Die Landesbeauftragte für
Datenschutz und Informationsfreiheit

30. Tätigkeitsbericht Datenschutz

UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

2021

30. Tätigkeitsbericht

der Landesbeauftragten für Datenschutz und Informationsfreiheit

Berichtszeitraum: 2021

Dem Landtag und der Landesregierung
vorgelegt am 22. Juni 2022
(Landtagsdrucksache 17/9)

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

Auch im Jahr 2021 stand der Datenschutz im Zeichen der Corona-Pandemie. Um mit der dynamischen Entwicklung des Pandemiegeschehens Schritt zu halten, mussten erneut sehr kurzfristig rechtliche Rahmenbedingungen geschaffen werden, die teils mit erheblichen Eingriffen in das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger verbunden waren. Neben der bereits seit 2020 geltenden Verpflichtung zur Erhebung von Kontaktdaten von Besuchern und Gästen wurden nunmehr zusätzlich private und öffentliche Stellen verpflichtet, auch sensible Gesundheitsdaten, wie den Immunisierungs-, den Genesenen- oder den Teststatus (sog. 3G), einer Vielzahl betroffener Personen zu erheben.

Häufig fand bei den pandemiespezifischen Rechtsetzungsverfahren die Expertise der Datenschutzaufsichtsbehörden auf Landes- und Bundesebene nur unzureichende Berücksichtigung. Dies dürfte mit dazu beigetragen haben, dass die Regelungen mitunter derart unklar formuliert waren, dass Umfang und Reichweite der Vorgaben zur Datenerhebung und -verarbeitung für die Regelungsadressaten missverständlich geblieben sind. Hier waren die Datenschutzbehörden dann im Nachhinein gefragt, im Rahmen individueller Beratungen oder mittels Anwendungshinweisen Orientierung zu geben. Insbesondere die Unsicherheiten im Umgang mit den zahlreichen neuen Pflichten in Bezug auf Gesundheitsdaten, wie etwa die Verarbeitung von 3G-Daten am Arbeitsplatz, führten bei unserer Behörde zu einer erheblichen Zahl an Beratungsanfragen und Beschwerden.

Auch unabhängig von einer förmlichen Beteiligung haben wir die Maßnahmen der Landesregierung zur Pandemiebekämpfung kritisch begleitet. Dies betraf unter anderem die exklusive Forcierung eines datenschutzrechtlich nicht unbedenklichen digitalen Dienstes zur Kontaktdatenerhebung. Leider blieben unsere wiederholten Appelle, eine datenschonendere Alternative zur Kontaktdatenerhebung durch Einbeziehung der Corona-

Warn-App in den pandemierechtlichen Regelungsrahmen vorzusehen, unberücksichtigt.

Insgesamt stellt die fortschreitende Digitalisierung nach wie vor einen Schwerpunkt in der Arbeit unserer Behörde dar. Dabei ist festzustellen, dass leider immer noch allzu oft elementare Vorgaben des Datenschutzes und der Datensicherheit von Anbietern oder Entwicklern digitaler Anwendungen vernachlässigt werden. Eine Folge davon sind nicht nur zahlreiche Beschwerden, sondern auch eine erhebliche Zahl an Meldungen von Verletzungen des Schutzes personenbezogener Daten aufgrund unzureichender technischer und organisatorischer Maßnahmen bei der Gestaltung von IT-Systemen. Einer Vielzahl von Akteuren scheint dabei nach wie vor die Bedeutung der Implementierung adäquater Schutzstandards bei der Entwicklung von Dienstleistungen und Produkten nicht bewusst zu sein. Neben der drohenden Sanktionierung dahingehender Umsetzungsdefizite kann für den Verantwortlichen durch eine öffentlichkeitswirksame Kompromittierung von IT-Systemen zudem ein erheblicher Vertrauens- und Akzeptanzverlust entstehen. Daher kann bei privaten wie öffentlichen Digitalisierungsvorhaben ausschließlich eine von Beginn an konsequente Berücksichtigung datenschutz- und datensicherheitsrechtlicher Rahmenbedingungen die Daten der Nutzerinnen und Nutzer ausreichend schützen und das nötige Vertrauen in die Anwendungen schaffen.

Neben der originären Aufsichtstätigkeit prägte vor allem der Vorsitz der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) das Berichtsjahr. Im Rahmen des turnusmäßigen jährlichen Wechsels hatte meine Behörde zu Jahresbeginn den Vorsitz der DSK von Sachsen übernommen. Da sämtliche Veranstaltungen pandemiebedingt im Rahmen von Videokonferenzen durchgeführt wurden, bewirkten die geänderten Rahmenbedingungen des Austauschs innerhalb der DSK jedoch auch wichtige Impulse für die Intensivierung der Zusammenarbeit. Hierauf aufbauend gilt es wei-

terhin die Potenziale zur Fortentwicklung der DSK und der Diskussions- und Abstimmungsformate auszuschöpfen. Ausdrücklich zu begrüßen ist daher das im Koalitionsvertrag der neuen Bundesregierung benannte Vorhaben, die institutionelle Ausgestaltung der DSK gesetzlich zu regeln. In den diesbezüglichen Diskussionsprozess wird sich die DSK intensiv einbringen. Dabei dürften vor allem die Gestaltung einer effizienten Arbeitsweise und Struktur sowie die Schaffung verbindlicher Instrumente unter Wahrung der Unabhängigkeit der Aufsichtsbehörden im Vordergrund stehen.

An dieser Stelle möchte ich mich besonders bei meinen Mitarbeiterinnen und Mitarbeitern bedanken, denen es in diesem Jahr gelungen ist, ohne weitere personelle Verstärkung mit viel persönlichem Einsatz die Doppelbelastung von Aufsichtstätigkeit und Konferenzvorsitz in hervorragender Weise zu meistern.

Mit dem neuen Jahr verbinde ich persönlich die Hoffnung, dass mit Blick auf die stetig wachsenden Herausforderungen und Mehraufgaben die Handlungsfähigkeit unserer Behörde durch einen sachgerechten Stellenzuwachs gewährleistet wird.

Saarbrücken, im Juni 2022

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 Dienststelle gerichteten Anregungen, einem als datenschutzwidrig angenommenen Sachverhalt aufsichtsbehördlich nachzugehen, fließen mithin nicht in die Statistik ein. Diese werden ebenso wie (fern-)mündliche Beschwerden nur dann statistisch erfasst, wenn sie verschriftlicht werden und zu weitergehenden Maßnahmen Veranlassung geben.

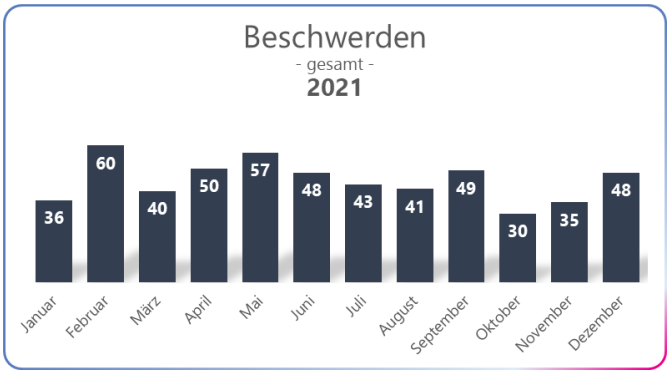

Abb. 1: Beschwerden (gesamt) 2021

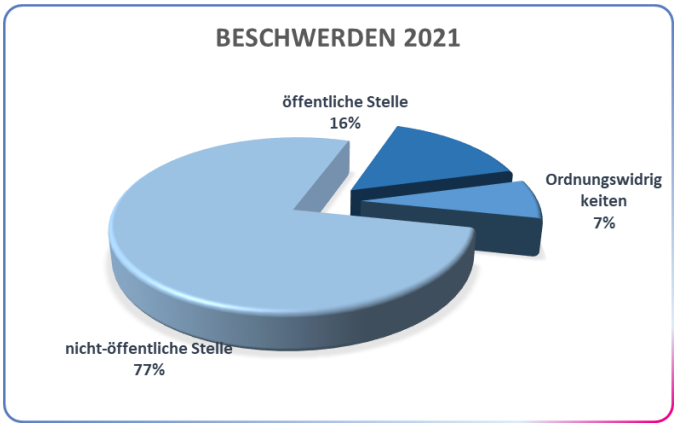

Abb. 2: Beschwerden (Aufteilung) 2021

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

Dienststelle gerichteten Anfragen darstellen und einen hohen zeitlichen Aufwand erfordern.

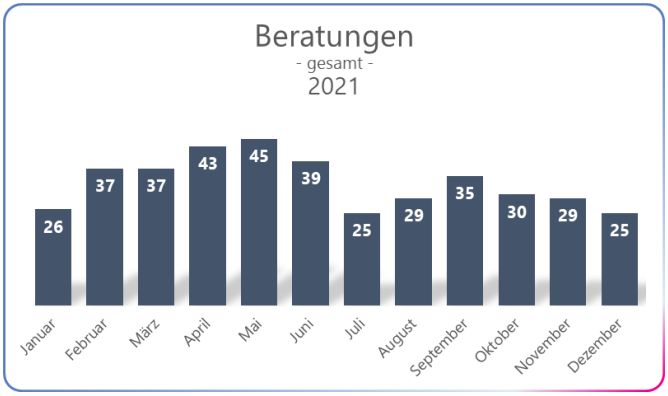

Abb. 3: Beratungen (gesamt) 2021

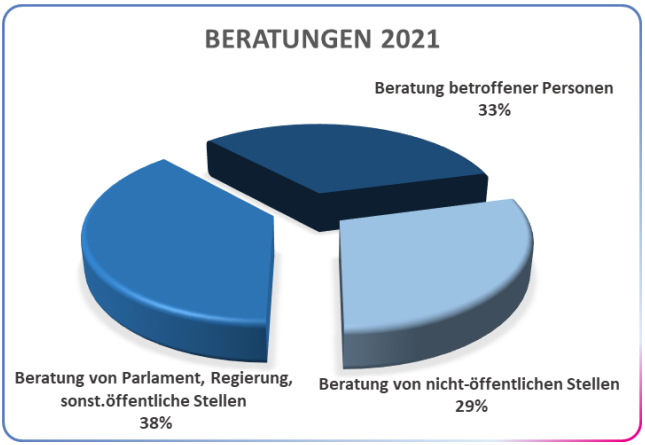

Abb. 4 Beratungen (Aufteilung) 2021

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.

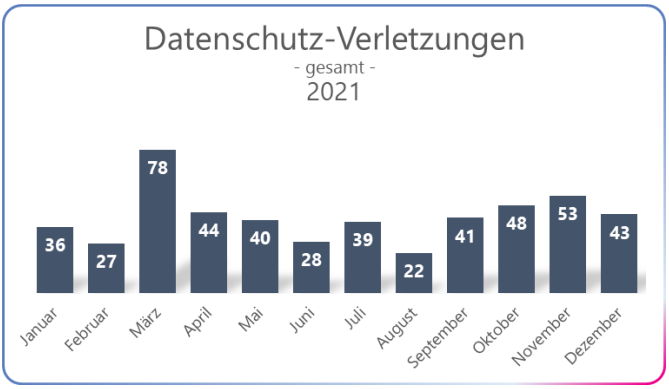

Abb. 5: Datenschutzverletzungen 2021

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.

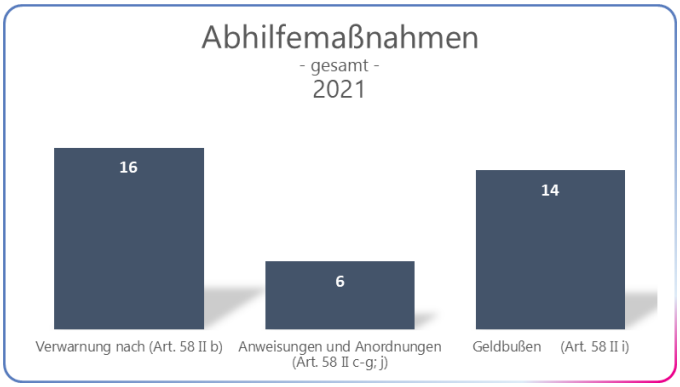

Abb. 5: Abhilfemaßnahmen (gesamt) 2021

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	382	11
Verfahren mit Federführung Art. 56 Abs. 2	65	0
Verfahren gem. Kapitel VII DSGVO	2053	858

Abb. 6: Europäische Verfahren (gesamt) 2021

Zu diesem Zweck hatte auch das UDZ im Jahr 2021 in insgesamt 553 Fällen zu beurteilen, inwieweit es als „betroffene Aufsichtsbehörde" im Sinne des Art. 4 Nr. 22 DSGVO gem. Art. 56 Abs. 1 DSGVO an diesen grenzüberschreitenden Verfahren zu beteiligen war, weil beispielweise eine Niederlassung der verarbeitenden Stelle im Saarland existiert oder weil auch saarländische Bürger von einer konkreten Verarbeitung erheblich betroffen sein könnten.
In 11 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.

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

1.6 Förmliche Begleitung von Rechtsetzungsvorhaben

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

Im Berichtzeitraum wurde das Unabhängige Datenschutzzentrum Saarland (UDZ) hiernach in 12 Rechtsetzungsvorhaben verfahrensbegleitend tätig.

II.

Aus der Dienststelle

2 Aus der Dienststelle

2.1 Vorsitz des Saarlandes in der Datenschutzkonferenz

Im Berichtsjahr hat die Landesbeauftragte für Datenschutz und Informationsfreiheit den Vorsitz der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) übernommen. Die DSK setzt sich aus insgesamt 18 unabhängigen Datenschutzaufsichtsbehörden[1] zusammen und hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und deutschen Datenschutzrechts zu erreichen sowie gemeinsam für seine Fortentwicklung einzutreten.[2] Die Aufgabe des Vorsitzes ist es dabei, die Sitzungen der DSK auszurichten, die Umsetzung der Arbeitsergebnisse zu veranlassen und die Konferenz nach außen zu vertreten.

Die DSK tagt zweimal im Jahr in sogenannten Hauptkonferenzen, die jeweils in einer Vorkonferenz von den Stellvertretern vorbereitet werden. Hinzu kommen in der Regel drei Zwischenkonferenzen sowie im Bedarfsfalle zusätzliche Sonderkonferenzen und schriftliche Umlaufverfahren. Des Weiteren findet zweimal im Jahr ein Austausch mit den sogenannten spezifischen Aufsichtsbehörden[3] statt. Für die in personeller Hinsicht kleinste aller Aufsichtsbehörden der DSK stellte dieses Programm eine besondere Herausforderung dar, da die reguläre Aufsichtstätigkeit parallel dazu mit dem vorhandenen Personal geleistet werden musste.

[1] Mitglieder der DSK sind 2021 namentlich der Bundesbeauftragte für den Datenschutz, die Landesbeauftragten für den Datenschutz und der Präsident des Bayerischen Landesamtes für Datenschutzaufsicht.

[2] Elektronisch abrufbar unter: https://www.datenschutzkonferenz-online.de/dsk.html

[3] z. B. der Kirchen, des Presserats sowie der Rundfunk- und Medienanstalten.

In der Summe gab es im Berichtsjahr 15 Konferenzen, die aufgrund der pandemischen Lage alle in Form von Videokonferenzen stattfinden mussten, und 17 schriftliche Umlaufverfahren. Ein immer wiederkehrendes Thema war auch im Jahr 2021 die Corona-Pandemie und die sich daraus ergebenden Maßnahmen. Zum Einsatz von digitalen Kontaktnachverfolgungssystemen wurde in diesem Zusammenhang eine entsprechende Orientierungshilfe[4] veröffentlicht. Auch zur Datenverarbeitung von Impf- und Testnachweisen in der Privatwirtschaft und im Beschäftigungsverhältnis hat die DSK Anwendungshilfen für Arbeitgeber veröffentlicht.

Des Weiteren beschäftigte sich die DSK wie bereits im Vorjahr mit dem Schrems-II-Urteil und den daraus folgenden Auswirkungen auf den Datentransfer in die USA und andere Drittstaaten. Neben anderen Fragestellungen hat diese Entscheidung auch Auswirkungen auf den Betrieb von Betriebssystemen und cloudbasierte Office-Anwendungen, die ebenfalls in der DSK thematisiert wurden.

Eine weitere Orientierungshilfe hat die DSK zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail erstellt, um den Verantwortlichen eine fachliche Handreichung zur Verfügung zu stellen.

Auch die Evaluierung des Bundesdatenschutzgesetzes (BDSG) fiel in den Zeitraum des Vorsitzes der DSK. Sowohl der Bund als auch einige Länder haben hierzu eine Stellungnahme abgegeben. Die Stellungnahme der Länder wurde in einem virtuellen Austausch mit dem Bundesministerium des Innern, für Bau und Heimat (BMI) und dem Bundesministerium für Justiz und Verbraucherschutz erörtert. Das BMI hat nunmehr auch seinen Evaluationsbericht vorgelegt.[5] Eine Überarbeitung des BDSG

[4] Alle Dokumente sind elektronisch abrufbar unter: https://www.datenschutzkonferenz-online.de/orientierungshilfen.html

[5] Elektronisch abrufbar unter: https://www.bmi.bund.de/SharedDocs/evaluierung-von-gesetzen/evaluierung-bdsg

konnte jedoch nicht mehr in der zu Ende gegangenen Legislaturperiode erfolgen und wird daher die Aufgabe des neuen Gesetzgebers sein. Es bleibt zu hoffen, dass die zahlreichen rechtlichen Erwägungen und praktischen Erfahrungen der Aufsichtsbehörden Beachtung finden werden und damit zu einer Klärung zahlreicher Rechtsunklarheiten beitragen.

Schließlich veröffentlichte die DSK eine Orientierungshilfe für Anbieter von Telemedien. Diese löst die bisherige Fassung ab und bietet Betreibern von Webseiten, Apps oder Smartphone-Anwendungen konkrete Hilfestellungen bei der Umsetzung der neuen Vorschriften des Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG). Mit der Veröffentlichung der Orientierungshilfe wurde zugleich beschlossen, Vertretern aus Politik, Wirtschaft, Wissenschaft, Gesellschaft und Verwaltung im Rahmen eines Konsultationsverfahrens Gelegenheit zur Stellungnahme hierzu zu geben.

Daneben gab es auch eine Reihe von spezifischen Themen wie etwa die Verarbeitung von Positivdaten durch Auskunfteien oder Anforderungen an datenschutzrechtliche Zertifizierungsprogramme.

Die DSK hat sich aber auch intern mit der Optimierung ihrer Zusammenarbeit befasst. In einem ersten Schritt wurde daher ein intensiverer Austausch zu aktuellen datenschutzrelevanten Themen auch außerhalb der regulären Konferenzen in einem wöchentlichen Jour fixe vereinbart. Des Weiteren wurde eine Änderung der Geschäftsordnung der DSK verabschiedet, in der das Ziel, möglichst einvernehmliche Entscheidungen innerhalb der DSK zu erzielen, zum Ausdruck gebracht wird. Die Anstrengungen der DSK zur Neugestaltung und Effektuierung ihrer Zusammenarbeit werden auch im kommenden Jahr fortgesetzt werden.

Zwar endete der Vorsitz offiziell mit Ablauf des Kalenderjahres 2021, jedoch verbleibt mit der Ausrichtung des 16. Europäischen Datenschutztages am 28.01.2022 noch eine Aufgabe, die dem jeweiligen Vorsitz des Vorjahres zufällt. Das Thema dieser

Veranstaltung lautet: „Die digitale Brieftasche in der EU – Datenschutz-Albtraum oder Meilenstein für die Gestaltung der digitalen Zukunft" und greift damit ein Vorhaben der EU-Kommission zur Einführung einer digitalen Identität auf, die es Bürgerinnen und Bürgern erlauben soll, sich EU-weit digital auszuweisen.

2.2 Zusammenarbeit mit dem Landtag

Im Berichtszeitraum hat das Unabhängige Datenschutzzentrum in dem im Landtag eingerichteten Unterausschuss für Datenschutz und Informationsfreiheit zu verschiedenen aktuellen datenschutzrechtlichen Themen Stellung genommen. Vermutlich pandemiebedingt kam der Ausschuss jedoch seltener zusammen, als dies in den Vorjahren üblich war.

Auch in weiteren Ausschüssen war die Expertise unserer Behörde sowohl im Rahmen von Anhörungen zu Gesetzgebungsverfahren als auch zu allgemeinen Datenschutzthemen, insbesondere zu datenschutzrechtliche Fragestellungen im Zusammenhang mit der fortdauernden Pandemie, gefragt. Hervorzuheben ist hierbei, dass sich die Abgeordneten des Gesundheitsausschusses ausdrücklich auch mit dem immer wieder erhobenen Vorwurf, der Datenschutz verhindere eine effektive Pandemiebekämpfung, auseinandergesetzt haben. Diesbezüglich konnten im Rahmen unserer Berichterstattung dahingehende Missverständnisse ausgeräumt werden

Da das Saarländische Datenschutzgesetz (SDSG) seit seiner Neufassung im Jahr 2018 der Landesbeauftragten für Datenschutz das Recht einräumt, auch dann an den Sitzungen der Ausschüsse des Landtages teilzunehmen, wenn dies nicht ausdrücklich durch den Ausschuss beantragt ist, konnte sich unsere Behörde in Ausschusssitzungen über Planungen und Projekte der Landesregierung informieren und, soweit erforderlich, diese kritisch begleiten.

Wie auch in den vorangegangenen Jahren war die Zusammenarbeit mit den verschiedenen Ausschüssen des Landtags durchgehend konstruktiv und vertrauensvoll.

2.3 Personal und Organisation

Bereits vor dem Geltungseintritt der DSGVO war die Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) trotz der Angliederung ihrer Dienststelle an den Landtag bei der Wahrnehmung ihrer Aufgaben an Weisungen nicht gebunden und insoweit auch keiner staatlichen Aufsicht unterworfen. Die hierdurch gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörde entsprach damit im Wesentlichen den Anforderungen der vor Inkrafttreten der DSGVO geltenden EU-Datenschutzrichtlinie und der Rechtsprechung des Europäischen Gerichtshofs.

Die Vorschriften der Art. 51 bis 54 DSGVO bekräftigen und konkretisieren die schon bisher geltenden Vorgaben an eine völlige Unabhängigkeit der Aufsichtsbehörden in Bezug auf organisatorisch-institutionelle, personelle und finanzielle Aspekte. Um diesen Vorgaben gerecht zu werden, wurde die Unabhängigkeit der LfDI sowohl durch entsprechende Regelungen im Saarländischen Datenschutzgesetz (SDSG) als auch hieran anknüpfende ergänzende Maßnahmen weiter gestärkt. So wurde eine weitere und entscheidende Stärkung der Unabhängigkeit dadurch erreicht, dass seit der Neufassung des SDSG im Jahr 2018 die Beschäftigten der Behörde nicht mehr nur im Einvernehmen mit der LfDI, sondern allein auf ihren Vorschlag ernannt und eingestellt werden. Konsequenterweise wurde mit dem Gesetz zur Anpassung des SDSG an die DSGVO zugleich klargestellt, dass künftig der Personalrat, die Frauenbeauftragte und die Schwerbehindertenvertretung unmittelbar bei der Dienststelle der LfDI zu wählen sind. Bis zu diesen Wahlen konnten deren Aufgaben durch die jeweiligen Interessenvertretungen der Landtagsverwaltung entsprechend der bisherigen Praxis weiterhin wahrgenommen werden. Daher wurden erstmals bei den im Berichtsjahr durchgeführten regulären Wahlen zu den Interessenvertretungen in der Dienststelle des Unabhängigen Datenschutzzentrums ein Personalrat sowie eine Frauenbeauftragte gewählt. Aus der institutionell-organisatorischen Unab-

hängigkeit der Behörde folgt zudem, dass nunmehr auch weitere Beauftragten-Funktionen, wie bspw. die für den Geheimschutz, die IT-Sicherheit oder die Korruptionsbekämpfung ausschließlich durch Mitarbeitende der Dienststelle und nicht mehr durch die jeweiligen Beauftragten der Landtagsverwaltung wahrgenommen werden.

Wenngleich diese weiteren, notwendigen Schritte auf dem Weg zur vollständigen institutionellen Unabhängigkeit der Aufsichtsbehörde unumwunden zu begrüßen sind, geht damit notwendigerweise einher, dass Mitarbeitende, die Tätigkeiten der Interessenvertretung oder Beauftragten-Funktionen wahrnehmen, von ihren sonstigen dienstlichen Aufgaben teilweise freizustellen oder zumindest angemessen zu entlasten sind. Angesichts der ohnehin äußerst knapp bemessenen Personalausstattung der Behörde, werden ohne sachgerechte Personalisierung die bestehenden Engpässe zu Lasten der Wahrnehmung der originären Aufsichtstätigkeit weiter verschärft.

Soweit die LfDI – wie dies auch bisher schon praktiziert wurde – nach § 16 Abs. 7 SDSG Aufgaben der Personalverwaltung und -wirtschaft auf die Landtagsverwaltung übertragen kann, wurde der Umfang und die Ausgestaltung dieser Übertragung nunmehr erstmals in einer Kooperationsvereinbarung zwischen der Landtagsverwaltung und unserer Behörde festgeschrieben.

Durch die regulatorischen Vorgaben und deren Umsetzung in der Praxis ist sichergestellt, dass eine externe Einflussnahme auf die Aufsichtsbehörde ausgeschlossen ist, auch wenn diese, anders als dies in anderen Bundesländern der Fall ist, bislang nicht den Status einer obersten Landesbehörde hat. Da indes zahlreiche landesgesetzliche Regelungen ein Handeln der obersten Landesbehörden auch für ihre nachgeordneten Behörden vorsehen, das Unabhängige Datenschutzzentrum jedoch weder als oberste Landesbehörde verfasst ist noch eine nachgeordnete Behörde des Landtags sein darf, ergeben sich mit Blick auf Zuständigkeiten häufig Unklarheiten und Fehleinschätzungen, die mitunter erhebliche Auswirkungen auf die Handlungsfähigkeit der Behörde haben. So verzögerte beispielsweise der aufgrund

nicht eindeutiger Vorgaben notwendige Abstimmungsprozess darüber, welche Stelle das für die ab 01.01.2022 verpflichtende Nutzung eines elektronischen Behördenpostfachs (beBPo) vorgeschaltete Identifizierungsverfahren[6] für das Unabhängige Datenschutzzentrum durchzuführen hat, die Implementierung dieser Kommunikationsinfrastruktur. Ohne den Zugang zu dem beBPO wäre jedoch in anhängigen verwaltungsgerichtlichen Verfahren die Abgabe von Prozesserklärungen nicht gewährleistet gewesen. Auch erreichen unsere Behörde aufgrund ihrer nicht eindeutigen Einordnung in die Behördenorganisation des Landes Informationen, die für die Verwaltungsabläufe aller Behörden des Landes relevant sind, häufig entweder nur über Umwege oder überhaupt nicht.

Um eine effektive Aufgabenwahrnehmung der Aufsichtsbehörde zu gewährleisten, bedarf es daher insoweit künftig klarer gesetzlicher Zuständigkeitsregelungen und verbindlicher administrativer Vereinbarungen.

[6] Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (§§ 6 Abs. 1 Nr. 2, 7 Abs. 1 ERVV).

III.

Datenschutz und Corona-Pandemie

3 Datenschutz und Corona-Pandemie

3.1 Kontaktnachverfolgungssysteme

3.1.1 Orientierungshilfe zu digitalen Kontaktnachverfolgungssystemen

Aufgrund der weiterhin anhaltenden Corona-Pandemie war unsere Dienststelle, wie viele andere Datenschutzaufsichtsbehörden auch, mit den datenschutzrechtlichen Implikationen von digitalen Kontaktnachverfolgungssystemen befasst. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) veröffentlichte in diesem Zusammenhang die „Orientierungshilfe zum Einsatz von digitalen Diensten zur Kontaktnachverfolgung anlässlich von Veranstaltungs-, Einrichtungs-, Restaurants- und Geschäftsbesuchen zur Verhinderung der Verbreitung von Covid-19“[7], in der die datenschutzrechtlichen Anforderungen insbesondere für Anbieter derartiger Systeme spezifiziert werden.

Die Orientierungshilfe hebt dabei unter anderem hervor, dass die datenschutzrechtlichen Verantwortlichkeiten aller Beteiligten vorab eindeutig zu bestimmen sind, da nur hierdurch hinreichende Klarheit dahingehend geschaffen wird, welche Stelle welchen datenschutzrechtlichen Anforderungen nachkommen muss und wer für die Rechte Betroffener einzustehen hat. Ausweislich der „Stellungnahme der DSK zur Verantwortlichkeit bei der Nutzung von Kontaktnachverfolgungssystemen wie der Luca App“[8] vom 21. Mai 2021 ist dabei eine datenschutzrechtliche Ausgestaltung des Verhältnisses zwischen Dienstbetreiber und Veranstaltern sowohl als Auftragsverarbeitung als auch als gemeinsame Verantwortlichkeit denkbar.

[7] Elektronisch abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20210429_DSK_OH_Kontaktnachverfolgung.pdf

[8] Elektronisch abrufbar unter: https://www.datenschutzkonferenz-online.de/media/st/DSK-Stellungnahme_Luca_Verantwortlichkeit.pdf

Besonderes Augenmerk beim Betrieb digitaler Kontaktnachverfolgungssysteme liegt auch auf den technischen und organisatorischen Maßnahmen. Es muss sichergestellt werden, dass ein Zugriff auf Kontaktdaten nur zweckgebunden durch die hierzu befugten Stellen erfolgen kann und dass die Daten kryptografisch hinreichend vor einem Zugriff durch unbefugte Dritte geschützt sind. Dabei sind eine dezentrale Speicherung von Daten bzw. eine dezentrale Erstellung und Speicherung der kryptografischen Schlüssel aus Gründen der Risikominimierung gegenüber zentral betriebenen Systemen vorzugswürdig. Aufgrund des konzeptionell denkbar vielgestaltigen Aufbaus derartiger Dienste ist eine detaillierte Analyse angezeigt, um die im Einzelfall erforderlichen Sicherheitsmaßnahmen bestimmen zu können. Diese Überprüfung muss vor Einsatz des Dienstes erfolgen und in einem Detailgrad dokumentiert werden, der es der Datenschutzaufsichtsbehörde ermöglicht, die Geeignetheit der ergriffenen technischen Maßnahmen zu überprüfen.

