeilichen Informationsverbunds (INPOL) einen Austausch von Erkenntnissen zwischen den Polizeibehörden der beteiligten drei Bundesländer ermöglichen soll. Hierdurch würde eine Abgleichbarkeit und Recherchierbarkeit von Daten aus niedrigschwelligen Phänomenbereichen – und somit auch unterhalb der „Verbundschwelle“[23] – ermöglicht. Erklärte Ziele der Beteiligten sind unter anderem, das bisher praktizierte und

[22] Als PoC wird grundsätzlich eine Art Machbarkeitsstudie bezeichnet, die dem Nachweis oder der Wiederlegung eines Konzepts dient und nicht zwingend ein tatsächlich nutzbares Produkt als Ergebnis haben muss.

[23] Die Verbundschwelle (§§ 29 ff. Bundeskriminalamtgesetz (BKAG)) bezeichnet eine notwendige Voraussetzung, um Daten im bundesweit abrufbaren Informationssystem INPOL-Z speichern zu dürfen. Es können nur solche Angaben aufgenommen werden, die eine länderübergreifende, internationale oder erhebliche Bedeutung besitzen oder für die Verarbeitung im Informationsverbund erforderlich sind („Verbundrelevanz“).

umständliche Verfahren sogenannter Erkenntnisabfragen zu ersetzen sowie die Feststellung einer etwaigen Verbundrelevanz von Daten zu erleichtern. Im Erfolgsfalle der Machbarkeitsstudie wird seitens der Polizeien eine bundesweite Ausweitung des Systems angestrebt.

5.1.2 Rechtliche Bewertung der Datenschutzbehörden und Warnung

Die Zulässigkeit eines solchen Informationssystems ist zwischen den Projektverantwortlichen und den beteiligten Aufsichtsbehörden derweil streitig. Erste Bedenken äußerte unsere Behörde bereits im Rahmen einer ersten Stellungnahme im August 2020. Ein gemeinsamer Workshop im November 2021 zeigte jedoch auf, dass unseren rechtlichen Einwänden nicht ausreichend Rechnung getragen wurde. Da bei dem geplanten Informationssystem datenschutzrechtliche Übermittlungen vorgenommen werden, sind die vom Bundesverfassungsgericht zur zweckändernden Weiterverarbeitung personenbezogener Daten entwickelten Grundsätze der sog. Hypothetischen Datenneuerhebung (HyDaNe)[24] zu beachten. Vor allem die Auslegung der diesbezüglichen verfassungsrichterlichen Aussagen und folglich auch die zu fordernden Maßstäbe bei der praktischen Ausgestaltung des geplanten Abrufverfahrens divergieren zwischen den Beteiligten stark.

Die Datenschutzaufsichtsbehörden aus Nordrhein-Westfalen, Rheinland-Pfalz und dem Saarland sprachen deswegen gegenüber den jeweiligen Projektverantwortlichen im Januar 2022 eine koordinierte Warnung (im Saarland nach § 6 Abs. 2 Satz 2 Saarländisches Polizeidatenverarbeitungsgesetz – SPolDVG) aus, die sich sowohl mit den Anforderungen der HyDaNe (hier vor allem, was unter „konkretem Ermittlungsansatz“ zu verstehen ist und wer die entsprechende

[24] siehe hierzu: BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220.

Prüfung zu welcherm Zeitpunkt vorzunehmen hat) als auch der Verwendung von Grunddaten einer Person (hier: zur Identifizierung bereits vorhandener Datensätze im System als eine Art Matching) beschäftigte.

Ebenfalls äußerte sich im Januar 2022 die AG INPOL[25] zum PoC, befasste sich in ihrer Stellungnahme aber vorwiegend mit verfassungsrechtlichen Fragen. So unter anderem, ob unter der Schwelle des polizeilichen Informationsverbundes nach § 29 BKAG überhaupt ein „Vorverbund“ bestehen kann. Denn das Grundgesetz geht abseits der Kriminalpolizei grundsätzlich von einer Dezentralisierung der Polizei aus.

Die Arbeiten am PoC wurden daraufhin zeitweilig eingestellt. In einer uns Mitte des Jahres 2022 zugegangenen, abgestimmten Stellungnahme der Projektverantwortlichen setzten sich diese dennoch kritisch mit der Argumentation aus unserer Warnung auseinander. Die von uns vorgetragene Rechtsauffassung wird demnach nicht geteilt.

Zwischenzeitlich wurde uns mitgeteilt, dass seitens der Projektleitung auch eine Fortführung des PoC angestrebt wird. Wir stehen diesbezüglich mit den Kolleginnen und Kollegen aus Nordrhein-Westfalen und Rheinland-Pfalz in engem Austausch, sehen jedoch derzeit keinen Grund, von unserer bereits mehrfach geäußerten Rechtsauffassung abzuweichen. Aufgrund der fortschreitenden Entwicklung des Gesamtprojekts P20 ist davon auszugehen, dass die vorstehenden Fragestellungen auch im Jahr 2023 umfassend durch die Datenschutzaufsichtsbehörden begleitet werden. Wie sich die Angelegenheit weiter entwickelt, bleibt derweil abzuwarten.

[25] Die Datenschutzkonferenz als Gremium der unabhängigen deutschen Datenschutzfsichtsbehörden wird in ihrer Arbeit durch Untergremien (sogenannte Arbeitskreise / AK) unterstützt. Die AG INPOL ist eine Arbeitsgruppe des AK Sicherheit, die sich mit Fragen im Zusammenhang mit polizeilichen Informationssystemen befasst.

VI.

Gesundheit und Soziales

6 Gesundheit und Soziales

6.1 Einrichtungsbezogene Impfpflicht

Auch im vergangenen Berichtszeitraum stellte die Befassung mit datenschutzrechtlichen Fragen rund um die Corona-Pandemie wieder einen Schwerpunkt unserer Tätigkeit im Gesundheitsbereich dar.

6.1.1 Grundlagen für die Datenverarbeitung

Mit dem Ziel, im weiteren Verlauf der Corona-Pandemie vulnerable Personengruppen z. B. in Krankenhäusern und Pflegeeinrichtungen bestmöglich zu schützen, hat der Bundesgesetzgeber im Berichtszeitraum mit § 20a Abs. 1 Infektionsschutzgesetz (IfSG) die sogenannte einrichtungsbezogene Impfpflicht eingeführt.[26] Durch die Regelung in § 20a Abs. 2 IfSG wurden Beschäftigte in den betreffenden Einrichtungen dazu verpflichtet, ihrem Arbeitgeber bis zum 15. März 2022 einen Nachweis über eine abgeschlossene Impfung, einen Genesenennachweis oder ein ärztliches Attest darüber, dass sie nicht geimpft werden können, vorzulegen.[27]

Diese viel diskutierte politische Entscheidung brachte auch einige datenschutzrechtliche Fragestellungen mit sich. So erreichten uns mehrere Anfragen betreffend die in diesem Zusammenhang vorgesehene Datenübermittlung von den betroffenen Einrichtungen an die Gesundheitsämter.

§ 20a Abs. 2 Satz 2 IfSG lautete: „Wenn der Nachweis nach Satz 1 nicht bis zum Ablauf des 15. März 2022 vorgelegt wird oder wenn Zweifel an der Echtheit oder inhaltlichen Richtigkeit

[26] Gesetz zur Stärkung des Schutzes der Bevölkerung und insbesondere vulnerabler Personengruppen vor COVID-19 vom 16. September 2022.

[27] § 20a IfSG wurde aufgehoben durch Art. 2 Nr. 1 i. V. m. Art. 23 Abs. 4 Satz 1 G v. 10.12.2021 I 5162 Satz 1 i.d.F. d. Art. 5 Nr. 2 G v. 16.9.2022 I 1454 m. W. v. 1.1.2023. Die einrichtungsbezogene Impfpflicht ist ab 01.01.2023 entfallen.

des vorgelegten Nachweises bestehen, hat die Leitung der jeweiligen Einrichtung oder des jeweiligen Unternehmens unverzüglich das Gesundheitsamt, in dessen Bezirk sich die jeweilige Einrichtung oder das jeweilige Unternehmen befindet, darüber zu benachrichtigen und dem Gesundheitsamt personenbezogene Angaben zu übermitteln."

Um welche personenbezogen Angaben es sich dabei handelt, ergab sich aus den Begriffsbestimmungen in § 2 IfSG. „Personenbezogene Angaben" sind demnach Name und Vorname, Geschlecht, Geburtsdatum, Anschrift der Hauptwohnung oder des gewöhnlichen Aufenthaltsortes und, falls abweichend, Anschrift des derzeitigen Aufenthaltsortes der betroffenen Person sowie, soweit vorliegend, Telefonnummer und E-Mail-Adresse (§ 2 Nr. 16 IfSG).

Diese Daten durften somit zwecks Überprüfung vom Arbeitgeber an das Gesundheitsamt übermittelt werden.

Das Gesundheitsamt konnte in der Folge weitere Maßnahmen bis hin zu einem Betretungsverbot ergreifen (§ 20a Abs. 5 IfSG).

Die Verarbeitung personenbezogener Daten durch das Gesundheitsamt war in diesem Kontext zur Aufgabenerfüllung erforderlich, so dass sich die Datenverarbeitung auf § 4 Abs. 1 Saarländisches Datenschutzgesetz (SDSG) i. V. m. Art. 6 Abs. 1 Satz 1 lit. e Datenschutz-Grundverordnung (DSGVO) stützen ließ. Danach ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen im Saarland zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der oder des Verantwortlichen liegenden Aufgabe erforderlich ist.

Soweit die Verarbeitung besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO wie z. B. Gesundheitsdaten betraf, war Rechtsgrundlage § 8 Abs. 1 Nr. 4 SDSG i. V. m. Art. 9 Abs. 2 lit. i DSGVO. Danach ist die Verarbeitung dieser Daten zulässig, soweit sie erforderlich ist aus Gründen des öffentlichen Interesses im

Bereich der öffentlichen Gesundheit und des Infektionsschutzes, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren. Der Schutz vor Gesundheitsgefahren aufgrund von ansteckenden Infektionskrankheiten, wie unter anderem COVID-19, stellt ein solches legitimes öffentliches Interesse dar. Diesem Interesse wurde mit den durch die Gesundheitsämter umzusetzenden Regelungen im IfSG Rechnung getragen.

6.1.2 Elektronisches Meldeportal

Um den Arbeitgebern die gesetzlich vorgeschriebenen Meldungen an das jeweils zuständige Gesundheitsamt zu erleichtern, wurde im Saarland wie auch in vielen anderen Bundesländern ein Webportal eingerichtet, über das die Meldungen auf elektronischem Wege erfolgen konnten. Das hierbei federführende Gesundheitsministerium hat sich hinsichtlich der technischen Umsetzung des Meldeportals mit unserer Dienststelle abgestimmt, so dass die sichere Übertragung der Daten gewährleistet werden konnte. Daneben wurde diesseits darauf hingewiesen, den Grundsatz der Datenminimierung einzuhalten und nur diejenigen Angaben verpflichtend abzufragen, die für die Aufgabenerfüllung der Gesundheitsämter auch erforderlich sind.

Dennoch wurden in Einzelfällen durch die meldepflichtigen Stellen nicht nur die Beschäftigten gemeldet, bei denen der Impfstatus nicht nachgewiesen war, sondern es wurden teilweise auch Listen mit dem Impfstatus aller Mitarbeiter über das Meldeportal versandt. Um diesem Vorgehen entgegenzuwirken, haben wir empfohlen, einen ergänzenden Hinweis vor der Datenübermittlung im Portal aufzunehmen, in dem ausdrücklich noch einmal darauf hingewiesen wird, dass nur für die gesetzlich vorgeschriebenen Sachverhalte eine Meldung vorgenommen werden darf. Diese Empfehlung wurde in der Folge durch alle Gesundheitsämter im Saarland umgesetzt.

Im weiteren Verlauf wurde durch die zuständigen Stellen beschlossen, das Portal auch für Meldungen im Zusammenhang mit der in § 20 Abs. 8 IfSG normierten Masernimpfpflicht zu nutzen. Da hierbei die gleichen technischen Vorgaben berücksichtigt wurden wie bei der einrichtungsbezogenen Impfpflicht, bestanden aus datenschutzrechtlicher Sicht keine Einwände gegen das Vorhaben. Wir haben auch hier angeregt, vor der Eingabe von Daten im Portal einen Hinweis einzublenden, der klarstellt, in welchen Fällen eine Meldung durch die betroffenen Einrichtungen zu erfolgen hat, um ungerechtfertigte Meldungen und somit nicht erforderliche Datenübermittlungen zu vermeiden.

Fazit/ Empfehlung:

Die Übermittlung von Beschäftigtendaten von Arbeitgebern an das Gesundheitsamt zur Umsetzung der einrichtungsbezogenen Impfpflicht war durch die entsprechenden Vorschriften im IfSG legitimiert. Das hierfür im Saarland eingerichtete Meldeportal begegnete keinen datenschutzrechtlichen Bedenken, so dass einer erweiterten Nutzung im Kontext des Nachweises der Masernimpfung nichts entgegen steht.

6.2 Software SORMAS

SORMAS (Surveillance Outbreak Response Management Analysis System) ist eine federführend durch das Helmholtz-Zentrum für Infektionsforschung (HZI) entwickelte Software, die bei der Bekämpfung von Pandemien und Epidemien zum Einsatz kommt. In der für den öffentlichen Gesundheitsdienst in Deutschland angepassten Version (SORMAS-ÖGD) sollte sie nach dem Wunsch der Bund-Länder-Konferenz flächendeckend in den deutschen Gesundheitsämtern eingeführt werden, um diesen die Kontaktnachverfolgung im Rahmen der Corona-Pandemie zu erleichtern.

Im Saarland wurde SORMAS lediglich in einem Gesundheitsamt produktiv eingesetzt.

Im Rahmen eines Vor-Ort-Termins in diesem Gesundheitsamt wurde uns die Anwendung vorgeführt und deren Funktionsweise erläutert. Zu diesem Zeitpunkt war die Kontaktnachverfolgung durch die Gesundheitsämter allerdings bereits weitgehend eingestellt, so dass das System ausschließlich zur Erfassung der gemeldeten Infektionsfälle, zur Errechnung der voraussichtlichen Isolationsdauer und bei Bedarf zur Ausstellung einer Genesenenbescheinigung genutzt wurde. Wie uns das Gesundheitsamt mitgeteilt hat, sollte die Nutzung von SORMAS voraussichtlich Ende des Jahres 2022 eingestellt werden. Als Gründe hierfür wurden die zu geringe Verbreitung der Software unter den Gesundheitsämtern genannt sowie die Aussicht, dass ab dem Jahr 2023 keine kostenlose Nutzung mehr möglich sein werde. Eine Kontaktverfolgung sei zudem auch über das bereits seit mehreren Jahren genutzte Fachverfahren R 23 möglich.

