Die Landesbeauftragte für
Datenschutz und Informationsfreiheit

29. Tätigkeitsbericht Datenschutz

UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

2020

29. Tätigkeitsbericht

der Landesbeauftragten für Datenschutz und Informationsfreiheit

Berichtszeitraum: 2020

Dem Landtag und der Landesregierung
vorgelegt am 14. April 2021
(Landtagsdrucksache 16/1560)

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

Vorwort

Das zurückliegende Jahr 2020 war in großem Umfang geprägt von den Auswirkungen und Herausforderungen der Corona-Pandemie.

In sehr kurzer Zeit mussten die öffentlichen Stellen des Landes und seiner Kommunen ebenso wie der private Sektor Lösungen finden, um die gewohnten zwischenmenschlichen Arbeitsweisen durch digitale Prozesse zu ersetzen und hierdurch der Verbreitung des Virus entgegenzuwirken.

Der ohne Übergangszeit zu bewältigende Wechsel der Beschäftigten von dem gewohnten Arbeitsplatz in das Homeoffice und die Umstellung von Präsenz- zu Distanzunterricht in den Schulen stellten nicht nur für die hiervon Betroffenen eine enorme Herausforderung dar. Auch die Verantwortlichen mussten innerhalb kürzester Zeit die hierfür notwendigen technischen und organisatorischen Voraussetzungen schaffen. Dass dem Datenschutz dabei oft nicht die nötige Aufmerksamkeit geschenkt wurde, ist bedauerlich, war unter diesen besonderen Umständen jedoch zunächst nachvollziehbar. Nachdem aber nunmehr das zweite Pandemiejahr angebrochen ist, sollte klar geworden sein, dass improvisierte Lösungen nicht dauerhaft tragfähig sind.

Vielmehr ist es von großer Bedeutung, den durch die Pandemie ausgelösten Digitalisierungsschub datenschutzkonform zu gestalten, da die digitale Transformation nur dann gelingen kann, wenn die Nutzerinnen und Nutzer auf einen ausreichenden Schutz ihrer Daten vertrauen können. Ohne dieses Vertrauen sinkt die Akzeptanz der Bevölkerung in die technischen Lösungen, was über kurz oder lang den verfolgten Zielen einer flexiblen Ausgestaltung staatlicher Verwaltung und privater Arbeitswelt zuwiderläuft.

Daher geben die gegenwärtige Krisensituation und ihre drängenden Herausforderungen entgegen vielfach zu hörenden

Forderungen auch keinen Anlass dazu, das hohe Niveau des europäischen Datenschutzes in Frage zu stellen.

Ganz im Gegenteil ist gerade auch der in diesem Zusammenhang von Teilen der Wirtschaft, der öffentlichen Verwaltung und nicht zuletzt aus dem schulischen Bereich häufig als alternativlos bezeichnete Einsatz von US-amerikanischen Diensten kritisch zu überprüfen. Nachdem der EuGH in seinem sog. Schrems II - Urteil im vergangenen Jahr klargestellt hat, dass eine Übermittlung von personenbezogenen Daten in die USA aufgrund umfangreicher Zugriffsmöglichkeiten durch die dortigen Behörden und fehlender Rechtsschutzmöglichkeiten für Betroffene mit erheblichen Risiken verbunden ist, sollte allen Verantwortlichen bewusst sein, dass ein Datenexport in die USA nur noch unter Einhaltung besonderer zusätzlicher Maßnahmen möglich ist, die das europäische Datenschutzniveau auch wirklich gewährleisten können.

Aber auch bei Datenübermittlungen in zahlreiche andere nichteuropäische Drittstaaten wird jeweils eine intensive Prüfung erforderlich sein, ob die dortige Rechtslage den Anforderungen des europäischen Rechts entspricht. Nur ausnahmsweise ist diese Prüfung entbehrlich, wenn bereits ein Angemessenheitsbeschluss der Europäischen Kommission existiert, der dem Drittland ein gleichwertiges Datenschutzniveau bescheinigt. Ist hingegen ein solches angemessenes Schutzniveau nicht gegeben und kann der Schutz auch nicht durch andere zusätzliche Maßnahmen hergestellt werden, muss die Datenübermittlung unterbleiben. Verantwortliche sollten daher künftig auf – durchaus verfügbare – europäische oder nationale Lösungen zurückgreifen, die nicht nur datenschutzkonform sind, sondern gleichzeitig auch eine Investition in die Innovationskraft unserer IT-Wirtschaft darstellen.

Wie sehr datenschutzkonforme Konzepte das Vertrauen der Bevölkerung in digitale Anwendungen fördern können, zeigt die durch das Robert-Koch-Institut herausgegebene Corona-Warn-App. Es dürfte maßgeblich der datensparsamen Ausgestaltung

dieser App, welche bewusst auf eine Rückverfolgbarkeit ihrer Nutzer verzichtet, geschuldet sein, dass sie mit mittlerweile über 25 Millionen Downloads einen beachtlichen Erfolg darstellt.

Umso bedauerlicher ist es, dass dieser Erfolg nunmehr von vielen Seiten wiederholt in Frage gestellt und das in der Corona-Warn-App realisierte Datenschutzkonzept teilweise pauschal dafür verantwortlich gemacht wird, dass die Pandemie noch immer nicht unter Kontrolle gebracht werden konnte. Abgesehen davon, dass die Corona-Warn-App von vorneherein nie mehr als einer von vielen Bausteinen in der gesamten Pandemiebekämpfung gedacht war, steht der Datenschutz einer effektiven Weiterentwicklung der App, bei der die Ziele des Gesundheitsschutzes mit dem informationellen Selbstbestimmungsrecht der Nutzer in einen angemessenen Ausgleich gebracht werden, in keiner Weise entgegen. Zugleich wird es aber erforderlich sein, die Digitalisierung der Gesundheitsämter und Labore zu forcieren, um die derzeit noch bestehenden Schwierigkeiten beim Austausch von Informationen zwischen diesen Stellen und der App zu vermindern. Jedoch anzunehmen, ein Verzicht auf den Datenschutz könne einen Mehrwert für die Nutzbarkeit der App darstellen, verkennt den Stellenwert der Pflicht des Staates, die personenbezogenen Daten und die Privatsphäre der Bürgerinnen und Bürger zu schützen.

Natürlich musste sich auch das Unabhängige Datenschutzzentrum im vergangenen Jahr auf die coronabedingt veränderten Rahmenbedingungen einstellen. Der Mitte März notwendig gewordene Übergang nahezu der gesamten Dienststelle in die Arbeit im Homeoffice konnte glücklicherweise ohne Schwierigkeiten erfolgen. Dies war zum einen der bereits vorhandenen IT-Ausstattung der Dienststelle, zum anderen aber vor allem der Flexibilität und dem großen Engagement aller Mitarbeiterinnen und Mitarbeiter zu verdanken, denen es auch bei nicht immer einfachen äußeren Rahmenbedingungen gelungen ist, trotz weiterhin steigender Verfahrenseingänge vorhandene Rückstände abzubauen. Im Gegenzug hat aber die drastische Beeinträchtigung des öffentlichen Lebens leider dazu geführt, dass

unsere Dienststelle die für unsere Aufgabenwahrnehmung häufig notwendigen Vor-Ort-Termine und –Kontrollen fast im gesamten Jahr nicht mehr durchführen konnte. Auch Veranstaltungen, die einen wichtigen Baustein für eine datenschutzrechtliche Sensibilisierung von Verantwortlichen und Betroffenen darstellen, konnten nicht wie ursprünglich geplant angeboten werden, waren aber in gewissem Umfang zumindest digital möglich.

Wie der vorliegende Tätigkeitsbericht zeigt, lag der Schwerpunkt unserer Tätigkeit im Berichtszeitraum verständlicherweise auf den verschiedensten datenschutzrechtlichen Fragestellungen rund um das Pandemiegeschehen. So haben wir uns intensiv mit den Vorschriften zur Kontaktnachverfolgung sowie mit den in diesem Zusammenhang auftretenden praktischen Umsetzungsfragen befasst. Aber auch unabhängig von unmittelbar mit der Corona-Bekämpfung in Zusammenhang stehenden Datenverarbeitungsprozessen, wurden zahlreiche andere datenschutzrechtliche Themen von unserer Dienststelle bearbeitet. So fand im vergangenen Jahr mit der Verabschiedung des Gesetzes zur Neuregelung der polizeilichen Datenverarbeitung im Saarland ein wichtiges und umfangreiches Gesetzgebungsvorhaben seinen Abschluss, das wir bereits seit 2018 intensiv begleitet haben und in dem es uns gelungen ist, in einigen zentralen Punkten dem Datenschutz zu mehr Gewicht zu verhelfen. Die hier erzielten Ergebnisse zeigen über den konkreten Sachverhalt hinweg, wie wichtig die stets gute und kooperative Zusammenarbeit unserer Dienststelle mit der Landesregierung und den zuständigen Gremien im Landtag für die Erarbeitung datenschutzgerechter Lösungen ist.

Wir alle hoffen, dass die Corona-Pandemie bald ein Ende finden wird und wir in unser gewohntes Leben zurückkehren können. Die technischen Lösungen, welche während der Pandemie entwickelt und etabliert wurden, werden uns erhalten bleiben und uns auch weiterhin mehr Flexibilität in den unterschiedlichsten Bereichen unseres Alltags ermöglichen. Ein Mehrwert für die Gesellschaft wird sich dauerhaft nur mit datenschutzkonformen

Lösungen erreichen lassen. Für die verantwortlichen Stellen lohnt es sich daher, auch und gerade in diesen Zeiten, dem Datenschutz eine besondere Aufmerksamkeit zu widmen.

Saarbrücken, im April 2021

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). 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 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 Beschwerden, die im Berichtszeitraum eingegangen sind, 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.