3.1.2 Corona-Warn-App

Mit ihrer Entschließung „Chancen der Corona-Warn-App 2.0 nutzen“[9] vom 29. April 2021 hatte die DSK Bund und Ländern empfohlen, der Corona-Warn-App (CWA) im Rahmen einer Evaluation und Anpassung der infektionsschutzrechtlichen Instrumente besondere Beachtung zu schenken und sie als datensparsamere Methode zur Benachrichtigung potentiell infizierter Personen zu berücksichtigen. Dabei ist bei der CWA positiv hervorzuheben, dass sie potentielle datenschutzrechtliche Risiken durch eine dezentrale Struktur minimiert und im Gegensatz zur klassischen Kontaktdatenerfassung auch eine pseudonyme Nutzung ermöglicht.

Der Bundesgesetzgeber hat dies mit der Neufassung des § 28a Abs. 7 Nr. 8 IfSG vom 22.11.2021 insoweit berücksichtigt, als nun

[9] Elektronisch abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20210429_DSK_Entschlie%C3%9Fung_Chancen_der_CWA_2.0_nutzen.pdf

durch die Bundesländer in den Corona-Verordnungen der Einsatz der Corona-Warn-App als Instrument vorgesehen werden kann. In der Gesetzesbegründung geht auch der Gesetzgeber davon aus, dass es sich bei der CWA *„mit ihrer besonders datensparsamen Ausgestaltung um eine sinnvolle Alternative zur Kontaktdatenverarbeitung"* handelt, eine *„Bereitstellung der QR-Registrierung (...) insofern ausreichend und abschließend [ist]"* und beim Einsatz der CWA auf eine Pflicht zur Erfassung von Kontaktdaten verzichtet werden kann (BT-Drs. 20/89, S.14 f.).

Auf die Sinnhaftigkeit des Einsatzes der CWA wurde das Ministerium für Soziales, Gesundheit, Frauen und Familie im Berichtszeitraum seitens unserer Dienststelle mehrfach hingewiesen. In diesem Zusammenhang wurde angeregt, bei einer erneuten Änderung des Saarländischen COVID-19-Maßnahmengesetzes den Einsatz der CWA als Alternative neben einer Kontaktdatenerfassung bei Kunden, Gästen oder Veranstaltungsteilnehmern zu ermöglichen, da die CWA nicht nur datensparsamer ist, sondern auch zu einer Entlastung der Gesundheitsämter beitragen würde, denen eine klassische Kontaktnachverfolgung je nach Ausmaß des Infektionsgeschehens in der Vergangenheit nicht immer möglich war.

Empfehlung:

Digitale Kontaktnachverfolgungssysteme unterliegen hohen datenschutzrechtlichen Anforderungen, die vom Betreiber des Systems vorher zu prüfen sind. Die Corona-Warn-App (CWA) ist aufgrund ihrer datenschutzfreundlichen Ausgestaltung anderen Diensten vorzugswürdig. Die vom Bundesgesetzgeber geschaffene Möglichkeit, die CWA als Alternative zur personenbezogenen Kontaktnachverfolgung anzubieten, sollte vom Landesgesetzgeber wahrgenommen werden.

3.2 System zur Terminvergabe in den saarländischen Impfzentren

Eine Impfung gegen das Coronavirus gilt als wichtigstes Mittel zur Eindämmung der Covid-19-Pandemie. Um möglichst zeitnah nach der Zulassung der ersten Impfstoffe in Deutschland einem großen Teil der Bevölkerung eine Impfung anbieten zu können, hatte die saarländische Landesregierung im Dezember 2020 vier Impfzentren im Saarland errichtet. Termine für eine Impfung konnten sowohl telefonisch als auch online gebucht werden.

Bei Prüfung der Online-Plattform zur Terminbuchung, welche unter https://www.impfen-saarland.de/ durch das Ministerium für Soziales, Gesundheit, Frauen und Familie (MSGFF) bereitgestellt wurde, mussten wir verschiedene datenschutzrechtliche Mängel feststellen.

So wurde in der Datenschutzerklärung der Website beispielsweise der externe Anbieter der Plattform als Verantwortlicher im datenschutzrechtlichen Sinne genannt und nicht das MSGFF als diesbezüglicher Aufgabenträger. Es war jedoch von einer datenschutzrechtlichen Auftragsverarbeitung nach Art. 28 DSGVO auszugehen, bei der das Ministerium als verantwortliche Stelle und der Anbieter als Auftragsverarbeiter einzustufen ist.

Auch war aus den Angaben in den Datenschutzhinweisen nicht eindeutig erkennbar, auf welche Rechtsgrundlage das MSGFF die Datenverarbeitung im Kontext der Impfterminvergabe stützt. Die Rechtsgrundlage ist jedoch den betroffenen Personen nach Art. 13 Abs. 1 lit. c DSGVO mitzuteilen.

Weitere Fragen ergaben sich hinsichtlich der Zulässigkeit der Einbindung von externen Diensten mit Drittlandtransfers und der Verschlüsselung der Website.

In Gesprächen zwischen dem MSGFF und unserer Dienststelle wurden die datenschutzrechtlichen Aspekte der Terminvergabe ausführlich erörtert, wobei das Ministerium Nachbesserungen und Klarstellungen zugesagt hat.

Im Zuge der teilweisen Wiederinbetriebnahme der saarländischen Impfzentren im November 2021 wurden die erforderlichen Änderungen im Online-Buchungssystem durch das MSGFF vorgenommen. Nach Überarbeitung der Datenschutzhinweise und durch technische Anpassungen war daher von einem datenschutzkonformen Zustand auszugehen, so dass von unserer Seite kein weiterer Handlungsbedarf festgestellt wurde.

Dass die Bekämpfung der Corona-Pandemie auch die saarländische Landesregierung und besonders das zuständige Ministerium vor immense Herausforderungen stellt, ist unbestritten. Angesichts sich stetig ändernder pandemischer Bedingungen müssen oft kurzfristig Regelungen zu komplexen Sachzusammenhängen getroffen und zeitnah Lösungen für akute Problemstellungen gefunden werden. Wenn unter diesem Zeitdruck neue Verfahren implementiert werden, die mit einer umfangreichen Verarbeitung personenbezogener Daten einhergehen, dürfen jedoch auch in dieser schwierigen Situation datenschutzrechtliche Belange nicht vernachlässigt werden. Unsere Dienstelle steht für Austausch und Beratung stets zur Verfügung und würde es begrüßen, wenn die zuständigen Stellen entsprechend den gesetzlichen Vorgaben in § 19 Abs. 2 SDSG bereits frühzeitig unsere Unterstützung in Anspruch nähmen.

Fazit/ Empfehlung:

Beim Online-Verfahren zur Vergabe von Impfterminen konnte in Zusammenarbeit mit dem zuständigen Ministerium ein datenschutzkonformer Zustand erreicht werden. Eine frühzeitige Einbindung des Datenschutzzentrums in derartige Prozesse wäre wünschenswert.

3.3 Datenverarbeitung in Corona-Testzentren

Nach den Vorgaben der Coronavirus-Testverordnung (TestV)[10] hatten ab dem 8. März 2021 alle asymptomatischen Bürgerinnen und Bürger mit Wohnsitz oder gewöhnlichem Aufenthalt in Deutschland Anspruch darauf, sich mindestens einmal pro Woche kostenlos mittels eines PoC-Antigen-Schnelltests auf eine Infektion mit SARS-CoV-2 testen zu lassen. Aus der TestV ergab sich eine Berechtigung zur Durchführung von Testungen für die zuständigen Stellen des öffentlichen Gesundheitsdienstes (insbesondere Gesundheitsämter) sowie medizinische Einrichtungen wie Arztpraxen und Apotheken. Daneben konnten aber auch weitere (private) Anbieter, die eine ordnungsgemäße Durchführung garantierten, mit der Leistungserbringung beauftragt werden.

Die Vorgabe der „ordnungsgemäßen Durchführung" wurde in späteren Fassungen der TestV dahingehend konkretisiert, dass die Leistungserbringer unter Einhaltung der infektionsschutzrechtlichen, medizinprodukterechtlichen und arbeitsschutzrechtlichen Anforderungen eine ordnungsgemäße Erbringung der Leistungen gewährleisten sowie die erforderliche Zuverlässigkeit aufweisen müssen. Konkrete datenschutzrechtliche Vorgaben für die weiteren Leistungserbringer enthielt die Verordnung bedauerlicherweise nicht. Allerdings wurde durch eine Änderung der TestV[11] zumindest eine Ergänzung dahingehend vorgenommen, dass die Leistungserbringer einer Geheimhaltungspflicht nach § 203 des Strafgesetzbuchs oder einer vertraglich vereinbarten Geheimhaltungspflicht unterliegen müssen.

[10] Verordnung zum Anspruch auf Testung in Bezug auf einen direkten Erregernachweis des Coronavirus SARS-CoV-2 (Coronavirus-Testverordnung – TestV) vom 8. März 2021 (BAnz AT 09.03.2021 V1).

[11] Verordnung zur Änderung der Coronavirus-Testverordnung, der DIVI IntensivRegister-Verordnung und der Coronavirus-Surveillanceverordnung vom 12. November 2021 (BAnz AT 12.11.2021 V1).

Im Saarland wurden neben den von der Landesregierung betriebenen Testzentren auch Testmöglichkeiten durch eine Vielzahl privater Anbieter geschaffen. Die Tätigkeit der Testzentren bedingt notwendigerweise die Verarbeitung sensibler personenbezogener Daten, da die Information über das Vorliegen oder Nicht-Vorliegen einer Infektion mit dem Coronavirus ein Gesundheitsdatum im Sinne von Art. 4 Nr. 15 DSGVO darstellt. Gesundheitsdaten gehören zu den besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO, für die ein erhöhter Schutzbedarf besteht.

Unter den Betreibern der Testzentren fanden sich zahlreiche Anbieter aus verschiedensten Bereichen, deren gewöhnliche Geschäftszwecke nicht mit der systematischen Verarbeitung von Gesundheitsdaten einhergehen. Auf Grund von Beschwerden und Anfragen, die das Unabhängige Datenschutzzentrum erreicht haben, ergaben sich Zweifel daran, dass die Umsetzung angemessener Schutzmaßnahmen bei der Datenverarbeitung immer zufriedenstellend erfolgt.

Gegenstand von Beschwerden waren beispielsweise der Fehlversand von Testergebnissen per E-Mail, die Abrufmöglichkeit von Testdaten über die Internetseite eines Testzentrums ohne angemessenen Zugriffsschutz und mangelnde Diskretion bei der Mitteilung des Ergebnisses vor Ort.

Wiederholt wurde die Frage aufgeworfen, ob die Personalausweisnummer bei Buchung eines Testtermins zwingend anzugeben ist. Hier wurde gegenüber den Betreibern klargestellt, dass diese nur auf freiwilliger Basis erhoben werden darf, beispielsweise wenn die betroffene Person im grenzüberschreitenden Verkehr einen Testnachweis mit Ausweisnummer benötigt. Eine Rechtsgrundlage für die generelle Erhebung der Ausweisnummer existiert jedoch nicht.

Unklar war zunächst, ob die Testzentren personenbezogene Daten speichern dürfen bzw. müssen und für welchen Zeitraum diese aufzubewahren sind. Zum Teil wurde die Auffassung ver-

treten, dass insbesondere zu Abrechnungszwecken anonymisierte Daten ausreichend seien und es für eine Speicherung personenbezogener Daten an der Erforderlichkeit fehle. Diesbezüglich erfolgte durch die Neufassung der TestV vom 24. Juni 2021[12] eine Klarstellung dahingehend, dass zwecks Auftrags- und Leistungsdokumentation eine Aufbewahrung der personenbezogenen Daten (unter anderem Name, Anschrift und Testergebnis) bis zum 31. Dezember 2024 zu erfolgen hat. Dies wurde in der Fassung der TestV vom 21. September 2021[13] dahingehend geändert, dass für das Testergebnis die Aufbewahrungsfrist auf den 31. Dezember 2022 verkürzt wurde, was aus datenschutzrechtlicher Sicht zu begrüßen ist.

Das Unabhängige Datenschutzzentrum hat vor dem Hintergrund der eingegangenen Anfragen und Beschwerden eine Fragebogenaktion durchgeführt, um stichprobenartig die Datenverarbeitungsprozesse in den Testzentren zu überprüfen. Dabei wurde unter anderem abgefragt, welche Daten bei Terminvereinbarung und Testung erhoben werden, welche Aufbewahrungsfristen zu Grunde gelegt werden, ob ein Berechtigungs- und Löschkonzept für das verwendete IT-System etabliert und ob ein Datenschutzbeauftragter benannt wurde. Nach Auswertung der Ergebnisse werden wir den Anbietern eine Orientierungshilfe für den datenschutzkonformen Betrieb der Testzentren zur Verfügung stellen.

Fazit/ Empfehlung:

Die Betreiber von Corona-Testzentren müssen sich der Sensibilität der von ihnen verarbeiteten personenbezogenen Daten bewusst sein und entsprechende technisch-organisatorische Maßnahmen zum Schutz der Daten ergreifen.

[12] Verordnung zum Anspruch auf Testung in Bezug auf einen direkten Erregernachweis des Coronavirus SARS-CoV-2 (Coronavirus-Testverordnung – TestV) vom 24. Juni 2021 (BAnz AT 25.06.2021 V1).

[13] Verordnung zum Anspruch auf Testung in Bezug auf einen direkten Erregernachweis des Coronavirus SARS-CoV-2 (Coronavirus-Testverordnung – TestV) vom 21. September 2021 (BAnz AT 21.09.2021 V1).

3.4 Corona-Testpflicht an Schulen

Am 19. April 2021 wurde für die Schüler/innen, Lehrkräfte und Beschäftigten an den saarländischen Schulen die Pflicht zur Durchführung von Covid-19-Schnelltests eingeführt.

Gem. § 1 Abs. 3 der Verordnung zum Schulbetrieb und zum Betrieb sonstiger Bildungseinrichtungen sowie zum Betrieb von Kindertageseinrichtungen während der Corona-Pandemie ist die Teilnahme am Präsenzschulbetrieb nur für Schüler/innen, Lehrkräfte und sonstige an der Schule tätige Personen zulässig, die zweimal in der Woche einen Nachweis über einen negativen Covid-19-Schnelltest vorlegen. Diese Testpflicht kann entweder durch die Teilnahme an den zweimal wöchentlich angebotenen schulischen Tests erfüllt werden oder indem ein anderweitiger Nachweis über das Nichtvorliegen einer Infektion mit dem Coronavirus vorgelegt wird, z. B. aus einem Testzentrum oder einer Apotheke. Ein anderweitiger Nachweis ist dann zu akzeptieren, wenn er auf einer Testung beruht, die am Vortag der an der Schule angebotenen Testung oder am gleichen Tag durchgeführt wurde. Wird kein negativer Test vorgelegt, gilt ein Zutrittsverbot zur Schule, soweit der Testung im Ausnahmefall keine zwingenden Gründe entgegenstehen. Das Vorliegen derartiger Gründe ist durch ärztliches Attest nachzuweisen.

Die von den Schulen angebotenen Tests werden in der Regel im Klassenverbund durchgeführt. Die Testergebnisse werden den Schüler/innen jeweils persönlich mitgeteilt. Bei einem positiven Testergebnis informiert die Schule umgehend die Eltern oder Sorgeberechtigten, damit sie ihre Kinder in der Schule abholen. Die positiv getesteten Schüler/innen werden nach Feststellung des positiven Ergebnisses in einen gesonderten Raum geführt und dort betreut oder nach Zustimmung der Erziehungsberechtigten unter Beachtung der Hygieneregeln (Maske tragen, Abstand halten) selbstständig nach Hause geschickt. Das zuständige Gesundheitsamt wird bei positivem Testergebnis von der Schule informiert und koordiniert dann die weiteren Schritte.

Die Absonderung der Schüler/innen nach Vorliegen eines positiven Testergebnisses sorgte bei einigen Eltern für Unmut, da sie befürchteten, ihre Kinder würden als „mit dem Coronavirus infiziert" stigmatisiert und ein besonders schützenswertes Gesundheitsdatum würde somit der kompletten Klassengemeinschaft bekannt gegeben, da der betroffene Schüler oder die betroffene Schülerin nicht mehr am anschließenden Unterricht teilnehmen könne. Mit dieser Befürchtung wandten sich die Eltern an unsere Dienststelle und kritisierten das Vorgehen der Testung in saarländischen Schulen als nicht datenschutzkonform.

Dadurch, dass der Verordnungsgeber den Erziehungsberechtigten die Möglichkeit eingeräumt hat, alternativ auch den Nachweis durch einen Test in einem anerkannten Testzentrum erbringen zu können, haben die Eltern die Möglichkeit, einer eventuellen Offenbarung eines Verdachts der Ansteckung mit dem Coronavirus bei ihren Kindern entgegenzuwirken. So kann gewährleistet werden, dass lediglich die Erziehungsberechtigten und das zuständige Gesundheitsamt von dem positiven Testergebnis erfahren und verpflichtet sind, alle erforderlichen weiteren Schritte zur Vermeidung der Weitergabe des Virus einzuleiten.

Fazit/ Empfehlung:

Durch die vom Verordnungsgeber eingeräumte Möglichkeit, den erforderlichen Testnachweis in der Schule auch durch einen Nachweis aus einem anerkannten Testzentrum zu erbringen, ist die klassenweise Testung in Schulen datenschutzrechtlich nicht zu beanstanden.

3.5 Abfrage des Impfstatus durch den Arbeitgeber

Das Infektionsschutzgesetz (IfSG) eröffnet dem Arbeitgeber die Möglichkeit, zu verschiedenen Zwecken den Impf-, Sero- oder Teststatus seiner Beschäftigten abzufragen und zu verarbeiten. Der Impf- oder Genesenenstatus sowie das Testergebnis eines

Covid-19-Tests gehören als Gesundheitsdaten zu den besonders geschützten Daten, die grundsätzlich nicht verarbeitet werden dürfen (Art. 9 Abs. 1 DSGVO). Allerdings lässt die DSGVO auch Ausnahmen von diesem Verarbeitungsverbot zu, etwa aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit (Art. 9 Abs. 2 lit. i DSGVO). Der Gesetzgeber hat im IfSG verschiedene Szenarien festgelegt, in denen das öffentliche Interesse im Bereich der Gesundheit eine Verarbeitung von Gesundheitsdaten durch den Arbeitgeber legitimiert. Die neu geschaffenen Befugnisse zur Abfrage der Daten bei den Beschäftigten sorgten für eine Flut von Anfragen an unsere Dienststelle, ob die jeweilige Datenverarbeitung im vorgesehenen Umfang legitim und datenschutzkonform ist. Um datenschutzrechtlich Klarheit in diesen und anderen Fragestellungen zu schaffen, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder eine Orientierungshilfe zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie veröffentlicht, die über die Website der Datenschutzkonferenz abrufbar ist.[14]

In den folgenden Berichten wird daher nur auf ausgewählte Aspekte der Abfrage des Impf- oder Serostatus oder von Testergebnissen der Beschäftigten durch den Arbeitgeber in den gesetzlich vorgesehenen Szenarien aus datenschutzrechtlicher Sicht eingegangen.

3.5.1 Entschädigungsleistung nach § 56 IfSG

Für viel Verwirrung und Unsicherheit sowohl auf Seiten der Arbeitgeber als auch auf Seiten der Arbeitnehmer sorgte die Möglichkeit, den Impfstatus abfragen zu dürfen, um bei einer Quarantäneanordnung den Entschädigungsanspruch für einen Verdienstausfall nach § 56 Abs. 1 S. 4 IfSG zu überprüfen.

Grundsätzlich haben Arbeitnehmer einen Anspruch auf eine Entschädigung nach dem Infektionsschutzgesetz, wenn sie auf

[14] Elektronisch abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_dsk _anwendungshilfe.pdf

Grund einer behördlichen Anordnung unter Quarantäne stehen und deswegen nicht arbeiten dürfen. In der Regel erhalten die Arbeitnehmer die Entschädigung als Lohnfortzahlung von ihren Arbeitgebern, die sich die Entschädigung im Nachhinein von dem zuständigen Ministerium erstatten lassen können. Beschäftigte, die eine Quarantäne durch Inanspruchnahme einer Schutzimpfung hätten vermeiden können, haben jedoch seit November 2021 keinen Anspruch mehr auf diese Entschädigung nach dem Infektionsschutzgesetz (§ 56 Abs. 1 S. 4 IfSG). Laut Beschluss der Gesundheitsministerkonferenz vom 22. September 2021 sind davon ausgenommen lediglich Beschäftigte, die sich aus medizinischen Gründen nicht impfen lassen konnten und ein entsprechendes Attest vorlegen sowie Personen, die zu einem Personenkreis gehören, für den es bis zu acht Wochen vor der Quarantäne keine öffentliche Impfempfehlung gab.

Die Lohnfortzahlung im Krankheitsfall ist davon nicht betroffen. Wer an Covid-19 erkrankt, hat unabhängig von seinem Impfstatus weiterhin Anspruch auf Entgeltfortzahlung und Krankengeld.

Zum Zweck der Prüfung, ob ein Ausschlussgrund gem. § 56 Abs. 1 S. 4 IfSG vorliegt, kann es demnach erforderlich sein, dass der Arbeitgeber im Falle einer behördlich verhängten Quarantänemaßnahme im Zusammenhang mit Covid-19 den Impf- oder Serostatus der Beschäftigten abfragt.

Eine Nachfrage unsererseits beim zuständigen Ministerium für Soziales, Gesundheit, Frauen und Familien zum Verfahrensablauf eines Entschädigungsanspruchs bei Verdienstausfall wegen Covid-19-Quarantänemaßnahmen blieb bis zur Einführung der 3G-Regelung am Arbeitsplatz leider unbeantwortet und konnte somit nicht zur rechtskonformen Auslegung der Vorschrift beitragen. Mangels genauerer Ausführungen im Gesetzestext verlangten viele Arbeitgeber in Folge dessen von jedem Beschäftigten im Unternehmen den Nachweis einer Schutzimpfung, unabhängig davon, ob eine Quarantäneverfügung vorlag. Als Begründung wurde angeführt, man wolle im Falle einer möglichen

Quarantäne bereits vorher wissen, bei wem ein Lohnfortzahlungsanspruch bestehen würde und bei wem nicht. Bei diesbezüglichen Beschwerden, die unsere Dienststelle erreichten, konnte durch Beratung der Arbeitgeberseite das Vorgehen dahingehend datenschutzkonform gestaltet werden, dass lediglich im Falle einer vorliegenden Quarantäneverfügung der Nachweis einer Schutzimpfung zur Geltendmachung des Entschädigungsanspruchs für einen Verdienstausfall bei Quarantäne nach § 56 Abs. 1 S. 4 IfSG erhoben werden darf. Eine Klarstellung durch den Gesetzgeber und das für die Umsetzung zuständige Ministerium wäre in diesem Zusammenhang wünschenswert gewesen, um unzulässigen Datenerhebungen auf Seiten der Arbeitgeber und Rechtsunsicherheiten auf Seiten der Beschäftigten entgegenzuwirken.

3.5.2 3G-Nachweis am Arbeitsplatz

Die Neufassung des § 28b IfSG im November 2021 verursachte aufgrund der nicht normenklaren Formulierung und der daraus folgenden Auslegungsbedürftigkeit der Norm ebenfalls viel Klärungsbedarf bei Arbeitgebern, Beschäftigten und Gewerkschaften und führte daher ebenfalls zu zahlreichen Anfragen an unsere Behörde. Nach der sog. „3G am Arbeitsplatz"-Regel dürfen Arbeitsstätten, in denen physische Kontakte untereinander oder zu Dritten nicht ausgeschlossen werden können, von Arbeitgebern und Beschäftigten nur betreten werden, wenn diese geimpft, genesen oder getestet sind und einen entsprechenden Nachweis mit sich führen, zur Kontrolle verfügbar halten oder bei dem Arbeitgeber hinterlegt haben.

Bei der Frage, ob eine Kopie des Impf- oder Genesenenausweises oder eines negativen Testergebnisses durch den Arbeitgeber angefordert werden kann, ist der Grundsatz der Datensparsamkeit gem. Art. 5 Abs. 1 lit. c DSGVO für die erforderliche Rechtsauslegung heranzuziehen. Nur das, was zur Erfüllung der gesetzlichen Vorgaben unbedingt erforderlich ist, darf auch verarbeitet werden. Grundsätzlich sind nur das Zutrittsdatum, der Vor- und Zuname des jeweiligen Beschäftigten sowie die Tatsa-

che, dass ein 3G-Nachweis vorgelegt worden ist, für die Zutrittskontrolle erforderlich und dementsprechend zu erheben. Die Dokumentation kann mittels einer Liste in Papierform oder in digitaler Form geschehen. Dabei ist nicht zu unterscheiden, um welche Art des 3G-Nachweises es sich handelt. Die verpflichtende Vorlage einer Kopie der Nachweise zur weiteren Verwendung durch den Arbeitgeber scheidet demnach aus.

Die Anfertigung einer Kopie des Impf- oder Genesenennachweises oder eines negativen Testergebnisses durch Arbeitgeber ist ausschließlich auf Grundlage einer freiwilligen Einwilligung nach § 26 Abs. 2 und Abs. 3 BDSG i. V. m. Art. 9 Abs. 2 lit. a DSGVO möglich. Dabei dürfen den Beschäftigten, die eine Vorlage der Kopie verweigern, keine rechtlichen Nachteile von Seiten der Arbeitgeber angedroht werden. Eine andere Rechtsgrundlage als die Einwilligung kommt hier nicht in Betracht.

3.5.3 Unzulässige 3G-Status-Abfrage durch eine Körperschaft des öffentlichen Rechts

Bei einer Körperschaft des öffentlichen Rechts, die von all ihren Beschäftigten schon vor der Einführung der 3G-Pflicht am Arbeitsplatz einen entsprechenden Nachweis einforderte, mussten wir erst eine Beanstandung gem. § 20 Abs. 2 SDSG aussprechen, bis die Körperschaft die beanstandete Datenverarbeitung einstellte und alle bis dahin erfassten Daten in diesem Sachzusammenhang löschte. Die Körperschaft berief sich als Rechtsgrundlage für die Datenverarbeitung auf eine Einwilligung ihrer Beschäftigten. Mit ihrer an die Beschäftigten gerichteten Aufforderung zur Erteilung der Einwilligung war unter anderem jedoch auch die Ankündigung verbunden, bei Versagung der Einwilligung den bisherigen Telearbeitsplatz oder die Möglichkeit, Außentermine wahrzunehmen, zu verlieren.

Eine Einwilligung kann jedoch nur dann eine wirksame Rechtsgrundlage für eine Datenverarbeitung darstellen, wenn sie freiwillig erteilt wird. Dass eine Einwilligung bei einem klaren Ungleichgewicht zwischen betroffener Person und dem Verantwortlichen nicht als freiwillig angesehen werden kann, ergibt

sich bereits aus Erwägungsgrund 43 der DSGVO. Daher ist gerade im Beschäftigungskontext aufgrund des strukturellen Ungleichgewichts zwischen Arbeitgeber und Beschäftigten die Freiwilligkeit einer Einwilligung regelmäßig zu hinterfragen. Wenn, so wie in der Dienstverfügung der Körperschaft erwähnt, eine Untersagung bestimmter Tätigkeiten (Außenkontakte, Telearbeit) mit der Nichterteilung der Einwilligung verbunden ist, kann nicht von einer freiwillig erteilten Einwilligung im Sinne der DSGVO ausgegangen werden. Dies bedeutete, dass die Erhebung des Impfstatus der Beschäftigten durch die Körperschaft datenschutzrechtlich unzulässig war, da sie auf einer den Anforderungen der DSGVO nicht entsprechenden und somit unwirksamen Einwilligungserklärung basierte.

Nachdem wir eine förmliche Beanstandung ausgesprochen hatten, konnte mit Unterstützung der für die Körperschaft zuständigen Fachaufsichtsbehörde ein datenschutzkonformer Zustand hergestellt werden.

Fazit/ Empfehlung:

Die Verarbeitung von Gesundheitsdaten durch Arbeitgeber unterliegt strengen Vorgaben. Im Zusammenhang mit den im Infektionsschutzgesetz genannten Ausnahmetatbeständen ist die Verarbeitung dieser Daten durch die Arbeitgeber gesetzlich vorgegeben und somit erforderlich zur Durchführung des Beschäftigungsverhältnisses. Eine normenklarere Ausführung durch den Gesetzgeber zu datenschutzrechtlich relevanten Abläufen im Betrieb wäre bei solchen kurzfristig umzusetzenden Maßnahmen und Eingriffen in die Persönlichkeitsrechte der Beschäftigten begrüßenswert gewesen, da auf Seiten der Arbeitgeber, Gewerkschaften und Beschäftigten eine große Unsicherheit herrschte, ob sie rechtskonform handeln.

3.6 „Homeoffice“ in Paraguay

Abgesehen von Datenübermittlungen in die USA im Kontext des Schrems II-Urteils des EuGH spielen Fragen aus dem Bereich des

internationalen Datenverkehrs in der täglichen Beratungspraxis unserer Dienststelle in der Regel keine große Rolle. Es kommt aber auch hier immer wieder vor, dass wir mit kurios anmutenden Beratungsanfragen konfrontiert werden.