6.3 Fehlversand einer Genesenenbescheinigung

In dem Termin mit dem Gesundheitsamt wurde eine bei hiesiger Dienststelle eingegangene Beschwerde wegen des Fehlversands einer Genesenenbescheinigung und eines nicht beantworteten Auskunftsersuchens nach Art. 15 DSGVO thematisiert.

Dabei wurde seitens des Gesundheitsamtes zunächst darauf hingewiesen, dass Genesenenbescheinigungen grundsätzlich an diejenige Anschrift versandt werden, welche die Teststelle, die das positive Testergebnis an die Behörde übermittelt, mitgeteilt hat. Im vorliegenden Fall war die übermittelte Adresse offenbar fehlerhaft, so dass ein Fehlverhalten des Gesundheitsamtes beim Versand nicht feststellbar war.

Weshalb das Auskunftsersuchen der von der Fehlversendung betroffenen Person zunächst nicht beantwortet wurde, konnte nicht abschließend geklärt werden.

Es wurde allerdings mitgeteilt, dass die Mitarbeiterinnen und Mitarbeiter der Behörde im Rahmen einer kurz zuvor erstellten Dienstanweisung für den Umgang mit Auskunftsersuchen und möglichen Datenpannen sowie für weitere datenschutzrechtliche Aspekte sensibilisiert und die internen Abläufe klargestellt werden.

Dies war von unserer Seite zu begrüßen, da die Implementierung eines Prozesses, der diese Abläufe innerhalb einer Organisation festlegt, eine notwendige organisatorische Maßnahme des Verantwortlichen darstellt, um eine korrekte und fristgerechte Umsetzung von Betroffenenrechten zu gewährleisten.

6.4 Anforderung von Einschulungsliste

Im Rahmen eines Beschwerdeverfahrens wurden wir darauf aufmerksam gemacht, dass ein Gesundheitsamt einmal im Jahr alle Kindergärten in seinem Zuständigkeitsbereich kontaktiert und dazu auffordert, eine Liste aller zur Einschulung anstehenden Kinder an das Gesundheitsamt zu übermitteln.

Hintergrund ist, dass die Gesundheitsämter gem. § 8 Abs. 3 Satz 1 Gesundheitsdienstgesetz (ÖGDG) die Aufgabe haben, vor der Einschulung flächendeckend ärztliche Einschulungsuntersuchungen durchzuführen. Die Untersuchungen haben den Zweck, gesundheitliche Einschränkungen der Schulfähigkeit oder die Teilnahme am Unterricht betreffende gesundheitliche Einschränkungen festzustellen und so einen eventuell vorliegenden Förderbedarf bei den zur Einschulung anstehenden Kindern zu erkennen.

Welche Daten in diesem Kontext erhoben werden dürfen, ergibt sich aus § 19 Abs. 5 Satz 1 ÖGDG. Aufgeführt sind dort Name, Vorname, Geburtstag und Anschrift des Kindes.

Im vorliegenden Fall hat das Gesundheitsamt die Kindergärten gebeten, die Kinder mit Förderbedarf in der zu übermittelnden Liste zu markieren. Diese Angabe stellt ein zusätzliches personenbezogenes Datum dar, welches der Gesetzgeber

nicht vorgesehen hat und für das als Gesundheitsdatum gem. Art. 9 DSGVO besondere Vorgaben gelten.

Das Gesundheitsamt hat die Erhebung des Datum damit begründet, dass durch die hohe Belastung der Behörde während der Corona-Pandemie die Einschulungsuntersuchungen nicht zeitnah bei allen einzuschulenden Kindern vorgenommen werden können. Mit der Abfrage des Förderbedarfs sollte sichergestellt werden, dass die betroffenen Kinder bevorzugt untersucht werden und nicht „durchs Raster fallen“.

Wenn auch die Begründung des Gesundheitsamtes angesichts der besonderen Situation nachvollziehbar war, bedarf es für diese Datenübermittlung jedoch einer rechtlichen Grundlage. Sofern diese Vorgehensweise dauerhaft beibehalten werden soll, etwa weil in naher Zukunft nicht mit einer geringeren Arbeitsbelastung der Gesundheitsämter zu rechnen ist, empfehlen wir eine Anpassung der einschlägigen Regelungen im ÖGDG.

Das Gesundheitsamt hat zugesagt, dies an die zuständige Fachaufsichtsbehörde heranzutragen.

6.5 Erhebung von Besucherdaten im Pflegeheim

Im Berichtszeitraum war das Unabhängige Datenschutzzentrum Saarland mit einer Beschwerde befasst, die die Erhebung von personenbezogenen Daten beim Besuch eines Pflegeheims betraf.

Der Beschwerdeführer bemängelte, dass man sich beim Betreten der Einrichtung in eine offene Liste eintragen müsse, welche auch personenbezogene Daten anderer Besucher enthielt. Er wies darauf hin, dass neben den Kontaktdaten (Name, Anschrift) auch Angaben zur Immunisierung und zum Vorliegen eines aktuellen Schnelltests mit Ergebnis gefordert würden. Darüber hinaus werde die Körpertemperatur der Besucher gemessen und dokumentiert. Der Beschwerdeführer bat um Prüfung der Rechtmäßigkeit dieser Datenverarbeitung.

Im Saarländischen COVID-19-Maßnahmengesetz (CovidMaßnG SL) waren zum Zeitpunkt der Beschwerde Vorgaben zur Kontaktnachverfolgung im Rahmen der Corona-Pandemie enthalten. Die Verpflichtung zur Erhebung von Kontaktdaten bestand danach unter anderem bei Besuchen in Alten- und Pflegeeinrichtungen (§ 5 Abs. 1 Nr. 7 CovidMaßnG SL in der bis zum 17.02.2022 gültigen Fassung).

Zudem ergab sich aus dem zum Zeitpunkt der Beschwerde gültigen „Landesrahmenkonzept zum Schutz vulnerabler Gruppen in Einrichtungen der Pflege“ die Pflicht, die Einhaltung der sogenannten „2G+“-Regel zu prüfen und zu dokumentieren, also einen Immunisierungsnachweis und ein negatives Testergebnis zu verlangen.

Die Erhebung der in der Liste vorgesehenen Besucherdaten war demnach dem Grunde nach zulässig. Allerdings muss die jeweilige Einrichtung, die für die Datenverarbeitung verantwortlich ist, technische und organisatorische Maßnahmen (TOM) treffen, um die personenbezogenen Daten der Besucher zu schützen. Diese Verpflichtung ergibt sich insbesondere aus Art. 32 i. V. m. Art. 5 Abs. 1 lit. f DSGVO. Hiervon ist umfasst, dass die verarbeiteten Daten nicht für unberechtigte Dritte einsehbar sein dürfen. Eine offene Liste, in die sich mehrere Besucher hintereinander eigenhändig eintragen müssen, erfüllt diese Vorgabe nicht, da so die Daten der übrigen Besucher zur Kenntnis genommen werden können. Das offene Auslegen bzw. Vorlegen der Liste mit den Besucherdaten stellt insofern eine Datenübermittlung an Dritte dar, für die keine Rechtsgrundlage existiert.

Bezüglich der Messung der Körpertemperatur der Besucher verwies das Pflegeheim zunächst darauf, dass diese im Landesrahmenkonzept vorgesehen sei. So hieß es darin unter Nr. 2.3.3, dass durch die jeweilige Einrichtung ein Schutz- und Hygienekonzept zu erstellen sei, das unter anderem Maßnahmen zur Temperaturmessung der Besucher beinhaltet.

Ob hiermit lediglich eine Messung oder auch die Dokumentation des Ergebnisses gemeint war, ließ das Landesrahmenkonzept allerdings offen.

Das Pflegeheim hat im Zuge des Beschwerdeverfahrens die Praxis der Datenerhebung angepasst und ist dazu übergegangen, die Daten der Besucher auf jeweils gesonderten Einzelblättern zu erheben. Zudem wurde die Dokumentation der Körpertemperatur gestoppt.

Somit konnte in der Folge von einem datenschutzkonformen Zustand ausgegangen werden.

Fazit/ Empfehlung:

Bei der Verarbeitung personenbezogener Daten kommt es nicht nur darauf an, dass eine legitimierende Rechtsgrundlage existiert, sondern auch darauf, dass die Daten durch geeignete technische und organisatorische Maßnahmen vor dem Zugriff unberechtigter Dritter geschützt werden. Nur so kann eine rechtmäßige Verarbeitung im Sinne der DSGVO erfolgen.

VII.

Schule und Hochschule

7 Schule und Hochschule

7.1 Datenschutz im Bildungsbereich

Damit bereits bei dem Aufbau informationstechnischer Systeme, in denen personenbezogene Daten verarbeitet werden, zu einem frühestmöglichen Zeitpunkt datenschutzrechtliche Erfordernisse berücksichtigt werden können, sieht § 19 Abs. 2 Satz 2 Saarländisches Datenschutzgesetz (SDSG) vor, dass die Landesbeauftragte für Datenschutz und Informationsfreiheit schon bei den entsprechenden Planungen des Landes, der Gemeinden und Gemeindeverbände sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts rechtzeitig zu unterrichten ist. Durch eine möglichst frühzeitige Unterrichtung der Aufsichtsbehörde kann vermieden werden, dass Aufwendungen für den Aufbau eines IT-Systems getätigt werden, die sich später als nicht datenschutzkonform einsetzbar erweisen.

Leider wird diese frühzeitige Einbindung unserer Behörde durch die verantwortlichen Stellen häufig – bewusst oder unbewusst – versäumt.

In den vergangenen Jahren konnten wir stets von einer guten Zusammenarbeit mit dem Ministerium für Bildung und Kultur berichten. So wurden wir bspw. bei der Einführung der Profil-Plattform, dem Vorgänger der Online-Schule-Saar (OSS), frühzeitig eingebunden und konnten datenschutzrechtliche Aspekte in die Entwicklung der Plattform einfließen lassen, die auch bei der Weiterentwicklung zur OSS Bestand hatten. Im Berichtszeitraum haben wir jedoch mitunter erst durch Berichterstattung in den Medien oder durch Anfragen von Betroffenen von datenschutzrelevanten Projekten erfahren, die unmittelbar vor der Einführung stehen sollten.

7.1.1 OSS-Messenger

Ende März informierte das Ministerium für Bildung und Kultur die Presse über einen für April geplanten Einsatz eines Messengerdienstes in der Online-Schule Saarland (OSS). Nach den veröffentlichten Angaben des Ministeriums handele sich hierbei um einen modernen, sicheren und datenschutzkonformen Messengerdienst als Alternative zu den herkömmlichen Diensten, der die sogenannte „Ranzenpost“ in den Schulen ablösen solle. Die Presseberichterstattung führte zu einer Reihe von Anfragen an unsere Behörde, im Rahmen derer sich Eltern die datenschutzrechtliche Unbedenklichkeit dieses Messengerdienstes bestätigen lassen wollten. Da uns jedoch keinerlei prüffähigen Informationen vorlagen und auch in der Folge bis zum Zeitpunkt der Erstellung des vorliegenden Berichts trotz mehrfacher Anforderungen die für unsere Aufgabenerfüllung erforderlichen Unterlagen nicht durch das Ministerium für Bildung und Kultur zur Verfügung gestellt wurden, können wir bislang keine datenschutzrechtliche Bewertung zu dem Messengereinsatz abgeben. Es wurde uns seitens des Ministeriums lediglich mitgeteilt, dass der Einsatz des Messengerdienstes rechtlich auf einer freiwilligen Einwilligung der Nutzer basieren würde und als Alternative nach wie vor die „Ranzenpost“ bemüht werden könne, um allen Betroffenen Informationen zur Verfügung stellen zu können.

Neben der hier nicht erfolgten frühzeitigen Beteiligung unserer Behörde nach 19 Abs. 2 Satz 2 SDSG kam das Ministerium für Bildung und Kultur damit zudem den Vorgaben des § 20 Abs. 4 SDSG nicht nach, wonach öffentliche Stellen die Landesbeauftragte für Datenschutz und Informationsfreiheit und ihre Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen und insbesondere Auskunft auf Fragen zu erteilen sowie Einsicht in alle Vorgänge und Aufzeichnungen zu gewähren haben, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen.

7.1.2 Digitales Schulzeugnis

Kenntnis über die Planungen des Ministeriums, im Jahr 2024 die ersten digitalen Schulzeugnisse im Saarland auszustellen, erhielten wir gleichfalls erst durch die Medien. Bei dem digitalen Schulzeugnis handelt es sich nach der entsprechenden Berichterstattung um eine Verwaltungsleistung nach dem Onlinezugangsgesetz (OZG), die durch das Land Sachsen-Anhalt gemeinsam mit der Bundesdruckerei entwickelt werden sollte.

Der Umstand, dass im Rahmen der OZG-Umsetzung die von einem Bundesland zentral entwickelten digitalen Leistungen von einem anderen Land nachgenutzt werden können (sog. EfA-Prinzip), entbindet bislang das nachnutzende Land jedoch nicht von seiner datenschutzrechtlichen Verantwortlichkeit im Sinne des § 4 Nr. 7 DSGVO. Dementsprechend haben wir das Ministerium auch hier gebeten, uns die für eine datenschutzrechtliche Prüfung erforderlichen Unterlagen zukommen zu lassen. Trotz mehrfacher Erinnerungen haben wir jedoch im Berichtszeitraum hierzu keine prüffähigen Unterlagen erhalten. Zwischenzeitlich konnten wir jedoch den Medien entnehmen, dass die Projektentwicklung durch Sachsen-Anhalt gestoppt wurde und überarbeitet werden soll. Daher dürften auch die Pläne für das digitale Schulzeugnis im Saarland derzeit nicht fortgeführt werden. Wir gehen aber davon aus, dass bei einem Neustart des Projekts eine zeitnahe Beteiligung unserer Dienststelle erfolgen wird.