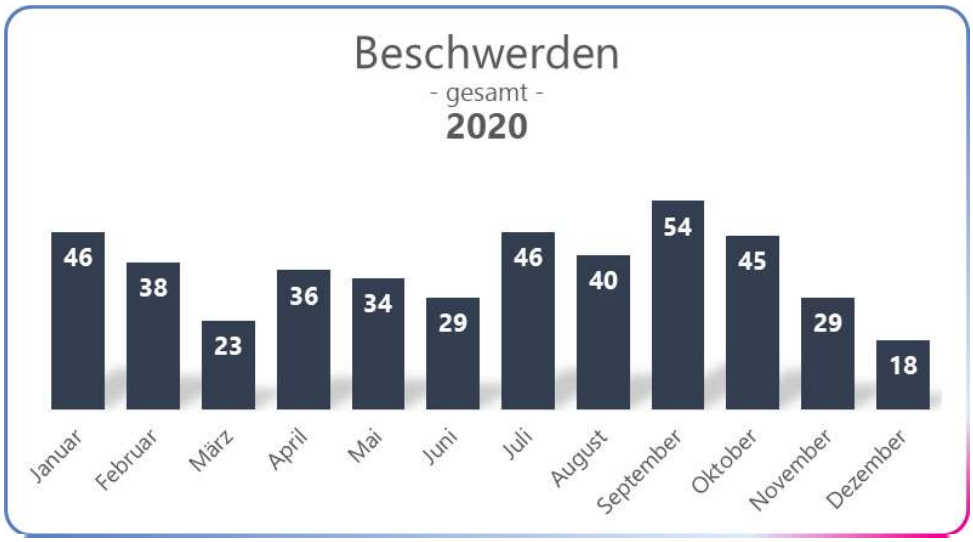

Abb. 1: Beschwerden (gesamt) 2020

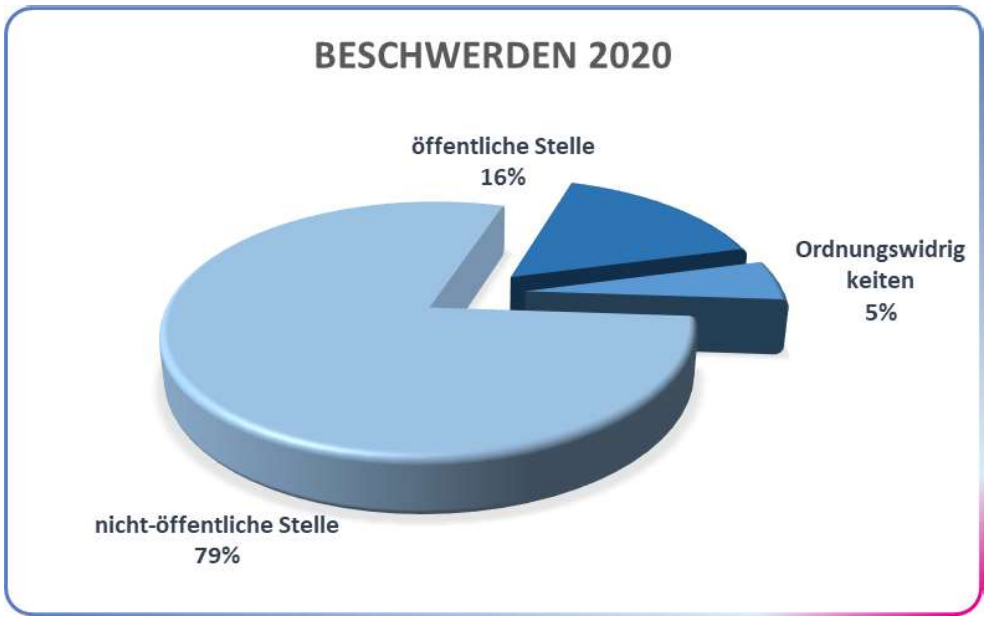

Abb. 2: Beschwerden (Aufteilung) 2020

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.

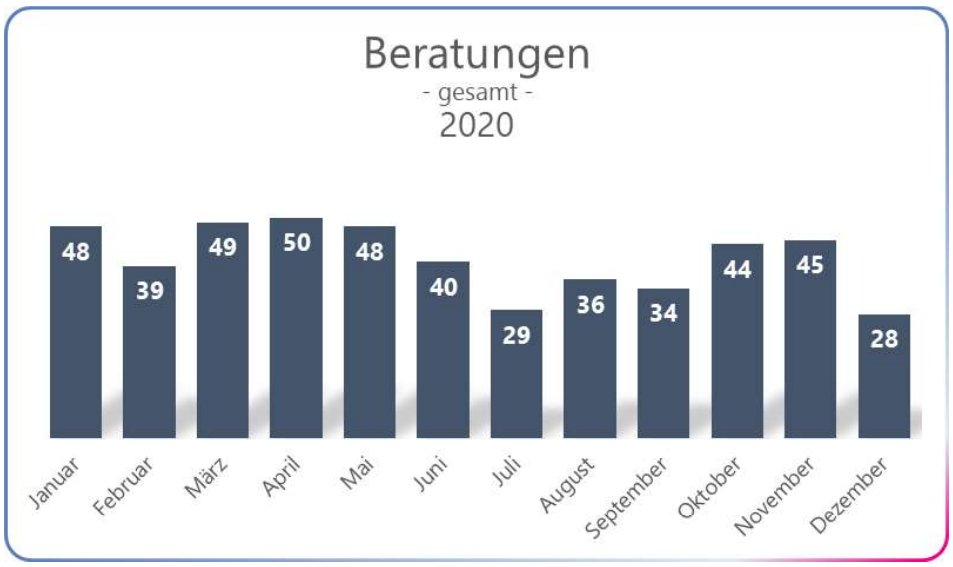

Abb. 3: Beratungen (gesamt) 2020

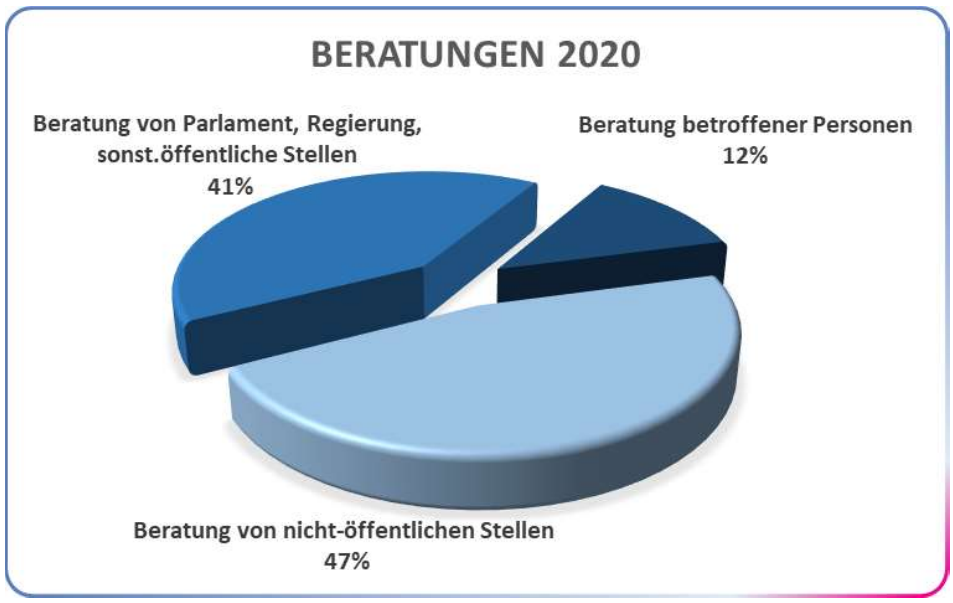

Abb. 4 Beratungen (Aufteilung) 2020

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 Datenschutz-Grundverordnung (DSGVO) gegeben.

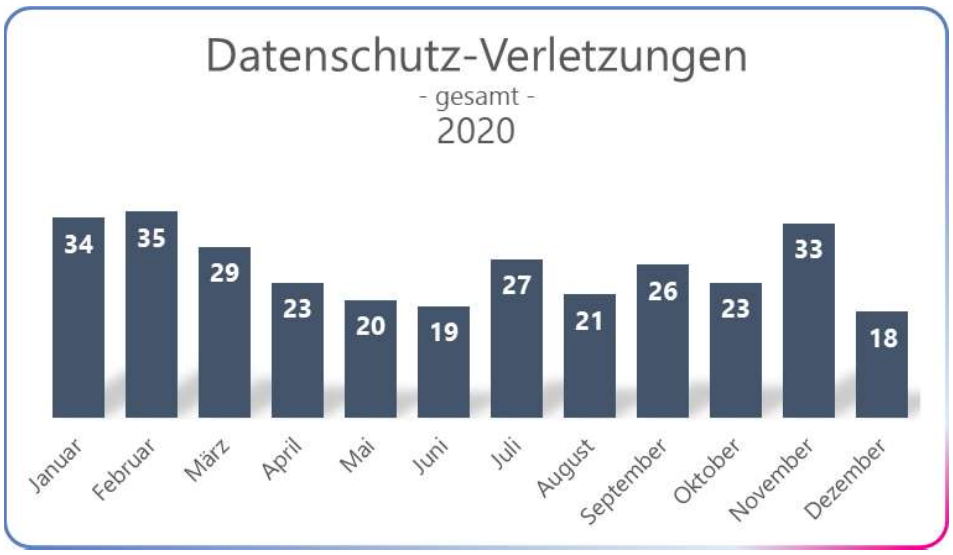

Abb. 5: Datenschutzverletzungen 2020

1.4 Abhilfemaßnahmen

Um drohende datenschutzrechtliche Verstöße zu verhindern oder festgestellte Verstöße zu sanktionieren, werden den Aufsichtsbehörden in Art. 58 Abs. 2 Datenschutz-Grundverordnung (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,
- Verwarnungen nach Art. 58 Abs. 2 lit. b,

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

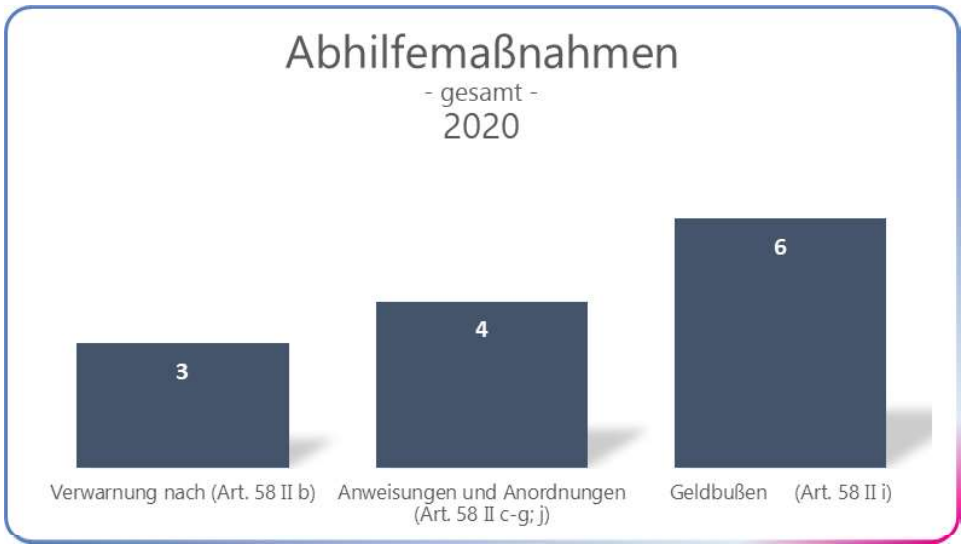

Abb. 5: Abhilfemaßnahmen (gesamt) 2020

1.5 Europäische Verfahren

Einen zunehmenden Stellenwert bei der Aufgabenwahrnehmung des Unabhängigen Datenschutzzentrums Saarland (UDZ) kommt der Zusammenarbeit mit anderen europäischen Datenschutzaufsichtsbehörden zu.