Aus nicht näher bekannten Gründen ist bei einer Mitarbeiterin einer saarländischen Kommune wohl die Idee gereift, nach Paraguay auszuwandern. Auf Grund der im Zuge der Corona-Pandemie durch ihren Arbeitgeber geschaffenen Voraussetzungen zum Homeoffice sah die Mitarbeiterin offensichtlich die Möglichkeit, ihren Lebensunterhalt auch in Paraguay zukünftig dadurch zu sichern, dass sie weiterhin als Beschäftigte für die Kommune tätig sein könne, nur dass sie ihre Arbeitsleistung nunmehr aus dem „Homeoffice" in Paraguay erfüllen wollte.

Dieses Ansinnen traf beim Arbeitgeber zunächst augenscheinlich auf Wohlwollen, da dieser sich an uns wandte mit der Bitte um Hinweise, wie eine solche Konstellation datenschutzrechtlich abgebildet werden könne, da die Mitarbeiterin auch Zugang zu personenbezogenen Daten habe.

Werden personenbezogene Daten an Stellen außerhalb des Europäischen Wirtschaftsraumes weitergegeben, so bedarf dies einer besonderen rechtlichen Grundlage. Diese sogenannten Drittlandtransfers sind in den Art. 44 bis 50 der Datenschutz-Grundverordnung (DSGVO) geregelt. Die Vorgaben gelten für alle Transfers personenbezogener Daten, bei denen der Datenexporteur dem europäischen Datenschutzrecht unterfällt und der Datenimporteur in einem Drittland ansässig ist. Hierzu zählen insbesondere auch Fälle, in denen – wie hier – aus dem Drittland Zugriff auf in der Europäischen Union gespeicherte personenbezogene Daten genommen wird.

Sofern ein solcher Drittlandtransfer vorliegt, sieht die DSGVO verschiedene Instrumente vor, mit denen dieser abgesichert werden kann. Zu den relevantesten Instrumenten gehören Datenübermittlungen auf der Grundlage eines sog. Angemessenheitsbeschlusses (Art. 45 DSGVO). In diesem stellt die Europäische Kommission fest, dass personenbezogene Daten in einem

bestimmten Drittland einen mit dem Europäischen Datenschutzrecht vergleichbaren adäquaten Schutz genießen. Liegt ein solcher Angemessenheitsbeschluss nicht vor, ist die Datenübermittlung in ein Drittland nur zulässig, sofern geeignete, in Art. 46 Abs. 2 und 3 DSGVO vorgesehene Garantien zur Gewährleistung eines angemessenen Schutzniveaus ergriffen werden oder wenn die Datenübermittlung ausnahmsweise für bestimmte Fälle zugelassen ist (Art. 49 DSGVO).

Da für Paraguay kein Angemessenheitsbeschluss der Europäischen Kommission existiert und auch die in Art. 49 DSGVO genannten Ausnahmefälle in dem uns geschilderten Fall nicht einschlägig waren, musste die datenschutzrechtliche Zulässigkeit am Maßstab des Art. 46 DSGVO beurteilt werden.

Nachdem wir die anfragende Kommune mit Blick auf die Anforderungen, die sich aus Art. 46 Abs. 1 DSGVO ergeben, umfassend beraten haben, hörten wir erst einmal nichts mehr. Im Rahmen einer weiteren Beratungsanfrage derselben Kommune wurde uns auf Nachfrage mitgeteilt, dass man seitens der Kommune von dem Vorhaben mittlerweile Abstand genommen habe. Ob die Mitarbeiterin trotzdem ausgewandert ist, ist hier nicht bekannt.

Wäre die Mitarbeiterin nicht nach Paraguay, sondern in das ebenfalls in Südamerika liegende Uruguay ausgewandert, wären die Erfolgsaussichten möglicherweise höher gewesen. Anders als im Falle Paraguays existiert für Uruguay nämlich ein Angemessenheitsbeschluss der EU-Kommission nach Art. 45 Abs. 3 DSGVO, der jedenfalls die datenschutzrechtlichen Hürden des geplanten Auswanderungsvorhabens erheblich reduziert hätte.

IV.

Ausgewählte Themen

4 Ausgewählte Themen

4.1 Datenschutz bei Wahlen

Die Bundestagswahl des vergangenen Jahres sowie die Landtagswahl im März 2022 gingen in unserer Behörde mit einer verstärkten Beratungstätigkeit im Bereich des Datenschutzes im Zusammenhang mit staatlichen Wahlen einher. Bei den datenschutzrechtlichen Fragen, welche sowohl von Behörden und sonstigen öffentlichen Stellen als auch von Seiten der Bürgerinnen und Bürger an unsere Behörde herangetragen wurden, handelte es sich vielfach um allgemeine wiederkehrende Rechtsfragen, welche in gewisser Regelmäßigkeit im Vorfeld anstehender Wahlen gestellt werden. Im Folgenden sollen ein paar ausgewählte Konstellationen aus diesem Bereich kurz erläutert werden.

4.1.1 Gruppenauskünfte an politische Parteien

Das Bundesmeldegesetz (BMG) regelt in seinen §§ 44 ff. neben Melderegisterauskünften, welche Auskünfte über Meldedaten einzelner bestimmter Personen ermöglichen, auch sog. *Gruppenauskünfte*, d. h. Auskünfte über eine Vielzahl nicht namentlich bezeichneter Personen.

Im Vorfeld von Wahlen sind diese Gruppenauskünfte oftmals der Anlass für Anfragen von Bürgerinnen und Bürgern, welche sich darüber wundern, dass sie Post von politischen Parteien in Form von Wahlwerbung erhalten, obwohl sie mit dieser Partei womöglich noch nie in Kontakt gestanden und ihre Adressdaten für die postalische Kontaktaufnahme demnach auch nicht selbst zur Verfügung gestellt haben.

Obgleich die Verwunderung über die Erlangung der Adressdaten aus dem Melderegister hierbei sicherlich in gewissem Maße nachvollzogen werden kann, liegt in diesen Fällen dennoch in der Regel eine rechtmäßige Datenverarbeitung vor. Die Meldebehörden dürfen nämlich Parteien, Wählergruppen und ande-

ren Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen und Abstimmungen auf staatlicher und kommunaler Ebene in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister erteilen. Ihre gesetzliche Grundlage findet diese besondere Form der Gruppenauskunft in § 50 Abs. 1 S. 1 BMG. Mit einem entsprechenden Antrag an die Meldebehörde ist es Parteien mithin möglich, Meldedaten und damit Adressdaten (vgl. § 44 Abs. 1 BMG) einer Wählergruppe eines bestimmten Lebensalters zu erhalten, bspw. von potentiellen Erstwählern/Erstwählerinnen im Alter von 18 Jahren.

Gemäß § 50 Abs. 5 BMG haben die betroffenen Personen jedoch das Recht, einer künftigen Übermittlung ihrer Daten an Parteien zu diesem Zweck zu widersprechen. Der Widerspruch kann dabei formlos und ohne Begründung bei der zuständigen Meldebehörde (Bürgeramt) eingelegt werden.

Ungeachtet dessen, unterliegen die so erlangten Daten auch einer strengen Zweckbindung, d. h., die über eine solche Gruppenauskunft erlangten Daten dürfen von den Parteien nicht für beliebige Zwecke weiterverarbeitet und gesammelt (gespeichert) werden, sondern dürfen gemäß § 50 Abs. 1 S. 3 BMG nur für die Werbung bei einer Wahl oder einer Abstimmung verwendet werden. Sie sind von dem Empfänger der Daten (der jeweiligen Partei) spätestens einen Monat nach der Wahl oder Abstimmung zu löschen oder zu vernichten.

4.1.2 Dankeskarten an die Wahlhelfer/innen

Beabsichtigt die Behördenleitung einer Kommune (Oberbürgermeister/in, Bürgermeister/in) nach Abschluss des Wahlverfahrens den Wahlhelferinnen und Wahlhelfern für ihre ehrenamtliche Tätigkeit ihren Dank auszusprechen und verwendet deren zu Zwecken der Organisation des Wahlverfahrens erhobenen Adressdaten für ein entsprechendes Dankesschreiben, so liegt hierin in der Regel kein Verstoß gegen datenschutzrechtliche Bestimmungen.

In einer solchen Datenverarbeitung ist insbesondere kein Zuwiderhandeln gegen den Grundsatz der informationellen Gewaltenteilung zu erblicken, welcher – ähnlich wie der Rechtmäßigkeitsgrundsatz des Art. 5 Abs. 1 lit. a DSGVO – im Kern besagt, dass nur diejenige staatliche Stelle eine Verarbeitung personenbezogener Daten vornehmen darf, welche sich hierzu auf eine entsprechende Rechtsgrundlage stützen kann. Die in diesem Zusammenhang gegenüber unserer Behörde geäußerte Ansicht, dass nur die Wahlleitung (Bundeswahlleiter/Landeswahlleiterin) über die betreffenden Daten der Wahlhelferinnen und Wahlhelfer verfügen darf, trifft nicht zu.

Dem Bundeswahlleiter und – auf das Saarland bezogen – der Landeswahlleiterin obliegen u. a. die Aufgaben der Organisation und Überwachung der Bundestagswahl/Landtagswahl. Sie sind damit die staatlichen Stellen, bei welchen in Durchführung der Wahl „die Fäden zusammenlaufen". Eine wesentliche Vorbereitung und Durchführung der Wahl wird jedoch bereits auf Ebene der Kommunen (Gemeinden/Städte) getroffen, welchen gemäß §§ 9 Abs. 2 S. 3 Bundeswahlgesetz (BWG), 6 Abs. 1, 2, 6 Bundeswahlordnung (BWO) die Aufgabe obliegt, die Wahlvorstände und damit die Wahlhelferinnen und Wahlhelfer zu berufen. Hierfür sind die Gemeindebehörden gemäß § 9 Abs. 4 BWG befugt, personenbezogene Daten von Wahlberechtigten zum Zweck ihrer Berufung zu Mitgliedern von Wahlvorständen zu erheben und zu verarbeiten.

Diese Verarbeitungsbefugnis umfasst auch eine entsprechende Dankeskarte an die Wahlhelfer. Zwar dient diese – zeitlich der Wahl nachgelagerte – Handlung nicht mehr der eigentlichen Durchführung der Wahl. Als Annex hierzu kann eine solche Geste jedoch noch als von den vorgenannten Verarbeitungsgrundlagen mitumfasst angesehen werden. Bei dem Amt des Wahlhelfers/der Wahlhelferin handelt es sich um ein zeit- und arbeitsintensives Ehrenamt, welches für die Sicherstellung eines reibungslosen und rechtsstaatlichen Wahlverfahrens unabdingbar ist.

Durch die Danksagung drücken die betreffenden Kommunen nochmals persönlich ihre besondere Anerkennung für die in Ausübung dieses Ehrenamts erbrachte Leistung aus und können die betreffenden Personen nicht zuletzt hierdurch womöglich auch für die kommenden Wahlen als freiwillige Wahlhelfer/Wahlhelferinnen gewinnen.

4.1.3 Verwendung eines QR Codes zu Beantragung der Wahlunterlagen

Die Verwendung eines QR-Codes zur Beantragung der Wahlunterlagen für die Briefwahl ist ein mittlerweile gängiges und in vielen Kommunen bereits etabliertes Verfahren, mit welchem sich die wahlberechtigten Personen auf einfache und komfortable Art und Weise die Briefwahlunterlagen postalisch übermitteln lassen können.

Der hierzu auf der Wahlbenachrichtigungskarte aufgedruckte QR-Code kann von den Bürgerinnen und Bürgern mit fast jedem gängigen Smartphonemodell (Fotofunktion) eingescannt und ausgelesen werden. Technisch läuft das Antragsverfahren dabei in Regel dergestalt ab, dass nach dem Einscannen des QR-Codes eine unmittelbare Weiterleitung auf ein Webportal (Antragsportal) erfolgt, bei welchem die Wahlberechtigten ihre Adressdaten nochmals einsehen und ggf. korrigieren können und durch Bestätigung den postalischen Versand der Briefwahlunterlagen auslösen. Die hierbei angezeigten Meldedaten sind dabei bereits Bestandteil des aufgedruckten QR-Codes und werden mit dessen Einscannen an das Antragsportal übermittelt.

Datenschutzrechtlich hat dies zur Folge, dass technisch-organisatorische Maßnahmen zu ergreifen sind, welche ein unbefugtes Auslesen des QR-Codes durch Dritte so weit wie möglich verhindern. Vor allem zwei Maßnahmen sind hierbei von Bedeutung. Zum einen sind die Meldedaten inhaltlich mit einem gängigen Verschlüsselungsverfahren (Bsp. AES 128 oder höher) zu verschlüsseln, bevor der zu erzeugende QR-Code aus ihnen generiert (gedruckt) wird. Der QR-Code verkörpert dann nicht

mehr die Meldedaten in "Reinform", sondern nur in verschlüsselter Form.

Zum anderen ist sicherzustellen, dass das mittels des QR-Codes aufgerufene Webportal zur Beantragung der Wahlunterlagen nach einem Abruf und einer Beantragung der Wahlunterlagen nicht mehr erreichbar ist, d. h. nur einmal abgerufen werden kann.

Durch diese beiden Maßnahmen kann insbesondere sichergestellt werden, dass weggeworfene Wahlbenachrichtigungskarten nicht von dritter Seite erneut ausgelesen werden und Dritte so unbefugt Einsicht in die Meldedaten von wahlberechtigten Personen erhalten.

4.2 Auskunft über die Verarbeitung von Meldedaten

Das Wissen über die Art und Weise der Verarbeitung der eigenen Daten ist die Grundvoraussetzung der informationellen Selbstbestimmung, gerade in Zeiten vollautomatisierter Datenverarbeitungen.

Diesem Umstand trägt das in Art. 15 DSGVO geregelte Recht auf Auskunft Rechnung, indem es den betroffenen Personen einen voraussetzungslosen Anspruch darauf gibt, nicht nur zu erfahren, welche Daten zu welchen Zwecken verarbeitet werden, sondern auch und vor allem Kenntnis darüber zu erlangen, an welche Empfänger die Daten übermittelt werden bzw. übermittelt worden sind. Den Bürgerinnen und Bürgern steht es demnach offen, sich jederzeit und ohne die Notwendigkeit der Darlegung eines besonderen Interesses an die Behörden und sonstigen öffentlichen Stellen zu wenden und diese um eine dahingehende Auskunft zu ersuchen.

Dass vor diesem Hintergrund ein gesteigertes Interesse an der Auskunft über die Verarbeitung der eigenen Meldedaten besteht, verwundert nicht, ist es doch durch das Rechtsinstitut der

Melderegisterauskunft in den §§ 44 ff. des Bundesmeldegesetzes (BMG)[15] jeder Person möglich, unter den dort genannten Voraussetzungen eine behördliche Auskunft über Meldedaten, insbesondere die derzeitigen Anschriften, einer anderen Person zu erhalten. Durch ein Auskunftsersuchen bei der örtlich zuständigen Meldebehörde kann dabei in Erfahrung gebracht werden, an welche Personen Meldedaten übermittelt wurden.

Im Rahmen eines solchen Auskunftsersuchens ist die angefragte Behörde dazu verpflichtet sicherzustellen, dass personenbezogene Daten nicht an unbefugte Dritte übermittelt werden. Gesteigerte Anforderungen an eine diesbezügliche Identitätsfeststellung der anfragenden Person bestehen insbesondere in Konstellationen, in welchen die Behörde begründete Zweifel an der Identität der Antragstellerin oder des Antragstellers hat. Hier ist die Behörde gemäß Art. 12 Abs. 6 DSGVO dazu berechtigt, sich vor einer Auskunftserteilung zusätzliche Informationen einzuholen, welche ihr eine Identitätsprüfung ermöglichen, etwa in Form eines persönlichen Vorsprechens unter Vorlage eines Personalausweises oder eines anderen Ausweisdokuments.

In Anbetracht der Sensibilität von Meldedaten trifft das Bundesmeldegesetz für das Auskunftsrecht gegenüber Meldebehörden in § 10 Abs. 1 BMG eine Sonderregelung gegenüber Art. 12 Abs. 6 DSGVO und verpflichtet die Meldebehörde explizit zu einer Identitätsprüfung der antragstellenden Person.

Diese Regelung bedeutet jedoch nicht, dass die Meldebehörde in sämtlichen Fällen von der antragstellenden Person die Vorlage eines legitimierenden Ausweisdokuments verlangen darf. Der Gesetzesbegründung zu § 10 Abs. 1 BMG ist vielmehr zu entnehmen, dass die Norm in erster Linie auf solche Situationen abzielt, in welchen es der angefragten Meldebehörde ohne Zusatzinformationen schlechterdings nicht möglich ist sicherzustellen, dass die übermittelten Daten auch tatsächlich der be-

[15] Bundesmeldegesetz vom 3. Mai 2013 (BGBl. I S. 1084), zuletzt geändert durch Gesetz vom 28. März 2021 (BGBl. I S. 591).

troffenen Person übermittelt werden und nicht einem unbefugten Dritten, welcher sich womöglich als diese Person ausgibt. In der Gesetzesbegründung zu § 10 BMG heißt es hierzu:

"*Die Identitätsprüfung dient dem Schutz der betroffenen Person (Artikel 23 Absatz 1 Buchstabe i der Verordnung (EU) 2016/679). Nur so kann sichergestellt werden, dass keine unberechtigte Person Auskunft über personenbezogene Daten erhält. Bei der Verwendung einer E-Mail-Empfangsadresse oder einer mündlichen Auskunft besteht in der Regel eine gewisse Gefahr, dass die Auskunft nicht die berechtigte Person, sondern einen unberechtigten Dritten erreicht. Die Meldebehörde muss daher vor der Erteilung des Auskunftsanspruchs die Identität der betroffenen Person überprüfen.*" (BT-Drs. 19/4674, S. 222).

Diese Gefahr der Offenbarung von Meldedaten an unbefugte Personen besteht indes nicht, wenn die Meldebehörde die angefragten Daten postalisch an die in ihrem Datenbestand hinterlegte Meldeadresse übersendet. Die Unterlagen befinden sich dann in einem verschlossenen Umschlag und dürfen nur von der adressierten Person geöffnet werden, d. h. nur von derjenigen Person, auf welche sich auch der Auskunftsanspruch nach Art. 15 DSGVO bezieht.

4.3 Zensus 2022

Im Jahr 2022 findet in Deutschland wieder ein Zensus statt. Im Rahmen des Zensus, allgemein auch als Volkszählung bekannt, werden grundlegende Daten über die Bevölkerung in Deutschland analog zum Zensus 2011 mit einem registergestützten Verfahren erhoben. Die Ergebnisse dienen der Feststellung der amtlichen Einwohnerzahlen von Bund, Ländern und Gemeinden sowie der Gewinnung soziodemografischer Basisdaten zur Bevölkerung, Erwerbstätigkeit und Wohnsituation.

Mit dem Zensus 2022[16] nimmt Deutschland an einer EU-weiten Zensusrunde teil, die seit 2011 alle zehn Jahre stattfinden soll.

[16] Detaillierte Informationen finden sich unter www.zensus2022.de

Aufgrund der Corona-Pandemie wurde der anstehende Zensus von 2021 in das Jahr 2022 verschoben.

4.3.1 Rechtliche Grundlagen

Auf Bundesebene wird die Durchführung des Zensus durch das Zensusgesetz 2022 geregelt. In diesem Gesetz werden die Erhebungsmerkmale für die Gebäude- und Wohnungszählung, die Haushaltebefragung auf Stichprobenbasis und die Erhebungen in Wohnheimen und Gemeinschaftsunterkünften festgelegt. Ebenso ist eine Auskunftspflicht normiert. Danach sind Eigentümerinnen und Eigentümer sowie Verwalterinnen und Verwalter von Wohnraum verpflichtet, Auskunft über bestimmte Angaben zu den von ihnen vermieteten Wohnungen zu geben. Die Auskunftspflicht umfasst auch die einmalige Mitteilung der Vor- und Nachnamen von bis zu zwei Bewohnerinnen bzw. Bewohnern.

Auch die Maßnahmen zur Gewährung des Datenschutzes, die Kostenaufteilung zwischen Bund und Ländern und der Stichprobenumfang sind im Zensusgesetz geregelt.

Verfahrensrechtliche und organisatorische Regelungen sind hingegen durch die Länder zu treffen.

Das Saarländische Zensusausführungsgesetz 2022 überführt das Zensusgesetz 2022 in Landesrecht und konkretisiert die Umsetzung dieses Gesetzes im Saarland.

4.3.2 Begleitung des Gesetzgebungsverfahrens

Im Rahmen der Anhörung zum Entwurf des Zensusausführungsgesetzes hat unsere Behörde Stellung zu datenschutzrechtlich relevanten Bestimmungen und Fragestellungen genommen.

Im Zentrum stand hierbei die Frage der datenschutzrechtlichen Einordnung der sogenannten Erhebungsstellen, deren Hauptaufgabe darin besteht, Erhebungsbeauftragte anzuwerben und die Befragung vor Ort zu koordinieren. Hierzu gibt weder das Zensusgesetz konkrete Vorgaben noch ist dies explizit im Zensusausführungsgesetz geregelt.

Für die Einschätzung, ob hier eine Auftragsverarbeitung nach Art. 28 DSGVO oder eine gemeinsame Verantwortlichkeit mit dem Statistischen Landesamt nach Art. 26 DSGVO vorliegt, war es erforderlich, einen Überblick über die geplante Ausgestaltung in tatsächlicher Hinsicht zu erhalten.

Nach einem Besprechungstermin unserer Behörde mit Vertreterinnen und Vertretern des Statistischen Landesamts konnte geklärt werden, dass es sich um eine Auftragsverarbeitung nach Art. 28 DSGVO handelt. Hierfür sprachen insbesondere die detaillierten Vorgaben zu Mittel und Zweck der Verarbeitung durch das Statistische Landesamt gegenüber den Erhebungsstellen.

Unsere Behörde hat darauf hingewirkt, dass mit den Erhebungsstellen jeweils ein Auftragsverarbeitungsvertrag abgeschlossen wird und die datenschutzrechtlichen Vorgaben in den Erhebungsstellen eingehalten werden.

4.4 Datenschutzaufsicht im Bereich der Justiz

Immer wieder erreichen uns Anfragen und Beschwerden, die mit der Datenverarbeitung durch die saarländische Justiz in Form der Zivil-, Straf- und Verwaltungsgerichte zusammenhängen.

So richtete sich beispielsweise im Berichtszeitraum eine Beschwerde dagegen, dass durch das Gericht in einem zivilrechtlichen Verfahren Akteneinsicht an einen Parteianwalt gewährt und hierdurch der Beklagtenseite die Wohnanschrift einer Zeugin bekannt wurde, obwohl diese anonym bleiben wollte.

Zwar können hier durchaus Fragen des Rechts auf informationelle Selbstbestimmung relevant werden, jedoch lautete in diesem und ähnlichen Verfahren unsere Antwort leider immer gleich: *„Wir sind nicht zuständig“*.

4.4.1 Datenschutzanforderungen im Bereich der Justiz

Dieser pauschale Satz zum Zuständigkeitsbereich der Aufsichtsbehörde bedeutet indes nicht, dass die Tätigkeit der saarländi-

schen Gerichte nicht an datenschutzrechtlichen Vorgaben auszurichten wäre. Die Vorschriften der DSGVO finden auch für den justiziellen Bereich Anwendung, was sich beispielsweise aus dem ersten Satz des dort verschriftlichten Erwägungsgrundes 20 ersehen lässt. Werden Justizbehörden zu Strafverfolgungszwecken tätig, ergeben sich die gleichen Schlussfolgerungen aus dem Inhalt der JI-Richtlinie (dort Erwägungsgrund 80).

Auch Gerichte (und allen voran die dort tätigen Richter) müssen sich als staatliche Stellen bewusst sein, dass die Verarbeitung personenbezogener Daten einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, welcher vor dem Hintergrund des Gesetzesvorbehalts (Art. 21 Abs. 4 GG) stets einer rechtlichen Grundlage bedarf. Exekutive und Judikative sind an Gesetz und Recht gebunden (Art. 20 Abs. 3 GG).

4.4.2 Datenschutzaufsicht bei „justizieller Tätigkeit"

Datenschutz kann somit von Gerichten nicht einfach ignoriert werden. Doch dort, wo für andere öffentliche Stellen eine Kontrollinstanz – in Form unserer Behörde – existiert, herrscht für justizielle Tätigkeiten ein „Vakuum". Grund hierfür ist Art. 55 Abs. 3 DSGVO, der folgenden Wortlaut besitzt:

„Die Aufsichtsbehörden sind nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen."

Gleiche Vorgaben macht die JI-Richtlinie (Art. 45 Abs. 2). Daraus ergibt sich das kurios anmutende Ergebnis, dass Datenschutznormen in solchen Fällen zwar Geltung besitzen, die Anwendung aber keiner Kontrolle durch die Datenschutzaufsichtsbehörde unterliegt. Stattdessen schlägt Erwägungsgrund 20 die Schaffung besonderer Aufsichtsstellen im Justizsystem vor. Bislang existieren solche in Deutschland aber nicht.

Kernstück des Problems stellt die Auslegung des Begriffs der **„Justiziellen Tätigkeit"** dar. Sinn und Zweck der Vorgabe ist es, die Unabhängigkeit der rechtsprechenden Staatsgewalt zu gewährleisten. Deshalb werden auf jeden Fall Handlungen des

Richters im Rahmen seiner richterlichen Beschlussfassung („spruchrichterliche Tätigkeit") von diesem Begriff erfasst.

Problematischer wird die Einordnung jedoch dann, wenn das Gericht in anderer Art und Weise tätig wird, beispielsweise durch Urkundsbeamte, Rechtspfleger oder Tarifbeschäftigte.

Ebenfalls zu beachten ist, dass das Saarländische Datenschutzgesetz (SDSG) weitere Einschränkungen vorsieht und unsere Zuständigkeit auf „Verwaltungstätigkeiten" der Gerichte beschränkt (§ 2 Abs. 1 S. 4 SDSG). Die Gesetzesbegründung geht davon aus, dass hierunter Akte im Bereich des Personals, der Organisation und der Finanzen zu verstehen sind.

4.4.3 Die Problematik am Beispiel des Rechtspflegers

Im Berichtsjahr wurde diese Problematik in einem Fall besonders relevant. Wir befassten uns hier mit der Person des **Rechtspflegers**, der im deutschen Rechtssystem eine Sonderrolle einnimmt. Auf der einen Seite handelt es sich bei ihm „lediglich" um einen Beamten des gehobenen Justizdienstes; andererseits stattet ihn § 9 RPflG mit einer speziellen „sachlichen Unabhängigkeit" aus, die als sachliche Weisungsfreiheit und Selbstständigkeit zu verstehen ist. Diese hat gewisse Ähnlichkeit zur Unabhängigkeit des Richters, ist aber nicht umfassend mit dessen verfassungsrechtlicher Stellung nach Art. 97 GG vergleichbar.

Anlass für unsere Befassung gab die Beschwerde einer Bürgerin mit folgendem Hintergrund: Die Petentin hatte aufgrund eines drohenden Rechtsstreits einen Antrag auf Gewährung von **Beratungshilfe** bei Gericht gestellt und musste zum Nachweis ihrer Bedürftigkeit entsprechende Belege beibringen. Hierzu übersandte sie teilweise geschwärzte Kontoauszüge, die von der zuständigen Rechtspflegerin als unzureichend bewertet wurden. Stattdessen erfolgte eine Aufforderung, ungeschwärzte Kontoauszüge zu übermitteln. Die Petentin äußerte hieran Zweifel und wandte sich mit dem Sachverhalt an unsere Behörde.

Folglich waren wir mit der bereits dargestellten Zuständigkeitsfrage konfrontiert. Von uns wird eine enge Auslegung des Art. 55 Abs. 3 DSGVO vertreten, wonach sich die intendierte Gewährleistung der „Unabhängigkeit der Justiz" auf den funktionellen Bereich der Rechtsprechung (als Kernstück der rechtsstaatlich garantierten Judikative) bezieht – somit die Unabhängigkeit des Richters sicherstellen soll.

Wie ausgeführt, ist allerdings die Stellung des Rechtspflegers nach § 9 RPflG nicht vollumfänglich mit dieser Position vergleichbar. Zudem hängt sie zusätzlich davon ab, ob übertragene Geschäfte nach § 3 RPflG oder sonstige Aufgaben nach §§ 29 ff. RPflG wahrgenommen werden. Gerade das Beratungshilfeverfahren ist zwar in § 3 Nr. 3 lit. f RPflG enthalten, weist aber nach unserer Auffassung eher einen Bezug zur Leistungsverwaltung als zur rechtsprechenden Tätigkeit auf, da hier allein eine Prüfung der Bedürftigkeit des Antragstellers vorgenommen wird. Dass der europäische Verordnungsgeber für einen solchen Fall eine Lücke schaffen wollte, erachten wir als fraglich.

Letztlich war es jedoch nicht Europa-, sondern Landesrecht, das uns unsere Befugnisse für den vorstehenden Fall eindeutig entzog. Wie erwähnt, beschränkt uns § 2 Abs. 1 S. 4 SDSG auf die Kontrolle von „Verwaltungstätigkeiten" der Gerichte. Da sich die Tätigkeit des Rechtspflegers hier als weder personelle, noch organisatorische oder finanzielle Entscheidung darstellte, mussten wir von unserer Unzuständigkeit ausgehen.

Die Auslegung des Begriffs der „justiziellen Tätigkeit" wird absehbar auch künftig zu Abgrenzungsschwierigkeiten führen. Deswegen sehen wir der Entscheidung des EuGH in einem derzeit anhängigen Vorabentscheidungsverfahren (Az.: C-245/20) entgegen, das die Thematik hoffentlich weiter beleuchten und klarstellen wird.