7.1.3 Rechtliche Anpassungen zur Umsetzung der DSGVO

Nach einer zweijährigen Übergangsfrist ist die DSGVO seit dem 25. Mai 2018 verbindlich in allen EU-Mitgliedstaaten anzuwenden. Die Übergangsfrist von 2016 bis zum Geltungsbeginn im Jahre 2018 sollte durch die Verantwortlichen und Behörden dazu genutzt werden, sich auf die Vorgaben der DSGVO vorzubereiten und entsprechend notwendige Änderungen zu veranlassen. Auch der saarländische

Gesetzgeber musste daher bestehende datenschutzrechtliche Vorschriften auf die Vereinbarkeit mit der DSGVO hin überprüfen und soweit erforderlich bereinigen. Dies ist durch eine Neufassung des Saarländischen Datenschutzgesetzes sowie durch Anpassungen in einer Vielzahl von Fachgesetzen erfolgt. Für den Bildungsbereich fehlen allerdings noch immer dringend notwendige Anpassungen in den Schulgesetzen oder den darauf beruhenden Verordnungen. Um die nötige Rechtsklarheit bei der Verarbeitung personenbezogener Daten im Bereich der Schulen sicherzustellen, ist eine zeitnahe Anpassung der datenschutzrelevanten Rechtsvorschriften dringend erforderlich.

7.1.4 Rechtssichere Begleitung der Lehrkräfte bei der Umsetzung der Digitalisierung

Ungeachtet der Rechtsunsicherheiten aufgrund der noch nicht erfolgten Anpassungen der schulrechtlichen Vorschriften an die europäischen Vorgaben, wirft auch der Einsatz digitaler Medien im Unterricht nach wie vor zahlreiche datenschutzrechtliche Fragen für Lehrkräfte, Eltern sowie Schülerinnen und Schüler auf: Ist die Nutzung von Tablets, Apps, der Online-Schule-Saar oder von Videokonferenzsystemen verpflichtend? Welche Apps darf ich auf mein zu schulischen Zwecken zur Verfügung gestelltes Tablet laden? Darf ich Daten der Schülerinnen und Schüler in der App oder im Internet hochladen? Was darf ich wo speichern und was muss gelöscht werden? Diese und ähnliche Fragen sind bislang rechtlich noch nicht geklärt.

Lehrkräfte dürfen jedoch nicht länger im Unklaren gelassen werden, ob ihr Umgang mit den digitalen Medien auch datenschutzrechtlich zulässig ist. Hilfreich wäre es in diesem Zusammenhang, wenn den Schulen bereits bei der Auswahl datenschutzkonformer digitaler Werkzeuge Vorgaben gemacht bzw. zumindest Hilfestellungen gegeben würde. Daneben sollten den Schulen und ihren Lehrkräften einheitliche Handlungsanleitungen zur Verfügung gestellt werden, die ihnen

Schulen und Lehrkräften Handlungssicherheit geben und eine rechtssichere Datenverarbeitung im Einzelfall gewährleisten. Gerne unterstützt unsere Behörde bei der Erarbeitung derartiger Anleitungen.

7.1.5 Datenschutzbeauftragte für saarländische Schulen

Gem. Art. 37 Abs. 1 lit. a DSGVO haben alle Behörden und öffentlichen Stellen und damit auch jede saarländische Schule Datenschutzbeauftragte zu benennen. Abs. 3 der Norm sieht für Behörden und öffentliche Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe auch die Möglichkeit der Benennung gemeinsamer Datenschutzbeauftragter für mehrere Behörden vor. Von dieser gesetzlichen Möglichkeit hat das Ministerium für Bildung und Kultur Gebrauch gemacht und sowohl für das Ministerium selbst als auch für alle Schulen des Landes eine Datenschutzbeauftragte und einen Stellvertreter als behördliche Datenschutzbeauftragte benannt, die die in Art. 39 DSGVO aufgeführten gesetzlichen Aufgaben einer/s Datenschutzbeauftragten wahrnehmen sollen. Zu diesen Aufgaben zählen unter anderem die Überwachung der Einhaltung datenschutzrechtlicher Vorgaben in der Behörde, die Beratung der Behördenleitung und der Beschäftigten in datenschutzrechtlichen Fragen sowie Schulungsmaßnahmen zur Sensibilisierung bei der Verarbeitung personenbezogener Daten. Dabei ist nach Art. 38 Abs. 1 DSGVO von dem Verantwortlichen sicherzustellen, dass die oder der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden ist. Daneben dienen die Datenschutzbeauftragten auch als Anlaufstelle für die Datenschutzaufsichtsbehörde, mit der sie gleichfalls zusammenarbeiten sollen. Zur Erfüllung des Aufgabenkatalogs hat die verantwortliche Stelle nach Art. 38 Abs. 2 DSGVO den behördlichen Datenschutzbeauftragten die erforderlichen

personellen und sachlichen Ressourcen zur Verfügung zu stellen.

Angesichts der großen Zahl der Daten verarbeitenden Stellen im Schulbereich[28], des Umfangs der im schulischen Kontext verarbeiteten personenbezogenen Daten und der – gerade angesichts der zunehmenden Nutzung digitaler Anwendungen – steigenden Komplexität der Verarbeitungsprozesse, kann nicht davon ausgegangen werden, dass eine einzelne Person einschließlich ihrer Vertretung in der Lage ist, an allen saarländischen Schulen sowie dem Ministerium alle ihr gesetzlich zugewiesenen Aufgaben zu erfüllen. Wir weisen daher bereits seit einigen Jahren nachdrücklich darauf hin, dass zur Gewährleistung einer sachgerechten Aufgabenerfüllung die Zahl der für den Schulbereich zuständigen Datenschutzbeauftragten deutlich erhöht werden muss. Zumindest für alle Schulen in einem Landkreis bzw. im Regionalverband sollten jeweils eigene Datenschutzbeauftragte bestellt werden, die – gegebenenfalls mit einem Team – als mit den jeweiligen Verhältnissen vor Ort vertraute Ansprechpersonen für betroffene Personen und andere Stellen leicht erreichbar sind.

Fazit/Empfehlung:

Angesichts der vielfältigen datenschutzrechtlichen Herausforderungen bei der Verarbeitung personenbezogener Daten im Schulbereich, ist das Ministerium für Bildung und Kultur gefordert, zeitnah die notwendigen Schritte einzuleiten, um sowohl den Lehrkräften als auch den Schülerinnen und Schülern sowie deren Eltern Rechtssicherheit zu geben.

[28] vgl. Kurzinformationen Statistisches Amt Saarland, 2022, S. 5: mehr als 500 allgemeinbildende und berufliche Schulen

7.2 Klassentreffen mit datenschutzrechtlichen Hindernissen

Bei Klassentreffen schwelgt man in Erinnerungen und lacht über Schulstreiche und Fotos aus alten Zeiten. Um zur besonderen Belustigung während eines solchen Klassentreffens zu sorgen, bat ein ehemaliger Schüler seine damalige Schule um Herausgabe der Klassenbücher seiner Klasse, um die darin getätigten Eintragungen bei der Zusammenkunft vorlesen zu können.

Neben den Inhalten des Unterrichts werden in den Klassenbüchern i. d. R. auch die Fehlzeiten der Schülerinnen und Schüler sowie besondere Vorkommnisse, wie deren Fehlverhalten in der Schule, dokumentiert.

Nachdem die Schule die Herausgabe der Klassenbücher unter Berufung auf den Datenschutz verweigert hatte, wandte der ehemalige Schüler sich mit einer Beschwerde an unsere Behörde. Entgegen seiner Auffassung hatte sich die Schule jedoch datenschutzkonform verhalten. Abgesehen davon, dass die in den Klassenbüchern enthaltenen Informationen für einige Teilnehmer des Klassentreffens möglicherweise kompromittierend gewesen wären, existiert keine Rechtsgrundlage, die die Übermittlung dieser Daten zu dem gewünschten Zweck legitimieren könnte.

Darüber hinaus sind Klassenbücher gem. § 6 Abs. 3 Nr. 4 der Verordnung über die Verarbeitung personenbezogener Daten in Schulen (PersDatSchulV SL) spätestens fünf Jahre nach Verlassen der Schulklasse von der Schule zu vernichten. Allerdings sieht diese Verordnung in § 4 Abs. 9 Satz 3 auch vor, dass zur Vorbereitung von Klassentreffen die Übermittlung der Anschriften der ehemaligen Schüler/-innen zulässig ist, soweit sich der Empfänger der Daten schriftlich dazu verpflichtet, die Daten zu keinem anderen Zweck zu verwenden.

Der Beschwerdeführer musste sich daher damit begnügen, seine Streiche aus der Schule aus seiner Erinnerung heraus zu

zitieren und konnte hierfür nicht die Klassenbücher der Schule heranziehen. Im Gegenzug erhielt er jedoch die Möglichkeit, auch „verschollene“ Mitschüler/-innen zu kontaktieren und zum Klassentreffen einzuladen.

Fazit/Empfehlung:

Die Herausgabe von Klassenbüchern zur Belustigung während eines Klassentreffens ist mangels entsprechender Rechtsgrundlage regelmäßig unzulässig. Die Herausgabe der Adressdaten ehemaliger Mitschüler/-innen zur Planung eines Klassentreffens ist unter den oben genannten Aspekten zulässig.

VIII.

Beschäftigtendatenschutz

8 Beschäftigtendatenschutz

8.1 GPS-Tracking mit Gewinnanreiz

Bereits im 27. Tätigkeitsbericht 2017/2018 (8.4, S. 82) sowie im 29. Tätigkeitsbericht 2020 (3.23, S.114) haben wir über die datenschutzrechtliche Bewertung von GPS-Tracking von Firmenfahrzeugen berichtet und darauf hingewiesen, dass der Einsatz solcher Systeme nur unter restriktiver Auslegung der für den Beschäftigtendatenschutz relevanten Norm des § 26 Bundesdatenschutzgesetz (BDSG) zulässig sein kann.

Im Rahmen einer bei unserer Behörde eingereichten Beschwerde wurde mitgeteilt, dass die gesamte Fahrzeugflotte eines Unternehmens mit GPS-Trackingsystemen ausgestattet wurde, ohne die Mitarbeitenden zuvor über den Umfang der damit verbundenen Datenverarbeitung hinreichend zu informieren. Zudem sollte als Anreiz für ein effizientes Fahrverhalten dem „sparsamsten“ Firmenbeschäftigten nach Auswertung der Fahr- und Verbrauchsdaten monatlich eine Belohnung in Höhe von 100 Euro ausgezahlt werden.

Der datenschutzrechtliche Aspekt dieser Maßnahme wurde durch den Arbeitgeber gänzlich vernachlässigt. Erst durch die Konfrontation mit der datenschutzrechtlichen Problematik durch unsere Behörde wurde dem Arbeitgeber bewusst, dass die Maßnahme wegen eines permanenten Überwachungsdrucks der Beschäftigten unzulässig sein könnte.

Auch war ihm nicht klar, dass durch privates „Zutanken“ das Ergebnis der Auswertung durch die Beschäftigten manipuliert werden könnte.

Im Ergebnis wurde mangels vorhandenem Betriebsrat in Zusammenarbeit mit unserer Behörde eine Verpflichtungserklärung durch den Arbeitgeber erstellt, wonach die GPS-Daten nicht zur Leistungs- und Verhaltenskontrolle der Mitarbeiter genutzt werden, keine Speicherung der Daten

erfolgt und diese nur zum sogenannten Live-Tracking genutzt werden, um das Fahrzeug bei einem Unfall oder Diebstahl orten zu können beziehungsweise bei Ausfall eines Fahrzeuges einen in der Nähe befindlichen Beschäftigten zwecks Hilfe/Unterstützung informieren zu können.

Von einem Wettbewerb, wer am sparsamsten fährt, wurde aufgrund der von uns vorgetragenen Bedenken verzichtet und die Beschäftigten in verständlicher und transparenter Form über das GPS-Tracking in der Firmenflotte informiert.

Fazit/Empfehlung:

Bei der Einführung von GPS-Trackingsystemen sollte sich der Arbeitgeber im Vorfeld über die datenschutzrechtliche Zulässigkeit der Maßnahme und die Zwecke, die mit der Maßnahme verfolgt werden, befassen und diese im Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DSGVO dokumentieren. Die frühzeitige Information und Beteiligung der Beschäftigten führt in der Regel zu einer größeren Akzeptanz solcher Maßnahmen.

8.2 Zweckbindung auch bei der Arbeitszeitkontrolle

Mitunter werden Beschäftigte eines Unternehmens zur Verrichtung spezieller Aufgaben vorübergehend in einem anderen Unternehmen als sogenannte Fremdfirmenmitarbeiter eingesetzt. Hierbei müssen die Fremdfirmenmitarbeiter bei der Verrichtung der ihnen übertragenen Arbeiten auch den Weisungen des auftraggebenden Unternehmens Folge leisten. Die Personalverantwortung sowie die Lohn- und Gehaltszahlung verbleiben bei ihrem Arbeitgeber.

In einem uns zur Kenntnis gebrachten Sachverhalt wurden alle Fremdfirmenmitarbeiter durch das auftraggebende Unternehmen verpflichtet, beim Betreten des Geländes einen Transponder an der Pforte zu betätigen, um die aktuell auf dem Gelände befindlichen Personen zu erfassen, damit im Falle

eines Notfalls eruiert werden könne, wer sich noch auf dem Gelände befindet. Die Verpflichtung zur Erfassung sowie der genaue Zweck dieser Erfassung wurden in den Verträgen zwischen den Fremdfirmen und dem auftraggebenden Unternehmen niedergeschrieben. Darüber hinaus wurde vertraglich vereinbart, ein sogenanntes Bautagebuch zu führen, in dem die Arbeitszeiten der Fremdfirmen und ihrer Beschäftigten dokumentiert und zu Abrechnungszwecken sowie zur Zeiterfassung der Beschäftigten genutzt werden sollten. Die beim Betreten und Verlassen des Betriebsgeländes erfassten Daten wurden mehr als sechs Monate im Unternehmen aufbewahrt.

Zur Klärung von aufgetretenen Unregelmäßigkeiten forderte der Arbeitgeber eines Fremdfirmenmitarbeiters vom auftraggebenden Unternehmen die an der Pforte beim Betreten und Verlassen des Geländes erfassten Daten des betroffenen Mitarbeiters an, um diese mit den ihm vorliegenden Zeiterfassungsdaten abgleichen zu können. Der betroffene Mitarbeiter bemängelte bei unserer Behörde die erfolgte Zurverfügungstellung dieser Daten durch das auftraggebende Unternehmen.

In Art. 5 Abs. 1 lit. b DSGVO wird der sogenannte Grundsatz der Zweckbindung normiert. Dieser besagt, dass personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen.