Wie bereits im letzten Tätigkeitsbericht beschrieben, enthält die Datenschutz-Grundverordnung (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	546	29
Verfahren mit Federführung Art. 56	78	1
Verfahren gem. Kapitel VII DSGVO	1453	726

Abb. 6: Europäische Verfahren (gesamt) 2020

Zu diesem Zweck hatte auch das UDZ im Jahr 2020 in 1392 Fällen zu beurteilen, inwieweit es als „betroffene Aufsichtsbehörde" im Sinne des Art. 4 Nr. 22 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 29 Fällen wurde diese Betroffenheit für das UDZ bejaht. Im Rahmen dieser Verfahren war das UDZ einmal „federführend" (Art. 56 Abs. 1 DSGVO) zuständig, so dass in diesem Verfahren die entsprechenden Verfahrenshandlungen gegenüber verantwortlichen Stellen direkt durch das UDZ vorzunehmen waren. Hierbei erfolgt eine Abstimmung mit anderen von der Verarbeitung betroffenen Datenschutzaufsichtsbehörden innerhalb der

EU. Sind diese etwa nicht mit dem Vorgehen und den durch die federführende Aufsichtsbehörde geplanten Maßnahmen einverstanden, weil sie den Sachverhalt abweichend beurteilen, haben sie die Möglichkeit, gegen den Entscheidungsentwurf der federführenden Aufsichtsbehörde Einspruch einzulegen. Bezogen auf hiesige Dienststelle wurde dabei eines der Verfahren ohne Einwände anderer europäischer Aufsichtsbehörden abgeschlossen.

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 oft 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 22 Rechtsetzungsvorhaben verfahrensbegleitend tätig.

II.

Datenschutz und Corona-Pandemie

2 Datenschutz und Corona-Pandemie

2.1 Rechtliche Grundlagen zur Kontaktnachverfolgung zur Bekämpfung der Corona-Pandemie

Die Corona-Pandemie und die damit einhergehenden Gesetze, Rechtsverordnungen und Maßnahmen zur Bekämpfung dieser Pandemie hat auch unsere Behörde intensiv beschäftigt. Im Rahmen der Anhörung nach § 19 Abs. 2 des Saarländischen Datenschutzgesetzes (SDSG) hatten wir die Möglichkeit, vor Erlass der Regelungen zur Sicherstellung einer Kontaktnachverfolgung sowie der Übermittlung personenbezogener Daten an die Gesundheitsämter gegenüber dem Gesetz- bzw. Verordnungsgeber zu den datenschutzrechtlichen Implikationen entsprechender Regelungen Stellung zu nehmen.

Für unsere erste Stellungnahme zu einer Regelung zur Kontaktnachverfolgung in der Verordnung der Landesregierung zur Bekämpfung der Corona-Pandemie (VO-CP) standen uns aufgrund der Eilbedürftigkeit nur wenige Stunden zur Verfügung. Dennoch konnten wir einige Hinweise zur datenschutzrechtlichen Einordnung und datenschutzkonformen Ausgestaltung geben, die auch (im Wesentlichen) umgesetzt wurden. Gleiches gilt für die zahlreichen Novellen der VO-CP, welche aufgrund des rasch wechselnden Infektionsgeschehens notwendig wurden. Da es sich insgesamt um einen sehr dynamischen Prozess handelte und schließlich aufgrund einer Entscheidung des Verfassungsgerichtshofes des Saarlandes ergänzend zu den Verordnungen ein Gesetz zur Kontaktnachverfolgung erlassen wurde, verzichten wir hier auf eine detaillierte Darstellung.

Im Rahmen der Anhörung durch die Landesregierung hatten wir bereits frühzeitig eine vertiefte Prüfung der Rechtsgrundlagen für die Pflicht zur Sicherstellung einer Kontaktnachverfolgung angemahnt. Denn wir hatten insbesondere Zweifel daran, dass die Verordnungsermächtigung in den §§ 32, 28 Infektionsschutzgesetz (IfSG) in der damaligen Fassung eine ausreichende

verfassungsrechtliche Grundlage für die Festlegung einer staatlich angeordneten Datenerhebungspflicht darstellte. Auf Grund der Kürze der seitens der Landesregierung eingeräumten Stellungnahmefrist mussten wir es jedoch bei einem kurzen Hinweis belassen und konnten keine abschließende Prüfung und Bewertung durchführen.

Hierzu bekamen wir im August 2020 die Möglichkeit. Im Rahmen einer Verfassungsbeschwerde, die sich – unter anderem – gegen § 3 VO-CP in der Fassung vom 21. August 2020 (Amtsbl. 2020 S. 768) und die dort vorgesehene Erhebung personenbezogener Daten richtete, wurde auch unsere Dienstelle durch den Verfassungsgerichtshof des Saarlandes um Abgabe einer Stellungnahme ersucht.

Im Rahmen unserer Stellungnahme hatten wir gegenüber dem Verfassungsgerichtshof die Auffassung vertreten, dass zum einen §§ 32, 28 IfSG in der damaligen Fassung keine ausreichende Ermächtigungsgrundlage für die Landesregierung darstelle, um eine Pflicht zur Sicherstellung der Kontaktnachverfolgung zu regeln, und dass zum anderen die damalige Regelung des § 3 VO-CP zwar eine Datenerhebungsverpflichtung für Gastronomen und Veranstalter, jedoch keine Übermittlungspflicht der so erhobenen Daten an die Gesundheitsämter (im Infektionsfall) vorsah, was wiederum Zweifel an der Geeignetheit der Datenerhebungspflicht aufwarf.

Mit Beschluss vom 28. August 2020 (Az.: Lv 15/20) hat der Verfassungsgerichtshof des Saarlandes § 3 der genannten Verordnung als mit Art 2 Satz 2 der Verfassung des Saarlandes unvereinbar erklärt. Auch das Gericht sah die sich aus §§ 32, 28 IfSG ergebende Befugnis, „die notwendigen Schutzmaßnahmen zu treffen“ – jedenfalls für den generell-abstrakten Eingriff in das Recht auf informationelle Selbstbestimmung – als zu unbestimmt an, um hierauf die sich aus einer Pflicht zur Kontaktdatenerfassung ergebenden Eingriffe in das Recht auf informationelle Selbstbestimmung zu rechtfertigen. Stattdessen forderte der Verfassungsgerichtshof in Fortsetzung seiner bisherigen Rechtsprechung, dass Eingriffe in das Recht auf informationelle

Selbstbestimmung in der Regel auf eine förmliche, parlamentarische Ermächtigung gestützt werden müssen, welche die zu erhebenden personenbezogenen Daten als solche, den Anlass und den spezifischen Zweck der Erhebung, die Art und Dauer der Aufbewahrung sowie ihre Löschung normenklar und bestimmt regelt sowie den Grundsatz der Verhältnismäßigkeit wahrt.

Auf Grund dieser Entscheidung des Verfassungsgerichtshofs wurde im September 2020 durch die Regierungsfraktionen der Entwurf eines Gesetzes in den Landtag eingebracht, das die Pflicht zur Sicherstellung einer Kontaktnachverfolgung auf eine förmliche, parlamentarische Grundlage stellen sollte.

Auch hier hatten wir die Möglichkeit, im Rahmen der parlamentarischen Anhörung zu dem geplanten Gesetzentwurf Stellung zu nehmen. Hierdurch konnten wir insbesondere erreichen, dass die schon im Gesetzentwurf vorgesehenen Verwendungsbeschränkungen und Löschverpflichtungen nochmals präzisiert und klargestellt wurden, um so eine strenge Zweckbindung der erhobenen Daten zu gewährleisten.

Aufgegriffen wurde auch unsere Forderung, die Tatbestandsvoraussetzungen der Abruf- und Übermittlungsbefugnis der erhobenen Daten durch das Gesundheitsamt zu konkretisieren und auf einen bestimmten Zeitraum zu begrenzen. Zudem hat der Gesetzgeber unseren Vorschlag übernommen, zum Schutz der Daten der Besucher eine Pflicht zur Umsetzung konkreter technischer und organisatorischer Maßnahmen bei der Verarbeitung der Daten in der Gastronomie bzw. durch Veranstalter zu normieren.

Die zur gleichen Zeit in der Öffentlichkeit diskutierte Frage, ob die in der Gastronomie und bei Veranstaltungen erhobenen Daten auch zu Strafverfolgungszwecken durch die Polizei und die Staatsanwaltschaft genutzt werden dürfen, hatten wir indes nicht aufgegriffen. Zwar sahen auch wir eine solche Nutzung kritisch, da sie die Gefahr begründete, dass die Akzeptanz der

Kontaktdatenerhebung und die Validität der Angaben der Besucher beeinträchtigt werde und so dem Ziel der Regelung, eine effektive Kontaktnachverfolgung zu gewährleisten, zuwiderliefe. Allerdings sahen wir keine Gesetzgebungsbefugnis des saarländischen Gesetzgebers, ein solches Nutzungsverbot für Strafverfolgungszwecke zu normieren.

Das Gesetz zur Kontaktnachverfolgung im Rahmen der Corona-Pandemie (Amtsbl. 2020, S. 1171, 1190) wurde am 11. November vom saarländischen Landtag verabschiedet und ist am 27. November 2020 in Kraft getreten.

Nahezu zeitgleich mit dieser gesetzlichen Neuregelung im Saarland hat der Bundesgesetzgeber am 18. November 2020 mit der Einfügung des § 28a IfSG (BGBl. I S. 2397) u. a. eine Konkretisierung der Verordnungsermächtigung auch für Maßnahmen der Kontaktnachverfolgung beschlossen. § 28a konkretisiert nunmehr die „notwendigen Schutzmaßnahmen“ und gestattet in § 28 Abs. 1 Ziffer 17 IfSG für die Dauer einer epidemischen Lage von nationaler Tragweite die Anordnung der Verarbeitung der Kontaktdaten von Kunden, Gästen oder Veranstaltungsteilnehmern, um nach Auftreten einer Infektion mit dem Coronavirus SARS-CoV-2 mögliche Infektionsketten nachverfolgen und unterbrechen zu können.

2.2 Kontaktdatenerhebung durch Gaststätten und andere Verpflichtete

Ursprünglich ausschließlich für Gastronomiebetriebe vorgesehen, hat die saarländische Landesregierung die verpflichtende Erhebung und Speicherung von Kontaktdaten von Gästen und Besuchern zur Kontaktnachverfolgung in den jeweiligen Fassungen der Verordnung zur Bekämpfung der Corona-Pandemie (VO-CP) schrittweise auf weitere Wirtschaftsbereiche ausgedehnt.