Fazit/ Empfehlung:

Die derzeitige Rechtslage entzieht gewisse Bereiche gerichtlicher Datenverarbeitung der aufsichtsbehördlichen Kontrolle. Diese Problematik beschränkt sich nicht nur auf die Person des Rechtspflegers, sondern betrifft diverse Bereiche, in denen gerichtliche Akteure außerhalb spruchrichterlicher Tätigkeit auftreten. Bis zu einer weiteren gerichtlichen oder legislativen Klarstellung des Begriffs der „justiziellen Tätigkeit" und des § 2 Abs. 1 S. 4 SDSG können wir lediglich im Bereich der eng begrenzten Verwaltungstätigkeit der Gerichte unsere Aufsichtsbefugnisse wahrnehmen. Wir appellieren an den saarländischen Gesetzgeber, hier umgehend tätig zu werden und bestehende Regelungslücken zu schließen.

4.5 Prüfung der Antiterrordatei (ATD) und Rechtsextremismusdatei (RED)

4.5.1 Allgemeines zu ATD/RED sowie Prüfpflichten

Zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland sowie des gewaltbezogenen Rechtsextremismus wurden in Deutschland mit der Antiterrordatei (ATD) und der Rechtsextremismusdatei (RED) gemeinsame standardisierte zentrale Datenbestände geschaffen, deren Ziel es ist, den Informationsaustausch zwischen den Polizeien und Nachrichtendiensten zu verbessern.[17]

Zur Gewährleistung der Einhaltung datenschutzrechtlicher Vorgaben sehen die Errichtungsgesetze zu ATD (ATDG) und RED (RED-G) Kontrollverpflichtungen vor. § 10 Abs. 2 ATDG bzw. § 11 Abs. 2 RED-G bestimmen, dass turnusmäßig (mind. alle zwei Jahre) die Durchführung des Datenschutzes bei der Eingabe von Datensätzen durch die verantwortlichen Länderbe-

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

hörden zu überprüfen ist. Die Kontrolle findet somit anlassunabhängig statt. Das letzte Mal hatten wir im 26. Tätigkeitsbericht[18] über die Durchführung einer solchen Prüfung berichtet.

In den Zuständigkeitsbereich der saarländischen Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) fallen die *„Abteilung V – Verfassungsschutz"* des Ministeriums für Inneres, Bauen und Sport sowie das *saarländische Landespolizeipräsidium (LPP)*. Aufgrund der hohen Prüfdichte und der geringen Personalkapazität unserer Behörde werden Abteilung V und LPP im Saarland alternierend kontrolliert; das im Jahr 2020 initiierte Prüfverfahren zu ATD/RED beschränkte sich deswegen dieses Mal auf die Datenverarbeitung durch die Landespolizei.

4.5.2 Ablauf der Prüfung

Mit Prüfankündigung Ende März 2020 leiteten wir die Prüfung von ATD und RED beim Landespolizeipräsidium ein. Zunächst baten wir um Mitteilung zum bestehenden Speicherbestand (Anzahl der gespeicherten Datensätze, Aufschlüsselung nach Hauptperson/Kontaktperson, Neueinspeicherungen seit dem 01. Januar 2020) und, zur Überprüfung der Plausibilität der daraufhin übermittelten Informationen, um Übersendung entsprechender Protokolldaten für eine festgelegte Zeitspanne (01. Mai 2020 bis 31. Juli 2020). Bezüglich letzterer wurde die protokollführende Stelle, das Bundeskriminalamt (BKA), um Übersendung von Standardreports (= standardisierte Auswertungen der vorhandenen Protokolldaten) und Benutzerprotokollierungen des Quellsystems („INPOL-Fall Innere Sicherheit") gebeten.

Ende Oktober 2020 erfolgte die Rückmeldung des Landespolizeipräsidiums durch Übermittlung der entsprechend angeforderten Unterlagen zur Vorprüfung.

Die durch das LPP bereitgestellten Informationen zu den dort vorliegenden Erkenntnissen aus den Dateien konnten hierbei als

[18] Vgl. 26. Tätigkeitsbericht, 2014/2015, Kapitel 4.1, S. 52-54, elektronisch abrufbar unter: https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/tberichte/tb26.pdf

vollständig, strukturiert und nachvollziehbar bewertet werden. Die vom BKA übersandten Standardreports und Benutzerprotokollierungen bedurften jedoch weiterer Klärung. So konnte die Auswertung der tabellarisch geführten Protokollierungen zunächst aufgrund unbekannter Spalten- und Objektbezeichnungen nicht durchgeführt werden. Mitte November 2020 wurden deswegen entsprechende Rückfragen gestellt, die allerdings erst Ende August 2021 vollumfänglich beantwortet wurden. An die Protokollauswertung Anfang September 2021 schloss sich Mitte September 2021 eine Einsichtnahme (Vor-Ort-Termin) in die im Prüfzeitraum angefallenen Neuspeicherungen und den zugrundeliegenden Aktenbestand an. Mit einer rechtlichen Würdigung schlossen wir das Prüfverfahren damit letztlich im selben Monat ab.

4.5.3 Feststellungen im Rahmen der Prüfung

Die Kontrolle von ATD und RED konzentrierte sich in diesem Prüfturnus auf die Rechtmäßigkeit von (Neu-)Einspeicherungen in die Dateien und deren ausreichende Nachvollziehbarkeit.

Bereits während der recht langen Vorprüfungsphase konnte festgestellt werden, dass in ATD und RED seitens der saarländischen Polizei nur relativ wenige Speicherungen unterhalten werden.

Ob Datenbestände von der zuständigen Behörde in die ATD einzuspeichern sind, beurteilt sich anhand der Voraussetzungen in § 2 Abs. 1 ATDG. Die Vorschrift verlangt, dass (aufgrund bestehender polizeilicher Erkenntnisse) eine Person, Vereinigung oder sonstige Information einen Bezug zu terroristischen Vereinigungen aufweisen muss. Diese Entscheidungsgrundlage ist Bestandteil normaler Strafakten, die im Vorgangsverarbeitungssystem der saarländischen Polizei (POLADIS) verwaltet werden und in die wir im Rahmen der Vor-Ort-Prüfung Einblick nehmen konnten:

In den von uns näher untersuchten Verfahren waren die Einspeicherungsvoraussetzungen im Sinne des § 2 Abs. 1 ATDG anhand der Aktenlage nachvollziehbar begründet und damit eine Verarbeitung ursprünglich gerechtfertigt. In einigen wenigen Fällen war jedoch dokumentiert, dass die die Einspeicherung auslösenden strafprozessualen Ermittlungsverfahren bereits mangels Tatverdachts nach § 170 Abs. 2 StPO eingestellt worden waren. Ein weiteres Vorhalten der Datensätze ist in einem solchen Fall nicht erforderlich. Das LPP bestätigte, dass eine entsprechende Datenlöschung bereits initiiert wurde. Insgesamt konnten wir deswegen die Datenverarbeitung durch das LPP in den von uns kontrollierten Fällen als rechtmäßig beurteilen.

Da das Vorliegen der Voraussetzungen des § 2 Satz 1 ATDG (bzw. RED-G) für eine aufsichtliche Prüfung von erheblicher Bedeutung ist, ist zur Gewährleistung der Transparenz auch eine entsprechende Dokumentation zu verlangen.

Als Ergebnis der letzten Prüfung der ATD beim Landespolizeipräsidium (2017) wurde in enger Kooperation ein Formblatt zur Dokumentation von Einspeicherungsanlässen entworfen. Die hier durchgeführte Prüfung ergab jedoch, dass dieses nicht in den Praxisbetrieb übernommen worden war. Stattdessen wird ein eigentlich für statistische Zwecke eingeführtes Formular (KTA – kriminaltaktische Anfrage) zum Nachweis der ATD- und RED-Relevanz verwendet. Das Dokument beinhaltet in der uns vorliegenden Ausgestaltung hinreichende Darstellungen der für die Kontrolle notwendigen Erkenntnisse. Wir gehen deshalb davon aus, dass grundsätzlich in hinreichender Art dokumentiert wird. Eine weitere Verbesserung ist deswegen nicht zwangsläufig notwendig, ließe sich aber durch kleinere Anpassungen des bestehenden Formulars (z. B. umfassende Auflistung der eingespeicherten Daten in Form der Auflistung in § 3 ATDG / RED-G; gesonderte Ausführungen zur „Erforderlichkeit“) oder durch (zusätzliche) Einführung des ursprünglich abgestimmten Formblattes erreichen. LPP und UDZ befinden sich hierzu im weiteren kooperativen Austausch.

4.5.4 Ergebnis

Das Ergebnis der turnusmäßigen Kontrolle von ATD und RED zeigt auf, dass – zumindest im Saarland – die überprüften Zentraldateien eine eher geringe Relevanz für die praktische polizeiliche Arbeit von heute aufweisen. Verglichen mit dem Umfang der Datenverarbeitung in den polizeilichen Informationssystemen kommt den Eintragungen in der ATD / RED nur eine untergeordnete Bedeutung zu.

Die überprüften Akten wiesen derweil keine datenschutzrechtlichen Verstöße auf. Die vorhandene Dokumentation war als ausreichend mit weiterem Potential für Verbesserung zu sehen.

Während die Zulieferung und Abklärung von Reports und Protokolldaten zu Verzögerungen im Prüfverfahren beitrugen, stellte sich die Zusammenarbeit mit den saarländischen Behörden insgesamt als sehr kooperativ und positiv dar.

In Ausübung der uns obliegenden Prüfpflichten wird die nächste Kontrolle von ATD und RED (dem hier praktizierten alternierenden Vorgehen folgend) im Jahr 2022 beim saarländischen Verfassungsschutz stattfinden.

4.6 Anhörung des Betroffenen im Rahmen von Zuverlässigkeitsüberprüfungen

Mit dem Inkrafttreten des Saarländischen Gesetzes über die Verarbeitung personenbezogener Daten durch die Polizei (SPolDVG) zum Jahreswechsel 2020/21 erlangte auch die neu eingefügte Vorschrift des § 28 Abs. 3 SPolDVG erstmalig Anwendung.

§ 28 Abs. 3 SPolDVG erlaubt mit Einwilligung der betroffenen Person den Abgleich personenbezogener Daten des Betroffenen mit polizeilichen Dateisystemen zum Zwecke der Durchführung einer Zuverlässigkeitsüberprüfung. Hierzu listet § 28 Abs. 3 SPolDVG abschließend die Fälle auf, in denen eine solche Zuverlässigkeitsüberprüfung durchgeführt werden darf.

Solche Überprüfungen sind aber datenschutzrechtlich problematisch, da sie tief in das Grundrecht auf informationelle Selbstbestimmung des Betroffenen eingreifen, ohne dass, wie sonst im Polizeirecht üblich, diese Person einen konkreten Anlass hierfür bietet oder eine konkrete Gefahr existiert. Entsprechend hatten wir uns bereits im Gesetzgebungsverfahren kritisch geäußert und Änderungen angemahnt.

Insbesondere hielten wir es für rechtsstaatlich problematisch, dass das Verfahren zur Durchführung der Zuverlässigkeitsüberprüfung ursprünglich keine Anhörung des Betroffenen vorsah[19] Zwar erteilt der Betroffene zunächst seine „Einwilligung". Das Ergebnis der Zuverlässigkeitsüberprüfung kann der Betroffene aber nicht vorhersehen; dies insbesondere deshalb, weil der Betroffene bspw. wegen möglicher verdeckter Maßnahmen gegen ihn bzw. ganz allgemein, weil er Art, Umfang und Qualität, sprich Aktualität und Richtigkeit der bei der Polizei gespeicherten personenbezogenen Daten, die Eingang in die Bewertung finden, nicht abschätzen und voraussehen kann. So sah der Gesetzentwurf vor, dass selbst im Falle eines negativen Ausgangs der Zuverlässigkeitsüberprüfung, wenn also Sicherheitsbedenken bestehen, der Betroffene weder vorher angehört werden, noch sonst eine Möglichkeit haben sollte, seinen Standpunkt und eventuell entlastende Angaben in das Verfahren einzubringen. Ebenso war nicht vorgesehen, dass die betroffene Person darüber zu informieren ist, aus welchen Erkenntnissen sich die Sicherheitsbedenken in ihrer Person konkret ergeben.

Diesen Bedenken hatte sich der Landtag des Saarlandes im Gesetzgebungsverfahren angeschlossen und mit § 28 Abs. 5 Satz 4 SPolDVG eine Pflicht zur Anhörung des Betroffenen vor einer negativen Zuverlässigkeitsentscheidung vorgesehen. Hiermit soll der betroffenen Person die Möglichkeit gegeben werden, sich zu den für die Entscheidung erheblichen Tatsachen zu äußern. Dies impliziert, dass der betroffenen Person die bei der

[19] Vgl. 29. Tätigkeitsbericht 2021, Kapitel 3.5, Seite 65, elektronisch abrufbar unter: https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/tberichte/ tb29_DS_2020.pdf

Polizei vorhandenen sicherheitsrelevanten Erkenntnisse mitgeteilt werden.

Dass sich die damit zusammenhängenden Abläufe noch nicht eingespielt haben, zeigte die Beschwerde eines Mitarbeiters eines Cateringunternehmens. Im Rahmen der Vorbereitung einer Veranstaltung in der Staatskanzlei wurden die Mitarbeiter des Cateringunternehmens einer Zuverlässigkeitsüberprüfung unterzogen. Auch unser Beschwerdeführer war hiervon betroffen und hatte der Durchführung einer Zuverlässigkeitsüberprüfung zugestimmt.

Allerdings fiel diese Zuverlässigkeitsüberprüfung nicht, wie vom Beschwerdeführer erwartet, positiv aus. Stattdessen wurden seitens des Landespolizeipräsidiums Zweifel an der Zuverlässigkeit des Mitarbeiters an die Staatskanzlei zurückgemeldet. Auf Grund dieser Rückmeldung lehnte die Staatskanzlei gegenüber dem Cateringunternehmen den Einsatz des Mitarbeiters wegen Sicherheitsbedenken ab.

Weder wurde der Mitarbeiter vor dieser Entscheidung und der Rückmeldung an den Arbeitgeber angehört, noch wurde ihm auf entsprechende Nachfrage durch die Staatskanzlei Auskunft darüber erteilt, auf Grund welcher Informationen die Zuverlässigkeit versagt wurde. Letztlich erhielt er erst mittels eines Ersuchens gegenüber der Polizei die begehrte Auskunft.

Fazit/ Empfehlung:

Fehlerhafte Sicherheits- und Zuverlässigkeitsüberprüfungen können gerade im beruflichen Kontext für die Betroffenen erhebliche und einschneidende Konsequenzen haben, die bis zum Arbeitsplatzverlust führen können. Von daher ist es extrem wichtig, dass die bestehenden Verfahren zur Durchführung von Zuverlässigkeitsüberprüfungen überprüft und an die neue Rechtslage angepasst werden und sichergestellt wird, dass vor einer negativen Entscheidung über die Zuverlässigkeit der Betroffene die Möglichkeit erhält, sich zu äußern und etwaige Unstimmigkeiten auszuräumen.

4.7 Lichtbildabgleich in Ordnungswidrigkeitenverfahren

Die bereits in unserem 28. Tätigkeitsbericht für den Berichtszeitraum 2019 unter dem Gliederungspunkt 4.16 (S. 94 ff.) eingehend erläuterte Thematik der datenschutzrechtlichen Zulässigkeit sog. "Lichtbildabgleiche" in Verkehrsordnungswidrigkeitenverfahren bildete auch im vorliegenden Berichtzeitraum den Gegenstand zahlreicher Beschwerdeverfahren.

Vor dem Hintergrund der immer wieder gleich gelagerten Sachverhalte, in welchen zwecks Identifizierung des Fahrzeugführers amtliche Passfotos aus den Pass- und Personalausweisregistern durch die Bußgeldbehörden oder die Polizei mit den Beweisfotos einer Geschwindigkeitsmessung abgeglichen werden, begrüßen wir es sehr, dass das Ministerium für Inneres, Bauen und Sport mit dem seit dem 9. Februar 2021 geltenden "*Erlass über die Nutzung personenbezogener Daten aus den Pass- und Personalausweisregistern zum Zwecke der Identifizierung von fahrzeugführenden Personen*" (D6 – 4.1 – GS/20 kr) nunmehr ein Regelwerk geschaffen hat, welches die Modalitäten des diesbezüglichen Verfahrens regelt und präzisiert. Durch die Vorschriften dieses Erlasses, an dessen Ausarbeitung das Ministerium unsere Behörde beteiligte, werden sowohl die datenschutzrechtlichen Positionen der betroffenen Personen gestärkt, als auch den das Ordnungswidrigkeitenverfahren durchführenden Bediensteten ein großes Maß an Rechtssicherheit in ihrem Handeln gegeben.

Als zentralen und wichtigsten Punkt regelt der Erlass nunmehr ausdrücklich, dass der Betroffene einer Verkehrsordnungswidrigkeit vor einem Abruf seiner in den Pass- und Personalausweisregistern hinterlegten Lichtbilder nach § 55 Ordnungswidrigkeitengesetz (OWiG), d. h. als Betroffener und nicht als Zeuge, angehört und auf die Möglichkeit des Lichtbildabgleichs hinzuweisen ist [I. b) des Erlasses].

Durch diese Anhörung wird dem Betroffenen die Gelegenheit gegeben, sich zu der Anschuldigung zu äußern. Er erhält hierdurch die Möglichkeit, der Behörde seine Sicht der Dinge vorzutragen, insbesondere den Tatvorwurf gegen ihn bereits im Ansatz der Ermittlungen zu entkräften. Die vorherige Anhörung soll dem Betroffenen hingegen nicht die Möglichkeit geben, einen Lichtbildabgleich nach den §§ 24 Abs. 2 Personalausweisgesetz (PAuswG) und § 22 Abs. 2 Paßgesetz (PaßG) bei fortbestehendem Tatverdacht zu verhindern.

Weiter wird nunmehr klargestellt, dass die Beiziehung dieser Lichtbilder grundsätzlich Aufgabe der zuständigen Bußgeldbehörde ist und gerade nicht im Rahmen einer durch die Vollzugspolizei geleisteten Amtshilfe bei der Fahrzeugführerermittlung durchgeführt werden soll [II. a) des Erlasses].

Unter dem Gesichtspunkt eines verhältnismäßigen staatlichen Handelns wird unter Gliederungspunkt II. i) des Erlasses abschließend klargestellt, dass Befragungen im persönlichen oder nachbarschaftlichen Umfeld der mutmaßlich fahrzeugführenden Person erst nach einem erfolglosen Lichtbildabgleich zulässig sind und selbige im Falle von geringfügigen Verstößen im Verwarngeldbereich in der Regel auch unterbleiben sollen. Diese Klarstellung ist aus hiesiger Sicht überaus begrüßenswert, da eine behördliche Befragung im persönlichen oder nachbarschaftlichen Umfeld ganz erhebliche und unabsehbare Auswirkungen auf die Datenschutz- und Persönlichkeitsrechte des Betroffenen haben kann und für diesen oftmals mit einer mehr oder weniger bloßstellenden Wirkung verbunden ist. Eine vorherige Beiziehung von Lichtbildern aus den Personalausweis- und Passregistern stellt demnach eine mildere und daher vorzugswürdige Ermittlungshandlung dar.

4.8 Fahreignungsregister-Abfragen

Die im vorstehenden Beitrag beschriebene Thematik des Lichtbildabgleichs und die diesbezüglich eingeleiteten Beschwerdeverfahren führten letztlich dazu, dass wir auf ein weiteres daten-

schutzrechtliches Problem im Zusammenhang mit der Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten aufmerksam wurden.

Aus beigezogenen Bußgeldakten des Landesverwaltungsamtes (Zentrale Bußgeldstelle) war ersichtlich, dass im Rahmen des Fahrerermittlungsverfahrens regelmäßig auch Abfragen des beim Kraftfahrtbundesamt betriebenen Fahreignungsregisters (FAER) stattfanden. Diese umgangssprachlich als „Verkehrssünderkartei" bezeichnete Datenbank beinhaltet neben den bekannten „Punkten" auch weitere konkrete Informationen über Verkehrsteilnehmer, die im Straßenverkehr auffällig geworden sind (Angaben zu Fahrerlaubnis, bestimmten rechtlichen Entscheidungen (vgl. § 28 Abs. 3 StVG) und sonstigen Eintragungen nach § 59 Fahrerlaubnis-Verordnung (FeV)). Die Abfragen wurden dabei durch das eingesetzte Fachprogramm (WinOWiG) zeitgleich mit der zu erfolgenden Anhörung des mutmaßlichen Fahrzeugführers automatisiert ausgelöst, also zu einem Zeitpunkt, zu dem sich das Verfahren noch nicht gegen einen konkreten Betroffenen im Sinne des Ordnungswidrigkeitengesetzes (OWiG) richtete.

Zentrale Normen für die Übermittlung und Verarbeitung von Daten aus dem FAER stellen die §§ 28 Abs. 2 und 30 Abs. 1, Abs. 6 Straßenverkehrsgesetz (StVG) dar. Charakterisiert werden sie durch enge Vorgaben an die verfolgten Zwecke und den Grundsatz der Erforderlichkeit.

Im Zusammenhang mit der Verfolgung einer Verkehrsordnungswidrigkeit sieht der abschließende Katalog der zulässigen Zwecke in § 28 Abs. 2 StVG lediglich die „Ahndung" vor (Nr. 3). Sprachgebräuchlich bezieht sich dieses Wort auf die „Bestrafung" eines Vergehens und erfasst somit lediglich einen Teil des Ordnungswidrigkeitsverfahrens, nämlich die Festlegung der Rechtsfolgenseite. Dies ergibt sich auch aus einer systematischen Schau des OWiG, das das Wort „ahnden" konsequent in diesem Sinne verwendet (vgl. § 117 Abs. 2 OWiG statt vieler; § 3 OWiG), und aus einem Blick in die Gesetzesmaterialien (BT-Drs. 13/6914, S. 50), die die Anwendung von § 28 Abs. 2 Nr. 3 StVG

nur für die „*Beurteilung* von Ordnungswidrigkeiten" vorsehen – nicht aber bereits zu deren *Ermittlung*. Für eine **Fahreridentifizierung** als Ermittlungs- bzw. Verfolgungshandlung konnten die genannten Vorschriften deswegen – unabhängig davon, ob FAER-Abfragen hierfür überhaupt geeignet wären – nicht herangezogen werden.

Als mögliche Zweckrichtung kam somit nur die Vorbereitung eines Bußgeldbescheids **(Bußgeldbemessung)** in Betracht. Vor dem Hintergrund des Prinzips der Erforderlichkeit musste die oben beschriebene Vorgehensweise der FAER-Abfragen hier jedoch als datenschutzrechtlich unzulässig bewertet werden. Im Rahmen der Erforderlichkeitsprüfung ist auch ein zeitlicher Aspekt zu berücksichtigen. Zum Zeitpunkt der Registerabfrage stand die Identität des Fahrers noch nicht fest; das Verfahren befand sich erst in der Ermittlungsphase. Eine gesicherte Erkenntnis in Form eines hinreichenden Tatverdachts lag nicht vor. Erfolgt ein Registerabruf zu einem Zeitpunkt, zu dem die so zu erlangenden Daten noch überhaupt nicht für die Bearbeitung eines Vorgangs benötigt werden, fehlt es an der Erforderlichkeit für die staatliche Aufgabenerfüllung. Solange sich ein Verkehrsordnungswidrigkeitenverfahren noch in einem Stadium befindet, in dem nicht gegen einen konkreten Betroffenen vorgegangen wird (es fehlt noch an einem Inkulpationsakt der Verfolgungsbehörde), ist das Einholen von Informationen zu einer möglichen Rechtsfolge verfrüht. FAER-Abfragen sind erst dann erforderlich, wenn die Behörde gegen eine ermittelte Person ein Bußgeld verhängen möchte und dessen konkrete Höhe unter Berücksichtigung bestehender Voreintragungen entsprechend festzusetzen hat.

Die vorstehende rechtliche Beurteilung mit dem Ergebnis einer datenschutzrechtlichen Unzulässigkeit des bislang praktizierten Vorgehens bei FAER-Abfragen unter Verwendung des Fachprogramms WinOWiG wurde dem betroffenen Landesverwaltungsamt im April 2021 zur Kenntnis gebracht und gleichzeitig Möglichkeit zur Stellungnahme gegeben. Dieses äußerte sich sehr

kooperativ und folgte den Erwägungen des Unabhängigen Datenschutzzentrums vollumfänglich. Bereits bis Ende Juli 2021 fand eine umfassende Verfahrensanpassung statt. Automatisierte FAER-Abfragen werden nun nicht mehr bereits im Fahrerermittlungsverfahren ausgelöst, sondern finden nur noch dann statt, wenn der Betroffene die Fahrereigenschaft zugegeben hat (Anhörung) oder der Fahrer auf andere Weise erfolgreich ermittelt werden konnte. Alle Mitarbeiter erhielten zudem die Weisung, manuelle FAER-Abfragen erst dann vorzunehmen, wenn die Fahrereigenschaft feststeht. Dieses Vorgehen entspricht nun den geltenden Vorgaben an Zweck und Erforderlichkeit.

Auch aus anderen Bundesländern wurde im länderübergreifenden Arbeitskreis Sicherheit von vergleichbaren Verfahren berichtet. Das Vorgehen bei FAER-Abfragen befindet sich somit deutschlandweit auf dem Prüfstand.

Fazit/ Empfehlung:

Wird das FAER durch Behörden zu Zwecken der Bußgeldbemessung abgerufen, so ist der Abruf erst nach erfolgter Identifizierung des betroffenen Fahrzeugführers zulässig. Vorherige Abfragen sind nicht erforderlich. Insbesondere eine Abfrage während des Fahrerermittlungsverfahrens ist verfrüht. Falls automatisierte Verfahren bestehen, sollte auf eine entsprechende Anpassung hingewirkt werden.

Neben dem Landesverwaltungsamt, dessen Abläufe zwischenzeitlich angepasst wurden, betrifft dies vor allem kommunale Ortspolizeibehörden, die ggf. Erstermittlungen in Verkehrsordnungswidrigkeiten durchführen.

4.9 Übermittlung personenbezogener Bauunterlagen

Für eine effiziente Form der öffentlichen Verwaltung erweisen sich automatisierte oder auf Anfrage hin stattfindende Datenübermittlungen zwischen Behörden als essentiell. Benötigt die

die Daten empfangende Stelle die übermittelten Informationen, um die ihr obliegenden Aufgaben zu erfüllen und liegt eine entsprechende Rechtsgrundlage für die Datenverarbeitung vor, käme es in vielen Konstellationen zu einem umständlichen Formalismus, wenn die Daten nach den Grundsätzen der Direkterhebung jedes Mal aufs Neue von der betroffenen Person erhoben werden müssten.

Diesem Umstand trägt § 4 Abs. 2 SDSG Rechnung, indem die Vorschrift bestimmt, dass die Übermittlung personenbezogener Daten an öffentliche Stellen zulässig ist, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stellen oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist.

Vor diesem Hintergrund ist jedoch zu berücksichtigen, dass eine Datenübermittlung auf Grundlage dieser Generalklausel in den Fällen ausscheidet, in welchen die Verarbeitungsgrundlagen personenbezogener Daten für bestimmte Rechtsgebiete bereichsspezifisch im jeweiligen Fachrecht geregelt sind. Diese Bestimmungen genießen insoweit Vorrang vor den allgemeinen Regelungen des SDSG.

Eine solche speziellere Übermittlungsnorm findet sich in § 84 der Landesbauordnung (LBO). Dessen Absatz 3 lautet wie folgt:

"*Die Übermittlung personenbezogener Daten an andere Behörden und Private ist unter folgenden Voraussetzungen zulässig:*

1. Personenbezogene Daten der antragstellenden Person dürfen an andere in Verfahren nach diesem Gesetz zu beteiligende Behörden nur weitergegeben werden, wenn sie für deren Entscheidung erforderlich sind. Bei der Weiterleitung des Antrags sind nur die Unterlagen beizufügen, die die anderen Behörden für ihre Entscheidung benötigen. Die Behörden dürfen die übermittelten Daten nur zu dem Zweck verarbeiten, zu dem sie übermittelt worden sind.

2. Im Verfahren nicht beteiligten Behörden, die zur Erfüllung der ihnen gesetzlich zugewiesenen Aufgaben Kenntnis von erteilten

Genehmigungen und Zustimmungen nach diesem Gesetz haben müssen, sind die erforderlichen personenbezogenen Daten mitzuteilen.

3. Personenbezogene Daten der am Bau Beteiligten dürfen an die oberste Bauaufsichtsbehörde, die Architektenkammer des Saarlandes oder die Ingenieurkammer weitergeleitet werden, soweit sie für Entscheidungen nach § 66 Abs. 4, § 67 Abs. 6, § 88 Abs. 4 Satz 3 oder § 88 Abs. 6 Satz 5 oder für Entscheidungen nach § 48 und § 50 Abs.2 des Saarländischen Architekten- und Ingenieurkammergesetzes erforderlich sind."

§ 84 Abs. 3 LBO regelt die Übermittlung personenbezogener Daten durch die Bauaufsichtsbehörden abschließend.