Übertragen auf den vorliegenden Sachverhalt durften daher die Daten, die an der Pforte zur Anwesenheitsfeststellung in einem Notfall erhoben worden sind, auch nur zu diesem Zweck genutzt und verarbeitet werden. Eine Übermittlung dieser Daten an den Arbeitgeber des Fremdfirmenmitarbeiters für Zwecke der Kontrolle der Anwesenheitszeiten stellt eine unzulässige Datenverarbeitung dar, da sie ohne legitimierende Rechtsgrundlage erfolgt ist. Auch die Speicherung dieser Daten

über einen Zeitraum von mehr als sechs Monaten hinweg stellte eine Datenschutzverletzung dar. Personenbezogene Daten müssen, soweit keine speziellen Aufbewahrungspflichten entgegenstehen, gelöscht werden, sobald sie für die Zwecke, für die sie erhoben oder verarbeitet wurden, nicht mehr erforderlich sind (Art. 5 Abs. 1 lit. e DSGVO). Zur Zweckerfüllung der Feststellung der Anwesenheit in einem Notfall wären die Daten spätestens 24 Stunden nach Verlassen des Geländes zu löschen gewesen. Für die Evakuierung des Geländes in einem Notfall und den Nachweis, dass alle Personen das Gelände verlassen haben, ist es nicht mehr erforderlich zu wissen, wer sich vor einem mehr als 24 Stunden zurückliegenden Zeitraum auf dem Gelände befunden hat.

Im vorliegenden Sachverhalt haben wir gegenüber dem auftraggebenden Unternehmen, das die Daten ohne eine erforderliche Rechtsgrundlage an den Arbeitgeber des Fremdfirmenmitarbeiters übermittelt hat, von unseren Abhilfebefugnissen nach Art. 58 Abs. 2 DSGVO Gebrauch gemacht. Das Unternehmen akzeptierte unsere Maßnahmen und stellte seine Systeme datenschutzkonform um.

Fazit/Empfehlung:

Die Zwecke, zu denen personenbezogene Daten verarbeitet werden, müssen im Vorfeld der Verarbeitung im Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) eindeutig und transparent festgehalten werden. Die Verwendung dieser Daten für andere Zwecke kann zu einer unrechtmäßigen Datenverarbeitung führen, die geahndet werden kann.

IX.

Wirtschaft

9 Wirtschaft

9.1 Verarbeitung der Privatanschrift von gesetzlichen Betreuern durch Kreditinstitute

Im Berichtszeitraum wurden wir mit der Frage befasst, inwieweit Banken dazu befugt sind, die Wohnanschrift von gesetzlichen Betreuern zu verarbeiten, wenn diese für die betreute Person gegenüber der kontoführenden Bank tätig werden wollen. Aus diversen Gründen können Betreuer ein Interesse daran haben, dass ihre private Wohnanschrift der betreuten Person nicht bekannt wird, bspw. wenn diese bereits straffällig wurde und sich auch für den Betreuer eine spezifische Viktimisierungsgefahr ergibt. Oft ist es daher der Wunsch der Betreuer, bei der Bank lediglich ihre geschäftliche Anschrift anzugeben.

Eine Verarbeitung personenbezogener Daten ist nach Art. 6 Abs. 1 Datenschutz-Grundverordnung (DSGVO) dann rechtmäßig, wenn eine der dort genannten Legitimationsgrundlagen einschlägig ist. Nach Art. 6 Abs. 1 lit. c DSGVO ist eine Verarbeitung personenbezogener Daten insbesondere dann zulässig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Eine solche rechtliche Verpflichtung folgt für das Kreditinstitut bspw. aus § 11 Abs. 4 Nr. 1 lit. e Geldwäschegesetz (GwG). Danach sind Kreditinstitute i. S. d. § 2 Abs. 1 Nr. 1 GwG dazu verpflichtet, in Bezug auf Vertragspartner und gegebenenfalls für diese auftretende Personen zum Zweck der Identifizierung diverse Angaben zu erheben, darunter bei natürlichen Personen auch eine Wohnanschrift.

Laut Auslegungshilfe der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zählen zu diesen für den Vertragspartner auftretenden Personen insbesondere auch Betreuer des Vertragspartners.[29] Vor diesem Hintergrund ist

[29] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Auslegungs- und

das Kreditinstitut grundsätzlich verpflichtet und zugleich berechtigt, die Wohnanschrift eines Betreuers bzw. einer Betreuerin auf Grundlage des Art. 6 Abs. 1 lit. c DSGVO i. V. m. § 11 Abs. 4 Nr. 1 lit. e GwG zu erheben. Eine Ausnahme von dieser Verpflichtung sieht § 11 Abs. 4 Nr. 1 lit. e 2. Alt GwG nur dann vor, wenn die natürliche Person keinen festen Wohnsitz mit rechtmäßigem Aufenthalt innerhalb der Europäischen Union hat. In diesem seltenen Ausnahmefall kann es ausreichend sein, die postalische Anschrift zu erheben, unter der die gegenüber dem Verpflichteten auftretende Person erreichbar ist.

Von datenschutzrechtlicher Relevanz sind in dem vorliegenden Zusammenhang aber insbesondere die vereinfachten Sorgfaltspflichten aus § 14 GwG. Danach sind die Kreditinstitute von einigen Pflichten entbunden bzw. wird das Ausmaß dieser Pflichten reduziert, wenn nur ein geringes Risiko der Geldwäsche und Terrorismusfinanzierung besteht. In diesem Fall kann das Kreditinstitut die Identifizierung der Person auf Grundlage sonstiger Dokumente durchführen, die von einer glaubwürdigen und unabhängigen Quelle stammen und die für die Überprüfung geeignet sind (§ 14 Abs. 2 Nr. 2 GwG). Ausweislich des Wortlautes des § 14 Abs. 2 GwG steht die Anwendung der vereinfachten Sorgfaltspflichten grundsätzlich im Ermessen des Kreditinstituts. Bei der Ausübung dieses Ermessens muss das Kreditinstitut einen risikoorientierten Ansatz verfolgen und abwägen, inwieweit es tatsächlich erforderlich ist, für Zwecke der Vermeidung von Geldwäsche und Terrorismusfinanzierung die Sorgfaltspflichten uneingeschränkt zu erfüllen.

Im Rahmen der vorzunehmenden Abwägung muss das Kreditinstitut aber auch den Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c DSGVO berücksichtigen. Kommt das Kreditinstitut unter Berücksichtigung des Grundsatzes der

---

Anwendungshinweise zum Geldwäschegesetz (AuA) i. d. F. vom 28.10.2021, S. 33.

Datenminimierung zu dem Ergebnis, dass für Zwecke der Vermeidung von Geldwäsche und Terrorismusfinanzierung die Erhebung einzelner Informationen – wie etwa der Wohnanschrift – nicht unbedingt erforderlich ist, ist unter Anwendung der vereinfachten Sorgfaltspflichten nach § 14 GwG auf die Erhebung der privaten Wohnanschrift zu verzichten und lediglich die Anschrift der Betreuungseinrichtung bzw. der Geschäftsanschrift des Betreuers unter Vorlage des Dienstausweises zu erheben.

Kreditinstitute müssen daher nicht nur im Hinblick auf § 10 Abs. 2 Satz 3 GwG ihre Risikobeurteilung dokumentieren, sondern auch der Datenschutzaufsichtsbehörde substantiiert darlegen können, aus welchen Gründen eine Erhebung von zusätzlichen Informationen erfolgt, obwohl ein Verzicht im Rahmen der vereinfachten Sorgfaltspflichten grundsätzlich in Betracht käme. Insbesondere im Beschwerdefall ist eine entsprechende Abwägung und deren Dokumentation der Datenschutzaufsichtsbehörde vorzulegen.

Fazit/ Empfehlung:

Kreditinstitute müssen bei der Anwendung vereinfachter Sorgfaltspflichten den datenschutzrechtlichen Grundsatz der Datenminimierung berücksichtigen. Die durch die Kreditinstitute vorzunehmende Abwägung ist zu dokumentieren und der Aufsichtsbehörde auf Verlangen vorzulegen.

9.2 Unangenehme Überraschung beim Fahrradkauf

Im Rahmen einer Beschwerde trug der Beschwerdeführer vor, über einen Onlineshop ein Fahrrad erworben zu haben, das sich seiner Ansicht nach als mängelbehaftet herausstellte und daher retourniert werden sollte. Als eine Einigung mit dem Shop-Betreiber nicht möglich war, veräußerte der Beschwerdeführer das Fahrrad weiter, verschwieg allerdings gegenüber dem Erwerber die vermeintlichen Mängel des

Fahrrads. Nachdem der getäuschte Käufer seinerseits Mängel an dem Fahrrad entdeckte, setzte sich dieser, da er die Rechnung samt Kundennummer von dem Beschwerdeführer erhalten hatte, unter Angabe der Kundennummer mit dem Onlineshop-Betreiber in Verbindung. Dieser wiederum stellte dem getäuschten Erwerber die gesamte mit dem Beschwerdeführer geführte Korrespondenz zur Verfügung. Anhand dieser konnte der Erwerber erkennen, dass ihm der Beschwerdeführer Mängel an dem Fahrrad verschwiegen hatte und konfrontierte diesen mit seinen Feststellungen. Der Beschwerdeführer sah sich durch die Offenlegung des Schriftverkehrs in seinen Rechten beeinträchtigt und bat die Aufsichtsbehörde um datenschutzrechtliche Prüfung der Angelegenheit.

Der Shop-Betreiber schilderte diesbezüglich, dass die Unternehmenspraxis bei Anfragen zu getätigten Einkäufen lediglich einen Abgleich der Kundennummer vorsehe, so dass es nicht auszuschließen sei, dass Dritte in Kenntnis der jeweiligen Kundennummer auf den kundenspezifischen Schriftverkehr zugreifen können. Dies hat vorliegend dazu geführt, dass dem getäuschten Erwerber ohne weiteren Sachvortrag und ohne weitere Prüfung durch den Shop-Betreiber personenbezogene Daten des Beschwerdeführers übermittelt wurden. Das Unternehmen änderte nach einem Hinweis unserer Behörde den Geschäftsprozess unter anderem dergestalt, dass künftig ein Abgleich zwischen der im Kundenaccount hinterlegten und der anfragenden E-Mail-Adresse vorgenommen wird.

Ungeachtet dessen wäre die Übermittlung des Schriftverkehrs an den getäuschten Erwerber unter bestimmten Voraussetzungen datenschutzrechtlich zulässig gewesen. So können im Rahmen einer vertraglichen 6 Abs. 4 in Verbindung mit Art. 6 Abs. 1 lit. f DSGVO zur Geltendmachung von Rechtsansprüchen an Dritte übermittelt werden.

Der getäuschte Erwerber hätte vorliegend gegenüber dem Onlineshop-Betreiber ein berechtigtes Interesse an der Kenntnis des Schriftverkehrs geltend machen können, um zivilrechtliche Ansprüche mit Blick auf die ihm verschwiegenen Mängel geltend machen zu können.

Fazit/ Empfehlung:

Der Verantwortliche hat durch technische und organisatorische Maßnahmen wie bspw. den Abgleich von Identifizierungsmerkmalen dafür Sorge zu tragen, dass personenbezogene Daten Dritten nicht anlasslos offenbart werden. Zur Geltendmachung zivilrechtlicher Ansprüche kann eine Datenübermittlung an Dritte unter bestimmten Voraussetzungen datenschutzrechtlich zulässig erfolgen.

9.3 Bildaufnahme als Voraussetzung für die Kletterhallennutzung

Einem begeisterten Klettersportler wurde der Zutritt zu einer Kletterhalle verwehrt, als er sich bei der Anmeldung weigerte, eine Bildaufnahme von sich anfertigen zu lassen. Darüber hinaus sollte er bei der Anmeldung weitere Angaben wie Name, Anschrift und Alter machen. Diese Informationen würden laut Aussage einer Servicemitarbeiterin der Verhinderung von Betrugsdelikten im Zusammenhang mit Monats- und Jahreskarten dienen. Für den Beschwerdeführer war dies umso befremdlicher, da er nicht im Besitz einer Dauerkarte war, sondern die Kletterhalle lediglich als Tagesbesucher aufsuchte.

Auf Nachfrage teilte die Hallenbetreiberin mit, dass eine Bildaufnahme ausschließlich Abonnenten auf freiwilliger Basis angeboten würde, um auch ohne Vorlage des Personalausweises Zugang zur Kletterhalle zu erhalten. Lediglich aufgrund eines Missverständnisses habe das Servicepersonal gegenüber dem Beschwerdeführer auf der Anfertigung der Bildaufnahme als Zutrittsvoraussetzung zur Kletterhallennutzung bestanden.

Die Erhebung und anschließende softwareseitige Speicherung von Namen und Geburtsdaten bei Nicht-Abonnenten erfolge laut Hallenbetreiberin zur Gewährleistung einer effektiven Zugangskontrolle. Das Alter der Kunden spiele bei der Ermittlung des Eintrittspreises, bei der Sicherheit der Hallennutzer und der Einhaltung des Jugendschutzes eine zentrale Rolle. Bei Unfällen, Bränden u.ä. sei es daneben erforderlich, dass die Hallenbetreiberin den Rettungskräften mitteilen können müsse, wer sich konkret in der Halle befinde. Die erhobenen Daten würden schließlich am gleichen Tage wieder gelöscht.

Im Hinblick auf die Freiwilligkeit bei der Anfertigung von Bildaufnahmen waren die Ausführungen der Hallenbetreiberin aus datenschutzrechtlicher Sicht nicht zu beanstanden. So kommt als Rechtsgrundlage für eine solche Datenverarbeitung ausschließlich die Einwilligung des Betroffenen im Sinne des Art. 4 Nr. 11 in Verbindung mit Art. 6 Abs. 1 lit. a und Art. 7 Datenschutz-Grundverordnung (DSGVO) in Betracht. Demgegenüber wäre die Bildaufnahme nicht im Sinne des Art. 6 Abs. 1 lit. b DSGVO zur Durchführung des Nutzungsvertrages mit Abonnenten erforderlich, da diese sich auch mit ihrem Personalausweis als berechtigte Nutzer legitimieren können.

Im Hinblick auf die Nutzung der Kletterhalle durch Nicht-Abonnenten ließ die Anfertigung von Bildaufnahmen keinerlei nachvollziehbaren Zweck erkennen. Vor diesem Hintergrund und zur Vermeidung künftiger unzulässiger Bildanfertigungen sicherte die Hallenbetreiberin zu, das eigene Servicepersonal entsprechend zu schulen und dafür Sorge zu tragen, dass künftig keine Bildaufnahmen von Nicht-Abonnenten angefertigt werden.