Die Pflicht zur Datenerhebung zum Zwecke der Kontaktnachverfolgung hat bei den hierzu verpflichteten Stellen zunächst erhebliche Verunsicherung hinsichtlich der Art und des Um-

fangs der zu erhebenden Daten nach sich gezogen, was in der Folge zu einem starken Anstieg der Zahl der Anfragen an unsere Dienststelle geführt hat.

Um den verantwortlichen Stellen eine Hilfestellung zur datenschutzkonformen Kontaktdatenerhebung zu geben, wurden daher auf der Webseite des Unabhängigen Datenschutzzentrums (UDZ) neben allgemeinen Informationen zu den datenschutzrechtlichen Bedingungen der diesbezüglichen Datenverarbeitung jeweils auch Muster für einen Erhebungsbogen und für die nach Art. 13 Datenschutz-Grundverordnung (DSGVO) erforderlichen Informationen für die betroffenen Personen zur Verfügung gestellt. Daneben wurden in Zusammenarbeit mit dem Dehoga Saarland Hotel und Gaststättenverband e.V. durch diese weitere Hinweise und Mustererhebungsbögen veröffentlicht.

Neben den verantwortlichen Stellen haben sich aber auch viele von der Kontaktdatenerhebung betroffene Personen mit Beschwerden hinsichtlich des Umgangs mit ihren Daten an unsere Dienststelle gewandt. Mehrfach wurde dabei eine zweckwidrige Verwendung der Kontaktdaten durch Gastronomiebetreiber für eigene, nicht mit der Corona-Kontaktnachverfolgung in Zusammenhang stehende Zwecke beklagt; daneben waren vor allem offen ausliegende Besucherlisten, denen sich die gesamte Besucherhistorie nebst Kontaktdaten entnehmen ließen, und die unsachgemäße Entsorgung von Kontaktbögen Gegenstand von Beschwerden.

Während der Schwerpunkt der Aufsichtstätigkeit zunächst auf die Sensibilisierung der Verantwortlichen für die Modalitäten der verpflichtenden Verarbeitung von Kunden- und Besucherdaten gelegt wurde, wurde im Berichtszeitraum gegen den Betreiber eines Gastronomiebetriebs, der Gästeregistrierungsformulare neben einem Altpapiercontainer entsorgte, ein Bußgeldverfahren eingeleitet.

2.3 Auskünfte über Corona-Infektionen durch die Gesundheitsämter

Zu Beginn der Corona-Pandemie im Frühjahr 2020 trat in mehreren Bundesländern die Frage auf, ob Listen von Personen, die mit dem Corona-Virus infiziert sind, vorsorglich durch die Gesundheitsämter an die Polizei übermittelt werden dürfen. Begründet wurde dieser Vorstoß mit dem Schutz der Gesundheit der Polizeibeamten im Einsatz, beispielsweise bei Personenkontrollen. Die Datenschutzaufsichtsbehörden waren sich hierbei weitgehend einig, dass es für eine solch umfangreiche Übermittlung sensibler Gesundheitsdaten ohne konkreten Anlass, also auf Vorrat, an einer datenschutzrechtlichen Grundlage fehlt. Die Frage, ob eine Auskunft im Einzelfall in bestimmten Konstellationen zulässig sein könne, wurde zunächst weitgehend offengelassen.

Im Saarland stand die Übermittlung von Listen mit infizierten Personen an die Polizei nicht im Raum.

Im August des Jahres wurden wir allerdings darüber in Kenntnis gesetzt, dass die saarländischen Gesundheitsämter gebeten werden sollten, anlassbezogen Auskünfte über Corona-Infektionen an Polizei und Staatsanwaltschaft zu erteilen. Hiervon betroffen wären Personen gewesen, bei denen Durchsuchungsmaßnahmen durch die Polizei beabsichtigt waren. Die beteiligten Beamten sollten so „vorgewarnt" werden, um sich besser schützen zu können.

Die Information über das Bestehen einer Corona-Infektion stellt ein Gesundheitsdatum im Sinne von Art. 4 Nr. 15 Datenschutz-Grundverordnung (DSGVO) dar. Gesundheitsdaten dürfen nur verarbeitet werden, wenn eine der Voraussetzungen aus Art. 9 Abs. 2 DSGVO erfüllt ist. In Betracht kommt vorliegend Art. 9 Abs. 2 lit. i DSGVO, wonach die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit auf der Grundlage des Rechts eines Mitgliedstaates zulässig sein kann. Eine solche Rechtsgrundlage findet sich im saarländischen

Gesetz über den öffentlichen Gesundheitsdienst (Gesundheitsdienstgesetz – ÖGDG), wo § 19 Abs. 3 Vorgaben zur Übermittlung personenbezogener Daten enthält. Demnach ist eine Übermittlung durch die Stellen des öffentlichen Gesundheitsdienstes unter anderem dann zulässig, wenn dies zur Abwehr einer Gefahr für Leben, Gesundheit oder Freiheit einer dritten Person erforderlich ist und die Gefahr nicht auf andere Weise beseitigt werden kann (§ 19 Abs. 3 Nr. 3 i. V. m. Abs. 2 S. 1 Nr. 3 ÖGDG).

Dass durch den Kontakt mit einer Person, die mit dem Corona-Virus infiziert ist, die Gesundheit der ermittelnden Polizeibeamten gefährdet werden kann, dürfte unstrittig sein. Eine vorherige Information über den Infektionsstatus kann ein Mittel sein, diese Gefahr zu reduzieren. Dass sie aber erforderlich ist, weil keine milderen Mittel zur Verfügung stehen, um die Gefahr auf andere Weise zu minimieren, erschließt sich nicht. So ist davon auszugehen, dass derzeit wie in allen anderen Lebensbereichen auch bei der Durchführung polizeilicher Maßnahmen verstärkt auf Eigenschutz und Hygiene geachtet wird. Das Tragen von Mund-Nasen-Bedeckungen sowie von Handschuhen dürfte obligatorisch sein, gegebenenfalls ergänzt durch Schutzkleidung. Ebenso sollte es in der Regel möglich sein, während einer Durchsuchung den gebotenen Abstand zur betroffenen Person einzuhalten. Da nach derzeitigem Erkenntnisstand viele Infektionen symptomfrei verlaufen, muss aktuell ohnehin immer auch mit dem Vorliegen einer (noch) unerkannten Infektion gerechnet werden, so dass entsprechende Schutzmaßnahmen zu treffen sind.

Von einer Erforderlichkeit einer vorherigen Information ist insoweit nicht auszugehen, da die Einsatzkräfte auch auf andere Weise geschützt werden können.

Auch ein Rückgriff auf die Vorschrift des § 8 Abs. 1 Nr. 4 Saarländisches Datenschutzgesetz (SDSG), wonach eine Verarbeitung besonderer Kategorien personenbezogener Daten zulässig ist, soweit es aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit und des Infektionsschutzes

erforderlich ist, kann hier nicht in Betracht kommen, da es aus den bereits aufgeführten Gründen an der Erforderlichkeit fehlt.

Im Ergebnis hat das saarländische Gesundheitsministerium als für die Gesundheitsämter zuständige Fachaufsichtsbehörde unsere Einschätzung geteilt und hat mitgeteilt, man werde die Gesundheitsämter entsprechend informieren.

Fazit/ Empfehlung:

Auch nach Einschätzung des saarländischen Gesundheitsministeriums ist die Übermittlung von Auskünften über eine Infektion mit dem Corona-Virus durch Gesundheitsämter an Ermittlungsbehörden datenschutzrechtlich unzulässig.

2.4 Nutzung von Corona-Kontaktlisten durch die Polizei

Die saarländische Verordnung zur Bekämpfung der Corona-Pandemie (VO-CP) verpflichtete in ihren Fassungen vom 29. Mai bis zum 27. November 2020 Betreiber von zahlreichen Betrieben, Einrichtungen oder Veranstaltungen dazu, eine Kontaktnachverfolgung ihrer Gäste zu gewährleisten. Aus der Presse erfuhren wir zu Beginn des Monats August, dass es durch die saarländische Polizei in insgesamt vier Fällen zu einer Nutzung von Gästedaten, die auf der Grundlage der vorgenannten Verordnung zur Nachverfolgung von Infektionsketten geführt werden müssen, kam.

Aus datenschutzrechtlicher Sicht stellte sich die Frage, ob personenbezogene Daten, die ausschließlich zur Nachverfolgung von Infektionsketten und zur Eindämmung der Corona-Pandemie erhoben werden, von der Polizei auch für deren Aufgaben genutzt werden dürfen, wobei zwischen präventivem und repressivem Handeln zu unterscheiden ist.

Die in der VO-CP enthaltene Pflicht zur Kontaktnachverfolgung regelte hinsichtlich des Umfangs der zu erfassenden personenbezogenen Daten: "Die Betreiber, Veranstalter oder sonstigen Verantwortlichen haben geeignete Maßnahmen zur vollständigen Nachverfolgbarkeit sicherzustellen. Hierzu gehört die Erfassung je eines Vertreters der anwesenden Haushalte mit Vor- und Familienname, Wohnort und Erreichbarkeit und der Ankunftszeit."

Diese staatlich veranlasste Erhebung der Kontaktdaten durch private Stellen stellt einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht aller Kunden dar. Durch die Verknüpfung der erhobenen Kontaktdaten mit der Information, wer sich wann an welchem Ort aufgehalten hat, kann nicht nur das gesamte Freizeitverhalten der Bürger nachvollzogen werden, sondern es werden auch Einblicke in ganz sensible Bereiche, wie familiäre Verhältnisse, religiöse oder weltanschauliche Überzeugungen bis hin zu der sexuellen Orientierung gegeben.

In der VO-CP war ausdrücklich vorgesehen, dass die erhobenen Daten nicht zu einem anderen Zweck als der Aushändigung auf Anforderung an die Gesundheitsämter verwendet werden dürfen. Auch die Tatsache, dass sich die Regelungen zur Kontaktnachverfolgung der VO-CP auf das Infektionsschutzgesetz (IfSG) des Bundes in der Fassung vom 27.03.2020 stützten, zeigt, dass die Kontaktnachverfolgung ausschließlich eine Weiterverbreitung der Pandemie verhindern soll und die erhobenen Daten einer engen Zweckbindung unterliegen sollen.

Weder die VO-CP noch das Saarländische Polizeigesetz (SPolG) enthielten Regelungen, die die Nutzung der erhobenen Kontaktdaten durch die Polizei für gefahrenabwehrrechtliches, präventives Handeln zugelassen hätten.

Soweit aber das Handeln der Polizei der Strafverfolgung diente und damit in einem Ermittlungsverfahren erfolgte, finden sich Befugnisse zur Einsichtnahme der Kontaktlisten in der Strafprozessordnung (StPO) in § 161 (Allgemeine Ermittlungsbefugnis),

§ 163 (Sachverhaltserforschung durch die Polizei) oder § 94 (Sicherstellung, Beschlagnahme).