Auch die Übermittlung personenbezogener Daten (Bauunterlagen mit personenbezogenem Inhalt) auf Grundlage der allgemeinen Amtshilfevorschiften (§§ 4 ff. SVwVfG) ist nur zulässig – dies ergibt sich bereits aus § 7 Abs. 1 SVwVfG – wenn die vorgenannten gesetzlichen Voraussetzungen erfüllt sind.[20]

Relevant wird dies vor allem im Bereich von Anzeigenpflichten des Bauherrn, etwa im Bereich der Sicherheit und des Gesundheitsschutzes auf Baustellen. Diesbezügliche Regelungen trifft der Bundesgesetzgeber u. a. in der Baustellenverordnung (BaustellV)[21]. In § 2 Abs. 2 BaustellV hat er sich für ein Verfahren entschieden, in welchem der Bauherr (§ 4 BaustellV) die betreffende Baustelle bei der zuständigen Behörde spätestens zwei Wochen vor Baustelleneinrichtung anzuzeigen hat (sog. Bauvoranküngigung). Eine Pflicht hierzu besteht, wenn die Voraussetzungen des § 2 Abs. 2 Nr. 1 und 2 BaustellV vorliegen. Dies ist der Fall, wenn die voraussichtliche Dauer der Arbeiten mehr als

[20] Das Erfordernis "amtshilfefester" bereichsspezifischer Verarbeitungsgrundlagen kann bereits dem Volkszählungsurteil des Bundesverfassungsgerichts entnommen werden, Urteil vom 15. Dezember1983 – 1 BvR 209/83 u. A., Rn. 154, zitiert nach der Veröffentlichung auf https://www.bundesverfassungsgericht.de

[21] Verordnung über Sicherheit und Gesundheitsschutz auf Baustellen – Baustellenverordnung vom 10. Juni 1998 (BGBl. I S. 1283), zuletzt geändert durch Gesetz vom 27. Juni 2017 (BGBl. I S. 1966).

30 Arbeitstage beträgt und auf der Baustelle mehr als 20 Beschäftigte gleichzeitig tätig werden, oder der Umfang der Arbeiten voraussichtlich 500 Personentage überschreitet. In diesen Fällen sind der zuständigen Behörde mindestens die in Anhang I der Baustellenverordnung enthaltenen Angaben über das Bauvorhaben zu übermitteln, d. h. insbesondere Ort der Baustelle, Name und Anschrift des Bauherren, bzw. der für die Baustelle verantwortlichen Personen, und Art des Bauvorhabens.

Aus datenschutzrechtlicher Sicht regelt § 2 Abs. 2 BaustellV damit ein Verfahren der Direkterhebung, bei der die Pflicht der eigeninitiativen Datenübermittlung dem Bauherrn selbst auferlegt wird. Dieses Verfahren kann nicht durch eine Datenübermittlung von der Bauaufsichtsbehörde an die für den Arbeitsschutz auf Baustellen zuständige Behörde ersetzt werden.

Der Problematik nichtangemeldeter Bauvorhaben und daraus resultierender Kontrolldefizite kann in diesem Bereich daher nur durch Schaffung einer entsprechenden Übermittlungsnorm begegnet werden.

4.10 Datenverarbeitung im Rahmen von Fahrkartenkontrollen

Nach dem in Artikel 5 Abs. 1 lit. c DSGVO niedergelegten Grundsatz der Datenminimierung (Datensparsamkeit) muss die Verarbeitung personenbezogener Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Es handelt sich bei diesem Grundsatz letztlich um eine Ausprägung des jeder Datenverarbeitung zugrundeliegenden allgemeinen Erforderlichkeitsprinzips, welches besagt, dass personenbezogene Daten nur insoweit und solange verarbeitet werden dürfen, wie sich dies für die Erreichung des Verarbeitungszweckes auch tatsächlich als notwendig erweist.

In der aufsichtsbehördlichen Praxis der letzten Jahre hat sich gezeigt, dass sich die betroffenen Personen in zunehmendem

Maße diesem Grundsatz bewusst zu werden scheinen und sich auch in privatwirtschaftlichen Vertragsverhältnissen vermehrt die Frage stellen, welche Daten sie ihrem Vertragspartner überhaupt offenbaren sollen bzw. offenbaren müssen.

Vor diesem Hintergrund hatte sich unsere Behörde mit einer Datenverarbeitung des Saarländischen Verkehrsverbundes (saarVV) im Rahmen des Ticket- und Abonnementmanagements für den öffentlichen Personennahverkehr zu beschäftigen. Hierbei ging es um die Frage, inwiefern bei der Nutzung des "saarVV eTickets" auch die Geburtsdaten der Ticketinhaber gespeichert und im Zuge einer Fahrkartenkontrolle ausgelesen werden dürfen.

Bei dem eTicket des saarVV handelt es sich um eine scheckkartengroße Plastikkarte mit einem integrierten Mikrochip. Auf diesem Chip sind neben den Informationen zur Beförderungsleistung (Ticketart, räumliche/zeitliche Gültigkeit, Übertragbarkeit, Kartennummer) im Falle eines personengebundenen Tickets auch der Vor- und Zuname sowie das Geburtsdatum des jeweiligen Ticketinhabers gespeichert. Im Falle einer Fahrkartenkontrolle wird das eTicket durch das kontrollierende Personal elektronisch ausgelesen, welchem sodann bereits vor Ort die auf der Karte gespeicherten Daten auf einem Lesegerät angezeigt werden.

Diese Form der Datenverarbeitung erachten wir als rechtskonform und von der Verarbeitungsgrundlage des Art. 6 Abs. 1 S. 1 lit. b DSGVO erfasst. In Bezug auf die Geburtsdaten der Ticketinhaber stellt sie insbesondere keinen Verstoß gegen den Grundsatz der Datenminimierung dar.

Das personengebundene eTicket berechtigt vertraglich nur den jeweiligen Ticketinhaber zur Beförderung. Zwecks eindeutiger Identifizierung dieser Person im Rahmen einer Fahrkartenkontrolle zeigt sich die Verarbeitung von Vor- und Zuname sowie Geburtsdatum als erforderlich. Insbesondere aufgrund des Umstands, dass auf dem Äußeren des eTickets nur der Name des

Ticketinhabers vermerkt, jedoch kein weiteres Personenmerkmal – etwa ein Lichtbild – aufgedruckt ist, genügt eine äußere Inaugenscheinnahme des Tickets für sich genommen noch nicht, um eine hinreichende Identifizierung zu gewährleisten; vor allem in Bezug auf häufig vorkommende Vor- und Nachnamen. Das die Fahrkarten kontrollierende Personal ist in diesen Fällen darauf angewiesen, auf ein zusätzliches eindeutiges Identifizierungsmerkmal – wie das Geburtsdatum einer Person – zurückgreifen zu können, um die Fahrberechtigung zu prüfen und gegebenenfalls mittels eines Abgleichs mit einem amtlichen Ausweisdokument (Personalausweis) verifizieren zu können.

4.11 Unabhängige Aufarbeitungskommission am Universitätsklinikum des Saarlandes

Zur Aufarbeitung der Missbrauchsverdachtsfälle in der Kinder- und Jugendpsychiatrie am Universitätsklinikum des Saarlandes (UKS) hat der Aufsichtsrat der Klinik im vergangenen Jahr eine unabhängige Aufarbeitungskommission eingesetzt. Die Kommission setzt sich aus Experten aus verschiedenen Bereichen zusammen und hat den Auftrag, die Vorgänge umfassend zu untersuchen mit dem Ziel, den Betroffenen Hilfe und Unterstützung zukommen zu lassen, Transparenz zu schaffen und innerorganisatorische Abläufe zu optimieren. Außerdem sollen geeignete Maßnahmen aufgezeigt werden, durch die am UKS zukünftig ein besserer Schutz vor sexuellem Missbrauch gewährleistet werden kann.

Nachdem wir in der Vergangenheit bereits den durch die Staatskanzlei des Saarlandes zur Aufklärung der Vorfälle eingesetzten Sonderermittler in datenschutzrechtlichen Belangen unterstützt hatten, ist der Vorsitzende der Aufarbeitungskommission mit der Bitte an das Unabhängige Datenschutzzentrum herangetreten, auch die Arbeit der Kommission datenschutzrechtlich zu begleiten. Vor dem Hintergrund, dass insbesondere die Auswertung von Patientenakten, die naturgemäß sensible personenbezogene Daten enthalten, ein wichtiger Bestandteil

der Arbeit der Kommission sein wird, sind wir dieser Bitte selbstverständlich nachgekommen.

In mehreren Gesprächen zwischen unserer Behörde und den Vertretern von Kommission sowie UKS wurden die datenschutzrechtlichen Vorgaben erörtert, die im Rahmen der Aufarbeitung zu beachten sind. Wir haben die Kommission bei der Erstellung eines Datenschutzkonzepts unterstützt, wobei sowohl die rechtlichen Grundlagen für die Datenverarbeitungsprozesse als auch erforderliche technisch-organisatorische Maßnahmen in den Blick genommen wurden.

Hierbei galt es zu berücksichtigen, dass die Daten, die zur Aufarbeitung herangezogen werden sollen, aus verschiedenen Quellen stammen, so dass für deren Erhebung und Nutzung zum Teil unterschiedliche rechtliche Vorgaben zu beachten sind. Hier haben wir Lösungswege aufgezeigt, die einerseits eine umfassende Aufarbeitung ermöglichen, andererseits aber auch die Patientenrechte wahren und die sensiblen Daten der Betroffenen hinreichend schützen.

So wurde unter anderem klargestellt, dass eine Auswertung der am UKS geführten Patientenakten hinsichtlich der Gesundheitsdaten grundsätzlich nur mit Einwilligung der betroffenen Patienten erfolgen darf. Bei fehlender Einwilligung werden die Akten lediglich im Hinblick auf die organisatorischen Abläufe untersucht, Gesundheitsdaten der Patienten werden der Kommission in diesen Fällen nicht zur Verfügung gestellt.

Thematisiert wurden weiterhin die im Datenschutzkonzept festzulegenden Löschfristen für die durch die Kommission verarbeiteten Daten sowie Regelungen für die Ausübung von Betroffenenrechten der Patienten.

Neben der Beachtung der rechtlichen Rahmenbedingungen ist der Schutz der verarbeiteten personenbezogenen Daten auch durch geeignete technisch-organisatorische Maßnahmen sicherzustellen, die der Sensibilität der Daten und dem Risiko der Verarbeitung für die Betroffenen angemessen sind.

So erfolgt die Datenverarbeitung durch die Aufarbeitungskommission beispielsweise auf einem abgeschotteten System, in das die Fachbereiche des UKS relevante Informationen einspeichern. Die Arbeit der Kommission findet folglich nicht auf den Livesystemen (Krankenhausinformationssystemen) statt. Hierauf erhalten die Kommissionsmitglieder keinen unmittelbaren Zugriff.

Als weitere Schutzmaßnahme wurde dem UKS empfohlen, den Mitgliedern der Kommission dienstliche Laptops zur Verfügung zu stellen, die nur für die Arbeit im Rahmen des Aufarbeitungsprozesses genutzt werden, so dass keine privaten Endgeräte verwendet werden müssen. Die Nutzung privater Endgeräte stellt regelmäßig ein vermeidbares Risiko bei der Datenverarbeitung dar. Das Klinikum hat dies umgehend aufgegriffen und umgesetzt.

Begrüßenswert ist auch, dass das Datenschutzkonzept eine regelmäßige Auditierung und Evaluierung der getroffenen technischen und organisatorischen Maßnahmen vorsieht.

Dank der konstruktiven Zusammenarbeit mit dem UKS und der Kommission konnten für den bevorstehenden Aufarbeitungsprozess datenschutzrechtliche Rahmenbedingungen im Sinne der Betroffenen geschaffen werden. Wir haben dabei rechtlich zulässige Wege aufgezeigt, um die Ziele der Aufarbeitungskommission datenschutzkonform zu erreichen.

4.12 Diskreter Postversand im Gesundheitsbereich

Beim Versand von Briefen und Paketen im Gesundheitswesen ist zu beachten, dass je nach Gestaltung von Umschlägen und Kartons Rückschlüsse auf den Inhalt der Sendung und damit verbunden auch auf bestehende Erkrankungen möglich sind, so dass Dritte Informationen über den Empfänger erhalten können. Dies kann unter Umständen eine unberechtigte Offenlegung von Gesundheitsdaten darstellen, wie folgende Beispiele zeigen.

4.12.1 Arztstempel mit Fachrichtung auf dem Briefumschlag

Im Rahmen einer Beschwerde wurde das Unabhängige Datenschutzzentrum Saarland darauf aufmerksam gemacht, dass eine Arztpraxis beim postalischen Versand von Rechnungen einen großen Stempel mit Angabe der Fachrichtung verwendet. Der Beschwerdeführer äußerte die Befürchtung, dass diese Information für jeden, der einen flüchtigen Blick auf den Briefumschlag wirft (z. B. Postbote, Nachbar), Rückschlüsse auf eine Behandlung in der betreffenden Praxis und somit auf die Art seiner Erkrankung zulässt. Er bat um Prüfung, ob die Angabe der Fachrichtung außen auf einem Briefumschlag aus datenschutzrechtlicher Sicht zulässig ist.

Die Angabe des Absenders auf einem Briefkuvert ist beim Postversand obligatorisch. Die Erwähnung der Fachrichtung eines Arztes dürfte hierbei in aller Regel jedoch nicht erforderlich sein; vielmehr sollten Name und Anschrift des Arztes genügen, um gegebenenfalls eine Rücksendung zu ermöglichen.

Ob aber das Aufbringen eines Stempels mit der Fachrichtung auch gegen datenschutzrechtliche Vorgaben verstößt, hängt zunächst davon ab, ob diese Angabe in Verbindung mit dem Adressaten ein personenbezogenes Datum des Empfängers gem. Art. 4 Nr. 1 DSGVO darstellt. Dafür spricht, dass die Tatsache, dass jemand von einem Facharzt angeschrieben wird, die Vermutung nahelegt, dass diese Person sich dort in Behandlung befindet. Hieraus können möglicherweise Rückschlüsse auf die Art der Erkrankung und somit auf den Gesundheitszustand der betreffenden Person gezogen werden. Erhält jemand beispielsweise Post von einem Facharzt für Psychiatrie und Psychotherapie, liegt es nahe, beim Empfänger eine psychische Erkrankung anzunehmen. Da gerade psychisch Kranke oftmals mit Vorurteilen und Diskriminierung konfrontiert werden, ist der berechtigte Wunsch nach Diskretion anhand dieses Beispiels gut nachvollziehbar.

Allerdings handelt es sich bei Adressaten, die Post von einer Arztpraxis erhalten, nicht immer zwingend um Patienten der Praxis. Als mögliche Empfänger von Rechnungen kommen beispielsweise auch Dritte wie Familienangehörige oder Betreuer in Betracht. Die schriftliche Korrespondenz von Arztpraxen erfolgt nicht ausschließlich mit Patienten. Zudem ist fraglich, ob eine Fachrichtung, die ein breites Spektrum an Krankheitsbildern abdeckt, eine derart konkrete Information darstellt, dass diese Angabe als personenbezogenes Gesundheitsdatum gewertet werden muss.

Hinzu kommt, dass die Information über die Fachrichtung bei Interesse mit einfachen Mitteln beispielweise im Internet recherchiert werden kann; in kleineren Orten dürfte ohnehin bekannt sein, welcher Fachrichtung ein Arzt angehört, wodurch bereits dessen Name aufschlussreich sein kann.

Trotz Zweifeln an der Einordnung des Aufdrucks als personenbezogenes Datum des Adressaten haben wir die Beschwerde zum Anlass genommen, die betreffende Praxis zu kontaktieren und auf die Problematik aufmerksam zu machen. Diese hat den Hinweis aufgegriffen und zugesagt, zukünftig einen Poststempel ohne Bezeichnung der Fachrichtung zu nutzen.

4.12.2 Neutrale Verpackung bei Paketen mit Medizinprodukten

Ähnlich zu beurteilen ist die Gestaltung von Paketen beim Versand medizinischer Produkte, wie beispielsweise Hilfsmitteln zur Unterstützung bei bestimmten Erkrankungen.

Werden für den Versand der Produkte Kartons genutzt, auf denen neben dem Firmennamen auch Angaben zum Inhalt aufgedruckt sind, lässt sich daraus unter Umständen ableiten, unter welcher Art von Beschwerden der Empfänger der Sendung vermutlich leidet. So lässt beispielsweise ein Paket, das erkennbar Inkontinenzhilfen enthält, vermuten, dass der Empfänger an Inkontinenz leidet. Die hiervon Betroffenen dürften in der Regel

ein Interesse daran haben, dass diese Information keinem Dritten bekannt wird.

Hilfsmittel, für deren Kosten die gesetzlichen Krankenkassen aufkommen, dürfen nur auf der Grundlage von Verträgen zwischen den Krankenkassen und Leistungserbringern oder deren Verbände an Versicherte abgegeben werden (vgl. § 126 Abs. 1 Satz 1 i. V. m. § 127 Abs. 1 und 3 SGB V[22]). In diesen Verträgen finden sich zum Teil auch Vorgaben zur Lieferung. Demnach hat die Lieferung in neutraler Verpackung zu erfolgen, d.h. es muss sichergestellt werden, dass die Verpackungen keinen Rückschluss auf den Inhalt und die Hilfsmittel zulassen.

Aus datenschutzrechtlicher Sicht stellt sich ähnlich wie im Falle der Fachrichtung auf dem Brief einer Arztpraxis wiederum die Frage, ob der Aufdruck auf dem Paket ein personenbezogenes Datum des Adressaten gem. Art. 4 Nr. 1 DSGVO darstellt. Zwar liegt hier die Vermutung nahe, dass der Empfänger der Sendung unter einer bestimmten Erkrankung leidet, zu deren Behandlung der offensichtliche Inhalt der Lieferung benötigt wird; andererseits ist die Person, die die Hilfsmittel benötigt, nicht unbedingt identisch mit dem Adressaten. Es ist daher nicht zwingend von einem personenbezogenen Datum auszugehen.

Dennoch sind die vorstehend genannten vertraglichen Regelungen aus datenschutzrechtlicher Sicht zu begrüßen.

Fazit/ Empfehlung:

Insbesondere im Gesundheitsbereich sollte durch eine neutrale Gestaltung von Postsendungen dafür Sorge getragen werden, dass keine Informationen über den Gesundheitszustand des Empfängers abgeleitet werden können.

[22] Sozialgesetzbuch (SGB) Fünftes Buch (V) – Gesetzliche Krankenversicherung – vom 20. Dezember 1988 (BGBl. I S. 2477), zuletzt geändert durch Gesetz vom 18.3.2022 (BGBl. I S. 473).

4.13 Löschanspruch bei Bewerberdaten

Abgelehnte Bewerber fordern ab und an von den Unternehmen oder Behörden, bei denen sie sich erfolglos beworben haben, die Löschung aller eingereichten Bewerbungsunterlagen. In Fällen, in denen das Unternehmen oder die Behörde dem Anliegen der abgelehnten Bewerber nicht zufriedenstellend nachgekommen ist, wurden wir als Aufsichtsbehörde im Berichtszeitraum mehrfach von den Betroffenen gem. Art. 77 DSGVO mit einer entsprechenden Beschwerde kontaktiert.

Bewerber für ein Beschäftigungsverhältnis gelten gemäß § 26 Abs. 8 S. 2 BDSG datenschutzrechtlich als Beschäftigte mit der Folge, dass die für die Beschäftigten geltenden Vorschriften auch im Bewerbungsverfahren anzuwenden sind. Nach § 26 Abs. 1 BDSG sowie gem. § 22 Abs. 1 SDSG für Bewerber im öffentlichen Dienst des Saarlandes dürfen Daten von Beschäftigten/Bewerbern unter anderem verarbeitet werden, wenn dies dem Zweck der Eingehung eines Beschäftigungsverhältnisses dient.

Jeder Bewerber hat jedoch grundsätzlich das Recht darauf, dass seine personenbezogenen Daten nach erfolglosem Ablauf des Einstellungsverfahrens gelöscht werden. Datenschutzrechtlich ergibt sich diese Verpflichtung aus den Art. 5 und 15 DSGVO, wonach Daten zu löschen sind, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Fällt dieser Zweck weg und liegt auch keine entsprechende Einwilligung des Bewerbers oder eine gesetzliche Vorschrift vor, die die weitere Speicherung erforderlich macht, sind die Daten zu löschen. Für den Bereich des öffentlichen Dienstes im Saarland existiert in § 22 Abs. 7 SDSG eine eigene Rechtsgrundlage zur Löschung von Bewerberdaten.

Etwas anderes gilt, wenn der Bewerber in die weitere Speicherung eingewilligt hat, etwa für den Fall, dass der Arbeitgeber die Bewerberdaten für eine mögliche zukünftige Stelle heranziehen möchte. In diesem Fall entfällt die Verpflichtung zur Löschung der Daten aufgrund der rechtmäßig erteilten Einwilligung des

Bewerbers, die aufgrund der gleichgelagerten Interessen zum Vorteil des Bewerbers im Beschäftigungskontext möglich ist.

Nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) besteht jedoch gem. § 15 für abgelehnte Bewerber ein Schadensersatzanspruch für den Fall, dass die Arbeitgeber sie in unzulässiger Weise diskriminiert haben. Solange ein Arbeitgeber mit einer solchen Klage rechnen muss, kann er die Bewerberdaten aufbewahren. Während eines laufenden Gerichtsverfahrens, zu dem die Unterlagen zu Beweissicherungszwecken erforderlich sind, dürfen diese natürlich ebenfalls nicht gelöscht werden.

Fazit/ Empfehlung:

Arbeitgeber müssen die Regelungen des Datenschutzrechts auch im Bewerbungsverfahren berücksichtigen und Bewerberdaten abgelehnter Bewerber grundsätzlich unverzüglich löschen, sobald der Zweck, zu dem sie gespeichert wurden, entfallen ist.

4.14 Veröffentlichung von Dienstplänen

Dienstpläne in Behörden und Unternehmen dienen dem Zweck, einen reibungslosen Arbeitsablauf sicherstellen zu können. Dabei muss kurzfristig und flexibel auf Ausfälle in der Belegschaft reagiert werden und Beschäftigte müssen unmittelbar erreicht und über Änderungen informiert werden können.

Aber auch bei der Dienstplangestaltung sind datenschutzrechtliche Aspekte zu berücksichtigen.

Dabei gilt es zunächst, den in Art. 5 Abs. 1 lit. c DSGVO verankerten Grundsatz der Datenminimierung zu beachten. Nach diesem Grundsatz dürfen nur die für den mit der Verarbeitung angestrebten Zweck erforderlichen Daten verarbeitet werden.

Bei der Abwesenheit von Beschäftigten ist es etwa zur Dienstplangestaltung nicht erforderlich, den Grund der Abwesenheit zu benennen. Um den o.g. Zweck eines Dienstplanes zu errei-

chen, müssen alle anderen Beschäftigten schlichtweg nicht wissen, ob Kollegen wegen Krankheit, Urlaub, einer Rehabilitationsmaßnahme, einer Fort- oder Weiterbildung oder anderweitiger Sachverhalte nicht zum Dienst erscheinen. Diese Informationen werden ausschließlich von der personalverwaltenden Stelle benötigt, um beispielsweise Entgeltfortzahlungsansprüche der Beschäftigten berechnen zu können.

Schließlich müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet (Art. 5 Abs. 1 lit. f DSGVO). Dies umfasst auch den Schutz vor unbefugter und unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Veränderung der personenbezogenen Daten. Hierfür sind geeignete technische und organisatorische Maßnahmen zu ergreifen, die insbesondere in Art. 32 DSGVO konkretisiert werden (Grundsatz der Integrität und Vertraulichkeit).

So ist der Kreis der betroffenen Beschäftigten, für die der Dienstplan von Relevanz ist, durch ein angemessenes Zugriffs- und Berechtigungskonzept so auszugestalten, dass nur diejenigen Personen die Informationen erhalten, für deren Tätigkeit sie von Belang sind. Ist eine Vertretung zwischen zwei unterschiedlichen Abteilungen nicht möglich, so hat Abteilung A nicht zu wissen, wie der Dienstplan von Abteilung B aussieht. Lediglich Beschäftigten der Abteilung A dürfen Zugriffsrechte auf den Dienstplan der Abteilung A eingeräumt werden.

Als technisch-organisatorische Maßnahme ist ein Dienstplan, der personenbezogene Daten enthält, nicht öffentlich ins Internet zu stellen. Andernfalls hätten auch Personen Zugriff auf diese Informationen, die nicht befugt sind, diese zu erhalten. Technische und organisatorische Maßnahmen, die dazu dienen, dass nur berechtigte Personen die erforderlichen Informationen erhalten, sind beispielsweise die Veröffentlichung in einem passwort-geschützen Bereich einer Homepage oder im Intranet. Die Nutzung geeigneter Kommunikationswege zur Information

der Beschäftigten ist ebenfalls datenschutzkonform zu gestalten. Eine Mitteilung an einen Beschäftigten, dass es Änderungen im Dienstplan gegeben hat (ohne Angabe von Details), ist inhaltlich nicht personenbezogen und kann auch per Messengerdienst mitgeteilt werden. Personenbezogene Daten aus dem Dienstplan selbst sollten indes nicht auf diesem Weg übermittelt werden, da nicht auszuschließen ist, dass auch Unbefugte Zugriff auf diese Information erhalten könnten.

Fazit/ Empfehlung:

Dienstpläne enthalten personenbezogene Daten, die nur Berechtigten zugänglich gemacht werden dürfen. Wir empfehlen geeignete Zugriffs- und Berechtigungskonzepte sowie die Veröffentlichung in passwortgeschützen Bereichen einer firmeneigenen Homepage oder dem Intranet

4.15 Drittlandübermittlungen: Neue Standarddatenschutzklauseln

Im 29. Tätigkeitsbericht für den Berichtszeitraum 2020 wurden bereits die Auswirkungen des Urteils des Europäischen Gerichtshofes (EuGH) vom 16. Juli 2020 (Rs. C-311/18 – Schrems II) hervorgehoben. Demnach ist eine Übermittlung personenbezogener Daten in die USA auf Grundlage des sog. „Privacy Shields" nicht mehr möglich, da das hierdurch gewährleistete Schutzniveau nicht dem der DSGVO entspricht. Auch im Jahr 2021 haben sich aus diesem Urteil weitere Entwicklungen ergeben. So hat die Europäische Kommission mit Durchführungsbeschluss vom 4. Juni 2021 neue Standardvertragsklauseln veröffentlicht, die nunmehr neue Konstellationen von Drittlandübermittlungen erfassen und deren Anspruch es ist, die Vorgaben des EuGH in Sachen „Schrems II" sowie die Vorgaben des Europäischen Datenschutzausschusses (EDSA) in seinen „Empfehlungen 01/2020

zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“[23] zu berücksichtigen.

Während die neuen Standardvertragsklauseln grundsätzlich zu begrüßen sind und den Verantwortlichen eine flexiblere Selektion der passenden Vertragsklauseln ermöglichen, ist in ihnen jedoch kein Allheilmittel zu sehen, welches Defizite des Datenschutzniveaus in einem Drittland in allen Fällen ausgleichen könnte. Denn sie sind gerade nicht als Instrument gedacht, das solche Drittlandübermittlungen legitimieren kann, die unter Berücksichtigung der Anforderungen des EuGH rechtswidrig sind, vielmehr übernehmen die neuen Klauseln die Anforderungen des EuGH und machen sie zum Vertragsgegenstand. Steht etwa das nationale Recht des Drittlandes im Widerspruch zu den in den Standardvertragsklauseln vereinbarten Pflichten, vermögen es auch die neuen Klauseln allein nicht, eine spezifische Drittlandübermittlung zu legitimieren. Das kann beispielweise dann der Fall sein, wenn das jeweilige nationale Recht den dortigen Sicherheitsbehörden Zugriff auf personenbezogene Daten einräumt. Es bleibt demnach auch bei Verwendung der neuen Standardvertragsklauseln erforderlich, die Rechtslage im jeweiligen Drittland zu überprüfen. Nur auf Basis einer solchen Prüfung kann der Verantwortliche beurteilen, ob die neuen Standardvertragsklauseln allein geeignet sind, das erforderliche Schutzniveau zu gewährleisten. Steht dem das nationale Recht entgegen, müssen die Vorgaben der o.g. Empfehlungen 01/2020 des EDSA berücksichtigt und demnach zusätzliche Schutzmaßnahmen implementiert werden. Sind im konkreten Fall auch keine der vom EDSA vorgeschlagenen, ergänzenden Maßnahmen umsetzbar, darf auch unter Verwendung der neuen Standardvertragsklauseln eine Drittlandübermittlung nicht erfolgen.

[23] Elektronisch abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/ recommendations-012020-measures-supplement-transfer_de

Dies hat auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Ländern (DSK) nochmals in ihrer Pressemitteilung vom 21. Juni 2021 „Ergänzende Prüfungen und Maßnahmen trotz neuer EU-Standardvertragsklauseln für Datenexporte nötig“[24] klargestellt.

4.16 Telemedien

4.16.1 TTDSG

Am 1. Dezember 2021 ist das Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutz-Gesetz – **TTDSG**) in Kraft getreten. § 25 TTDSG stellt die fällige Umsetzung des an den Bundesgesetzgeber adressierten Regelungsauftrags aus Art. 5 Abs. 3 ePrivacy-Richtlinie dar, die ursprünglich schon bis 25. Mai 2011 hätte erfolgt sein müssen.

§ 25 Abs. 1 TTDSG sieht vor, dass

„eine Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, (...) nur zulässig [sind], wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat“.

Die Vorschrift sieht in den genannten Fällen einen grundsätzlichen **Einwilligungsvorbehalt** vor, den der BGH bereits mit seinem Urteil vom 28. Mai 2020 (Az. I ZR 7/16 - Cookie-Einwilligung II) im Wege einer richtlinienkonformen Auslegung des § 15 Abs. 3 TMG a.F. statuiert hatte. § 15 TMG a.F. wurde nunmehr, wie der gesamte 5. Abschnitt des TMG (Datenschutz), zum 1. Dezember 2021 zugunsten der Regelungen des TTDSG aufgehoben.

Nach § 25 Abs. 2 Nr. 2 TTDSG muss ausnahmsweise dann keine Einwilligung der Webseitenbesucher eingeholt werden, wenn die Verarbeitung *„unbedingt erforderlich ist, damit der Anbieter*

[24] Elektronisch abrufbar unter: https://www.datenschutzkonferenz-online.de/media/pm/2021_pm_neue_ scc.pdf

eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann".