Die Erhebung und Speicherung von Namen und Geburtsdatum bei Nicht-Abonnenten stieß hingegen auf datenschutzrechtliche Bedenken. So war diese Datenverarbeitung für die von der Hallenbetreiberin kommunizierten Zwecke nicht erforderlich

und mithin nicht legitimiert. Die Erhebung und nachgehende Speicherung des Geburtsdatums zur Gewährleistung des Jugendschutzes nach Art. 6 Abs. 1 lit. c DSGVO war bereits deshalb nicht erforderlich, als hierfür auch im jeweiligen Einzelfall das bloße Vorzeigen eines geeigneten Altersnachweises ausreichend gewesen wäre. Auch die Ermittlung des nach dem Alter des Besuchers bemessenen Eintrittspreises ließe sich im Rahmen einer entsprechenden Kontrolle gewährleisten, weshalb das systematische Speichern des Geburtsdatums zu diesem Zweck auch nicht als nach Art. 6 Abs. 1 lit. b DSGVO erforderlich zu bezeichnen war. Gänzlich unklar blieb darüber hinaus, inwiefern die Erhebung von Namen und Geburtsdatum zur Aufklärung bei Unfällen erforderlich sein sollte. Konkrete Ausführungen darüber, welcher Mehrwert einer auf Vorrat erfolgenden Speicherung dieser Daten zukommen solle, blieb die Hallenbetreiberin auch auf weitere Nachfrage schuldig. Weshalb im Falle von Bränden etc. die Hallenbetreiberin gegenüber dem Rettungspersonal Angaben über die konkreten Hallennutzer machen solle, blieb ebenso unbelegt. Um Rettungskräften eine Übersicht über das Ausmaß der zu rettenden Personen geben zu können, wäre auch eine Angabe über die Anzahl der derzeitigen Hallennutzer ausreichend.

Die Hallenbetreiberin sicherte schließlich zu, auf die Verarbeitung personenbezogener Daten bei Nicht-Abonnenten künftig gänzlich zu verzichten. Die bereits gespeicherten Daten wurden ebenfalls gelöscht.

Fazit/ Empfehlung:

Die Nutzung von Freizeiteinrichtungen sollte grundsätzlich auch ohne die Preisgabe personenbezogener Daten möglich sein, sofern kein mitgliedschaftliches Verhältnis zu Grunde liegt.

9.4 Videoüberwachung in der Gastronomie

Im zurückliegenden Berichtszeitraum nahmen Videoüberwachungsmaßnahmen erneut einen erheblichen Teil der an die Aufsichtsbehörde adressierten Anliegen ein. Neben einer großen Zahl von Beschwerden und Prüfanregungen in Bezug auf den Einsatz von Kameras an Privathäusern sind auch immer wieder Überwachungsmaßnahmen in der Gastronomie Gegenstand von Verfahren.

Anlass für eine Kontrollmaßnahme in einem Gastronomiebetrieb war der Hinweis eines Gastes auf einen von der Straßenverkaufstheke erkennbaren Aushang. Dieser richtete sich an die Mitarbeitenden des Betriebs und enthielt ein Verbot zur Nutzung von Mobiltelefonen im gesamten Restaurant. Laut Aushang würde die Einhaltung dieser Vorgabe durch eine Videoüberwachungsmaßnahme geprüft. Für den Fall einer Zuwiderhandlung wurden rechtliche Konsequenzen, wie eine schriftliche Abmahnung und überdies eine Kündigung angedroht.

Der Beschwerdeführer brachte vor, dass in Anbetracht der kameragestützten Überwachung der Mitarbeitenden notwendigerweise auch Gäste des Restaurants von einer permanenten Überwachung und einer damit einhergehenden Datenverarbeitung betroffen sein müssen.

Nach Aufforderung zur Stellungnahme teilte der Inhaber des Gastronomiebetriebs mit, dass zwölf schwenkbare Kameras ganztägig in Betrieb seien und die Aufnahmen für sechzig Tage gespeichert würden. Die Erfassungsbereiche der Kameras erstreckten sich weiträumig über Kassen-, Theken-, Eingangs-, Gastbereiche sowie Büros, den Hintereingang, Keller, Küche, Treppe und einen Teil der unmittelbar im Umfeld des Restaurants gelegenen Einkaufspassage. Hinweisschilder, die die betroffenen Personen transparent über Gründe und Bedingungen der Videoüberwachung im Sinne des Art. 13 DSGVO informiert hätten, waren nicht angebracht.

Als Zwecke der Überwachung wurden die Ausübung des Hausrechts sowie die Diebstahl- und Vandalismusprävention benannt. Dass eine dahingehende Gefährdungslage gegeben war, die eine ständige Überwachung der Gäste und Mitarbeitenden getragen und den damit einhergehenden Grundrechtseingriff legitimiert hätte, wurde von dem Restaurantbetreiber nicht konkretisiert. Einem mit Blick auf Diebstähle geringwertiger Waren und einen Einbruchsversuch begründetem Überwachungsinteresse stand dabei ein überwiegend anlassloser Eingriff in das nach Art. 7 Grundrechtscharta der EU (EU-GRCh) geschützte Privatleben der Gäste, soweit sich der Schutzbereich auch auf das private Zusammentreffen mit Vertrauten im öffentlichen Raum erstreckt, sowie in den Schutz personenbezogener Daten der betroffenen Gäste und Passanten nach Art. 8 EU-GRCh gegenüber.

Als kritisch erwies sich zudem die permanente und auf eine Einwilligung gestützte Überwachung der Mitarbeitenden. Einwilligungserklärungen von Beschäftigten im Sinne des Art. 4 Nr. 11 DSGVO i. V. m. § 26 Abs. 2 BDSG kommen im Beschäftigungsverhältnis aufgrund ihrer regelmäßig nicht zu bejahenden Freiwilligkeit nicht als Legitimationsgrundlage für eine Videoüberwachungsmaßnahme in Betracht. Auch die von dem Restaurantbetreiber vorgelegten Einwilligungserklärungen waren nicht als wirksam zu qualifizieren.

Nach Gesamtwürdigung des Sachvortrags des Inhabers war von einem Überwiegen der Interessen und Grundrechte der betroffenen Personen auszugehen, so dass der Verantwortliche angewiesen wurde, einen datenschutzkonformen Zustand in Form der Einstellung der Überwachung des Innenbereichs während der Öffnungszeiten sowie eine vollständige Deaktivierung der Erfassung des Außenbereichs herzustellen. Außerdem waren eine Reduzierung der Speicherdauer sowie eine Ergänzung der Angaben des vorgelegten Hinweisschilds und die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten unabdingbar.

9.5 Datenoffenlegung im Unternehmen

Für Unternehmen dürften sie zwar überwiegend nicht erwünscht sein, allerdings gehört der Umgang mit ihnen zum Standardrepertoire unternehmerischer Tätigkeit: Reklamationen und Beschwerden. Soweit damit regelmäßig eine Verarbeitung personenbezogener Daten verbunden ist, sind auch aus datenschutzrechtlicher Notwendigkeit heraus unternehmensintern geeignete Geschäftsprozesse zu implementieren und eindeutige Zuständigkeiten festzulegen, so dass sich weder für betroffene Personen noch für die Mitarbeitenden des Verantwortlichen Unklarheiten bei Befassung und Abwicklung von Reklamationen bzw. Beschwerden ergeben.

9.5.1 Nicht erforderliche Datenoffenlegung im Unternehmen

Ein Beschwerdeführer wandte sich im Berichtszeitraum an die Aufsichtsbehörde und trug vor, dass seine an ein Unternehmen, dessen Geschäftstätigkeit im Wesentlichen in der Verteilung von Printwerbung besteht, gesandte Reklamation von wiederholten Zustellungsmängeln in einer Auseinandersetzung mit einem Zusteller endete. Im Detail monierte der Beschwerdeführer gegenüber dem Unternehmen per E-Mail im Auftrag seiner Schwiegereltern, dass diese die nicht persönlich adressierten Werbebotschaften wiederholt nicht erhalten hätten. Diese E-Mail sei sodann an den zuständigen Zusteller weitergeleitet worden, mit der Folge, dass dieser in Begleitung weiterer Personen den Beschwerdeführer an seiner in der E-Mail angegebenen Anschrift aufsuchte und bedrohte.

Da sich die in der E-Mail genannte Adresse der Schwiegereltern von der Wohnanschrift des Beschwerdeführers unterschieden hat, erschloss sich für diesen die Notwendigkeit der vollständigen Weitergabe seiner Nachricht an den Zusteller nicht. Überdies rügte er, zu keinem Zeitpunkt transparent über die Bedingungen der diesbezüglichen Datenverarbeitung informiert worden zu sein.

Nach Aufforderung zur Stellungnahme teilte das Unternehmen mit, dass die Weiterleitung von Beschwerden über Zustellungsmängel an die jeweiligen Zusteller zur Sachverhaltsaufklärung grundsätzlich notwendig und ein Filtern der Nachrichten nicht möglich sei. Ferner sei, soweit für die Zusteller keine unternehmensinternen E-Mail-Accounts eingerichtet wurden, die beschwerdegegenständliche E-Mail an den privaten E-Mail-Account des Zustellers gesandt worden.

Dass die E-Mail-Weiterleitung und damit die Offenlegung der Daten des Beschwerdeführers gegenüber dem Zusteller im Sinne des Art. 6 Abs. 1 lit. f DSGVO zur Reklamationsabwicklung erforderlich gewesen sein soll, war nicht ersichtlich. Dafür wäre hinsichtlich der nicht persönlich adressierten Printwerbung lediglich die Offenlegung der Adresse, für die die reklamierte Nichtzustellung geltend gemacht wurde, ausreichend gewesen. Das Gewährleistungsziel der Vertraulichkeit bei der Verarbeitung personenbezogener Daten war dabei nicht nur mit Blick auf die nicht erforderliche Offenlegung der personenbezogenen Daten des Beschwerdeführers gegenüber dem Zusteller beeinträchtigt, sondern auch angesichts der Weiterleitung der Beschwerde-E-Mail an den privaten E-Mail-Account des Zustellers. Dass die E-Mail und die darin enthaltenen Informationen des Beschwerdeführers Dritten zur Kenntnis gelangen, konnte daher durch das Unternehmen nicht ausgeschlossen werden

Mit der diesseitigen Bewertung konfrontiert, effektivierte das Unternehmen das Beschwerdemanagment auch in datenschutzrechtlicher Hinsicht, indem Mitarbeitende der Qualitätssicherung die Beschwerdeabwicklung überwachen und den Informationsfluss auch unter dem Gesichtspunkt der Erforderlichkeit kanalisieren.

Gegenüber dem Unternehmen wurde wegen eines Verstoßes gegen Art. 5 Abs. 1 lit. a i. V. m. Art. 6 Abs. 1 DSGVO und Art. 5

Abs. 1 lit. f i. V. m. Art. 32 Abs. 1 lit. b DSGVO eine Verwarnung nach Art. 58 Abs. 2 lit. b DSGVO ausgesprochen.

9.5.2 Beschwerden zu öffentlichen Äußerungen von Mitarbeitenden

Der öffentlich abrufbare Kommentar zum politischen Tagesgeschehen in einem Karrierenetzwerk war Anlass für eine Beschwerde-E-Mail an den Arbeitgeber des kommentierenden Nutzers. Die beschwerdeführende Person erwartete eine dahingehende Rückäußerung des Unternehmens, ob die öffentlichen Aussagen des Mitarbeiters mit dem Unternehmensleitbild in Einklang stehen. Da keine Antwort des Unternehmens erfolgte, aber die beschwerdeführende Person unmittelbar von dem angeschwärzten Mitarbeiter über dessen privaten E-Mail-Account kontaktiert wurde, machte diese bei dem Unternehmen einen Auskunftsanspruch nach Art. 15 DSGVO geltend. Eine Antwort des Unternehmens blieb trotz Erinnerung aus, so dass schließlich die Aufsichtsbehörde mit dem Sachverhalt befasst wurde.

Das Unternehmen teilte mit, dass es noch eine Erwiderung an den Beschwerdeführer zu senden beabsichtigte und die Beschwerde-E-Mail – somit auch dessen Daten – an mit der Aufklärung des Sachverhalts befasste unternehmensinterne Instanzen weitergeleitet worden seien. Die Beschwerde-E-Mail sei auch nach deren Eingang unmittelbar an den Mitarbeiter, der Anlass für die Beschwerde gegeben habe, weitergeleitet worden, allerdings sei dies eigentlich zunächst nicht intendiert gewesen und auf den Fehler bei der Posteingangsstelle zurückzuführen. Der Mitarbeiter habe ferner ausdrücklich weisungswidrig die Angaben des Beschwerdeführers für eine private Kontaktaufnahme verwendet.

Soweit das Unternehmen die Daten des Beschwerdeführers aus der zugesandten E-Mail mit dem Zweck verarbeitet hat, um diesem eine Erwiderung auf die öffentlichen Äußerungen des Mitarbeiters zukommen zu lassen, war dieses somit auch als

Verantwortlicher nach Art. 4 Nr. 7 DSGVO für die damit verbundene Datenverarbeitung anzusehen. Ersichtlich wurde jedoch, dass der Prozess der dahingehenden Beschwerdebearbeitung weder hinreichend institutionalisiert war noch Transparenzvorgaben genügte. So wurde die Beschwerde-E-Mail zwar nach Erhalt an verschiedene unternehmensinterne Stellen weitergeleitet, eine mit Blick auf den verfolgten Verarbeitungszweck abgestimmte Stellungnahme erhielt der Beschwerdeführer zusammen mit der Auskunft nach Art. 15 DSGVO allerdings erst nach erneuter Nachfrage der Aufsichtsbehörde.

Das Unternehmen nahm das Verfahren zum Anlass die Geschäftsprozesse betreffend das Beschwerdemanagement und die Geltendmachung von Betroffenenrechten zu effektivieren, indem unter anderem konkrete Zuständigkeiten von unternehmensinternen Instanzen festgelegt und den betroffenen Personen die diesbezüglichen Verarbeitungsprozesse transparent dargestellt werden.

Aufgrund eines Verstoßes gegen Art. 5 Abs. 1 lit. a in Verbindung mit Art. 12 Abs. 1 und 3 sowie Art. 15 DSGVO wurde gegenüber dem Unternehmen eine Verwarnung ausgesprochen. Gegen den Mitarbeiter wurde aufgrund der zweckwidrigen Verwendung der Kontaktdaten des Beschwerdeführers zur privaten Kontaktaufnahme ein Verwaltungsverfahren eröffnet.

X.