Die bundesrechtlichen Regelungen der StPO gingen aufgrund des Geltungsvorranges des Bundesrechts vor Landesrecht gemäß Art. 31 Grundgesetz (GG) den Bestimmungen der VO-CP vor. Mithin konnte die vorgenannte enge Zweckbindung in der VO-CP diese Regelungswirkung der bundesrechtlichen Vorschriften der Strafprozessordnung nicht durchbrechen. Daher war im Ergebnis ein Zugriff der Polizei auf die Kontaktdaten im Rahmen von Ermittlungsverfahren nach der damaligen Rechtslage durchaus als zulässig zu bewerten.

Mit Blick auf den dennoch erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen haben wir angeregt, dass vor jedem Zugriff durch die Polizei eine sorgfältige Verhältnismäßigkeitsprüfung mit vorheriger richterlicher Prüfung der Maßnahme erfolgen sollte.

Dies hätte angesichts der in der VO-CP formulierten strikten Zweckbindung für die erhobenen Kontaktdaten auch den Betreibern der Betriebe hinsichtlich einer möglichen Datenweitergabe an die Polizei Rechtssicherheit gegeben.

Unabhängig von der Rechtmäßigkeit des polizeilichen Zugriffs auf die Daten kann es zudem zu einem Vertrauensverlust führen, wenn die ausweislich der Verordnung ausschließlich zur Pandemiebekämpfung erhobenen Daten auch zu anderen Zwecken genutzt werden können. Allein die Unsicherheit, ob und ggf. welche anderen Stellen ebenfalls auf die Daten zugreifen dürfen, könnte manche Menschen davon abhalten, ihre Kontaktdaten wahrheitsgemäß anzugeben.

Durch das Inkrafttreten des § 28a IfSG zum 19. November 2020 ist hier nunmehr Rechtsklarheit geschaffen worden.

§ 28a Abs. 4 IfSG regelt den Umfang der zulässig erhebbaren Kontaktdaten und die Verantwortlichkeiten der Datenverarbeitung. Nach Satz 3 dieser Vorschrift unterliegen die Daten einer strengen Zweckbindung und dürfen nach Satz 3 nicht zu einem

anderen Zweck als der Aushändigung auf Anforderung an die nach Landesrecht für die Erhebung der Daten zuständigen Stellen verwendet werden. Damit ist nunmehr bundesgesetzlich eindeutig festgelegt, dass die Kontaktdaten durch die Polizei weder zu Zwecken der Strafverfolgung noch zu gefahrenabwehrrechtlichen Zwecken verwendet werden dürfen.

Das im Saarland in Umsetzung der Entscheidung des Verfassungsgerichtshofs des Saarlandes vom 28. August 2020 (Az.: Lv 15/20) am 27. November 2020 in Kraft getretene Covid-19-Kontaktnachverfolgungsgesetz sieht ebenso wie § 28a Abs. 4 Satz 5 IfSG ausdrücklich vor, dass die erhobenen Daten nur zum Zwecke der Nachverfolgung von Infektionsketten an die Gesundheitsämter übermittelt werden dürfen.

Eine Weitergabe der übermittelten Daten durch die Gesundheitsämter oder eine Weiterverwendung durch diese auch zu anderen Zwecken als der Kontaktnachverfolgung ist mithin nunmehr generell ausgeschlossen.

2.5 Datenübermittlung von Hotelgastdaten

Aufgrund des Umstands, dass von staatlicher Seite insbesondere die Nachverfolgung potentieller Infektionskontakte (Infektionsketten) als wesentlicher Bestandteil einer erfolgreichen Bekämpfung des Infektionsgeschehens angesehen wurde – und nach wie vor wird –, mussten insbesondere in der Anfangszeit der Pandemie von staatlicher und privater Seite unter hohem Zeitdruck Lösungen zur Kontaktnachverfolgung gefunden werden, von denen manche sich letztlich als nicht mit den datenschutzrechtlichen Bestimmungen vereinbar erwiesen.

In diesem Zusammenhang wurde unsere Behörde Ende März 2020 auf die Datenerhebung einer Kommunalverwaltung im Zuge der Beherbergung von Hotelgästen aufmerksam gemacht, für welche keine Rechtsgrundlage (Verarbeitungsgrundlage) existierte und die daraufhin einzustellen war.

Zum besseren Verständnis sind die pandemiebezogenen landesrechtlichen Regelungen im Hotelgewerbe in Bezug zu nehmen, die zum damaligen Beurteilungszeitraum Ende März 2020 in Kraft waren.

Gemäß Nr. 1 der damaligen Allgemeinverfügung zum Vollzug des Infektionsschutzgesetzes (Anpassung der Allgemeinverfügungen vom 16.3.2020 und vom 20.03.2020) des Ministeriums für Soziales, Gesundheit, Frauen und Familie vom 25.03.2020[1], wurde der Betrieb von Hotels, Beherbergungsbetrieben und Campingplätzen sowie die Zurverfügungstellung jeglicher Unterkünfte zu privaten touristischen Zwecken untersagt. Als Ausnahme zulässig war der Betrieb "*zu beruflich veranlassten erforderlichen Reisen*" oder "*bei Vorliegen unabweisbarer persönlicher Gründe der Reisenden*".

Zum Nachweis der jeweiligen Gründe genügte deren Glaubhaftmachung, etwa in Form einer schriftlichen Versicherung oder mittels Bescheinigung des Arbeitgebers. Zur Überprüfung der Vorgaben waren die Ortspolizeibehörden sodann u. a. befugt, Vor-Ort-Kontrollen durchzuführen, bei welchen auch die betreffenden Dokumente eingesehen werden konnten.

Eine saarländische Kommune sah es in Auslegung vorgenannter Verordnung zudem als erforderlich an, sich von den Hotel- und Beherbergungsbetreibern die Buchungen und Belegungen von Unterkünften schriftlich anzeigen zu lassen. Die Datenerhebung sollte hierbei – vermutlich zu Zwecken einer antizipierten Kontrollmöglichkeit – bereits im Vorfeld der eigentlichen Beherbergung stattfinden.

In diesem Zusammenhang sollten die Personalien der Gäste (Name, Geburtsdatum und -ort, private Anschrift), der Zeitraum

[1] Elektronisch abrufbar unter: https://corona.saarland.de/DE/service/downloads/_documents/corona-verfuegungen/dld_2020-03-25-allgemeinverfuegung.pdf?__blob=publicationFile&v=1 (letzter Zugriff: 08.12.2020).

der Buchung sowie deren Anlass von dem Hotelier mittels vorgegebenen Formblättern der Kommunalverwaltung übermittelt werden.

Ungeachtet des Umstands, dass eine derartig weitgehende Datenübermittlung die Kontrolle der Einhaltung der pandemiebedingten Schutzvorschriften im Hotelgewerbe vielleicht erleichtern und zu effektivieren vermag, ist festzustellen, dass sie weder zum damaligen noch zum heutigen Zeitpunkt eine Grundlage im Gesetz fand bzw. findet.

§ 29 des Bundesmeldegesetzes (BMG) enthält bereichsspezifische besondere Meldepflichten in Beherbergungsstätten, welche allesamt den Zeitpunkt der Ankunft bzw. Aufnahme einer Person in einer Beherbergungsstätte in Bezug nehmen. Insbesondere der nach § 29 Abs. 2 BMG von den Gästen auszufüllende Meldeschein kann den zuständigen Behörden im Bedarfsfall Auskunft über Identität und Herkunft der Gäste geben.

Eine Datenerhebung, welche eine allgemeine Übermittlung von Hotelgastdaten bereits zum Zeitpunkt der Buchung zum Gegenstand hat, greift dagegen tief in persönlichkeits- und datenschutzrechtliche Positionen der betroffenen Personen ein. Insbesondere in Verbindung mit dem Beherbergungsanlass würde sie weitreichende Einblicke in die persönlichen Lebensverhältnisse von Personen, bis hin zur Erstellung von Bewegungsprofilen, ermöglichen.

Auch in Zeiten einer Pandemie oder eines vergleichbaren Krisenfalls kann eine solch weitgehende Datenverarbeitung nach hiesiger Rechtsauffassung nicht auf untergesetzlicher Ebene geregelt werden, sondern bedürfte einer bereichsspezifischen normativen Grundlage in Form eines Parlamentsgesetzes.

2.6 Apps zur Gestaltung des digitalen Unterrichts

Durch die erforderliche Umstellung des Präsenzunterrichts auf Homeschooling haben engagierte Lehrkräfte zur Aufrechterhaltung des Unterrichts ihre Schüler dazu verpflichtet, bestimmte Apps auf ihren Endgeräten zu installieren. Nicht alle Apps sind

jedoch datenschutzkonform gestaltet und übermitteln beispielsweise ohne die Einwilligung der Nutzer Daten in unsichere Drittländer. Was bei der Datenübermittlung in datenschutzrechtlich unsichere Drittländer zu beachten ist, kann im Kapitel 3.1 dieses Tätigkeitsberichts zum sogenannten Schrems II-Urteil des EuGH nachgelesen werden.

Bevor spezielle Apps im Unterricht eingesetzt werden können, ist deshalb zu prüfen, welche rechtlichen Voraussetzungen eingehalten werden müssen. Diese Prüfung sollte in Abstimmung mit dem Ministerium für Bildung und Kultur und dem zuständigen behördlichen Datenschutzbeauftragten erfolgen, damit sichergestellt wird, dass nur datenschutzrechtlich unbedenkliche Apps Einzug ins digitale Klassenzimmer erhalten. Dabei sind beispielsweise sowohl die Vorgaben zur Auftragsverarbeitung gem. Art. 28 der Datenschutz-Grundverordnung (DSGVO) als auch Vorgaben aus § 15 Saarländisches Datenschutzgesetz (SDSG) im erforderlichen Freigabeverfahren zu beachten.

Fazit/ Empfehlung:

Auch wenn es viele Apps zur Gestaltung eines digitalen Unterrichts gibt, sind die rechtlichen Voraussetzungen im Vorfeld des Einsatzes durch den Verantwortlichen zu prüfen.