Welcher Dienst gewünscht ist, ist also aus Nutzerperspektive zu bestimmen. Dabei sind einzelne abgrenzbare Dienste innerhalb des Gesamtangebots gesondert in Betracht zu nehmen. In der Regel kann erst dann von einem ausdrücklichen Wunsch des Nutzers ausgegangen werden, falls bzw. sobald er mit dem konkreten Dienst interagiert.

Haben Daten, die in der Endeinrichtung des Nutzers gespeichert werden bzw. auf die zugegriffen wird, einen Personenbezug i. S. d. Art. 4 Nr. 1 DSGVO, sind für die nachfolgenden Verarbeitungsvorgänge zudem die Vorgaben der DSGVO einzuhalten. In vielen Fällen wird demnach eine Prüfung sowohl nach dem TTDSG als auch nach der DSGVO erfolgen müssen.

Die Einwilligung nach § 25 Abs. 1 S. 2 TTDSG muss den Anforderungen der DSGVO genügen. Zu den weiteren Einzelheiten der neuen gesetzlichen Regelungen haben die Aufsichtsbehörden Ende 2021 eine aktualisierte Orientierungshilfe für Anbieter von Telemedien veröffentlicht. [25]

4.16.2 Anforderungen an Einwilligungen

Besonderer Nachholbedarf besteht regelmäßig auf Webseiten im Bereich der konkreten Ausgestaltung von sog. „Cookie-" bzw. „Einwilligungsbannern". Entgegen einer teilweise verbreiteten Fehlannahme muss ein derartiger Banner nicht auf jeder Webseite vorhanden sein, sondern nur dann, wenn Verarbeitungsvorgänge entweder nach § 25 TTDSG oder nach den Vorgaben der DSGVO einwilligungsbedürftig sind. Verzichtet der Webseitenbetreiber auf einwilligungsbedürftige Verarbeitungsvorgänge, ist ein Banner hingegen nicht erforderlich.

[25] Elektronisch abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf

Je nach Aufbau und Komplexität der Webseite erfolgen eine Vielzahl unterschiedlicher Verarbeitungsprozesse und Implementierungen unterschiedlicher Dienste (z. B. Dienste zur statistischen Erfassung oder Analyse des Nutzerverhaltens, personalisiertes Ausspielen von Werbung, Einbindung von Inhalten externer Dienstleister wie Videos, Social-Media-Posts etc., (Kontakt-)Formulare, Newsletter-Dienste, Dienste zur technischen Gewährleistung der IT-Sicherheit, Kunden-Accounts u.v.m.). Bezüglich jedes einzelnen Dienstes, der auf der Webseite eingesetzt wird, ist zu überprüfen, welche Rechtsgrundlage hierfür herangezogen werden kann. Kommen andere Rechtsgrundlagen wie Art. 6 Abs. 1 lit. b, f DSGVO nicht infrage, und möchte der Betreiber der Webseite einen Dienst dennoch einsetzen, ist es erforderlich, dass er eine Einwilligung der Nutzer mittels eines Einwilligungsbanners einholt. Bei der Ausgestaltung dieses Banners ist besonderes Augenmerk darauf zu legen, dass dessen Ausgestaltung den Anforderungen der Art. 4 Nr. 11, 7 DSGVO genügt.

Das bedeutet insbesondere, dass eine Einwilligung der Nutzer nur dann wirksam ist, sofern die Nutzer im Rahmen des Einwilligungsbanners hinreichende Informationen erhalten, um Art, Ausmaß und Zwecke der beabsichtigten Verarbeitungen erkennen zu können. Erhält der Nutzer lediglich kursorische bzw. unvollständige Informationen, wird ihm die Gelegenheit zur nötigen Willensbildung verwehrt und er kann eine Einwilligung nicht wirksam erteilen.

Dem Nutzer muss regelmäßig auch die Möglichkeit gegeben werden, die Einwilligung im Rahmen des Banners zu verweigern. Denn nur dann kann die Einwilligung „freiwillig" i. S. d. Art. 4 Nr. 11 DSGVO erfolgen. Dabei darf die Ablehnung der Einwilligung nicht mit einem höheren Aufwand verbunden sein als deren Erteilung. Nicht ausreichend ist es etwa, wenn der Ablehnen-Button erst in einem gesonderten Fenster mit weitergehenden Einstellmöglichkeiten vorhanden ist. Es müssen vielmehr beide Optionen gleichwertig auf erster Ebene des Banners vorgehalten werden.

Weitere Hinweise zur Ausgestaltung des Einwilligungsbanners sind in der veröffentlichten Orientierungshilfe für Anbieter von Telemedien zu finden.

4.17 Datenübermittlung bei Mandatierung von Rechtsanwälten

Regelmäßig erreichen uns Beschwerden, welche die Übermittlung personenbezogener Daten an Rechtsanwälte zum Gegenstand haben. Beschwerdeführer hierbei sind Verfahrensgegner in einem Rechtsstreit oder Dritte, die monieren, dass ihre Daten im Rahmen eines Mandatsverhältnisses einem Rechtsanwalt ohne deren Einverständnis zur Verfügung gestellt werden, etwa in Form von E-Mails oder Schriftstücken.

4.17.1 Datenschutzrechtliche Verantwortlichkeit

Soweit ein Rechtsanwalt in einem Mandatsverhältnis personenbezogene Daten verarbeitet, ist er aufgrund seiner Rechtsstellung als unabhängiges Organ der Rechtspflege datenschutzrechtlich selbst als Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO einzuordnen. Dies gilt auch hinsichtlich personenbezogener Daten Dritter, die ihm von Seiten der Mandanten zur Verfügung gestellt werden.

Diese datenschutzrechtliche Verantwortlichkeit des Rechtsanwalts spielt jedoch erst zu einem späteren Zeitpunkt des Mandatsverhältnisses eine Rolle. Zunächst ist hiervon losgelöst die Übermittlung personenbezogener Daten an den Rechtsanwalt zu betrachten, bevor dieser seine konkrete Tätigkeit aufnimmt. Verantwortlicher für die Datenübermittlung an den Rechtsanwalt ist der Mandant, sodass es für die datenschutzrechtliche Zulässigkeit der Zurverfügungstellung personenbezogener Daten durch den Mandanten auf die Rechtsgrundlagen im Rahmen von dessen Verantwortlichkeit ankommt.

4.17.2 Rechtliche Grundlagen der Übermittlung an den Rechtsanwalt

Die Übermittlung von personenbezogenen Daten fällt gemäß der Definition des Art. 4 Nr. 2 DSGVO unter den Begriff der „Verarbeitung". Grundsätzlich ist für die Verarbeitung personenbezogener Daten in Form einer Datenübermittlung (Art. 4 Nr. 2 DSGVO) eine der in Art. 6 Abs. 1 DSGVO abschließend aufgeführten Rechtsgrundlagen erforderlich.

Zu unterscheiden ist hier zunächst, ob einem Mandanten bereits personenbezogene Daten vorliegen, welche er dem Rechtsanwalt zur Verfügung stellen möchte oder ob seitens des Mandanten die Daten der betroffenen Person vor Übermittlung an den Rechtsanwalt erst erhoben werden (müssen).

Liegen dem Mandanten die Daten bereits vor, zum Beispiel im Rahmen eines Vertragsverhältnisses, aus welchem er Rechte durchsetzen möchte, so werden mit der Übermittlung an einen Rechtsanwalt die Daten zu einem anderen als dem ursprünglichen Zweck verarbeitet, es liegt eine Weiterverarbeitung vor. Als Rechtsgrundlage greift hier Art. 6 Abs. 4 S. 1 DSGVO i. V. m. § 24 Abs. 1 S. 2 BDSG. Danach ist die Verarbeitung personenbezogener Daten durch nichtöffentliche Stellen zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, zulässig, wenn sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen. Im Regelfall wird hier die Interessenabwägung aufgrund des Rechtsschutzinteresses zugunsten desjenigen ausfallen, der seine zivilrechtlichen Ansprüche verfolgen möchte. Selbstverständlich entbindet diese Annahme jedoch nicht von der Erforderlichkeit, eine umfassende Interessenabwägung unter Berücksichtigung aller Faktoren durchzuführen.

Möglich ist aber auch, dass der Mandant erst Daten erhebt, um diese dann dem Rechtsanwalt zur Verfügung zu stellen. Diese Erhebung kann dabei in verschiedenen Szenarien erfolgen. Die

Datenerhebung und Übermittlung erfolgt hier zur Durchsetzung von Rechtsansprüchen und fällt damit unter die Wahrung berechtigter Interessen gemäß Art. 6 Abs. 1 lit. f DSGVO, welche gegen die berechtigten Interessen der betroffenen Person abzuwägen sind. Im Regelfall überwiegt auch hier das Rechtsschutzinteresse desjenigen, der seinen Rechtsanspruch durchsetzen möchte, gegenüber den Interessen der betroffenen Person.

In diesem Rahmen ist es einem Verantwortlichen gestattet, diejenigen personenbezogenen Daten zu verarbeiten, welche zur gerichtlichen oder außergerichtlichen Anspruchsverfolgung notwendig sind. Eine vorherige Einwilligung der von der Datenverarbeitung betroffenen Person ist hierfür nicht erforderlich.

Gemäß Art. 9 Abs. 2 lit. f DSGVO ist darüber hinaus auch die Verarbeitung sensibler Datenkategorien, wie etwa Gesundheitsdaten, möglich, sofern diese Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

4.17.3 Gewährleistung effektiven Rechtsschutzes

Der Grund für diese weitreichenden Verarbeitungsmöglichkeiten liegt in der Gewährleistung eines effektiven Rechtsschutzes. Durch das Datenschutzrecht soll der Verantwortliche nicht daran gehindert werden, seine rechtlichen Ansprüche gegen den Betroffenen durchzusetzen, auch wenn dies eine Verarbeitung – auch sensibler – Daten des Betroffenen erfordert.

Aufsichtsbehördliche Maßnahmen sind unserer Behörde dabei nur bezüglich solcher Datenverarbeitungen möglich, welche in evidenter Weise nicht zur Anspruchsdurchsetzung erforderlich sind. Im Übrigen ist aufgrund der vorangegangenen Erläuterungen eine Datenübermittlung an Rechtsanwälte grundsätzlich nicht zu beanstanden.

Fazit/ Empfehlung:

Im Rahmen eines Mandatsverhältnisses ist die Übermittlung personenbezogener Daten an einen Rechtsanwalt zur Durchsetzung von Rechtsansprüchen im Regelfall datenschutzrechtlich legitimiert.

4.18 Bonitätsauskünfte

Bonitätsauskünfte sollen Prognoseentscheidungen hinsichtlich der Kreditwürdigkeit potenzieller Vertragspartner ermöglichen.

Nach Maßgabe von Art. 6 Abs. 1 lit. f DSGVO sind Bonitätsabfragen nur zulässig, soweit sie zur Wahrung der berechtigten Interessen des abfragenden Unternehmens erforderlich sind und keine überwiegenden schutzwürdigen Interessen der betroffenen Person der Datenverarbeitung entgegenstehen. Ein berechtigtes Interesse im Sinne der Vorschrift liegt regelmäßig dann vor, wenn ein Unternehmen Kredite gewährt oder ein sonstiges finanzielles Ausfallrisiko (Rechnungskauf, Ratenkauf etc.) für selbiges gegeben ist. Um das Risiko eines möglichen Zahlungsausfalls einschätzen zu können, liegt es in seinem Interesse, die Bonität eines potentiellen Vertragspartners vor Vertragsschluss zu prüfen. Liegen zu diesem Informationen über negatives Zahlungsverhalten vor (bspw. nicht bezahlte Rechnungen), kann sich aus Sicht eines Unternehmens die Annahme rechtfertigen, dass der Betroffene auch seinen künftigen finanziellen Verpflichtungen nicht bzw. nur teilweise nachkommen wird. Zur Minimierung des Ausfallrisikos können solchen Personen eben nur bestimmte Zahlungsmethoden wie bspw. Vorkasse angeboten werden.

Im aktuellen Berichtszeitraum wurden wir auf eine Reihe unzulässiger Bonitätsabfragen aufmerksam gemacht. Die Anlässe für derartige Abfragen stellten sich dabei als sehr heterogen dar und reichten von unternehmensfremden Interessen, wie beispielsweise das aus Neugier veranlasste Ausspähen der finanziellen Situation einer betroffenen Person, bis hin zur eklatanten

Fehleinschätzung der datenschutzrechtlichen Voraussetzungen für die Durchführung einer Bonitätsabfrage.

In einem konkreten Fall holte ein Unternehmen über sämtliche Personen, mit denen es ein Erstberatungsgespräch für die Vorstellung seines Leistungsspektrums im Rahmen einer telefonischen Werbeansprache vereinbart hatte, Bonitätsauskünfte ein. Das Unternehmen selbst argumentierte, dass dies eine bedarfsgerechte Steuerung des Leistungsangebots ermögliche. Die Datenverarbeitung sei daher auf der Grundlage von Art. 6 Abs. 1 lit. f DSGVO zulässig erfolgt.

Diese Auffassung überzeugte jedoch nicht. Auch wenn in dem kommunizierten Zweck grundsätzlich ein berechtigtes Interesse im Sinne der Vorschrift anzuerkennen war, bestanden bereits Zweifel daran, ob die Bonitätsprüfung zur Steuerung des Leistungsangebots überhaupt erforderlich war. Da zum Zeitpunkt der Einholung der Bonitätsauskunft noch nicht absehbar war, ob die betroffenen Personen mit dem Unternehmen überhaupt in ein vertragliches Verhältnis eintreten würden, war insoweit von einem Überwiegen der schutzwürdigen Interessen der betroffenen Personen gegenüber dem Verarbeitungsinteresse des Unternehmens auszugehen. Da das Unternehmen seinen Informationspflichten gemäß Art. 13 DSGVO nicht nachgekommen war und die betroffenen Personen somit nicht darüber informiert wurden, dass eine Bonitätsprüfung im Vorfeld des Beratungsgesprächs erfolgen würde, war unter Berücksichtigung von Erwägungsgrund 47 der DSGVO eine solche Datenverarbeitung für die betroffenen Personen zu diesem Zeitpunkt auch nicht erwartbar.

Aus Sicht unserer Behörde kann die Einholung von Bonitätsauskünften zu dem vom Unternehmen kommunizierten Zweck allenfalls mit ausdrücklicher Einwilligung der betroffenen Personen unter Gewährleistung der gesetzlichen Transparenzpflichten zulässig sein. Aufgrund dieses Hinweises hat das Unternehmen seine Praxis entsprechend angepasst.

Betroffene können nach Art. 15 DSGVO jederzeit gegenüber Auskunfteien Informationen darüber verlangen, welche Stellen über ihre Person eine Bonitätsabfrage getätigt haben. Erfahrungsgemäß wird von diesem Recht immer häufiger Gebrauch gemacht, weshalb Unternehmen nicht darauf vertrauen sollten, dass potenziell unzulässige Bonitätsabfragen von betroffenen Personen nicht wahrgenommen würden.

Verantwortliche müssen sich mithin darüber bewusst sein, dass unzulässige Bonitätsabfragen sanktioniert werden können.

Fazit/ Empfehlung:

Zur Minimierung des finanziellen Ausfallrisikos (bei Ratenkauf, Kreditgeschäften u. ä.) können Bonitätsabfragen auf der Grundlage von Art. 6 Abs. 1 lit. f DSGVO vor dem unmittelbarem Vertragsschluss zulässig sein. Betroffene Personen sind dabei transparent im Sinne des Art. 13 DSGVO über die sie betreffende Datenverarbeitung zu informieren.

4.19 Die Bedeutung transparenter Auskünfte durch Auskunfteien

Von Auskunfteien erteilte Auskünfte führten im Berichtszeitraum vermehrt zu Beschwerden. Die Beschwerdeführer hatten gegenüber Auskunfteien Auskünfte nach Art. 15 DSGVO eingefordert. In einem konkreten Beschwerdeverfahren wurden unter Herkunft bzw. Empfänger der Daten die Worte „Wirtschaftsteilnehmer", „angeschlossene Vertragspartner" oder „Behörden" pauschal angeführt.

Nach Art. 15 DSGVO haben Betroffene gegenüber einer für die Datenverarbeitung verantwortlichen Stelle das unentgeltliche Recht auf Auskunft über dort gespeicherte personenbezogene Daten. Der Umfang des Auskunftsrechts ergibt sich unmittelbar aus Art. 15 Abs. 1 DSGVO. So hat die betroffene Person einerseits einen Rechtsanspruch auf Auskunft darüber, ob überhaupt

personenbezogene Daten durch den Verantwortlichen verarbeitet werden. Soweit keine personenbezogenen Daten verarbeitet werden, ist eine Negativanzeige durch die verantwortliche Stelle erforderlich. Werden personenbezogene Daten jedoch verarbeitet, ist der betroffenen Person konkret Auskunft darüber zu erteilen, welche personenbezogenen Daten von der verantwortlichen Stelle verarbeitet werden (z. B. Vor- und Familienname, Anschrift, Geburtsdatum, Beruf etc.). Darüber hinaus erstreckt sich die Datenauskunft auf eine Reihe weiterer Angaben, die in der Vorschrift stichpunktartig aufgelistet werden; dies sind Informationen über die Verarbeitungszwecke, die Kategorien personenbezogener Daten, die verarbeitet werden, die Empfänger bzw. Kategorien von Empfängern, die geplante Speicherdauer, die Betroffenenrechte, die Herkunft der Daten und das Bestehen einer automatisierten Entscheidungsfindung.

Dem Auskunftsanspruch kommt insoweit eine gewichtige datenschutzrechtliche Bedeutung zu, als dass er der betroffenen Person überhaupt erst eine Überprüfung ermöglicht, ob die sie betreffende Datenverarbeitung im Einklang mit der DSGVO steht. Art. 15 DSGVO verpflichtet die verantwortliche Stelle dabei zu größtmöglicher Transparenz bei der antragsbedingten Auskunftserteilung, wobei grundsätzlich die vorhandenen Informationen zur Verfügung zu stellen sind.

Nach dem Wortlaut der Verordnung hat der Verantwortliche der antragstellenden Person auf Verlangen insbesondere auch die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, zu beauskunften. Durch das *„oder"* könnte der Eindruck entstehen, dass es letztlich der Entscheidung des Verantwortlichen obliegen würde, ob er Auskünfte über die konkreten Empfänger oder lediglich allgemein über (potentielle) Kategorien von Empfängern mitteilt. Dieses Verständnis würde der zentralen Bedeutung des Auskunftsrechts jedoch nicht gerecht werden, soweit es der betroffenen Person gerade erst ermöglicht, Unrichtigkeiten oder potenziell

datenschutzwidrige Verarbeitungen erkennen zu können. Pauschale Angaben von Kategorien werden diesem Anspruch nicht gerecht, soweit eine Datenübermittlung bereits stattgefunden hat.

Es ist insofern ein dahingehendes echtes Wahlrecht zwischen den beiden Alternativen abzulehnen. Nur für den Fall, dass konkrete Empfänger mit Blick für die Zukunft noch nicht feststehen, beschränkt sich der Auskunftsanspruch auf Empfängerkategorien. Demzufolge sind Informationen über solche Empfänger, die über einen Betroffenen eine Bonitätsabfrage eingeholt haben, im Rahmen eines geltend gemachten Auskunftsanspruchs unmittelbar und nicht erst auf weitere Nachfrage zu erteilen. Diese Argumentation wird ebenso durch Erwägungsgrund 63 der DSGVO gestützt, der die Empfänger und nicht lediglich die Kategorien der Empfänger in Bezug nimmt.

Die behördliche Aufsichtspraxis zeigt, dass unzulässige Bonitätsabfragen oftmals erst auf ein gestelltes Auskunftsersuchen hin erkannt werden. Da in derartigen Fällen der betroffenen Person die konkreten Datenempfänger, mithin abfragende Unternehmen, mitgeteilt wurden, konnte diese prüfen, ob mit dem abfragenden Unternehmen eine Geschäftsbeziehung bestand bzw. sich anbahnte und damit ein berechtigtes Interesse an der Datenverarbeitung im Sinne des Art. 6 Abs. 1 lit. f DSGVO bestanden haben könnte. Wäre der betroffenen Person in gleichgelagerten Fällen lediglich mitgeteilt worden, dass Bonitätsauskünfte grundsätzlich an Wirtschaftsteilnehmer übermittelt wurden bzw. werden, wären diese Datenschutzverstöße nicht erkannt worden. Dem Auskunftsanspruch kommt demnach gerade im Bereich von Bonitätsauskünften eine zentrale Bedeutung zu.

Darüber hinaus hat die verantwortliche Stelle der antragstellenden Person nach Art. 15 Abs. 1 lit. h DSGVO alle verfügbaren Informationen über die Herkunft der Daten mitzuteilen, wenn die personenbezogenen Daten nicht bei der betroffenen Person

erhoben wurden. Sinn und Zweck der Regelung ist u. a., es der betroffenen Person zu ermöglichen, gegen die Stellen vorzugehen, welche initial potenziell unrichtige Daten möglicherweise datenschutzwidrig verarbeitet haben. Um mögliche Korrektur- oder Löschungsansprüche überhaupt erst geltend machen zu können, muss der betroffenen Person die Identität der Quelle bekannt sein. Hierfür spricht auch der Wortlaut der Regelung, der von *allen verfügbaren Informationen* ausgeht.

Die im Zusammenhang mit einer Beschwerde von einer Auskunftei erläuterte Geschäftspraxis, ausführliche Informationen regelmäßig erst auf konkretisierende Nachfrage der betroffenen Personen nachzureichen, genügte den gesetzlichen Erfordernissen demnach gerade nicht. Im Rahmen des Verwaltungsverfahrens konnte mit der betreffenden Auskunftei ein rechtsgültiges Verfahren abgestimmt werden.

Fazit/ Empfehlung:

Der betroffenen Person sind nach Art. 15 DSGVO mitunter alle verfügbaren Informationen über die Herkunft ihrer Daten zu erteilen. Soweit eine Datenübermittlung stattgefunden hat, sind sämtliche Empfänger von Bonitätsdaten mitzuteilen. Allgemeine Verweise sind demgegenüber nicht ausreichend.

4.20 Verarbeitung von Positivdaten durch Auskunfteien

Bereits im 29. Tätigkeitsbericht wurde über das Thema *Branchenpool Energieversorger* (Ziffer 3.16) berichtet. Das in den überregionalen Medien kritisierte Vorhaben der großen Wirtschaftsauskunfteien für den Bereich der Energieversorger eine Datenbank aufzubauen, in der sog. Positivdaten wie die Dauer eines Energieversorgungsvertrags, der Kündigungszeitpunkt und weitere Daten gespeichert werden sollten, stieß bei den Datenschutzbehörden des Bundes und der Länder auf erhebliche

Kritik. Hierdurch wäre ermöglicht worden, vertragstreuen Kunden günstige Neukundenrabatte zu verwehren, allein weil aufgrund der Historie zu der betroffenen Person ein wiederholter Wechsel des Energieversorgers mit dem Ziel, günstige, quersubventionierte Tarife abschließen zu können (sog. *Bonus-Hopper*), ersichtlich wird. Der fachliche Diskurs mündete schließlich in dem Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) „Energieversorgerpool darf nicht zu gläsernen Verbraucher*innen führen".[26] Darin wird betont, dass Datenerhebungen zu störungsfreien Verträgen mit Ausnahme des Kreditwesensbereichs rechtswidrig sind. Selbst in der Annahme eines berechtigten Interesses im Sinne des Art. 6 Abs. 1 lit. f DSGVO würden in diesem Zusammenhang die schutzwürdigen Interessen der Verbraucher, selbst über die sie betreffende Datenverarbeitung entscheiden zu können, höher zu gewichten sein als die wirtschaftlichen Interessen der Auskunfteien und der Energieversorger. Letztlich wurde das Vorhaben auch bedingt durch den breiten Gegenwind, der den Wirtschaftsauskunfteien entgegenschlug, aufgegeben.

Daneben bestand auch Klärungsbedarf hinsichtlich der Frage, ob die Verarbeitung von Positivdaten aus Verträgen über Mobilfunkdienste und Dauerhandelskonten durch Auskunfteien zulässig erfolgen kann. Dabei handelt es sich um solche Verträge, die aufgrund von Vorausleistungsverpflichtungen oder Finanzierungselementen mit einem kreditorischen Risiko verbunden sein können. Dies ist im Telekommunikationsbereich dann der Fall, wenn ein Kunde das Endgerät über die Vertragslaufzeit finanziert. Dauerhandelskonten fungieren ähnlich wie Kreditkarten, bei denen ein Einkauf nicht unmittelbar, sondern periodisch (z. B. quartalsmäßig) abgerechnet wird. Die Auskunfteien argumentierten hierbei, dass bei steigender Anzahl abgeschlossener Verträge die Ausfallwahrscheinlichkeit zunehme.

[26] Elektronisch abrufbar unter: https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/datenschutz/dsk_beschluesse/2021/Beschluss-Energieversorgerpool_final.pdf

Die DSK bestätigt für die Verarbeitung von Positivdaten zu dem Zweck, die Qualität von Bonitätsbewertungen hierdurch zu verbessern und die beteiligten Wirtschaftsakteure potenziell vor kreditorischen Risiken zu schützen, grundsätzlich ein berechtigtes Interesse. Allerdings kommt den schutzwürdigen Interessen der betroffenen Personen, selbst über die sie betreffende Positivdatenverarbeitung bestimmen zu können, auch in diesen Bereichen eine gewichtige Bedeutung zu, zumal sich die Betroffenen vollkommen vertragskonform verhalten haben. Im Rahmen der vorzunehmenden Abwägung konnten demgegenüber keine besonderen Umstände wie im Bereich des Kreditwesens[27] festgestellt werden, die ein überwiegendes Interesse der Verantwortlichen oder Dritter erkennen ließen.

Eine gegen den Willen der betroffenen Person erfolgende Verarbeitung von Positivdaten genügt demnach den Voraussetzungen von Art. 6 Abs. 1 lit. f DSGVO in den genannten Bereichen nicht.[28]

Fazit/ Empfehlung:

Mit Ausnahme des Kreditbereichs ist die Verarbeitung von Positivdaten durch Auskunfteien grundsätzlich nur mit ausdrücklicher Einwilligung der betroffenen Personen zulässig.

[27] Nach § 18a Abs. 1 Kreditwesengesetz (KWG) prüfen Kreditinstitute vor Abschluss eines Verbraucherdarlehensvertrages die Kreditwürdigkeit des Darlehensnehmers.

[28] vgl. Ergebnisse der 3. Zwischenkonferenz der DSK vom 22. September 2021, TOP 7, elektronisch abrufbar unter: https://www.datenschutzkonferenz-online.de/media/pr/20210922_protokoll_zwischenkonferenz.pdf

4.21 Kreditwirtschaft

4.21.1 Allgemeines

Lediglich einige wenige Kreditinstitute haben ihre Hauptniederlassung im Saarland, so dass sich der Fokus der aufsichtsbehördlichen Tätigkeit im Wesentlichen auf die regional ansässigen Sparkassen- und Volksbankenniederlassungen richtet.

Neben Beschwerden, Hinweisen und Anfragen sind regelmäßig Meldungen von Datenschutzverletzungen im Sinne des Art. 33 DSGVO durch die Kreditinstitute an unsere Dienststelle adressiert worden. Darüber hinaus versteht sich unsere Aufsichtsbehörde auch als Ansprechpartnerin für datenschutzrechtliche Fragen der Verantwortlichen und befindet sich in einem regelmäßigen Austausch mit den für Datenschutz zuständigen Vertreterinnen und Vertretern der hiesigen Sparkassen.

4.21.2 Beschwerden

Im Berichtszeitraum waren im Rahmen zweier Beschwerden, die sich gegen unterschiedliche Kreditinstitute richteten, das Protokollierungs- und Berechtigungskonzept der betroffenen Kreditinstitute Gegenstand einer Untersuchung. In beiden Fällen erhoben die betroffenen Personen den Vorwurf, es sei durch einen Mitarbeiter der Bank unberechtigt und zu privaten Zwecken Einsicht in das Konto der jeweiligen Beschwerdeführer genommen worden. Im Rahmen der Verfahren konnte ein dahingehender Verstoß in beiden Fällen nicht festgestellt werden, wobei allerdings eine Aufklärung der Vorwürfe auch mangels Protokollierung der Kontenzugriffe nicht möglich war. Zwar wurde auf Nachfrage der Aufsichtsbehörde ein entsprechendes Berechtigungs- und Zugriffskonzept durch die verantwortlichen Kreditinstitute dargelegt, welches auch durch eine Zugriffsprotokollierung flankiert wird. Jedoch stellte sich heraus, dass die in den beiden Verfahren betroffenen Kreditinstitute die Protokolldaten lediglich für eine Dauer von drei bzw. fünf Monaten aufbewahren. Dies scheint mit Blick auf die diesbezügliche Einschätzung unter den Aufsichtsbehörden mit den Vertretern der Kreditwirt-

schaft sowie der BaFin im Arbeitskreis Kreditwirtschaft der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ein zu kurzer Zeitraum. Indessen wurde seitens eines betroffenen Kreditinstitutes die Auffassung vertreten, der Aufbewahrungszeitraum von drei Monaten sei mit Blick auf die geringe Anzahl entsprechender Anfragen und den zugleich hohen Kostenaufwand im Falle einer Ausweitung der Speicherdauer sowie mit Blick auf den Grundsatz der Datenminimierung und der Speicherbegrenzung sachgerecht und verhältnismäßig. Die betroffenen Kreditinstitute wurden darauf hingewiesen, dass aus Sicht der hiesigen Aufsichtsbehörde ein Zeitraum von mindestens sechs Monaten erforderlich sein dürfte, um eine ausreichende Kontrolle gewährleisten und ggf. notwendige Aufklärungen vornehmen zu können.