Internet und Werbung

10 Internet und Werbung

10.1 Authentifizierung bei der Registrierung eines Kundenaccounts

Im Bereich der Versicherungen gehört es zunehmend zum Leistungsumfang der Anbieter, dass Kunden über einen Online-Account Informationen zu ihrem bestehenden Vertragsverhältnis abrufen und über diesen das Versicherungsverhältnis betreffende Handlungen vornehmen und Erklärungen abgeben können. In einem uns als Beschwerde zugetragenen Fall wurde es Kunden ermöglicht, einen solchen Online-Account optional zum bestehenden Vertragsverhältnis noch nachträglich anzulegen. Zur Registrierung mussten dabei lediglich der vollständige Name, die Adresse sowie das Geburtsdatum der versicherten Person angegeben werden. Soweit diese Angaben mit denen des bestehenden Kundenverhältnisses übereinstimmten, wurde ein damit verknüpfter Online-Account angelegt, für den der Kunde sodann ein Passwort festlegen konnte.

Der Beschwerdeführer hatte die Befürchtung, dass seine personenbezogenen Daten nicht ausreichend geschützt seien, da auch unbefugte Dritte sich bei Kenntnis obiger Informationen zur versicherten Person einen mit seinem Versicherungsverhältnis verknüpften Online-Account anlegen und dementsprechend Informationen einsehen und Handlungen im Rahmen des Versicherungsverhältnisses vornehmen könnten.

In dem sich daran anschließenden aufsichtsbehördlichen Verfahren sind wir zu der Einschätzung gelangt, dass die Ausgestaltung des Registrierungsprozesses im dargestellten Sinne mit Blick auf die dafür notwendigen Angaben nicht den datenschutzrechtlichen Anforderungen genügt.

Nach Art. 32 Abs. 1 DSGVO müssen Verantwortliche geeignete technische und organisatorische Maßnahmen treffen, um ein

dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten. Dabei sind insbesondere der Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen bei der Bestimmung der erforderlichen Maßnahmen zu berücksichtigen. Die zu ergreifenden technischen und organisatorischen Maßnahmen umfassen nach Art 32 Abs. 1 lit. b DSGVO vor allem auch solche, die die Vertraulichkeit der personenbezogenen Daten im Zusammenhang mit dem betriebenen (Online-)Dienst sicherstellen, also gewährleisten, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind. Technisch erfolgt dies bspw. durch die Implementierung eines sicheren Authentifizierungsverfahrens.[30]

Die Vertraulichkeit der über einen Online-Account abrufbaren Informationen ist jedoch nicht hinreichend gesichert, wenn zur Authentifizierung lediglich Angaben gefordert werden, die einem größeren Personenkreis bekannt sein können. Name, Geburtsdatum und Adresse eines Versicherten sind Informationen, die einerseits in dessen gesellschaftlich-sozialem Umfeld regelmäßig bekannt und in vielen Fällen auch frei im Internet, etwa über soziale Netzwerke, auffindbar sind. Name und Adresse bieten als Authentifizierungsmerkmal daher nahezu keinen, das Geburtsdatum kaum Schutz vor einem Zugriff durch unbefugte Dritte.

Gerade das Risiko eines unbefugten Zugangs zu personenbezogenen Daten muss nach Art. 32 Abs. 2 DSGVO aber bei der Bestimmung des erforderlichen Schutzniveaus berücksichtigt werden. Der Zugang zu personenbezogenen Daten eines Versicherten darf daher regelmäßig nur mittels

[30] vgl. Standarddatenschutzmodell, Version 2.0b, D.1.3, elektronisch abrufbar unter: https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/Download/ SDM-Methode_V20b.pdf

eines Authentifizierungsmerkmals möglich sein, das in aller Regel allein dem Versicherten bekannt ist. Zwar bleibt die weitere technische Ausgestaltung der Authentifizierung der verantwortlichen Stelle überlassen soweit sie dem Stand der Technik hinreichend Rechnung trägt. Absolute Mindestanforderung ist aber, dass bei einem bestehenden Vertragsverhältnis im Rahmen der Registrierung etwa eine Kundennummer erfragt wird.

Je nach Ausgestaltung des Online-Accounts, nach Umfang und Reichweite der hierüber eingeräumten Handlungsmöglichkeiten der versicherten Person sowie Sensibilität der dort abrufbaren Informationen, kann auch das Abfragen einer Kundennummer ggf. nicht ausreichend sein, um den Account den Anforderungen des Art. 32 DSGVO entsprechend zu sichern. In diesen Fällen ist es erforderlich, dass der Kunde sich bei der erstmaligen Registrierung durch ein zusätzliches Merkmal - etwa durch einen spezifisch für diesen Zweck zugesendeten Code - authentifiziert, was unter Berücksichtigung des Umfangs heutiger Nutzer-Accounts den Regelfall darstellen dürfte. Bei der Beurteilung der Sensibilität der personenbezogenen Daten sollte dabei bedacht werden, dass auch Informationen, die auf den ersten Blick ggf. weniger sensibel zu sein scheinen, für spezifischere und damit glaubwürdigere Phishingangriffe gegenüber Versicherten verwendet werden könnten, was bei der Bestimmung des Schutzbedarfs nicht außer Acht gelassen werden sollte.

Zudem ist zu berücksichtigen, dass für das obligatorische Maß der technisch-organisatorischen Maßnahmen auch der derzeitige Stand der Technik maßgeblich ist. Dies macht eine regelmäßige Evaluierung der technisch-organisatorischen Maßnahmen erforderlich, infolge derer Anpassungsbedarf entstehen kann.

Der Sachverhalt ist hier derzeit Gegenstand eines anhängigen Bußgeldverfahrens.

10.2 Ausgestaltung von Einwilligungsbannern

Ein wiederkehrendes Problem bei der datenschutzrechtlichen Kontrolle von Webseiten ist die Ausgestaltung von Einwilligungsbannern bzw. sog. „Cookie-Bannern“, über die für den Einsatz von Cookies und/oder eine folgende Verarbeitung personenbezogener Daten eine Einwilligung eingeholt werden soll. In vielen Fällen musste dabei festgestellt werden, dass die Banner nicht so ausgestaltet waren, dass von einer wirksam erteilten Einwilligung ausgegangen werden konnte. Dabei wurden insbesondere zwei Aspekte nicht hinreichend beachtet, die zwar bereits im letzten Tätigkeitsbericht Erwähnung fanden,[31] aber weiterhin von vielen Webseitenbetreibern verkannt werden:

Erstens ist es nach Auffassung der DSK[32] erforderlich, dass Nutzer die Möglichkeit haben, ihre Einwilligung im Rahmen des Banners bereits auf erster Ebene zu verweigern, sofern die Webseite nicht ohne eine Interaktion mit dem Banner besucht werden kann. Nicht zulässig ist es damit, wenn in derartigen Fällen die Möglichkeit zum Ablehnen der Einwilligung in Untermenüs „versteckt“ wird und Nutzer so entgegen ihrem eigentlichen Wunsch zur Einwilligung veranlasst werden, da unnötige Hürden für deren Ablehnung geschaffen werden.

Zweitens sind in einer überwiegenden Zahl der Fälle die Texte der Einwilligungsbanner nicht geeignet, die Nutzer über die geplanten Verarbeitungsvorgänge ausreichend zu informieren. Daher können Nutzer in vielen Fällen gar nicht wirksam in Verarbeitungen einwilligen. Der Text des Banners muss einen

---

[31] 30. Tätigkeitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit, 2021, S. 93f., elektronisch abrufbar unter: https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/tberichte/tb30_DS_2021.pdf

[32] vgl. Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien, Version 1.1, Stand Dezember 2022, S. 37, Rn. 122, elektronisch abrufbar unter: https://www.datenschutzkonferenz-online.de/media// 20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf

durchschnittlichen Nutzer der Webseite in die Lage versetzen, Art und Ausmaß der beabsichtigten Verarbeitungen auch wirklich erkennen zu können. Insbesondere sind im Einwilligungsbanner alle einwilligungsbedürftigen Dienste und ihr konkreter Zweck zu benennen.

10.3 Einsatz von Consent-Management-Platforms

In vielen Fällen verwenden Betreiber von Webseiten keine bei der Entwicklung der Webseite eigenständig entworfenen Einwilligungsbanner, sondern sie greifen auf Banner zurück, die von Dienstleistern entwickelt und Webseitenbetreibern, oft gegen Entgelt, zur Verwendung auf der eigenen Webseite angeboten werden (z. B. sog. Consent-Management-Platforms).

In einem Beschwerdeverfahren wurde gegenüber hiesiger Dienststelle vom Betreiber der Webseite vorgebracht, der Anbieter der von ihm verwendeten Consent-Management-Platform habe auf Nachfrage mitgeteilt, dass eine Konfiguration und Ausgestaltung des Einwilligungsbanners auf die von hiesiger Aufsichtsbehörde geforderte Art und Weise nicht vorgesehen sei. Daher sei ihm eine Anpassung des Banners technisch nicht möglich.

Wir haben den Betreiber der Webseite darauf hingewiesen, dass die datenschutzrechtlichen Vorgaben unabhängig vom Funktionsumfang des jeweiligen Dienstleisters zu beachten sind und demnach auch eine entsprechende Durchsetzung der Vorgaben durch hiesige Dienststelle erfolgen wird. Falls der eingesetzte Dienstleister eine Anpassung des Einwilligungsbanners dergestalt, dass er den datenschutzrechtlichen Anforderungen genügt, nicht ermöglicht, ist der Einsatz des Dienstleisters faktisch ausgeschlossen.

10.4 Daten unklarer Herkunft für Werbebriefe

Neben der Erhebung personenbezogener Daten für Zwecke der Direktwerbung unmittelbar bei der betroffenen Person, bspw. im Rahmen einer bestehenden Geschäftsbeziehung, können Daten von werbenden Stellen auch ohne Mitwirkung des Werbeadressaten durch Eigenrecherche, über Branchenverzeichnisse oder über Adresshändler beschafft werden. Diese Dritterhebung von personenbezogenen Daten, die ohne Beteiligung und zunächst ohne Kenntnis der betroffenen Person erfolgt, war im Berichtszeitraum wiederholt Gegenstand der aufsichtsbehördlichen Befassung. Informationsdefizite stellen dabei nicht nur einen Verstoß gegen datenschutzrechtliche Vorgaben dar, sondern diese können auch die Unzulässigkeit der diesbezüglichen Datenverarbeitung für Zwecke der Direktwerbung nach sich ziehen.

Studierende des Abschlussstudiengangs an einer saarländischen Hochschule erhielten postalisch von einem Versicherungsbüro individuell adressierte Beratungsangebote für Berufsanfänger. Da die Herkunft der Angaben der Studierenden mangels transparenter Angaben im Sinne des Art. 14 DSGVO nicht ersichtlich war und das Versicherungsbüro auf Nachfragen von Studierenden zur Datenherkunft keine Auskünfte erteilte, wandten sich Betroffene an den Datenschutzbeauftragten der Hochschule. Über die zunächst durch den Hochschuldatenschutzbeauftragten befasste Staatsanwaltschaft gelangte der Sachverhalt schließlich an die Aufsichtsbehörde.

Nach diesbezüglicher Aufforderung nahm die Geschäftsleitung des Versicherungsbüros zunächst lediglich in unzureichender Form Stellung zu dem Sachverhalt. Nachdem die Erteilung eines Auskunftsheranziehungsbescheids in Aussicht gestellt wurde, wurde von der Geschäftsleitung mitgeteilt, dass die Herkunft der Daten nicht nachvollziehbar sei. Es sei lediglich ein Briefumschlag, der eine Liste mit Namen und Adressen der Studierenden des Abschlussjahrgangs enthielt, in den

Briefkasten des Versicherungsbüros eingeworfen worden. Diese Angaben seien für die sodann erfolgte Werbeansprache automatisiert verarbeitet und anschließend gelöscht worden.

Diese Datenverarbeitung für Zwecke der postalischen Direktwerbung konnte nicht über Art. 6 Abs. lit. f DSGVO legitimiert werden. Ungeachtet der Tatsache, dass der Vortrag der Geschäftsleitung hinsichtlich der Herkunft der Daten als wenig glaubhaft wahrgenommen wurde, war bereits die Verfolgung eines berechtigten Interesses an der Datenverwendung angesichts der Gesamtumstände des Sachverhalts und mit Blick auf die nebulöse Datenherkunft anzuzweifeln. Letztlich führte allerdings die für die Werbeadressaten intransparente und weder nach objektiven noch subjektiven Maßstäben erwartbare Datenverarbeitung ein Überwiegen schutzwürdiger Interessen und Grundrechte der betroffenen Personen nach sich.

Aufgrund eines Verstoßes gegen Art. 5 Abs. 1 lit. a in Verbindung mit Art. 6 Abs. 1 sowie Art. 12 und 14 DSGVO in einer Vielzahl von Fällen wurde die Bußgeldstelle mit dem Vorgang befasst.

10.5 Bevorratung von Daten für Zwecke der Direktwerbung im B2B-Bereich

Im Rahmen eines Beschwerdeverfahrens, das zunächst die Umstände der Einholung von Bonitätsauskünften über freiberuflich tätige Personen durch ein saarländisches Unternehmen betraf, wurde ersichtlich, dass das Unternehmen Namen und geschäftliche Adressen der Betroffenen über einen Adresshändler bezogen hatte, mit dem Ziel diese zur Geschäftsanbahnung zu kontaktieren.

Das Unternehmen holte nicht nur vor Herstellung eines ersten werblichen Kontaktes rechtsgrundlos eine Bonitätsauskunft über Werbeadressaten ein, sondern versäumte es zudem, die betroffenen Personen nach Art. 14 DSGVO über die Dritterhebung zu informieren. Im Rahmen des

Verwaltungsverfahrens wurde ersichtlich, dass von dem Unternehmen Daten von über 148.000 betroffenen Personen über Adresshändler bezogen oder über Eigenrecherche erhoben worden sind. Diese wurden teils über Jahre ungenutzt gespeichert. Nach Aussage des Unternehmens war eine Verselbständigung der für das Marketing verantwortlichen operativen Bereiche Anlass für die Fehlentwicklung.

Neben der Unterlassung ungerechtfertigter Bonitätsabfragen, gab sich das Unternehmen als Folge des Verwaltungsverfahrens eine Richtlinie zur Verarbeitung von Daten für Zwecke der Direktwerbung und operationalisierte die diesbezüglichen Geschäftsabläufe. Dazu gehörte auch ein den inhaltlichen und fristspezifischen Vorgaben von Art. 14 Abs. 1 bis 3 DSGVO genügender Geschäftsprozess und ein Löschkonzept.