2.7 Online Schule Saar (OSS)

Die Online Schule Saar (OSS) wurde vom Ministerium für Bildung und Kultur als Plattform für Schüler und Lehrer zum Homeschooling entwickelt. Sie umfasst vom strukturierten Bereitstellen von Lern-Materialien über geführte Lernsettings mit Kurscharakter, Tests und Leistungskontrollen bis hin zu komplexen freien und individualisierten Lernarrangements mit starken

sozialen Komponenten eine Vielzahl von Möglichkeiten und pädagogischen Freiräumen.[2]

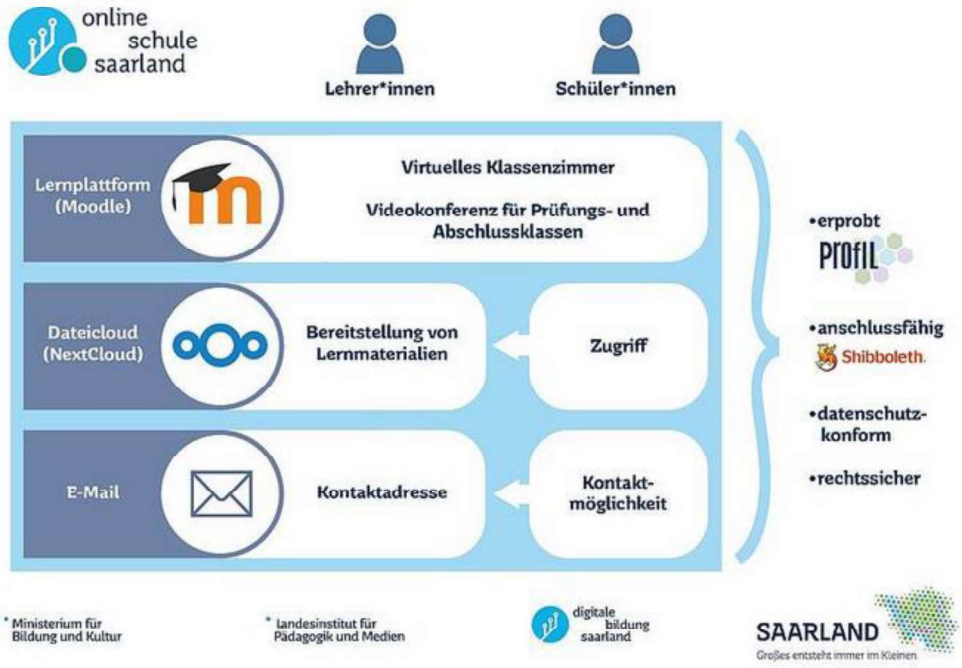

Abb. 7: Die Zusammensetzung der Online Schule Saar aus verschiedenen Komponenten
Quelle: Ministerium für Bildung und Kultur Saarland

Grundstein der OSS war die sogenannte Profil-Plattform, die in Zusammenarbeit mit unserer Dienststelle entwickelt wurde, um eine schulübergreifende Zusammenarbeit zu ermöglichen. So konnten Lernmaterialien unter den Schulen ausgetauscht und gemeinsame Projekte in einer Klassenstufe zu einem Thema organisiert und durchgeführt werden.

Bedingt durch die Corona-Pandemie musste schnellstmöglich ein Werkzeug bereitgestellt werden, das Lehrern und Schülern das Arbeiten im Homeoffice ermöglicht. Dazu erfolgte eine Erweiterung der Profil-Plattform, die den saarländischen Schulen zur Verfügung gestellt wurde. War der ursprüngliche Zweck der

[2] Auszug aus der Online-Vorstellung des Ministeriums für Bildung und Kultur zur OSS.

Profil-Plattform eine schulübergreifende Zusammenarbeit, musste nun auf eine schulinterne Zusammenarbeit mit einer großen Anzahl an Nutzern umgestellt werden. Diese Umstellung führte nicht nur zu anfänglichen Kapazitätsproblemen, da die Plattform nicht für so viele User ausgelegt war, sondern auch zu datenschutzrechtlichen Problemen, die vom Ministerium gelöst werden mussten.

Aufgrund der schulübergreifenden Grundstruktur der Profil-Plattform als Vorgänger der OSS konnte man Lerngruppen aus allen an der Profil-Plattform angeschlossenen Schulen erstellen. Dieses Zugriffs- und Berechtigungskonzept, das durch eine Einwilligung datenschutzrechtlich legitimiert wurde, konnte bei der Umstellung zur OSS nicht mehr beibehalten werden. Es musste daher ein Konzept entwickelt werden, mit dem gewährleistet werden konnte, dass jede Schule lediglich auf ihre eigenen Schüler- und Lehrerdaten zugreifen kann. Dies hat aufgrund der Notwendigkeit, zunächst eine funktionierende Plattform zur Verfügung zu stellen, zwar etwas Zeit in Anspruch genommen, letztendlich wurde jedoch ein datenschutzkonformes Zugriffs- und Berechtigungskonzept entwickelt und umgesetzt.

Als Rechtsgrundlage für die Verarbeitung der Schuldaten innerhalb der OSS konnte aufgrund der coronabedingten Umstellung auf Homeschooling auch nicht mehr auf die Einwilligung der Betroffenen zurückgegriffen werden. Die Erfüllung des Unterrichts- und Erziehungsauftrages konnte eben teilweise nur noch per Homeschooling erfüllt werden, so dass die damit zusammenhängende Datenverarbeitung durch die Regelung des § 2 der Verordnung über die Verarbeitung personenbezogener Daten in den Schulen (PersDatSchulV SL) legitimiert werden konnte.

Fazit/ Empfehlung:

Das Ministerium für Bildung und Kultur hat den Betroffenen in Abstimmung mit unserer Dienststelle ein datenschutzkonformes Werkzeug an die Hand gegeben, um Homeschooling umsetzen zu können.

2.8 Hackerangriff auf die HPI-Cloud einer Schule

Im Mai 2020 wies uns ein anonymer Beschwerdeführer auf Sicherheitslücken in der Schul-Cloud des Hasso-Plattner-Instituts (HPI) hin. Die Schul-Cloud ermöglicht die Vorbereitung von digitalen Unterrichtseinheiten und wurde im Anfangsstadium der Corona-Pandemie als ein Werkzeug ausgebaut, das es Schülern und Lehrern ermöglicht, Homeschooling effektiv umzusetzen. Die HPI-Cloud wurde mit Fördermitteln der Bundesregierung entworfen und sollte schon vor Ausbruch der Pandemie als bundesweit einheitliche Cloud-Lösung für Schulen angeboten werden. Zum Zeitpunkt der Beschwerde nutzten fünf saarländische Schulen die Schul-Cloud des Hasso-Plattner-Instituts.

Als Beleg für seine Behauptungen fügte der Beschwerdeführer seinen Ausführungen eine Liste mit 103 Namen bei, die seiner Darstellung nach aus der HPI-Schul-Cloud einer saarländischen Schule stammten. Nachdem der Rektor der entsprechenden Schule die Namen der Schüler verifizieren konnte, haben wir unverzüglich das hiesige Ministerium für Bildung und Kultur sowie die für die datenschutzrechtliche Aufsicht über das HPI zuständige Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg (LDA) als auch alle anderen Datenschutz-Aufsichtsbehörden in Deutschland über die dargestellte Sicherheitslücke der bundesweit eingesetzten Schul-Cloud informiert.

Das Ministerium reagierte umgehend und untersagte den Schulen die weitere Nutzung der HPI-Cloud bis zur abschließenden Klärung des Vorfalls. Die betroffenen Schulen handelten ebenso umsichtig und baten das HPI, die Schul-Cloud bis zur Klärung des Sachverhaltes abzuschalten. Diesem Anliegen folgte das HPI und schaltete die HPI-Schul-Cloud für alle saarländischen Schulen ab.

Bei der Klärung des Vorfalls teilte uns das Hasso-Plattner-Institut mit, dass sich der Angreifer über eine Sicherheitslücke im System einen eigenen Schüleraccount anlegen und über eine weitere Funktion Zugriff auf alle an der Schule gemeldeten Teilnehmerdaten in der HPI-Cloud erlangen konnte. Auch zeitlich konnte der Angriff nachvollzogen werden. Das HPI konnte im weiteren Verlauf feststellen, dass bundesweit 13 Schulen einem solchen Angriffsszenario ausgesetzt waren.

Aus der Presse sowie zuletzt auch vom HPI selbst war zu entnehmen, dass es sich bei dem Angriff um ein gezieltes Vorgehen gehandelt hat, durch das Spezialisten Sicherheitslücken in der von der Bundesregierung geförderten HPI-Cloud aufdecken wollten.

Im weiteren Verlauf wurden wir auf unsere Nachfrage zum Vorfall durch das Hasso-Plattner-Institut leider nur unzureichend informiert. Zwar wurde zwei Tage später eine weitere Sicherheitslücke gemeldet, über die Daten, die über ein Ticketsystem von den Schulen an das HPI gesandt worden waren, abgefangen und eingesehen werden konnten. Letztendlich musste das HPI uns auf mehrfache Nachfrage jedoch insgesamt 19 aufgedeckte Sicherheitslücken eingestehen.

Befremdlich war in diesem Zusammenhang insbesondere, dass trotz Kenntnis offener Sicherheitslücken sowohl gegenüber der Presse als auch gegenüber den betroffenen Schulen der Eindruck vermittelt wurde, ein datenschutzkonformer Zustand sei jedenfalls schon früher wieder hergestellt worden und unsere Dienststelle habe die erneute Nutzung der Schul-Cloud ohne sachlichen Grund verzögert.

Erst als uns glaubhaft durch das HPI versichert und nachgewiesen wurde, dass keine weiteren ausnutzbaren Sicherheitslücken bekannt seien und nunmehr von einem datenschutzkonformen Zustand auszugehen sei, haben wir diese Information unverzüglich an das hiesige Ministerium für Bildung und Kultur weitergeleitet mit der Anmerkung, dass aus unserer Sicht nunmehr keine Bedenken gegen eine weitere Nutzung der Schul-Cloud bestehen würden.

Gemäß Artikel 57 Abs. 1 Datenschutz-Grundverordnung (DSGVO) i. V. m. § 19 Saarländisches Datenschutzgesetz (SDSG) ist es unsere Aufgabe, die Einhaltung datenschutzrechtlicher Vorgaben auch bei den öffentlichen Stellen in unserem Bundesland zu kontrollieren und durchzusetzen. Dabei ist es uns ein besonderes Anliegen, gerade auch die Daten von Kindern und Jugendlichen gut geschützt zu wissen.

Es war daher die logische Konsequenz, nach Bekanntwerden der Sicherheitslücken beim HPI das Ministerium für Bildung und Kultur umgehend darauf hinzuweisen, dass der Betrieb der HPI-Cloud bis zur Wiederherstellung eines datenschutzkonformen Zustands zu untersagen ist. Dies war gerade in dieser Situation, in der Schulen auf die Nutzung solcher Systeme angewiesen waren, ein harter, aber konsequenter Schritt, um die Daten der Schülerinnen, Schüler und Lehrkräfte vor weiteren unbefugten Zugriffen zu schützen.

Fazit/ Empfehlung:

Die enge Zusammenarbeit zwischen dem Ministerium für Bildung und Kultur und unserer Dienststelle führte dazu, dass auf die bekannt gewordenen Sicherheitslücken schnell reagiert werden konnte und damit weitere unbefugte Zugriffe auf Schüler- und Lehrerdaten vermieden werden konnten.