Die Thematik wird mit Blick auf die länderübergreifende Relevanz in dem nächsten Treffen der Aufsichtsbehörden im Rahmen des zuständigen Arbeitskreises erneut erörtert und hieran anschließend geprüft, ob weitere Maßnahmen in den beiden betreffenden Verfahren zu ergreifen sind.

4.21.3 Meldungen von Datenschutzverletzungen

Im Berichtszeitraum ist eine erhebliche Anzahl von gemeldeten Datenschutzverletzungen nach Art. 33 DSGVO auf Kreditinstitute zurückzuführen. Dabei handelt es sich in aller Regel um Fehlversendungen von Kontoauszügen oder anderen vermögensrelevanten Dokumenten. Die Kreditinstitute werden in diesem Zusammenhang in Einzelfällen zur Darlegung ihrer allgemeinen oder in Folge des Vorfalls getroffenen technisch-organisatorischen Maßnahmen nach Art. 24 und Art. 32 DSGVO zum Schutz personenbezogener Daten und zur Gewährleistung der Sicherheit der Verarbeitung aufgefordert. Den gemeldeten Datenschutzverletzungen lagen dabei aus hiesiger Sicht regelmäßig Unachtsamkeiten von Mitarbeiterinnen und Mitarbeitern zu Grunde, ohne dass bislang eine mangelnde Umsetzung tech-

nisch-organisatorischer Maßnahmen im Rahmen des Datenschutz-Compliance-Systems der Verantwortlichen erkennbar war.

4.21.4 Offene Auslegungsfragen

Die Aufsichtsbehörden befinden sich in einem gegenseitigen, regelmäßigen Austausch, um länderübergreifende Entwicklungen und datenschutzrechtliche Fragestellungen im Bereich der Kreditwirtschaft zu erörtern.

In diesem Rahmen wurden im Berichtszeitraum erneut Fragestellungen im Zusammenhang mit der zweiten Zahlungsdiensterichtlinie (Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 23. Dezember 2015 – PSD2[29]) behandelt. Die Richtlinie enthält Vorschriften zur Modernisierung des Rechtsrahmens für den europäischen Zahlungsverkehr und normiert u.a. Regeln für die Nutzung von Zahlungsauslösediensten für das Initiieren von Überweisungen im Onlinebanking oder von Kontoinformationsdiensten zur Abfrage und Auswertung von Kontodaten. Zum Zusammenspiel der zweiten Zahlungsdiensterichtlinie und der DSGVO hat der Europäische Datenschutzausschuss (EDSA) die Leitlinien 06/2020[30] veröffentlicht, die wichtige Ausführungen und Klarstellungen enthalten.

Nach wie vor gibt es jedoch offene Anwendungs- und Auslegungsfragen in diesem Zusammenhang. So stellt sich bspw. die Frage, welche Maßnahmen von welchem Verantwortlichen zu treffen sind, um mit Blick auf den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO sicherzustellen, dass ein Zugang nur hinsichtlich der für die jeweilige Zahlungsdienstleistung erforderlichen personenbezogen Daten erfolgt.

---

[29] Elektronisch abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32015L2366

[30] Elektronisch abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062020-interplay-second-payment-services_de

Ebenfalls mit Blick auf den Grundsatz der Datenminimierung ist aufgrund einer Änderung des § 8 Abs. 2 Geldwäschegesetz (GwG) zum 1.1.2020 fraglich, ob nunmehr die Unkenntlichmachung nicht erforderlicher Angaben bei der Anfertigung von Kopien von Ausweisdokumenten zu Identifikationszwecken geboten ist[31]. Dies lässt sich mit Blick auf die Streichung des Wortes „vollständig" aus der neuen Fassung des § 8 Abs. 2 Satz 2 GwG, wonach nun lediglich Kopien und nicht wie bis dahin „vollständige" Kopien anzufertigen sind, durchaus vertreten.

Gleichfalls nicht abschließend geklärt ist die Frage nach Inhalt und Reichweite des Auskunftsanspruchs nach Art. 15 Abs. 3 DSGVO und ob hiernach ein Anspruch auf unentgeltliche Überlassung einer Kopie der Kontoauszüge besteht.

Nach dem Wortlaut des Art. 15 Abs. 3 DSGVO ist jedenfalls keine bestimmte Form und damit keine strukturierte Aufbereitung in Form eines Kontoauszugs geschuldet, sondern lediglich eine Zurverfügungstellung der Daten, wie sie dem Verantwortlichen vorliegen bzw. bei elektronischer Beantragung in einem gängigen elektronischen Format.

In diesem Zusammenhang ist zu berücksichtigen, dass es eine Vielzahl unterschiedlicher Auffassungen und Rechtsprechung zu Inhalt, Reichweite und Grenzen des Art. 15 Abs. 3 DSGVO gibt. So wird teilweise die Konkretisierung und Bejahung eines nach Art. 15 Abs. 1 DSGVO umfassten Zwecks gefordert, welcher in der Kontrollfunktion im Hinblick auf die Richtigkeit und Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten zu sehen ist.

Während ein Teil der Rechtsprechung eine dahingehende einschränkende, enge Auslegung vertritt, wird von anderen Teilen der Rechtsprechung die Grenze des Auskunftsrechts allein in

[31] Vgl. 29. Tätigkeitsbericht 2020, Kapitel 3.18.4, Seite 103ff, elektronisch abrufbar unter: https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/tberichte/tb29_DS_2020.pdf

der Rechtsmissbräuchlichkeit gesehen, welche nicht bereits aufgrund der Verfolgung eines über die Kontrollfunktion des Art. 15 Abs. 1 DSGVO hinausgehenden Zwecks zu bejahen sei. Mithin könne ein Entgelt nicht mit der Begründung verlangt werden, dass bereits einmal Kontoauszüge bspw. im Rahmen des Online-Bankings zur Verfügung gestellt wurden, da dies nicht in Ansehung des datenschutzrechtlichen Auskunftsanspruchs, sondern in Erfüllung der vertraglichen Verpflichtungen erfolgt sei.

Eine höchstrichterliche Klärung dieser und weiterer umstrittener Fragen hinsichtlich der Art und des Umfangs von Auskunftsansprüchen steht indessen nach wie vor aus und wäre mit Blick auf die kontroversen Diskussionen in diesem Zusammenhang und die sich hieraus ergebende Rechtsunsicherheiten zweifellos zu begrüßen.

4.22 Direktmarketing

Unternehmen, die im Zusammenhang mit Direktmarketingmaßnahmen personenbezogene Daten verarbeiten, sollten ein besonderes Augenmerk auf die Operationalisierung von Geschäftsprozessen bei der Geltendmachung von Auskunftsersuchen nach Art. 15 DSGVO, Widersprüchen nach Art. 21 Abs. 2 DSGVO und Löschansprüchen nach Art. 17 DSGVO legen. Die Mehrzahl der diesbezüglich im Berichtszeitraum an hiesige Dienststelle gerichteten Beschwerden hatte nicht die datenschutzrechtliche Zulässigkeit der Datenverarbeitung für Zwecke des Direktmarketing zum Gegenstand, sondern die Nichtbeachtung eines geltend gemachten Betroffenenrechts. Im Rahmen dieser Verwaltungsverfahren ist dann jedoch oftmals auch die datenschutzrechtliche Unzulässigkeit der jeweiligen Direktmarketingmaßnahme zu Tage getreten, die sodann von Amts wegen zum weiteren Gegenstand des Verfahrens wurde.

Da postalische Werbebotschaften im Beschwerdevolumen nahezu kaum noch vertreten sind und die Mehrzahl der Werbebotschaften per E-Mail oder telefonisch abgesetzt werden, ist die datenschutzrechtliche Zulässigkeit der Datenverarbeitung

im Wesentlichen an den wettbewerbsrechtlichen Vorgaben für den jeweils genutzten Werbekanal im Bereich Business-to-Business (B2B) oder Business-to-Consumer (B2C) zu messen.

4.22.1 B2C

Mit Beschluss vom 16. Februar 2021 – 2 A 355/19 hat das Oberverwaltungsgericht des Saarlandes (OVG) einen Antrag auf Zulassung der Berufung abgewiesen und damit letztinstanzlich die datenschutzrechtliche Unzulässigkeit einer telefonischen Direktmarketingmaßnahme bestätigt. Die dem Verfahren zugrundeliegende Klage[32] eines Versicherungsunternehmens richtete sich gegen die durch hiesige Behörde erfolgte Untersagung einer im Zusammenhang mit telefonischen Marketingmaßnahmen erfolgenden Datenverarbeitung. In der Entscheidung schließt sich das Gericht dem in dem Urteil des Verwaltungsgerichts des Saarlandes vom 29. Oktober 2019 – 1 K 732/19 dargestellten Verhältnis zwischen Wettbewerbs- und Datenschutzrecht im Zusammenhang mit an Privatpersonen adressierte Direktmarketingmaßnahmen an und konstatiert, dass ein nach Art. 7 Gesetz gegen den unlauteren Wettbewerb (UWG) vorgegebener Einwilligungsvorbehalt für einen spezifischen Werbekanal auch datenschutzrechtlich das nachweisbare Vorliegen einer Einwilligung nach Art. 6 Abs. 1 lit. a i. V. m. Art. 4 Nr. 11 und 7 Abs. 1 DSGVO der betroffenen Person bedingt. Ein Abweichen von dem Einwilligungsvorbehalt unter Rückgriff auf die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO scheidet im Hinblick auf die der DSGVO als spezifisches Recht vorgehenden Vorgaben in Art. 13 Abs. 3 Richtlinie 2002/58/EG und deren mitgliedstaatlicher Umsetzung in § 7 UWG daher aus. Lediglich ergänzend betont das Gericht, dass eine wettbewerbswidrige Maßnahme, die mithin kein von der Rechtsordnung gebilligtes Interesse darstellt, nicht als berechtigt im Sinne des Art. 6 Abs. 1 lit. f DSGVO qualifiziert werden könne.

[32] Vgl. 27. Tätigkeitbericht 2017/2018, Kapitel 14.1, S. 129 ff.; 28. Tätigkeitbericht 2019, Kapitel 4.20., S. 166 ff.

4.22.2 B2B

Hinsichtlich der datenschutzrechtlichen Zulässigkeit von an Zahnärzte adressierte Werbeanrufe nach der bis zum 24. Mai 2018 geltenden Rechtslage und der diesbezüglichen Entscheidung des Verwaltungsgerichts des Saarlandes vom 9. März 2018 – 1 K 257/17 wurde bereits im 27. Tätigkeitsbericht[33] ausführlich berichtet.

Das Gericht hat die gegen eine Untersagungsverfügung hiesiger Dienststelle gerichtete Klage des Werbetreibenden abgewiesen und sich der Einordnung der Direktmarketingmaßnahme als wettbewerbswidrig und damit als datenschutzrechtlich unzulässig angeschlossen. Die klägerseitig vorgetragene Ansicht, dass die Werbeansprache im B2B-Bereich nach der ab dem 25. Mai 2018 wirksamen DSGVO zulässig wäre, überzeugte die Kammer nicht, so dass die Berufung nicht zugelassen wurde.

Das OVG hat den diesbezüglichen Antrag auf Zulassung der Berufung mit Beschluss vom 10. September 2019 – 2 A 174/18 zurückgewiesen. Unter Berücksichtigung der Rechtsprechung des Bundesverwaltungsgerichts[34] entschied das OVG, dass allein auf die Rechtslage zum Zeitpunkt der letzten behördlichen Entscheidung abzustellen war und nachträgliche Rechtsänderungen nicht zu berücksichtigen waren. Ferner legte das Gericht dem Kläger im Ablehnungsbeschluss nahe, hiesige Dienststelle über die Vorschriften der §§ 49 ff. Saarländisches Verwaltungsverfahrensgesetz erneut mit einer dahingehenden Prüfung, ob an der nach der bis zum 24. Mai 2018 geltenden Rechtslage ergangenen Untersagungsverfügung nach Geltungseintritt der DSGVO festgehalten wird, zu befassen. Eigene Ausführungen zur datenschutzrechtlichen Zulässigkeit der Direktmarketingmaßnahme nach der DSGVO im B2B-Bereich hat das OVG in diesem Zusammenhang nicht getroffen.

[33] Vgl. 27. Tätigkeitbericht 2017/2018, Kapitel 14.3., S. 132 ff.

[34] Urteil vom 27. März 2019 – 6 C 2/18.

Der diesbezügliche Antrag auf erneute Prüfung der Untersagungsverfügung wurde durch Bescheid hiesiger Behörde zurückgewiesen. Der Ablehnungsentscheidung lag dabei zugrunde, dass eine Änderung der Sach- und Rechtslage zugunsten der Antragstellerin nicht eingetreten war und die angefochtene Untersagungsverfügung nunmehr auf Grundlage des Art. 58 Abs. 2 lit. f DSGVO ergehen würde.

Mangels Vorliegen einer mutmaßlichen Einwilligung nach § 7 Abs. 2 Nr. 2 2. Alt. UWG war für die datenschutzrechtliche Bewertung eine im verwaltungsgerichtlichen Verfahren bestätigte Wettbewerbswidrigkeit der Direktmarketingmaßnahme zugrunde zu legen. Im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO, die das datenschutzrechtliche Pendant zur mutmaßlichen Einwilligung im Sinne des § 7 UWG darstellt, konnte somit kein berechtigtes Interesse unterstellt[35] und damit auch keine datenschutzrechtliche Zulässigkeit der telefonischen Marketingmaßnahme angenommen werden.

Mit Urteil vom 15. Dezember 2021 – 5 K 461/20 hat das Verwaltungsgericht des Saarlandes die gegen die hiesige Ablehnungsentscheidung gerichtete Klage abgewiesen und sich im Wesentlichen den im Verwaltungsakt angeführten Gründen angeschlossen. Eine Berufung gegen das Urteil wurde allerdings zugelassen.

4.23 Wohnungswirtschaft

My home is my castle – die eigenen vier Wände sind nicht nur in sprichwörtlicher, sondern auch in rechtlicher Hinsicht ein geschützter Kernbereich der privaten Lebensführung. Während für die individuelle Lebensgestaltung im Schutzbereich der Wohnung weitestgehend die Regeln der Bewohnerinnen und Bewohner gelten, bedingt das Mieten oder der Erwerb einer Woh-

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

nung den Eintritt in ein komplexes Gefüge aus miet- bzw. eigentumsrechtlichen Rechten und Pflichten sowie aus Interessen und Verantwortlichkeiten verschiedener Akteure.

Wohnungsrechtliche Rahmenbedingungen und deren datenschutzrechtliche Implikationen stellen private Mieter, Vermieter oder Wohnungseigentümer sowie gewerbliche Stellen, wie etwa Verwalter im Sinne des Wohnungseigentumsgesetzes und Wohnungsunternehmen, regelmäßig vor Herausforderungen und sind oftmals Ausgangspunkt für erhebliche Konflikte zwischen den Beteiligten. Vor diesem Hintergrund wurde im Berichtszeitraum eine beträchtliche Anzahl an Beschwerden, Anfragen und Hinweisen mit einem wohnungswirtschaftlichen Sachzusammenhang an hiesige Dienststelle adressiert.

4.23.1 Weitergabe von Kontaktdaten an Handwerksbetriebe und Dienstleister

Die Weitergabe von Kontaktinformationen von Wohnungseigentümern und Mietern im Zusammenhang mit Schadensmeldungen und Reparaturaufträgen an Handwerksbetriebe oder Dienstleister stellt angesichts der vorliegenden Äußerungen der Datenschutzaufsichtsbehörden im Beschwerdevolumen wohl eine häufig vorkommende Fallgestaltung dar.[36]

In diesbezüglichen Veröffentlichungen wird als Legitimationsgrundlage für die Datenweitergabe entweder auf die Einwilligung des betroffenen Mieters nach Art. 4 Nr. 11 in Verbindung mit Art. 6 Abs. 1 lit. a DSGVO oder das berechtigte Interesse des Vermieters im Sinne des Art. 6 Abs. 1 lit. f DSGVO abgestellt. Soweit die Übermittlung mittelbar auf den Mietvertrag gestützt und somit Art. 6 Abs. 1 lit. b DSGVO als Legitimationsgrundlage herangezogen wird, ist diese Auffassung zumindest streitbar und greift hiesigen Erachtens überwiegend nicht.

[36] TLfDI, 3. Tätigkeitsbericht zum Datenschutz nach der DS-GVO 2020, Kapitel 4.16; LfDI BW, 35. Tätigkeitsbericht 2019 – 9. Arbeitswelt, S. 100/101, BayLDA, 10. Tätigkeitsbericht 2020, Kapitel14.4.

Für die im Berichtszeitraum in diesem Zusammenhang eingegangen Beschwerden konnte die Weitergabe von Kontaktinformationen nicht über die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO beziehungsweise die Zweckänderung im Sinne des Art. 6 Abs. 4 DSGVO legitimiert werden. Nahezu allen Beschwerden lag dabei zugrunde, dass die mitgeteilten Ursachen von Beeinträchtigungen und Schäden außerhalb der Einflussmöglichkeit der betroffenen Mieter und Wohnungseigentümer lagen und im Wesentlichen den Zutritt zu Heizungsräumen oder Zugang zu technischen Anlagen erforderlich machten. Soweit die Mieter und Eigentümer den mit der Instandsetzung beauftragten Betrieben gerade keinen Zutritt zu Räumen mit technischen Anlagen verschaffen konnten, konnte eine Übermittlung der Kontaktdaten durch Vermieter oder Wohnungsverwalter an die beauftragten Firmen bereits nicht als zur Erreichung des verfolgten Zwecks der Beseitigung einer technischen Störung oder Reparatur eines Defekts geeignet qualifiziert werden. Eine Erforderlichkeit im Sinne des Art. 6 Abs. 1 lit. f DSGVO schied daher aus.

Da die jeweilige Übermittlung in diesen Fällen datenschutzrechtlich nicht legitimiert war und die Betroffenen im Übrigen nicht transparent über die Datenweitergabe informiert wurden, wurden die Verantwortlichen nach Art. 58 Abs. 2 lit. b DSGVO verwarnt.

4.23.2 Weiterleitung von E-Mails und Disclaimer

Während überwiegend Mieter und Wohnungseigentümer als Beschwerdeführer in Erscheinung treten, wandte sich ein Wohnungsverwalter an hiesige Dienststelle und monierte die seines Erachtens unzulässige Weiterleitung von E-Mails durch einen Immobilienmakler.

Der Makler, der durch eine Wohnungseigentümerin mit dem Verkauf der Immobilie betraut wurde, stand per E-Mail in Kontakt mit dem Wohnungsverwalter, um von diesem für die Veräußerung relevante Unterlagen zu erhalten. Die E-Mails wurden für den Verwalter erkennbar durch den Makler per „CC-Feld“ an

eine ihm unbekannte E-Mailadresse weitergeleitet. Da der Verwalter in seiner E-Mail-Signatur einen Disclaimer eingefügt hatte, wonach eine Weitergabe der E-Mails von seiner erteilten Einwilligung abhängig zu machen sei, erkannte er in dem Vorgehen des Maklers eine ungerechtfertigte Offenlegung seiner personenbezogenen Daten. Neben der Beschwerde nach Art. 77 DSGVO machte der Verwalter auch einen Schadenersatzanspruch nach Art. 82 DSGVO geltend.

In der Weiterleitung der E-Mails des Maklers war jedoch keine unzulässige Offenlegung von personenbezogenen Daten zu erkennen. Der bereits im Hinblick auf die Geltendmachung eines Schadensersatzanspruchs geführten anwaltlichen Korrespondenz konnte entnommen werden, dass es sich bei dem Inhaber der E-Mail-Adresse im „CC-Feld" um den Sohn der Wohnungseigentümerin handelte, welcher diese bei der Veräußerung unterstützte und auch mit dem Makler diesbezüglich wiederholt in Kontakt stand. Für einen Dritten war die Annahme naheliegend, dass das Auftreten des Sohnes auf eine dahingehende Bevollmächtigung der Wohnungseigentümerin zurückgeht.

Die Weiterleitung der E-Mail-Korrespondenz durch den Makler konnte gestützt auf Art. 6 Abs. 1 lit. f DSGVO erfolgen, soweit es im Rahmen des Maklerauftrags ein berechtigtes Interesse des Maklers darstellt, den Sohn der Wohnungseigentümerin über Einzelheiten und den Fortgang der Veräußerung zu informieren und es aus Sicht des Maklers – als berücksichtigungsfähiges Drittinteresse – ein Anliegen des Sohnes war, darüber informiert zu werden. Auch eine besondere Schutzwürdigkeit der personenbezogenen Daten war nicht ersichtlich, da der Gehalt der beschwerdegegenständlichen E-Mail im Wesentlichen lediglich Informationen umfasste, die sich im Kontext der beruflichen Funktion als Verwalter im wohnungseigentumsrechtlichen Sinne ergeben, und im Übrigen gerade Belange der Eigentümergemeinschaft bzw. der Sondereigentümerin betrafen.

Auch unter Berücksichtigung des Disclaimers in der E-Mail-Signatur ergab sich keine Unzulässigkeit der Datenweitergabe in

Form der E-Mail-Weiterleitung.[37] Weder konnte der Verwalter die datenschutzrechtliche Legitimationsgrundlage für eine Datenverarbeitung im Vorfeld determinieren noch eignete sich der Inhalt des Disclaimers, um als (vorgreifender) Widerspruch im Sinne des Art. 21 Abs. 1 DSGVO ausgelegt werden zu können.

4.23.3 Betroffenenrechte und Schadensdaten

Eine Wohnungseigentümerin meldete einen Wasserschaden in ihrem Privatkeller der Wohnungsverwaltung. Das von dem Versicherungsunternehmen der Eigentümergemeinschaft mit der Schadensbegutachtung beauftragte Unternehmen stellte als Schadensort und -ursache einen Schmutzwasseraustritt an einem Ableitungsrohr vor dem Privatkeller fest und übersandte den Schadensbericht an die Auftrag gebende Versicherung. Besagter Bericht enthielt neben Angaben zu Schadensort und -ursache auch den Namen der Wohnungseigentümerin, soweit diese über den Privatkeller verfügte.

Da nach Ansicht der Wohnungseigentümerin der Schmutzwasseraustritt innerhalb ihres Privatkellers stattfand, machte sie mit Blick auf den im Schadensbericht genannten Schadensort und die -ursache gegenüber dem Schadensermittler einen Berichtigungsanspruch nach Art. 16 DSGVO geltend bzw. forderte diesen zur Löschung der sie betreffenden personenbezogenen Daten nach Art. 17 DSGVO aus dem ihres Erachtens fehlerhaften Schadensbericht auf. Nach Weigerung des Schadensermittlers wandte sich die Wohnungseigentümerin beschwerdeführend an hiesige Dienststelle.

Die diesbezügliche Beschwerde wurde mit der Begründung abgewiesen, dass es sich bei den Angaben zu Schadensort und -ursache bereits nicht um personenbezogene Daten handelte und keine Anhaltspunkte dafür ersichtlich waren, dass die die Beschwerdeführerin eindeutig identifizierenden Angaben im Schadensbericht in unzulässiger Weise verarbeitet wurden. Zwar gebietet sich unter Berücksichtigung der Rechtsprechung

[37] SaarlOLG, Urteil vom 13. Juni 2012 – 5 U 5/12-2.

des Europäischen Gerichtshofs (EuGH)[38] bei der Bewertung, ob eine Angabe eine Information im Sinne des Art. 4 Nr. 1 DSGVO darstellt, eine extensive Auslegung,[39] allerdings kann dies für den Schadensbericht als solchen nicht angenommen werden. Angesichts eines unmittelbar die Schadensdaten adressierenden Berichtigungsanspruchs war die Auslegung des EuGH in der Entscheidung vom 17. Juli 2014 – verbundene Rechtssachen C-141/12 und C-372/12 – zum Begriff der personenbezogenen Daten zu berücksichtigen, nach welcher für eine rechtliche Analyse, auch wenn diese eindeutig identifizierende Angaben enthält, kein Personenbezug angenommen werden kann.

Bei dem beschwerdegegenständlichen Schadensbericht handelte es sich zwar nicht um eine solche rechtliche Analyse, allerdings kann diese Einordnung grundsätzlich auch auf gutachterliche Stellungnahmen außerhalb eines juristischen Sachzusammenhangs übertragen werden.[40] Der Schadensbericht war als eigenständige, unter Heranziehung spezifischer Fachkenntnisse angefertigte Einordnung der Ursachen, Umstände und Weiterungen eines Schadensereignisses anzusehen und wurde an das Versicherungsunternehmen zur Abwicklung des Schadensfalls gesandt; unter Berücksichtigung der EuGH-Entscheidung war damit naheliegend, den Schadensbericht nicht als personenbezogenes Datum zu qualifizieren und einen datenschutzrechtlichen Berichtigungsanspruch im Hinblick auf das Ergebnis der Schadensermittlung abzulehnen.

Auch für die im Schadensbericht aufgeführten, eindeutig identifizierenden Angaben zur Beschwerdeführerin kam ein isolierter Berichtigungs- bzw. Löschanspruch nicht in Frage, da diese

[38] EuGH, Urteil vom 20. Dezember 2017 – C 434/16, Rn. 35 ff.

[39] So bspw. VGH Baden-Württemberg, Urteil vom 17. Dezember 2020 – 10 S 3000/18; VG Schwerin, Urteil vom 29. April 2021 – 1 A 1343/19 SN Rn. 36, juris.

[40] Schlussanträge der Generalanwältin Eleanor Sharpston vom 12. Dezember 2013 – verbundene Rechtssachen C-141/12 und C -372/12.

Daten durch den Schadensermittler weder inhaltlich unzutreffend noch im Rahmen der Schadensbegutachtung datenschutzrechtlich unzulässig verarbeitet wurden.

Die Beschwerdeführerin erhob gegen die Abweisung der Beschwerde Klage beim Verwaltungsgericht des Saarlandes. Eine Entscheidung steht noch aus.

4.23.4 Offenlegung der Daten von Wohnungseigentümern

Ein Wohnungsverwalter setzte ein Administrationstool ein, über das Wohnungseigentümer jeweils beschränkt auf die eigene Gemeinschaft Informationen online abrufen konnten. Aufgrund eines Fehlers eines Mitarbeiters waren Informationen einer Eigentümergemeinschaft mit Daten von Wohnungseigentümern für Mitglieder einer anderen Gemeinschaft abrufbar.

Anlässlich einer diesbezüglichen Beschwerde nach Art. 77 DSGVO wurde der Hausverwalter zur Stellungnahme aufgefordert. Dieser bat zunächst um Akteneinsicht, mit dem Ergebnis, dass der Beschwerdevortrag im Originalwortlaut in das Onlineportal unter Nennung des Namens der beschwerdeführenden Person und ergänzt mit einer Würdigung der Angelegenheit aus Sicht des Verwalters eingestellt wurde.

Auch dies wurde als Beschwerde an hiesige Dienststelle adressiert. Der Verwalter machte geltend, dass die Offenlegung der Daten des Beschwerdeführers in Form der wertenden Veröffentlichung des Beschwerdeinhalts gestützt auf den mit der Eigentümergemeinschaft geschlossenen Verwaltervertrag erforderlich sei, um diese über die anlasslose und seines Erachtens rufschädigende Beschwerde eines Mitglieds zu informieren. Darüber hinaus sei die Datenverarbeitung unter Verweis auf den Beschluss des OLG Köln vom 4. Februar 2000 – 16 W 5/2000 von der Meinungsäußerungsfreiheit gedeckt.

Die Offenlegung konnte jedoch weder auf den Verwaltervertrag und somit Art. 6 Abs. 1 lit. b DSGVO noch auf die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO und Art. 6 Abs. 4 DSGVO gestützt werden.

Ob dabei die Daten des individuellen Mitglieds der Eigentümergemeinschaft als Vertragspartei im Sinne des Art. 6 Abs. 1 lit. b DSGVO verarbeitet werden können, ist vor dem Hintergrund der mit der Novelle des Wohnungseigentumsgesetz (WEG) von 2020 erfolgten Betonung der Rechtsfähigkeit des Verbands und der Personenverschiedenheit von Gemeinschaft und Eigentümern in § 9a[41] und § 18 WEG zweifelhaft. Eine für die Vertragsbeziehung vorauszusetzende autonome Willensentscheidung der betroffenen Person ist dann nicht gegebenen, wenn diese durch den Verwaltervertrag ausschließlich über die wohnungseigentumsrechtlich vorgegebene Zugehörigkeit zur Gemeinschaft der Wohnungseigentümer mittelbar tangiert wird.[42]

Allerdings war die Offenlegung der Daten in der Form der wertenden Stellungnahme selbst in der Annahme, dass der Beschwerdeführer als Mitglied der Gemeinschaft als Vertragspartei im Sinne der Vorschrift anzusehen wäre, weder zur Erfüllung des Verwaltervertrages noch der sich daraus ergebenden Sekundärpflichten erforderlich. Für die Erforderlichkeit war in diesem Zusammenhang maßgeblich auf den Vertragszweck und -inhalt abzustellen, der im Wesentlichen in der Konkretisierung der Aufgaben und Befugnisse der Vertragsparteien bestand. Eine Offenlegung mit dem Ziel, die Eigentümergemeinschaft über ein aus Sicht des Verwalters schädigendes Verhalten eines Mitglieds zu seinen Lasten zu informieren, war damit weder vom Verwaltervertrag erfasst noch durch ein angenommenes Informationsinteresse der Gemeinschaft an der Darstellung der individuellen Beschwerde nach Art. 77 DSGVO und der gemutmaßten Hintergründe gerechtfertigt.

---

[41] Falkner, in beck-online. Großkommentar WEG, § 9a Rn. 48.

[42] In diesem Sinne wohl auch BT-Drs. 19/18791, S. 59; Emmerich, in: Bärmann/Pick, Wohnungseigentumsgesetz (20. Aufl. 2020), § 26 Rn. 61.