Für den bereits vorliegenden Datenbestand wurde eine Nachholung der vollumfänglichen Informationserteilung nach Art. 14 DSGVO umgesetzt, verbunden mit einem Hinweis auf den Anlass der verspäteten Information und der anstehenden Löschung der Daten. Im Nachgang des Verwaltungsverfahrens wurde die Bußgeldstelle mit dem Sachverhalt befasst.

10.6 Verhaltenslenkung zur Generierung von Werbeeinwilligungen

Über eine Prüfanregung wurde die Aufsichtsbehörde auf den Kontaktprozess eines Versicherungsunternehmens und die damit verbundene Einholung von Werbeeinwilligungen aufmerksam gemacht. Ein Online-Kontaktformular, über das versicherte oder interessierte Personen laut der auf der Website aufgeführten beispielhaften Aufzählung, Fragen zu Angeboten, Anträgen und Verträgen stellen, Änderungen von Kundendaten vornehmen und datenschutzrechtliche Anliegen geltend machen konnten, diente dem Unternehmen gleichsam zur Generierung von Werbeeinwilligungen nach Art. 4 Nr. 11 in Verbindung mit Art. 6 Abs. 1 lit. a DSGVO.

Dabei umfasste die Gestaltung des Kontaktformulars zwei unterschiedliche Konzepte der Einwilligungserteilung für verschiedene Kontaktwege.

Während die Angabe der E-Mail-Adresse im Formular obligatorisch war, deren Verwendung für Zwecke des Marketingzwecke allerdings erst durch Aktivieren einer Checkbox legitimiert wurde, konnte die Telefonnummer optional angegeben werden, jedoch mit der Folge, dass durch deren Eintragung konkludent eine Einwilligung in die werbliche Nutzung erteilt wurde. Eine dies erläuternde Fußnote war zwar am Ende des Kontaktformulars angefügt, zu jedem Zeitpunkt war allerdings im Formularfenster ein „Nachricht senden"-Button hervorgehoben eingeblendet. Für Nutzende des Kontaktformular war somit ein Absenden des Anliegens noch vor Lesen der Fußnote naheliegend.

Unter Berücksichtigung der Vorgaben von Art. 4 Nr. 11 DSGVO ist für die Wirksamkeit einer Einwilligungserklärung unter anderem maßgeblich, dass diese in informierter und unmissverständlicher Weise abgegeben wurde. Das Ausfüllen eines Formularfelds auf einer Webseite kann dabei grundsätzlich eine eindeutige bestätigende Handlung, die für eine in unmissverständlicher Weise abgegebene Willenserklärung spricht, darstellen,[33] sofern im Weiteren die einwilligungsspezifischen Bedingungen für deren Wirksamkeit Berücksichtigung finden. In diesem Zusammenhang ist insbesondere die nach Art. 7 Abs. 2 Satz 1 DSGVO und Erwägungsgrund 42 zu fordernde Unterscheidbarkeit der Einwilligung von sonstigen Erklärungen maßgeblich.

Das vorgefundene Design der Formularstrecke, das heißt die nahezu unterschiedslose Einbettung der Einwilligungserklärung betreffend die werbliche Verwendung der Telefonnummer in den Kontaktprozess, die Verwendung unterschiedlicher

[33] Europäischer Datenschutzausschuss (EDSA): Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, Rn. 94.

Einwilligungskonzepte für den Kontaktweg E-Mail und Telefon sowie die permanente Einblendung des „Nachricht senden“-Buttons, wurde diesem Unterscheidbarkeitsgebot nicht gerecht. Die Konzeption des Einwilligungsprozesses ließ auf dessen zielgerichtete Ausgestaltung in der vorliegenden Form und eine damit verbundene Verhaltenssteuerung, mit dem Ziel Werbeeinwilligungen zu generieren, schließen. Für die dergestalt eingeholten Einwilligungserklärungen in die Verwendung der Telefonnummer für Werbezecke ergaben sich somit durchgreifende Zweifel an deren Wirksamkeit.

Nach Aufforderung zur Stellungnahme teilte das Unternehmen mit, dass weitere Kontakt- und Antragsstrecken ähnlich konzipiert waren, allerdings die dargelegten Zweifel an der Unterscheidbarkeit der Einwilligung von der sonstigen Formularstrecke nicht geteilt werden. Ungeachtet dessen hat das Unternehmen die Antrags- und Kontaktstrecken nachträglich modifiziert und vereinheitlicht, mit der Folge, dass auch die Einwilligung in die werbliche Verwendung der Telefonnummer nur durch Aktivieren einer Checkbox erteilt wird.

Soweit in dem ursprünglich konzipierten Design des Einwilligungsprozesses ein Verstoß gegen Art. 25 Abs. 1 DSGVO erkennbar wurde, wurde die Bußgeldstelle mit dem Sachverhalt befasst.

11.1 Kommunale Mandatsträger versus Bürgerinitiativen

XI.

Vereine und Parteien

11 Vereine und Parteien

11.1 Kommunale Mandatsträger versus Bürgerinitiativen

Die Wahrnehmung kommunaler Ehrenämter gestaltet sich für Lokalpolitiker zunehmend als Herausforderung. Voraussetzung für Bürgernähe und transparente Entscheidungsprozesse ist der unmittelbare Austausch mit Bürgerinnen und Bürgern, allerdings können der konstruktive Dialog und die öffentliche Meinungswerbung auch in Agitation und zielgerichtete Anfeindungen gegenüber Mandatsträgern umschlagen. Auf politische Entscheidungsträger wird mitunter nicht mehr nur im öffentlich ausgetragenen Diskurs, sondern zunehmend auch im privaten Umfeld Druck ausgeübt, wie unlängst Medienberichte über Mahnwachen oder Fackelmärsche vor Wohnanwesen zeigten.

Durch eine Presseanfrage und mehrere Prüfanregungen wurden wir auf die Veröffentlichung personenbezogener Daten von kommunalen Entscheidungsträgern durch eine Bürgerinitiative aufmerksam gemacht. Im Zuge einer geplanten Unternehmensansiedlung formierte sich in einer saarländischen Kommune eine Bürgerinitiative, die durch medienwirksame Meinungswerbung die Ansiedlung zu verhindern versuchte. Vor dem Hintergrund dieses verfolgten Ziels richteten sich die Maßnahmen der Bürgerinitiative gerade auch gegen die kommunalen Entscheidungsträger, die letztlich über das Planungsvorhaben zu entscheiden hatten.

Die Bürgerinitiative erstellte einen Flyer, der an die örtlichen Haushalte verteilt und auf der Internetseite der Bürgerinitiative veröffentlicht wurde. Neben der Darstellung der aus ihrer Sicht nachteiligen Auswirkungen der geplanten Unternehmensansiedlung und der mangelnden Transparenz in der Planungsphase wurden in dem Flyer die Mitglieder des Gemeinderats namentlich und mit Anschrift und Berufsbezeichnung genannt, ergänzt mit dem Hinweis, dass

dieser Personenkreis schließlich über das Vorhaben und die künftige Lebensqualität der Anrainer der Unternehmensansiedlung entscheide. Die Bürgerinitiative stützte diese Veröffentlichung nach eigenen Angaben auf Art. 6 Abs. 1 lit. f Datenschutz-Grundverordnung (DSGVO). Die Vorschrift erlaubt eine Datenverarbeitung dann, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die schutzwürdigen Interessen der Betroffenen nicht überwiegen. Das mit der Veröffentlichung der Angaben zu politischen Entscheidungsträgern verfolgte Interesse der Bürgerinitiative bestand nach eigenen Angaben darin, diesen mit Nachdruck deutlich zu machen, dass ihre Beteiligung an einem solchen Projekt auch künftig nicht vergessen werde.

Nach Ansicht der Akteure der Bürgerinitiative war auch nicht von einem Überwiegen schutzwürdiger Interessen der Ratsmitglieder auszugehen, da die Flyer nur im gemeindenahen Umfeld verteilt worden seien und die Angaben zu den Gemeinderatsmitgliedern ohnehin bereits vor mehreren Jahren im amtlichen Bekanntmachungsblatt der Kommune veröffentlicht waren. Zudem übten die Mandatsträger ein öffentliches Amt aus und müssten damit rechnen, als Entscheidungsträger auch im privaten Umfeld adressiert zu werden.

Das dahingehende Vorbringen der Bürgerinitiative hielt einer datenschutzrechtlichen Prüfung nicht stand. Entgegen der Auffassung der Bürgerinitiative konnte sie sich bei der Veröffentlichung der Wohnanschriften von Mitgliedern des Gemeinderats weder auf Art. 6 Abs. 1 lit. f DSGVO noch auf eine andere datenschutzrechtliche Legitimationsgrundlage berufen. Grundsätzlich besteht zwar ein berechtigtes Interesse der Bürgerinitiative im Rahmen der Meinungswerbung über nachteilige Auswirkungen der Unternehmensansiedlung zu informieren und am politischen Entscheidungsfindungsprozess durch Einwirkung auf die Mitglieder des Gemeinderats zu partizipieren; für die Wahrnehmung dieses Interesses war

jedoch die Veröffentlichung der Angaben zu den Ratsmitgliedern, insbesondere deren Wohnanschriften, nicht erforderlich im Sinne der Vorschrift.

Die von der Bürgerinitiative verfolgten Ziele der Information über die Folgen der Unternehmensansiedlung und der beabsichtigten Einflussnahme auf die politischen Entscheidungsträger ließe sich grundsätzlich auch ohne Veröffentlichung von privaten Angaben der Ratsmitglieder erreichen. Sachanliegen hätten über offizielle Kontaktwege des Gemeinderats an dessen Mitglieder adressiert werden können, so dass keine Notwendigkeit bestand, die öffentlichkeitswirksame Artikulierung von Kritik an der Ansiedlung und dem Ablauf des diesbezüglichen Entscheidungsprozesses in das private Umfeld der Mandatsträger hineinzutragen.

Vielmehr stellte die Veröffentlichung der Privatadressen in dem genannten Zusammenhang einen erheblichen Eingriff in die Privatsphäre der Ratsmitglieder dar, so dass schutzwürdige Interessen der Kommunalpolitiker einer solchen Veröffentlichung entgegenstanden. Gerade angesichts einer allgemein zunehmenden Gefährdungslage für politische Entscheidungsträger und der im vorliegenden Fall sehr emotional geführten öffentlichen Debatte, war eine Verlagerung der Auseinandersetzung in das persönliche Umfeld der Ratsmitglieder, die die Unternehmensansiedlung befürworteten, nicht fernliegend. Dies galt insbesondere auch mit Blick darauf, dass der Flyer der Bürgerinitiative entgegen deren Darstellung nicht nur einem regional begrenzten Personenkreis zugänglich war, sondern über deren Webseite zum Abruf bereit gestellt wurde.

Eine andere Bewertung ergab sich auch nicht aufgrund der Tatsache, dass die Daten der Ratsmitglieder bereits zu einem früheren Zeitpunkt von der Kommune im Vorfeld der damals anstehenden Kommunalwahl im Amtsblatt veröffentlicht worden waren. Die damalige Veröffentlichung erfolgte aufgrund einer

gesetzlichen Verpflichtung und diente alleine der ordnungsgemäßen Durchführung der Kommunalwahl und gerade nicht dem Zweck die später gewählten Ratsmitglieder jederzeit für die Öffentlichkeit zum Zwecke der Konfrontation mit ihren politischen Entscheidungen erreichbar zu machen. In diesem Zusammenhang ist auch zu berücksichtigen, dass die damalige Veröffentlichung ausschließlich in gedruckter Form im Amtsblatt der Kommune erfolgte und damit sowohl zeitlich als auch örtlich nur begrenzt wahrnehmbar war.

Im Laufe des Verwaltungsverfahrens teilte die Bürgerinitiative mit, dass der Flyer von der Webseite der Bürgerinitiative entfernt wurde. Im Hinblick auf den festgestellten Datenschutzverstoß wurde der Vorgang zunächst an unsere Bußgeldstelle zur Einleitung eines Verfahrens nach dem Ordnungswidrigkeitengesetz abgegeben. Da überdies eine strafbare Handlung gemäß § 42 Bundesdatenschutzgesetz im Raum stand, wurde das Verfahren schließlich an die Staatsanwaltschaft abgegeben

11.1.1 Wahlwerbung per E-Mail

Ein Mitglied der freiwilligen Feuerwehr einer Kommune erhielt von einem Kandidaten für das Amt des Bürgermeisters per E-Mail eine Einladung zu einer Veranstaltung, die dem Austausch von in der Kommune ehrenamtlich Tätigen mit dem Kandidaten dienen sollte. Da für die Kontaktaufnahme eine private E-Mail-Adresse, die nur im Rahmen der ehrenamtlichen Tätigkeit Verwendung fand, genutzt wurde, vermutete der Adressat der E-Mail einen Datenschutzverstoß und legte bei der Aufsichtsbehörde Beschwerde ein. Dabei trug der Beschwerdeführer vor, dass der Bürgermeisterkandidat bereits kommunaler Funktionsträger sei und im Rahmen dieser Tätigkeit an die private E-Mail-Adresse des Empfängers gelangt sein könnte. Da die von dem Beschwerdeführer vorgelegte Einladungs-E-Mail keine Angaben nach Art. 13 oder 14 DSGVO enthielt, blieb die Datenherkunft intransparent.

Nach Aufforderung zur Stellungnahme teilte der Bürgermeisterkandidat mit, dass er die E-Mail als Privatperson und nicht als kommunaler Funktionsträger versandt habe und diese keinen wahlwerblichen Charakter habe, sondern lediglich für eine Veranstaltung eingeladen werde, in deren Mittelpunkt der Informationsaustausch mit den Teilnehmenden stehe. Zur Herkunft der Daten führte er aus, dass ihm diese über seine bisherige kommunale Tätigkeit sowie im privaten Umfeld bekannt geworden seien sowie teilweise aus öffentlich zugänglichen Webauftritten entnommen wurden; eine Entnahme aus kommunalen Registern sei dabei ausdrücklich nicht erfolgt. Schließlich sei die dem E-Mail-Versand zugrundeliegende Datenverarbeitung über die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO legitimiert.

Eine datenschutzrechtliche Zulässigkeit der beschwerdegegenständlichen Ansprache war allerdings nicht ersichtlich.

Zunächst drängte sich unter Berücksichtigung des Gehalts der versandten Einladung, des Zwecks der angekündigten Veranstaltung und dem Zeitpunkt der Aussendung vor der anstehenden Wahl, der wahlwerbliche Charakter der Nachricht auf; während den Teilnehmenden der Veranstaltung die Möglichkeit gegeben werden sollte, Bedarfe, Anliegen und Erwartungen an den Bürgermeisterkandidat zu adressieren, diente der Informationsaustausch diesem gleichsam als Forum, um sich als Ansprechpartner für die Belange der Ehrenamtlichen in der Kommune darzustellen.