2.9 Corona-Auswirkungen und Beschäftigtendatenschutz

2.9.1 Homeoffice

Viele Arbeitnehmer mussten während der Corona-Pandemie ihren herkömmlichen Arbeitsplatz gegen einen Homeoffice-Arbeitsplatz eintauschen. Damit einhergehend sind jedoch auch datenschutzrechtliche Aspekte zu beachten.

Der Arbeitgeber bleibt auch bei der Datenverarbeitung im Homeoffice weiterhin Verantwortlicher im Sinne des Art. 4 Nr. 7 Datenschutz-Grundverordnung (DSGVO) und hat die Mittel zur Verfügung zu stellen, die für ein datenschutzkonformes Arbeiten im Homeoffice erforderlich sind. Insbesondere müssen technische und organisatorische Maßnahmen gem. Art. 25 Abs. 1, 32 Abs. 1 DSGVO ergriffen werden, um die verarbeiteten personenbezogenen Daten vor unbefugten Zugriffen zu schützen. Maßnahmen beispielsweise zur Zugangskontrolle sind im Homeoffice ebenso zu berücksichtigen wie am herkömmlichen Arbeitsplatz. So muss bei der Verwendung eines dienstlichen Laptops dieser mit einem sicheren Passwort vor unbefugten Zugriffen geschützt sein; dies gilt im Unternehmen gegenüber Arbeitskollegen wie auch im Homeoffice beispielsweise gegenüber dem Ehepartner. Auch müssen personenbezogene Unterlagen so aufbewahrt werden, dass keine Unbefugten darauf zugreifen können (bspw. abschließbarer Container, abschließbares Arbeitszimmer, ...).

Besonderen Wert muss der Verantwortliche auf die Datenübertragungswege legen, die bei digitaler Übertragung durch geeignete Verschlüsselungstechniken datenschutzkonform gestaltet werden können. Aber auch der analoge Datentransfer von der Arbeitsstätte zum Homeoffice muss datenschutzkonform umgesetzt werden. Dass dies nicht immer umgesetzt wird, haben Datenpannenmeldungen gezeigt, mit denen zum Beispiel der Verlust ganzer Patientenakten nach einem Diebstahl einer auf dem Beifahrersitz gelagerten Tasche auf dem Parkplatz eines Einkaufszentrums gemeldet wurde.

Besondere Risiken bestehen beim Einsatz privater Endgeräte der Beschäftigten zu dienstlichen Zwecken (BYOD). Die verwendeten Endgeräte unterliegen nicht dem Einfluss und der Kontrolle des Arbeitgebers als verantwortlicher Stelle. Ob der Beschäftigte auf seinen privaten Endgeräten aktuelle Software (Virenscanner, Firewall, …) einsetzt, die vor unbefugten Zugriffen auf personenbezogene Daten des Arbeitgebers schützen soll, kann der Verantwortliche nicht mehr kontrollieren. Von der dienstlichen Nutzung privater Endgeräte wird deshalb aus datenschutzrechtlicher Sicht abgeraten. Bei firmeneigenen Geräten können die erforderlichen Maßnahmen hingegen (beispielsweise durch ein Mobil-Device-Management) zentral und umfassend gesteuert werden.

Um die Arbeit im Homeoffice rechtssicher gestalten zu können, empfehlen wir den Abschluss einer Betriebsvereinbarung bzw. die Implementierung einer Homeoffice-Richtlinie, die den gesamten Prozess der Arbeit im Homeoffice rechtlich begleitet und klare und verständliche Vorgaben zur Arbeit im Homeoffice gibt. Neben verpflichtenden Sensibilisierungsveranstaltungen zum datenschutzgerechten Arbeiten im Homeoffice sollten etwaige Kontrollmechanismen der Beschäftigten als auch zu treffende technische und organisatorische Maßnahmen hierbei in verständlicher Form festgehalten werden.

Fazit/ Empfehlung:

Arbeitgeber sollten ihre Beschäftigten für die zusätzlichen datenschutzrechtlichen Risiken im Homeoffice sensibilisieren und geeignete Maßnahmen treffen, um die erforderliche Datenverarbeitung datenschutzkonform zu gestalten. Eine Betriebsvereinbarung bzw. eine Homeoffice-Richtlinie zu dieser Thematik ist empfehlenswert.

2.9.2 Welche Daten darf der Arbeitgeber im Zusammenhang mit Corona verarbeiten?

Häufig wurden wir von Unternehmern kontaktiert, die uns fragten, welche Möglichkeiten sie haben, von einer Corona-Erkrankung der Beschäftigten zu erfahren, welche Daten sie dabei verarbeiten dürfen und wie sie diese Information innerhalb des Unternehmens nutzen können.

Bei der Information über eine mögliche Infektion eines Beschäftigten mit dem Corona-Virus handelt es sich um ein Gesundheitsdatum im Sinne des Art. 4 Nr. 15 Datenschutz-Grundverordnung (DSGVO), da Rückschlüsse auf den Gesundheitszustand des Beschäftigten möglich sind. Die Verarbeitung von Gesundheitsdaten unterliegt den besonderen Schutzanforderungen nach Art. 9 der DSGVO. Demnach ist die Verarbeitung dieser Daten grundsätzlich verboten, es sei denn, ein in der Norm genannter Ausnahmetatbestand wird erfüllt.

Die Berechtigung zur Verarbeitung personenbezogener Beschäftigtendaten ergibt sich allgemein im nicht-öffentlichen Bereich aus Art. 88 DSGVO i. V. m. § 26 Abs. 1 BDSG sowie den einschlägigen tarif-, arbeits- und sozialrechtlichen Regelungen des nationalen Rechts.

Soweit Gesundheitsdaten im Beschäftigungsverhältnis verarbeitet werden, kann diese Datenverarbeitung durch § 26 Abs. 3 BDSG und Art. 9 Abs. 2 lit. b) DSGVO legitimiert werden.

Zur Unterbrechung von Infektionsketten und zur Eindämmung der Corona-Pandemie dürfen demnach Daten von Beschäftigten verarbeitet werden. Dies muss dem Schutz der Beschäftigten dienen und die Daten müssen dem Grundsatz der Verhältnismäßigkeit folgend datenschutzkonform erhoben und verarbeitet werden.

Davon ist in folgenden Fällen auszugehen:

1. Eine Infektion wurde beim Beschäftigten festgestellt oder es hat ein Kontakt mit einer nachweislich infizierten Person stattgefunden.

2. Es lag ein Aufenthalt in einem vom Robert-Koch-Institut als Risikogebiet eingestuften Gebiet vor.

Die Offenlegung personenbezogener Daten von nachweislich infizierten oder unter Infektionsverdacht stehenden Personen zur Information von Kontaktpersonen ist demgegenüber nur rechtmäßig, wenn die Kenntnis der Identität für die Vorsorgemaßnahmen der Kontaktpersonen ausnahmsweise erforderlich ist. Meist ist der Hinweis ausreichend, dass ein Beschäftigter an Covid-19 erkrankt ist, und es müssen nur die betroffenen Kontaktpersonen im Unternehmen ohne Namensnennung des Erkrankten informiert werden. Ist jedoch die Kontaktkette im Unternehmen nicht nachvollziehbar, ist im Einzelfall bei nachgewiesener Infektion die Nennung des Namens des Erkrankten zulässig, damit sich alle Kontaktpersonen beim Arbeitgeber melden können, um eine weitere Verbreitung der Infektion schnellstmöglich unterbinden zu können.

Der Arbeitgeber ist im Rahmen der Fürsorgepflicht gem. § 618 Bürgerliches Gesetzbuch (BGB) und § 3 Abs. 1 Arbeitsschutzgesetz (ArbSchG) dazu verpflichtet, den Gesundheitsschutz der Gesamtheit seiner Beschäftigten sicherzustellen. Hierzu zählt auch die angemessene Reaktion auf die pandemische Verbreitung des Corona-Virus, die insbesondere der Vorsorge und der Nachverfolgbarkeit der Kontaktpersonen dient. Die Daten müssen vertraulich behandelt und ausschließlich zweckgebunden verwendet werden. Nach Wegfall des jeweiligen Verarbeitungszwecks sind die erhobenen Daten unverzüglich zu löschen.

Fazit/ Empfehlung:

Wir empfehlen den Arbeitgebern, eine transparente Vorgehensweise im Umgang mit einer Corona-Infektion im Unternehmen und die dazu erforderlichen Maßnahmen schriftlich zu fixieren und zu veröffentlichen. Dies führt bei den Beschäftigten zu einer höheren Akzeptanz und Bereitschaft, im Kampf gegen die weitere Verbreitung des Virus mitzuhelfen.

2.10 Einsatz von Thermalkameras

Eine Presseanfrage hatte im Berichtszeitraum die Befassung mit der Zulässigkeit eines bei einem Lebensmitteleinzelhändler eingesetzten Kamerasystems mit Temperaturdetektion zur vermeintlichen Erkennung einer SARS-CoV-2-Infektion zur Folge. Das System war als Monitoring ausgestaltet, welches Kunden im Eingangsbereich mittels Kamera erfasste, auf einem Monitor als Live-Bild darstellte und diese Darstellung um eine grafische Angabe der detektierten Temperatur ergänzte. Durch Warnhinweis wurde ein im Eingangsbereich eingesetzter Mitarbeiter des Einzelhändlers beziehungsweise des beauftragten Sicherheitsdienstes darauf aufmerksam gemacht, dass eine Temperatur detektiert wird, die einen festgelegten Referenzbereich verlässt. In der Presseanfrage wurde dargestellt, dass aufgrund der geltenden zahlenmäßigen Besucherbeschränkung vor dem Markt wartende Kunden einer erheblichen Sonnenstrahlung ausgesetzt waren und somit eine Vielzahl falschpositiver Ergebnisse detektiert wurden. Die Kunden sahen sich dabei gegenüber dem abgestellten Personal des Einzelhändlers in Hör- und Sichtweite der übrigen wartenden Kunden gezwungen, Auskünfte zu ihrem Gesundheitszustand zu geben, um den Markt betreten zu können. Da der Sachverhalt ein erhebliches mediales Echo auslöste, hat der Einzelhändler die Wärmebildkamera unmittelbar nach Einleitung eines Verwaltungsverfahrens durch hiesige Aufsichtsbehörde demontiert.