Ferner war die verfahrensgegenständliche Offenlegung von Daten des Beschwerdeführers auch nicht nach Art. 6 Abs. 1 lit. f und Art. 6 Abs. 4 DSGVO legitimiert. Das Ziel, vermeintlich geschäftsschädigende Aussagen des betroffenen Beschwerdeführers im Kreis der zugriffsberechtigten Mitglieder der Wohnungseigentümergemeinschaft aus Sicht der Verwaltung darzustellen, war zunächst als berechtigtes Interesse anzuerkennen. Aber auch wenn der Verwaltung zugestanden werden konnte, sich auch bei der beschwerdegegenständlichen Stellungnahme auf die Meinungsäußerungsfreiheit zu berufen, galt dieses Recht nicht schrankenlos und war notwendigerweise mit dem Recht auf Schutz personenbezogener Daten nach Art. 8 Charta der Grundrechte der Europäischen Union und den sekundärrechtlichen Vorgaben der DSGVO in Einklang zu bringen.

Der intendierte Zweck der Richtigstellung von den gegenüber dem Verwalter erhobenen Vorwürfen im Kreis der Wohnungseigentümer wäre in gleichem Maße erreicht worden, wenn lediglich auf der reinen Sachebene und ohne Verwendung wörtlicher Zitate und deren Konnotation als datenschutzrechtliche Beschwerde sowie insbesondere ohne Nennung des Urhebers der Beschwerde eine Auseinandersetzung mit den ursprünglich an die Aufsichtsbehörde adressierten Vorwürfen stattgefunden hätte. Mit der namentlichen Nennung und der ergänzenden konfrontativ-wertenden Einordnung der Beschwerde im Rahmen der veröffentlichten Stellungnahme des Verwalters war zudem erkennbar eine teilöffentliche Herabwürdigung des Verhaltens des Beschwerdeführers intendiert. Gegen die zweckändernde Verwendung der im Rahmen der Akteneinsicht gewonnen Daten waren daher auch überwiegende schutzwürdige Interessen des betroffenen Mitglieds der Eigentümergemeinschaft anzuführen.

Erst nachdem die Löschung der diesbezüglichen Offenlegung von Daten nach Art. 58 Abs. 2 lit. g DSGVO angeordnet wurde, hat der Verwalter diese entfernt.

4.23.5 Einsichtnahme in Einzelabrechnungen

Das Recht auf Einsichtnahme in die dem Wohnungsverwalter vorliegenden Verwaltungsunterlagen durch einzelne Mitglieder der Eigentümergemeinschaft ist trotz seiner mittlerweile im Rahmen der Novelle des Wohnungseigentumsgesetzes erfolgten gesetzlichen Klarstellung in § 18 Abs. 4 WEG nach wie vor wiederholt Gegenstand von Anfragen, Hinweisen und Beschwerden. Die häufig problematisierte Offenlegung personenbezogener Daten durch Wohnungsverwalter im Wege der Einsichtnahme von fremden Einzelabrechnungen – als Verwaltungsunterlagen im Sinne der Vorschrift[43] – ist, selbst wenn sich über die festgestellten Verbrauchswerte für das Einsicht nehmende Mitglied der Eigentümergemeinschaft teils weitreichende Einblicke in individuelle Lebensgestaltungen ergeben können, letztlich über Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 18 Abs. 4 WEG datenschutzrechtlich legitimiert. Dem liegt zugrunde, dass dem gesetzlich statuierten Informationsrecht notwendigerweise eine Rechtspflicht zur Gewährung der Einsichtnahme durch die Unterlagen führende Stelle immanent ist. Auch wenn der Einsichtsanspruch nach § 18 Abs. 4 WEG unmittelbar die Eigentümergemeinschaft adressiert, bedienen sich diese zumeist Wohnungsverwaltungen, so dass die Abwicklung des geltend gemachten Informationsrechts regelmäßig in deren Verantwortungsbereich erfolgen wird.

Auch wenn ein gegen die Gemeinschaft gerichteter Individualanspruch auf Einsicht normiert ist, sind durch den für die Gemeinschaft handelnden Wohnungsverwalter gleichwohl datenschutzrechtliche Vorgaben zu beachten (BT-Drs 19/18791, S. 60). Ob daraus eine Pflicht zur Begrenzung des Anspruchs auf Einsichtnahme unter Berücksichtigung des Zweckbindungsgrundsatzes und des Gebots der Datenminimierung dahingehend abgeleitet werden kann, dass bspw. Informationen wie E-

[43] Sommer/Heinemann in: Jennißen, Wohnungseigentumsgesetz 7. Aufl. 2021, § 18 WEG Rn. 146.

Mail-Adressen und Bankverbindung der übrigen Wohnungseigentümer nicht offengelegt werden dürfen,[44] ist vor dem Hintergrund des voraussetzungslos geltenden Informationsrechts und dessen zentraler Funktion im Beziehungsgefüge der Akteure (vgl. BT-Drs. 19/18791, S. 60) letztlich nicht überzeugend. Zu beachtende datenschutzrechtliche Vorgaben dürften in diesem Zusammenhang vorrangig in der transparenten Information der übrigen Wohnungseigentümer über die Möglichkeit der Datenoffenlegung im Rahmen der Einsichtnahme durch ein Mitglied der Gemeinschaft und in der Gewährleistung der Sicherheit der Verarbeitung im Sinne der Art. 5 Abs. 1 lit. f und Art. 32 DSGVO durch die Unterlagen führende Stelle bestehen.

Eine Verarbeitung der im Rahmen der Einsichtnahme gewonnenen Daten durch das einzelne Mitglied der Gemeinschaft erfolgt – soweit im Hinblick auf die Haushaltsausnahme im Sinne des Art. 2 Abs. 2 lit. c DSGVO hierfür der Anwendungsbereich des Datenschutzregimes eröffnet ist – allein in dessen datenschutzrechtlicher Verantwortlichkeit.

Von dem voraussetzungslosen Informationsrecht nach § 18 Abs. 4 WEG zu unterscheiden ist allerdings eine zweckspezifisch proaktive oder auf Anforderung erfolgende Übermittlung von Angaben zu Mitgliedern der Gemeinschaft. Bei einer solchen Übermittlung kann die Unkenntlichmachung von spezifischen Daten von Miteigentümern geboten sein.[45] Eine – in der Praxis häufig vorkommende – proaktive Zurverfügungstellung aller Einzelabrechnungen an jedes Mitglied der Gemeinschaft mit dem Ziel der Vorbereitung der Beschlussfassung über die Jahresabrechnung, ist mangels Erforderlichkeit[46] datenschutzrechtlich nicht legitimiert.

[44] Beckers, Umgang mit Eigentümerdaten, ZWE 2019, S. 297 (303); Sommer/Heinemann a. a. O. unter Hinweis auf LG Düsseldorf, Urteil vom 4. Oktober 2018 – 25 S 22/18.

[45] LG Düsseldorf a. a. O. Rn. 22, juris.

[46] BGH, Urteil vom 27. Oktober 2017 – V ZR 189/16 Rn. 12, juris.

4.24 Baustellenüberwachung

Der Diebstahl von teils hochwertigen Maschinen, Werkzeugen und Materialien von Baustellen ist ein allseits bekanntes Problem für Bauträger und –firmen, so dass diese häufig dazu übergehen, Videoüberwachungstechnik zum Schutz ihres Eigentums vor Diebstahl und zur Identifikation von Tätern im Schadensfall einzusetzen.

Die datenschutzrechtliche Zulässigkeit der Videoüberwachung einer Baustelle beurteilt sich nach Art. 6 Abs. 1 lit. f DSGVO. Danach ist eine kameragestützte Verarbeitung personenbezogener Daten nur zulässig, wenn diese zur Wahrung berechtigter Interessen des Anlagebetreibers oder eines Dritten erforderlich ist und die schutzwürdigen Interessen der betroffenen Personen das berechtigte Interesse des Verantwortlichen nicht überwiegen. Erforderlich ist eine Videoüberwachung dann, wenn mit ihrer Hilfe die verfolgten Zwecke tatsächlich erreicht werden können und es hierfür keine milderen, gleich geeigneten Mittel gibt.

Zur Wahrung des im Sinne der Vorschrift anzuerkennenden Überwachungsinteresses, das unternehmerische oder private Eigentum vor Diebstahl zu schützen, ist eine Videoüberwachung grundsätzlich geeignet. Sie bietet einerseits einen präventiven Schutz, da potentielle Störer von der Begehung von Diebstählen abgeschreckt werden, andererseits können Videoaufzeichnungen im Schadensfall auch die nachträgliche Identifikation von Störern ermöglichen.

Für Überwachungsmaßnahmen zur Verhinderung und Aufdeckung von in der Regel außerhalb der üblichen Arbeitszeiten stattfindenden Schadensereignissen ist mit Blick auf den Grundsatz der Datenminimierung ein ganztägiger Kameraeinsatz indes nicht als erforderlich anzusehen. Auch stehen einer ganztägigen Baustellenüberwachung die schutzwürdigen Interessen der betroffenen Mitarbeitenden, Lieferanten und sonstigen Personen, die sich berechtigterweise und über einen längeren Zeitraum im überwachten Bereich der Baustelle aufhalten und sich

dem Kameraeinsatz nicht entziehen können, regelmäßig entgegen. Der dadurch bedingte gravierende Eingriff in das Recht auf Schutz ihrer personenbezogenen Daten nach Art. 8 Grundrechte-Charta der Europäischen Union lässt sich nicht mit Verweis auf einen unbedingten Diebstahlschutz legitimieren. Die Videoüberwachung ist daher regelmäßig auf die Zeiträume außerhalb der üblichen Arbeitszeiten (Abend- und Nachtstunden, Sonn- und Feiertage) zu begrenzen.

Ferner sind ebenfalls aus Gründen der tatbestandlichen Erforderlichkeit und unter Beachtung des Gebots der Datenminimierung die Erfassungsbereiche der Kameras so zu wählen, dass ausschließlich der unmittelbare Baustellenbereich und keine öffentlich zugänglichen Bereiche wie Gehwege oder Straßen erfasst und somit unbeteiligte Personen wie Passanten und Anwohner nicht zum Objekt der Überwachung werden.

Darüber hinaus ist durch ausreichend wahrnehmbare Hinweisschilder transparent im Sinne des Art. 13 DSGVO auf die Videoüberwachung hinzuweisen. Diese Informationspflichten umfassen insbesondere Angaben zur verantwortlichen Stelle, zu den Zwecken und zur Rechtsgrundlage der Videoüberwachung, zur Speicherdauer, zu den Empfängern der verarbeiteten Daten sowie zu den Betroffenenrechten.

Für den Fall, dass sich ein begründbarer Diebstahlsverdacht gegen Mitarbeiter richtet, wäre als ultima ratio eine Videoüberwachungsmaßnahme während der Arbeitszeiten denkbar. Nach § 26 Abs. 1 Satz 2 BDSG dürfen Beschäftigtendaten zur Aufdeckung von Straftaten verarbeitet werden, sofern ein konkreter und dokumentierter Verdacht auf ein strafrechtlich relevantes Verhalten eines Beschäftigten gegeben ist. Eine Überwachungsmaßnahme, die gerade auch zweckspezifisch Mitarbeitende erfassen soll, stellt einen gravierenden Grundrechtseingriff dar; vor diesem Hintergrund ist die Videoüberwachung auf das zur Zweckerreichung unbedingt erforderliche Ausmaß zu beschränken. Dies kann in räumlicher Hinsicht eine Fokussierung der

Überwachung auf gefahrträchtige Bereiche, in denen hochwertige Gerätschaften abgestellt sind oder in der mit einer Tathandlung potenziell gerechnet werden kann, bedeuten. In zeitlicher Hinsicht ist bspw. eine Einschränkung der Videoüberwachung dahingehend zu prüfen, dass ein Kameraeinsatz beispielsweise nur dann erfolgt, wenn Diebstähle anhand der belegbaren Feststellungen auf bestimmte Schichten eingegrenzt werden können.

Fazit/ Empfehlung:

Bei einer Baustellenüberwachung zum Zwecke des Diebstahlschutzes ist die Überwachung auf die Zeiten zu beschränken, in denen sich keine Personen berechtigterweise auf dem überwachten Baustellengelände aufhalten. In begründeten Ausnahmefällen, bspw. bei dokumentiertem Verdacht des Diebstahls durch Mitarbeitende, kann eine räumlich fokussierte und zeitlich eingeschränkte Überwachung zu den üblichen Arbeitszeiten zulässig sein.

4.25 Hafnium-Fälle

Microsoft schloss im März 2021 mit einem außerplanmäßigen Sicherheitsupdate mehrere Schwachstellen in seinem Exchange-Server (Version 2010-2019) und stufte die mögliche Bedrohung zunächst noch als recht gering ein. In den Folgemonaten häuften sich jedoch die Angriffe auf Exchange-Server, woraufhin das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Alarmstufe Rot ausrief.

Durch die Ausnutzung der bestehenden Schwachstelle bestand die Möglichkeit, dass Angreifer die reguläre Authentifizierung umgehen, sich als Administrator am Exchange-Server anmelden und somit weitere Installationsdateien für eine Remote-Code-Ausführung implementieren konnten. Damit konnten sie sich in großem Umfang Zugang zu ganzen E-Mail-Postfächern verschaffen, wodurch eine große Zahl personenbezogener Daten

betroffen war. In einem solchen Fall einer Verletzung des Schutzes personenbezogener Daten ist der Verantwortliche verpflichtet, diese gem. Art. 33 DSGVO unverzüglich der zuständigen Aufsichtsbehörde zu melden, es sei denn, die Datenschutzverletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.

Bei unserer Behörde gingen in der Folge 39 solcher sog. Datenpannenmeldungen ein. Die Dunkelziffer der Angriffe kann an dieser Stelle jedoch nicht beziffert werden. Denn nicht jede Organisation hat entsprechende IT-Sicherheitswerkzeuge im Einsatz, um einen solchen Angriff abzuwehren bzw. zu detektieren.

Nach einer entsprechenden Analyse der uns gemeldeten Vorfälle konnte in fast allen Fällen festgestellt werden, dass ein mangelndes Patch- und Updatemanagement für die gemeldeten Probleme bzw. Schutzverletzungen verantwortlich war. Darüber hinaus erfüllen die IT-Infrastrukturen oft nicht die Mindestsicherheitsvorgaben des BSI (z. B. kein bestehender Virenschutz, offene bzw. ungeschützte Zugriffsmöglichkeit von außen, keine weiteren IT-Sicherheitswerkzeuge, insb. zur Angriffsdetektion, usw.). Unsere Behörde hat den Betroffenen entsprechende technisch-organisatorische Empfehlungen ausgesprochen. Ferner wurde darum gebeten, diese Maßnahmen in das Informationssicherheitsmanagementsystem zu integrieren bzw. ein solches aufzubauen.

Dieser Sicherheitsvorfall zeigt wieder einmal beispielhaft, dass Schwachstellen in der IT zu erheblichen Gefahren für personenbezogene Daten führen können. Daher muss der Betreiber von IT-Infrastrukturen als Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO nach Art. 5 Abs. 1 lit. f, Art. 24, 32 DSGVO durch geeignete technische und organisatorische Maßnahmen ein angemessenes Schutzniveau gewährleisten.

V. Bußgeldverfahren

5 Bußgeldverfahren

Mit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) wurden die Aufsichtsbehörden in die Lage versetzt, Datenschutzverstöße durch Unternehmen oder Privatpersonen künftig mit wirksamen Bußgeldern zu ahnden. Ein Anlass für die Prüfung eines Bußgeldverfahrens kann sich z. B. dann ergeben, wenn aufgrund einer Beschwerde eines Betroffenen im Verwaltungsverfahren ein Datenschutzverstoß festgestellt wird, eine Anzeige bei der Staatsanwaltschaft an uns abgegeben wird oder aufgrund disziplinarischer Ermittlungen ein Datenschutzverstoß eines Beschäftigten oder Bediensteten vermutet wird.

Im Berichtszeitraum stellten Datenschutzverstöße im Zusammenhang mit Bonitätsabfragen, Corona-Kontaktdatenlisten, offenen E-Mail-Verteilern und der Videoüberwachung von Mitarbeitern einen Schwerpunkt im Bereich der Bußgeldverfahren dar.

5.1 Unzulässige Bonitätsabfragen

Gegenstand mehrerer Bußgeldverfahren war die Einholung von Bonitätsauskünften durch saarländische Unternehmen.

Bonitätsabfragen werden meist von Banken, Versandhändlern, Telekommunikationsunternehmen, Energieversorgern und Inkassounternehmen an sogenannte Auskunfteien gerichtet. Dies sind in der Regel private gewerbliche Unternehmen, die Daten über das Zahlungsverhalten von Unternehmen und Privatpersonen erheben und verarbeiten, um das künftige Zahlungsverhalten und damit mittelbar die Kreditwürdigkeit dieser Unternehmen oder Privatpersonen zu prognostizieren.

Eine Bonitätsabfrage zu einer Person oder einem Unternehmen ist nach Art. 6 Abs. 1 lit. f DSGVO zulässig, soweit die angeforderten Daten zur Wahrnehmung berechtigter Interessen des Anfragenden erforderlich sind und sofern nicht schutzwürdige Interessen der Betroffenen der Datenverarbeitung entgegenstehen. Dies setzt voraus, dass die Bonitätsabfrage im Rahmen

einer Geschäftsanbahnung oder der Fortführung eines bereits bestehenden Vertragsverhältnisses zwischen dem Anfragenden und dem von der Anfrage betroffenen Schuldner zur Bewertung der Kreditwürdigkeit benötigt wird.

In den von uns verfolgten Fällen mangelte es gerade an dieser rechtlichen Voraussetzung. Es bestand weder ein Vertragsverhältnis noch eine entsprechende Geschäftsanbahnung. Vielmehr waren die Bonitätsabfragen privat motiviert und standen mit dem Geschäftsbetrieb des Anfragenden in keinem Zusammenhang. Die Datenabfragen erfolgten somit ohne Rechtsgrundlage und waren demnach als unzulässig zu bewerten.

Da es sich hierbei um einen Missbrauch von beruflich zur Verfügung stehenden Instrumenten handelte, waren die entsprechenden Vorwürfe nicht nur als geringfügige Ordnungswidrigkeiten einzuordnen, was bei der Bemessung der Bußgeldhöhe zu berücksichtigen war. Verstöße dieser Art werden regelmäßig von unserer Bußgeldstelle geahndet.

Fazit/ Empfehlung:

Immer wieder ist festzustellen, dass Bonitätsabfragen unzulässig getätigt werden. Um zu prüfen, wer Informationen zu ihrer Person abgefragt hat, sollten sich Verbraucher daher nicht scheuen, kostenfreie Auskünfte nach Art. 15 DSGVO bei den Auskunfteien einzuholen.

5.2 Corona-Kontaktdatenlisten

Die saarländische Verordnung zur Bekämpfung der Corona-Pandemie (VO-CP) verpflichtete in ihrer Fassung vom 17. September 2020 Betreiber von Betrieben, Einrichtungen oder Veranstaltungen dazu, eine Kontaktnachverfolgung ihrer Gäste zu gewährleisten. Hierzu waren nach § 3 Abs. 2 Satz 2 VO-CP je ein Vertreter eines anwesenden Haushalts mit Vor- und Familienname, Wohnort, Erreichbarkeit und Ankunftszeit zu erfassen. In der Praxis waren von den Gästen entsprechende Formulare zur Kontaktdatenerhebung auszufüllen. Die so erhobenen Daten

durften nur zweckgebunden den Gesundheitsämtern auf deren Anforderung ausgehändigt werden (§ 3 Abs. 3 VO-CP).

Anlass für ein bei uns geführtes Bußgeldverfahren war die Anzeige einer saarländischen Kommune, deren Mitarbeiter des kommunalen Betriebshofs im Rahmen einer Streife festgestellt hatten, dass etwa 120 ausgefüllte Gästeregistrierungsformulare zur Kontaktdatenerhebung eines Restaurantbetriebes frei zugänglich in einer Kiste an einem Papier-Containerstandort abgestellt worden waren. Im Rahmen der sich anschließenden Ermittlungen unserer Dienststelle wurde weiterhin festgestellt, dass schon innerhalb des Gaststättenbetriebs unzureichende Vorkehrungen zum Schutz der bei der Gästeregistrierung verarbeiteten Daten umgesetzt worden sind. So wurden die ausgefüllten Gästeregistrierungsformulare in einem für alle Mitarbeiter zugänglichen Nebenraum ohne besondere Sicherungsmaßnahmen, wie beispielsweise einem verschlossenen Schrank aufbewahrt.

Demnach wurden seitens der Restaurantbetreiber keine ausreichend wirksamen technisch-organisatorischen Maßnahmen nach Art. 32 i. V. m. Art. 5 Abs. 1 lit. f und Art. 24 DSGVO getroffen, um eine unbefugte Kenntnisnahme oder einen unbefugten Zugang zu den von den Restaurantbesuchern erhobenen personenbezogenen Daten auszuschließen. Mithin lag ein Verstoß gegen die Grundsätze der Verarbeitung personenbezogener Daten vor, sodass gemäß Art. 83 Abs. 1 und 5 lit. a DSGVO ein Bußgeld zu verhängen war.

Der Ordnungswidrigkeit kam eine nicht nur geringfügige Bedeutung zu, da der Verstoß mit geringem Aufwand, wie der Verwahrung unter Verschluss sowie einer ordnungsgemäßen und datenschutzkonformen Entsorgung, hätte verhindert werden können. Das Bußgeld wurde unter Berücksichtigung des Vorjahresumsatzes der Restaurantbetreiber, aber auch unter Berücksichtigung der pandemiebedingt allgemein schwierigen wirtschaftlichen Situation von Gastronomiebetrieben festgesetzt.

Fazit/ Empfehlung:

Betriebe sind verpflichtet, die von ihnen erhobenen personenbezogenen Daten sicher gegen die Zugriffsmöglichkeit unberechtigter Personen zu verwahren.

5.3 Offener E-Mail-Verteiler

Immer wieder erhalten wir auch Anzeigen wegen des Versands von E-Mail mit offenem Verteiler. Gegenstand eines dieser Bußgeldverfahren war der Versand einer E-Mail mit offenem Verteiler durch einen Mitarbeiter eines Mitgliederbüros einer politischen Organisation. Die Ermittlungen ergaben, dass der Mitarbeiter versehentlich eine E-Mail offen, ohne Verwendung des BCC-Feldes, an mehr als 400 Adressaten verschickt hatte, wobei sich aus dem Verteiler Vor- und Zuname und die dazugehörige E-Mail-Adresse des Adressaten ergaben und aufgrund des Inhalts der E-Mail auf die politische Gesinnung der Adressaten zu schließen war.

Interessant an diesem Fall war, dass die verantwortliche Stelle die datenschutzrechtliche Verantwortlichkeit allein bei ihrem Mitarbeiter sah. Gestützt auf die Entscheidung des LG Bonn (9. Kammer), Urteil vom 11. November 2020 – 29 OWi 1/20 Rn. 30 ff war nach unserer Auffassung das Fehlverhalten des Mitarbeiters – unabhängig von einem etwaigen Verhalten einer Leitungsperson – nach Art. 83 Abs. 4 bis 6 DSGVO jedoch der verantwortlichen Stelle zuzurechnen. In der Konsequenz erging daher auch der Bußgeldbescheid nach Art. 83 Abs. 5 lit. a DSGVO sowie die damit verbundene Bußgeldforderung an das Mitgliederbüro als verantwortliche Stelle.

Auch hier war mit Blick auf die Bußgeldhöhe die Ordnungswidrigkeit nicht als lediglich geringfügig einzustufen, da aufgrund der Offenlegung der politischen Gesinnung der betroffenen Adressaten besondere Kategorien personenbezogener Daten i. S. d. Art. 9 DSGVO betroffen waren.

5.4 Videoüberwachung von Mitarbeitern

Anlass für ein weiteres Bußgeldverfahren war der Betrieb einer Videoüberwachungsanlage mit insgesamt 14 Kameras durch ein saarländisches Unternehmen. Die Überwachung erfolgte ganztägig und war technisch so ausgestaltet, dass sowohl eine optische als auch eine akustische Überwachung möglich war.

Aufgrund von elf im Innenbereich des Unternehmens installierten Kameras wurden Mitarbeiter gezwungen, sich für längere Zeiträume im Überwachungsbereich aufzuhalten. Auch Kunden und Lieferanten waren hiervon betroffen. Drei weitere im Außenbereich des Unternehmens installierte Kameras erfassten darüber hinaus nicht nur das eigene Firmengelände, sondern auch die nahe gelegene Straße, so dass hier neben Mitarbeitern des eigenen Unternehmens und Kunden auch Mitarbeiter eines benachbarten Unternehmens sowie Passanten betroffen waren.

Für die Videoüberwachung existierte weder ein Verzeichnis der Verarbeitungstätigkeit nach Art. 30 DSGVO noch eine transparente Hinweisbeschilderung gemäß Art. 13 DSGVO, ebenso wenig wie ein Auftragsverarbeitungsvertrag mit dem technisch eingebundenen Dienstleister.

Das Unternehmen rechtfertigte seine Vorgehensweise mit dem beabsichtigten Schutz vor Einbrüchen und dem Schutz seines Eigentums. Darüber hinaus legte es von einem Teil der Belegschaft Einwilligungserklärungen zur Videoüberwachung vor.

Hierzu ist anzumerken, dass nach § 26 Abs. 2 BDSG eine Verarbeitung personenbezogener Daten auch durch die Einwilligung der betroffenen Person rechtmäßig sein kann. Voraussetzung für eine solche Einwilligung ist aber, dass sie von der betroffenen Person freiwillig abgegeben wird. In einem Über-Unterordnungsverhältnis, wie vorliegend in einem Beschäftigungsverhältnis, wird eine Freiwilligkeit nur selten gegeben sein. In Kombination aber mit einer Videoüberwachungsanlage, die Arbeit-

nehmer umfassend und während nahezu ihrer gesamten Arbeitszeit filmt, ist nach hiesiger Auffassung eine Freiwilligkeit i. S. d. § 26 Abs. 2 BDSG nicht gegeben.

Darüber hinaus müssten sämtliche Arbeitnehmer einwilligen, um eine konkrete Verarbeitung von personenbezogenen Arbeitnehmerdaten für konkret festzulegende Zwecke nach § 26 Abs. 2 BDSG gesetzlich legitimieren zu können, was im dargestellten Fall ebenfalls nicht gegeben war.

Auch eine gesetzliche Verarbeitungsbefugnis auf der Grundlage von Art. 6 Abs. 1 lit. f DSGVO schied im konkreten Fall aus. Der insofern für sämtliche Kameras vom Unternehmen angegebene Zweck „Schutz vor Einbruch" kann zwar grundsätzlich ein berechtigtes Interesse gem. Art. 6 Abs. 1 lit. f DSGVO darstellen. Die hierfür erforderliche Voraussetzung, wonach die Datenverarbeitung für den zu erreichenden Zweck erforderlich sein muss, war jedoch hier nicht gegeben. Aufgrund der Anwesenheit der Mitarbeiter zu den Betriebszeiten bestand nur eine äußerst geringe Wahrscheinlichkeit eines Einbruchs. Der Rund-um-die-Uhr-Betrieb sämtlicher Kameras im Innen- und Außenbereich des Unternehmens war – zumindest während der Betriebszeiten – für den vorgenannten Zweck nicht erforderlich.

Mit Blick auf die Rechtsprechung des Bundesarbeitsgerichts (BAG, Urt. v. 28.3.2019 – 8 AZR 421/17, Rn. 39) und die tatsächlich umfassend und nahezu durchgängig ausgestaltete Überwachung der Mitarbeiter wäre auch die erforderliche Interessensabwägung mit den Interessen der Betroffenen – hier der Mitarbeiter – zu deren Gunsten ausgefallen.

Erst recht war die Videoüberwachung der betroffenen Kunden, Lieferanten und Passanten als unzulässig zu bewerten, da auch hier keine Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO vorlag und es nach Art 6 Abs. 1 lit. f DSGVO aufgrund der Anwesenheit der Mitarbeiter an der Erforderlichkeit der Datenverarbeitung für den benannten Zweck „Schutz vor Einbruch" jedenfalls während der Betriebszeiten mangelte.

Das Fehlen des Verzeichnis nach Art. 30 DSGVO, einer transparenten Hinweisbeschilderung gemäß Art. 13 DSGVO und eines Auftragsverarbeitungsvertrages nach Art. 28 DSGVO stellten weitere Datenschutzverstöße dar.

Die vorgenannten Verstöße stellten in ihrer Gesamtheit einen erheblichen Eingriff in die Rechte der betroffenen Personen dar.

Nach Würdigung der Gesamtumstände war daher gemäß Art. 83 Abs. 5 lit. a DSGVO ein angemessenes Bußgeld zu verhängen.

Fazit/ Empfehlung:

Vor Einsatz einer Videoüberwachungsmaßnahme sollten Unternehmen umfassend prüfen, in welchem zeitlichen als auch räumlichen Ausmaß die Maßnahme für den angestrebten Zweck erforderlich ist und wie sich dies auf den betroffenen Personenkreis auswirkt.

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)

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 (ABI. Nr. L 119, S. 1, ber. ABI. Nr. L 314, S. 72 und ABI. 2018 Nr. L 127, S. 2)

ePrivacy-Richtlinie: Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Abl. L 201 S. 37), zuletzt geändert durch Art. 2 ÄndRL 2009/136/EG vom 25.11.2009 (ABl. L 337 S. 11, ber. 2013 ABl. L 241 S. 9, ber. 2017 ABl. L 162 S. 56)

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)

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)

TMG – Telemediengesetz: Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Gesetz vom 12.8.2021 (BGBl. S. 3544)

TTDSG – Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien: Vom 23.6.2021 (BGBl. S. 1982), zuletzt geändert durch Gesetz vom 12.8.2021 (BGBl. I S. 3544)

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