Ungeachtet der nach Art. 21 Grundgesetz (GG) und Art. 12 Grundrechtecharta der Union (EU-GRCh) garantierten institutionellen Sonderrolle von Parteien und dem besonderen Schutz, den die parteipolitische Tätigkeit genießt, ist eine Privilegierung von Wahlwerbemaßnahmen und eine Suspendierung des datenschutzrechtlichen Regelrahmens für damit verbundene Datenverarbeitungen durch Parteien oder

Parteimitglieder nicht ersichtlich.[34] Die beschwerdegegenständliche Wahlwerbung war damit im Wesentlichen an denselben datenschutzrechtlichen Vorgaben zu messen, die auch für kommerzielle Werbeansprachen gelten.[35]

Soweit der Bürgermeisterkandidat die Datenverarbeitung auf die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO stützte, war unter Berücksichtigung der gewählten Kontaktaufnahme per E-Mail und des wahlwerblichen Inhalts der Nachricht auch auf die weiteren Vorgaben im Unionsrecht abzustellen.[36] Für die Frage nach der Verfolgung eines berechtigten Interesses im Sinne des Art. 6 Abs. 1 lit. f DSGVO war somit auch die Regelung des Art. 13 Abs. 1 Richtlinie 2002/58/EG maßgeblich.

Nach dieser Vorschrift ist die Zulässigkeit der werblichen Nutzung des Kontaktwegs E-Mail von dem Vorliegen einer wirksamen Einwilligung des Werbeadressaten abhängig zu machen. Aufgrund der spezifischen Verschränkung von Richtlinie 2002/58/EG und DSGVO wurde somit ohne eine legitimierende Einwilligung auch kein berechtigtes Verarbeitungsinteresse gemäß Art. 6 Abs. 1 lit. f DSGVO verfolgt.[37]

Selbst für den Fall, dass ein berechtigtes Interesse unterstellt werden könnte, war allerdings auch für die Adressaten der E-Mail angesichts der unklaren Herkunft der für die Wahlwerbung verwendeten E-Mail-Adressen und mangels jeglicher Information nach Art. 13 oder 14 DSGVO die stattgefundene Datenverarbeitung vernünftigerweise nicht erwartbar, so dass im Weiteren von einem Überwiegen der schutzwürdigen

---

[34] Deutscher Bundestag, Wissenschaftliche Dienste: Politische Parteien und Datenschutz, WD - 3000 - 153/20, S. 4.

[35] OLG München, Urteil vom 12. Februar 2004 - 8 U 4223/03, juris.

[36] EuGH, Urteil vom 1. Oktober 2019 - C-673/17, Rn. 48, juris.

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

Interessen und Grundrechte der betroffenen Personen auszugehen war.

Aufgrund eines Verstoßes gegen Art. 5 Abs. 1 lit. a i. V. m. Art. 6 Abs. 1 sowie Art. 12 Abs. 1 und Art. 14 DSGVO wurde eine Verwarnung nach Art. 58 Abs. 2 lit. b DSGVO ausgesprochen.

11.1.2 Fremdnutzung der Daten von Parteimitgliedern

Datenschutzrechtliche Probleme im Kontext von Parteien treten häufig bei Zerwürfnissen zwischen einzelnen Parteimitgliedern auf.

Im Berichtszeitraum erreichten uns mehrere Beschwerden von Betroffenen, die von einem Parteifunktionär ein Wahlwerbeschreiben erhalten hatten. In diesem warb der Absender des Schreibens um die Stimme der Mitglieder der Partei, um bei der anstehenden Landtagswahl als Spitzenkandidat ins Rennen gehen zu können. Aufgrund der Aufmachung des Schreibens war davon auszugehen, dass das Schreiben kein förmliches Parteischreiben darstellte, sondern von dem Verantwortlichen als Privatperson verfasst wurde.

Die betroffenen Personen teilten mit, mit dem Verfasser des Schreibens in keiner unmittelbaren Verbindung zu stehen. So hätten sie diesem weder Daten zur Verfügung gestellt noch ihre Einwilligung in die Datenverarbeitung erteilt. Nach Ansicht der Beschwerdeführer habe der Verfasser des Anschreibens auf die parteiinterne Mitgliederliste zugegriffen und die Daten zu eigenen Zwecken verwendet.

Bei Name und Anschriften der betroffenen Personen handelt es sich aufgrund der Verknüpfung zum Datum der Parteizugehörigkeit um Daten im Sinne des Art. 9 DSGVO, für die eine besondere Schutzwürdigkeit zu unterstellen ist. Für die Verarbeitung personenbezogener Daten betreffend die politische Meinung kann neben der Einwilligung der betroffenen Person grundsätzlich die Regelung des Art. 9 Abs. 2 lit. d DSGVO Anwendung finden. Die Vorschrift privilegiert die

Verarbeitung solcher Daten, wenn sie auf der Grundlage geeigneter Garantien durch eine politische Vereinigung erfolgt. Da aber das zugrundeliegende Schreiben ersichtlich von einer Privatperson verfasst wurde, hätte die verfahrensgegenständliche Datenverarbeitung allenfalls auf die Einwilligung der Betroffenen gestützt werden können.

Der Verantwortliche gab auf Nachfrage an, nur solche Mitglieder angeschrieben zu haben, mit denen er in der Vergangenheit in innerparteilichem Kontakt gestanden habe und mit denen er einen schriftlichen Austausch pflegte. Die angeschriebenen Personen hätten ihm in der Vergangenheit auf unterschiedlichsten Wegen zu verstehen gegeben (bspw. durch Aushändigung von Visitenkarten), über parteipolitische Informationen auf dem Laufenden gehalten werden zu wollen. Als Rechtsgrundlage berief er sich insoweit auf das Vorliegen einer Einwilligung der Betroffenen Personen,

An diesen Ausführungen bestanden aufgrund der ergänzenden Sachvorträge der Beschwerdeführer, die eine direkte Verbindung zu dem Verantwortlichen und die Abgabe einer Einwilligungserklärung bestritten, durchgreifende Zweifel.

Art. 9 Abs. 2 lit. a DSGVO sieht vor, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt haben muss. Der Nachweis, dass eine Einwilligung abgegeben wurde, obliegt dabei dem Verantwortlichen (Art. 7 Abs. 1 DSGVO). Auch wenn die Vorschrift kein Schriftformerfordernis vorsieht, sind durch den Verantwortlichen im Rahmen der Rechenschaftspflicht geeignete Maßnahmen zu ergreifen, um im Bestreitensfall das Vorliegen einer wirksamen Einwilligung belegen zu können.

Da durch den Verantwortlichen kein Nachweis über das Vorliegen der Einwilligung erbracht werden konnte und die Abgabe einer ebensolchen durch die Beschwerdeführer verneint wurde, erfolgte die Verarbeitung der personenbezogenen Daten ohne Rechtsgrundlage. Der

tatsächliche Ursprung der Daten konnte im Rahmen des Verwaltungsverfahrens nicht ermittelt werden.

Der Verantwortliche wurde abschließend nach Art. 58 Abs. 2 lit. b DSGVO verwarnt.

XII.

Bußgeldverfahren

12 Bußgeldverfahren

12.1 Bußgeldverfahren gegen Polizeibeamte wegen unzulässiger Abfragen

12.1.1 Einleitung

Bereits in vorhergehenden Tätigkeitsberichten haben wir über Bußgeldverfahren gegen Polizeibeamte berichtet. Während diese Datenschutzverstöße eher zufällig aufgedeckt wurden, resultieren nunmehr die meisten Bußgeldverfahren gegen Polizeibedienstete aus regelmäßigen Datenschutzkontrollen des behördlichen Datenschutzbeauftragten des Landespolizeipräsidiums.

Die Zuleitung der Fälle an unsere Dienststelle erfolgt in der Regel direkt durch das Landespolizeipräsidium aufgrund disziplinarischer Ermittlungen oder nach Abschluss eines Strafverfahrens durch die Staatsanwaltschaft. Anlass für die Zuleitung geben Datenabfragen durch Polizeibeamte in polizeilichen Informationssystemen, die nach Prüfung der für Zwecke der Datenschutzkontrolle zur Verfügung stehenden Protokolldaten nicht zweifelsfrei dem dienstlichen Aufgabenbereich des jeweiligen Polizeibeamten zugeordnet werden können.

Für die Erfüllung polizeilicher Aufgaben wie der Gefahrenabwehr, Verhütung und Verfolgung von Straftaten stehen der Polizei zahlreiche polizeiinterne als auch behördenübergreifende Informationssysteme zur Verfügung. Hierzu zählen Anwendungen wie das Polizeiliche Informationssystem POLIS, das polizeiliche Vorgangsbearbeitungssystem POLADIS, das Melderegister MR, das Zentrale Verkehrsinformationssystem ZEVIS u.a.

12.1.2 Datenschutzverstöße aus privaten Interessen

Nach § 27 Abs. 1 Nr. 2 Saarländisches Datenschutzgesetz (SDSG) handelt ordnungswidrig, wer entgegen der Verordnung (EU) 2016/679, dem SDSG oder einer anderen Rechtsvorschrift

zum Schutz personenbezogener Daten geschützte personenbezogene Daten, die nicht offenkundig sind, unbefugt abruft, sich oder einem anderen verschafft oder durch unrichtige oder unvollständige Angaben ihre Übermittlung an sich oder andere veranlasst.

Bei den im Berichtszeitraum mit einem Bußgeld sanktionierten Verfahren handelte es sich ausschließlich um Abfragen aus dem polizeilichen Informationssystem POLIS und mithin um nicht offenkundige Daten. Die Abrufe konnten durch die zur Verfügung stehenden Protokolldaten, die Zeitpunkte der Abfrage, Benutzerkennung, eingegebene Suchkriterien wie Name und Vorname sowie den Abfrageanlass – z. B. das Aktenzeichen eines Ermittlungsverfahrens – enthalten, nachgewiesen werden. In den konkreten Fällen wurden Abfragen zu befreundeten Personen und zu Freunden von nahen Familienangehörigen vorgenommen. Aus den Protokolldaten ergab sich, dass kein Abfrageanlass oder ein unrichtiger Abfrageanlass, z.B eine beliebige Ziffernfolge, die kein gültiges Aktenzeichen eines polizeilichen Ermittlungsverfahrens darstellt, eingegeben wurden. Weitere Ermittlungen unserer Dienststelle zeigten auf, dass gegen die abgefragten Personen entweder kein Ermittlungsverfahren seitens der Polizei geführt wurde oder geführte Ermittlungsverfahren zu keinem Zeitpunkt den beschuldigten Polizeibeamten dienstlich zugeordnet waren. Im Ergebnis handelte es sich daher um unbefugte Abrufe ohne Rechtsgrundlage und zugleich das Veranlassen einer Übermittlung durch unrichtige Angaben aus rein persönlichen Interessen.

Da Polizeibediensteten für die Ausübung ihrer dienstlichen Tätigkeit in der Regel ein weitreichender Zugriff auf eine Vielzahl von sensiblen personenbezogenen Daten gewährt wird, war ebenso zu berücksichtigen, dass gerade einem Mitarbeiter der Polizei ein besonderes Vertrauen hinsichtlich des ordnungsgemäßen Umgangs mit den Daten Dritter entgegengebracht wird.

In der Gesamtschau waren die Verstöße daher als nicht nur geringfügige Ordnungswidrigkeiten einzustufen, was auch bei der Bemessung der Bußgeldhöhe zu bewerten war.

Fazit/ Empfehlung:

Die Protokollierung automatisierter Datenabrufe ist ein wichtiges Instrument zur Gewährleistung einer effektiven Datenschutzkontrolle wie auch zur Sanktionierung schwerer Datenschutzverstöße.

Anlagenverzeichnis

Anhang 1: Verzeichnis wichtiger Rechtsgrundlagen

BDSG – Bundesdatenschutzgesetz: Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), zuletzt geändert durch Gesetz vom 23.6.2021 (BGBl. I S. 1858)

BKAG – Bundeskriminalamtgesetz: Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten 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)

DSGVO – Datenschutz-Grundverordnung: Verordnung (EU) 2016/679 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. Nr. L 119, S. 1, ber. ABl. Nr. L 314, S. 72 und ABl. 2018 Nr. L 127, S. 2)

GeschGehG – Geschäftsgeheimnisgesetz: Gesetz zum Schutz von Geschäftsgeheimnissen vom 18. April 2019 (BGBl. I S. 466)

GWG – Geldwäschegesetz: Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten, Artikel 1 des Gesetzes vom 23.06.2017 (BGBl. I S. 1822), in Kraft getreten am 26.06.2017, zuletzt geändert durch Gesetz vom 22.02.2023 (BGBl. I S. 51) m. W. v. 01.03.2023

IfSG – Infektionsschutzgesetz: Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen vom 20. Juli 2000 (BGBl. I S. 1045), zuletzt geändert durch Gesetz vom 18.3.2022 (BGBl. I S. 473)

OWiG – Ordnungswidrigkeitengesetz: Gesetz über Ordnungswidrigkeiten vom 24. Mai 1968 in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), zuletzt geändert durch Artikel 5 des Gesetzes vom 14. März 2023 (BGBl. 2023 I Nr. 73)

RiStBV – Richtlinien für das Strafverfahren und das Bußgeldverfahren: vom 1. Januar 1977, zuletzt geändert mit Wirkung vom 1. Dezember 2021 durch Bekanntmachung vom 8. November 2021 (BAnz AT 24.11.2021 B1)

SDSG – Saarländisches Datenschutzgesetz: Gesetz zur Anpassung des Saarländischen Datenschutzgesetzes an die Verordnung (EU) 2016/679 vom 16. Mai 2018 (Amtsbl. I S. 254), zuletzt geändert durch Gesetz vom 8.12.2021 (Amtsbl. I S. 2629)

SPolG – Saarländisches Polizeigesetz: Vom 26. März 2001 (Amtsbl. S. 1074), zuletzt geändert durch Gesetz vom 8.12.2021 (Amtsbl. I S. 2629)

SPolDVG – Saarländisches Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei: Vom 6./7. Oktober 2020 (Amtsbl. I S. 1133), zuletzt geändert durch Gesetz vom 8.12.2021 (Amtsbl. I 2022 S. 52)

UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

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

Telefon 0681 94781 – 0
Telefax 0681 94781 – 29

E-Mail poststelle@datenschutz.saarland.de

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