Ein solcher Thermalkameraeinsatz ließe sich im Hinblick auf die damit verbundene Verarbeitung von Gesundheitsdaten im Sinne des Art. 4 Nr. 15 i. V. m. Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO) jedes einzelnen Kunden durch den Betreiber eines Lebensmittelmarktes als essentieller Bereich der Daseinsvorsorge datenschutzrechtlich nicht nach Art. 9 Abs. 2 DSGVO und Art. 6 Abs. 1 DSGVO legitimieren. Soweit als Zweck der Schutz der Kunden und Mitarbeiter vor einer Infektion mit SARS-CoV-2 angeführt wird, ist eine derartige Temperaturde-

tektion zudem angesichts einer Vielzahl prä- oder asymptomatisch infizierter Personen als Schutzmaßnahme nicht geeignet.[3] Für eine Vielzahl von Personen, deren erhöhte Körpertemperatur (oder sonstige Symptomatik) gerade nicht auf eine SARS-CoV-2-Infektion, sondern auf individuelle körperliche Befindlichkeiten oder chronische Erkrankungen zurückzuführen ist, würde ein derartiges Temperaturscreening zudem bedeuten, entweder mit Mitarbeitern eines Einzelhändlers oder Sicherheitsdienstes Details zum individuellen Gesundheitszustand erörtern zu müssen oder – im Hinblick auf die drohende Verweigerung des Zutritts – für die Beschaffung von Gütern des täglichen Lebens auf Dritte zurückgreifen zu müssen.

Da eine Temperaturerfassung als Mittel einer Zutrittsbeschränkung nicht nur bei dem genannten Lebensmittelhändler zum Einsatz kam, sondern in zahlreichen Geschäften, Behörden, Arbeitsstätten, Flughäfen etc. als eine wirksame Maßnahme angesehen wird, um den Zutritt zu ihren Betriebsräumen zu regulieren, wurde seitens der Datenschutzkonferenz ein Beschluss zum Einsatz von Wärmebildkameras und elektronischer Temperaturerfassung veröffentlicht.[4]

Fazit/ Empfehlung:

Im Einzelhandel ist eine kameragestützte Temperaturdetektion regelmäßig als Maßnahme zur Pandemiebekämpfung nicht geeignet und begegnet datenschutzrechtlichen Bedenken.

[3] Robert-Koch-Institut, Epidemiologisches Bulletin 20/2020 vom 14. Mai 2020, elektronisch abrufbar unter: https://www.rki.de/DE/Content/Infekt/EpidBull/Archiv/2020/Ausgaben/20_20.pdf?__blob=publicationFile (letzter Zugriff: 3.3.2021).

[4] https://www.datenschutz.saarland.de/datenschutz/datenschutzkonferenz/beschluesse.

III.

Ausgewählte Themen

3 Ausgewählte Themen

3.1 EuGH: „Schrems II“

Zu den wichtigsten und auch folgenreichsten datenschutzrechtlichen Entscheidungen des vergangenen Jahres zählt unzweifelhaft das Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 (C-311/18 - Facebook Ireland und Schrems; „Schrems II“). Anlass des Verfahrens war ein Vorabentscheidungsersuchen des irischen High Courts in einem Rechtsstreit, der wiederum auf Antrag der irischen Datenschutzaufsichtsbehörde geführt wurde und in dem diese geklärt wissen wollte, inwiefern das sog. EU-US Datenschutzschild (Privacy-Shield-Beschluss 2016/1250) für Datenübermittlungen in die USA auf der Grundlage der Datenschutz-Grundverordnung (DSGVO) Gültigkeit besaß.

Personenbezogene Daten dürfen nach den Vorgaben der DSGVO nur dann an ein Drittland, d.h. an oder in einen Staat außerhalb der Europäischen Union/des Europäischen Wirtschaftsraums transferiert werden, wenn dort für die Verarbeitung der personenbezogenen Daten ein angemessenes Schutzniveau gewährleistet ist.

Der Maßstab für dieses Schutzniveau ergibt sich aus Kapitel V (Art. 44 ff.) DSGVO. Dabei können personenbezogene Daten zunächst auf der Grundlage von Angemessenheitsbeschlüssen übermittelt werden, mit denen die Europäische Kommission ein angemessenes Datenschutzniveau im Drittland festgestellt hat. Gibt es für das Drittland, an das Daten übermittelt werden sollen, keinen entsprechenden Angemessenheitsbeschluss, muss die Datenübermittlung durch andere geeignete Garantien abgesichert werden. Verbreitet kommen als solche Garantien dabei die von der Europäischen Kommission erlassenen Standarddatenschutzklauseln nach Art. 46 Abs. 2 lit. c DSGVO zur Anwendung.

Mit dem Urteil in der Rechtssache C-311/18 hat der EuGH nochmal bekräftigt, dass personenbezogene Daten, die in ein Drittland übermittelt werden, im Lichte des von der Charta der

Grundrechte der Europäischen Union garantierten Schutzniveaus dort einen im Wesentlichen gleichwertigen Schutz wie unter der DSGVO genießen müssen.

Für die USA verneint der EuGH dabei ein im Wesentlichen gleichwertiges Schutzniveau. Dabei stützt sich der EuGH im Wesentlichen auf zwei Aspekte. Zum einen stellen die umfangreichen Zugriffsmöglichkeiten durch die US-Behörden im Rahmen der US-Überwachungsprogramme einen unverhältnismäßigen Eingriff in die Grundrechte der Betroffenen dar, deren personenbezogene Daten in die USA übermittelt werden. Zum anderen stehen den EU-Bürgern gegenüber derartigen Überwachungsmaßnahmen in den USA keine hinreichenden Rechtsschutzmöglichkeiten zur Verfügung. In Konsequenz erklärte der EuGH den Angemessenheitsbeschluss der EU-Kommission zum EU-US Datenschutzschild für ungültig und befand gleichzeitig den streitgegenständlichen Beschluss der EU-Kommission über Standarddatenschutzklauseln im Lichte der Charta der Grundrechte der Europäischen Union als geeignete Garantie grundsätzlich für wirksam. Das Gericht weist aber gleichzeitig darauf hin, dass die in den Standarddatenschutzklauseln vertraglich vereinbarten, durchsetzbaren Rechte und wirksamen Rechtsbehelfe im Drittland auch durch wirksame Mechanismen praktisch zur Verfügung stehen müssen.

Für Datenexporteure (ob Verantwortliche oder Auftragsverarbeiter, private oder staatliche Stellen, die im Anwendungsbereich der DSGVO personenbezogene Daten verarbeiten) hat dies zur Konsequenz, dass sie vor der Übermittlung von personenbezogenen Daten in Drittländer (und speziell in die USA) auf der Grundlage von geeigneten Garantien nach Art. 46 DSGVO (z.B. Standarddatenschutzklauseln) prüfen müssen, ob diese Daten im jeweiligen Drittland bei Anwendung der geeigneten Garantien einen im Wesentlichen gleichwertigen Schutz genießen. Verhindert das Recht des Drittlandes die Einhaltung der Garantien, müssen zusätzliche Maßnahmen ergriffen werden, die im konkreten Einzelfall diesen Schutz herstellen. Speziell für die

USA bedeutet dies, dass nicht nur eine Übermittlung personenbezogener Daten auf der Grundlage des Privacy-Shields nunmehr unzulässig ist, sondern dass bei der Übermittlung auf der Grundlage von Standardvertragsklauseln diese Übertragung nunmehr nur zulässig ist, wenn zusätzliche Maßnahmen getroffen werden, die die übermittelten Daten im konkreten Einzelfall angemessen vor dem unbeschränkten Zugriff der US-Sicherheitsbehörden und Geheimdienste schützen. Solche zusätzlichen Maßnahmen können vertraglicher, technischer oder organisatorischer Art sein.

Am 10. November 2020 hat der Europäische Datenschutzausschuss Empfehlungen erlassen (Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten), die die Datenexporteure dabei unterstützen sollen, die Datenschutzsituation in einem Drittland zu beurteilen und erforderlichenfalls geeignete zusätzliche Maßnahmen festzulegen.

3.2 Aktuelle Entwicklungen im Bereich der Telemedien

3.2.1 BGH: „Planet49“

Im 28. Tätigkeitsbericht wurde unter Abschnitt 4.7.2 (S. 67) bereits die Rechtsprechung des EuGH in Sachen „planet49“ aus dem Jahre 2019 dargestellt. Im damaligen Urteil hatte der Europäische Gerichtshof (EuGH) klargestellt, dass insbesondere auf Webseiten eine datenschutzrechtliche Einwilligung nur durch ein aktives Tun des Nutzers erteilt werden kann, mithin dass vorangekreuzte Checkboxen oder Ähnliches den Anforderungen des Datenschutzrechts nicht genügen. Unter Berücksichtigung dieser Vorgaben des EuGH hatte der Bundesgerichtshof (BGH) im Jahr 2020 im o.g. Verfahren eine abschließende Entscheidung unter Berücksichtigung der einschlägigen nationalen Gesetze zu treffen.

Mit Urteil vom 28. Mai 2020 hat der BGH entschieden, dass auch nach der nationalen Regelung des § 15 Abs. 3 Telemediengesetz (TMG) *„für den Einsatz von Cookies zur Erstellung von Nutzerprofilen für Zwecke der Werbung oder Marktforschung die Einwilligung des Nutzers erforderlich ist."*[5]

Zwar ist nach dem Wortlaut des § 15 Abs. 3 TMG eine Erstellung von Nutzerprofilen bereits zulässig, wenn der Nutzer nicht „widerspricht". Unter richtlinienkonformer Auslegung im Hinblick auf Art. 5 Abs. 3 ePrivacy-Richtlinie[6] geht der BGH jedoch davon aus, dass es als Widerspruch des Nutzers zu verstehen sei, wenn dieser keine Einwilligung abgibt, die den Anforderungen der DSGVO genügt.

Wenn auch dieser „Kunstgriff" des BGHs im dortigen Fall den europäischen Vorgaben der ePrivacy-Richtlinie auch im nationalen Recht hinreichend Geltung verschaffen mag, so verbleibt bei vielen weiteren Fallgestaltungen die Rechtslage nach wie vor ungeklärt.

Grund hierfür ist, dass auch nach derzeitigem Stand keine vollumfängliche nationale Umsetzung des Art. 5 Abs. 3 ePrivacy-Richtlinie existiert, die allen dort geregelten Fallgestaltungen Rechnung trägt. Insbesondere bleibt unklar, auf welcher Rechtsgrundlage und in welchem Umfang der Einsatz etwa von Cookies auf Webseiten über den in § 15 Abs. 3 TMG spezifisch geregelten Sonderfall hinaus zulässig ist. Denn § 15 Abs. 3 TMG betrifft lediglich das Erstellen von Nutzungsprofilen bspw. zu Werbezwecken. Dementgegen regelt Art. 5 Abs. 3 ePrivacy-Richtlinie die Verarbeitung von Endgeräteinformationen im Allgemeinen. Der Anwendungsbereich der Regelungen ist damit nicht deckungsgleich.

---

[5] BGH, Urteil vom 28. Mai 2020 - I ZR 7/16 - Cookie-Einwilligung II, Rn. 47, juris.

[6] 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 (Datenschutzrichtlinie für elektronische Kommunikation), (ABl. L 201 S. 37).

Vor diesem Hintergrund hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder im November 2020 eine Entschließung veröffentlicht, die den Bundesgesetzgeber auffordert, die europarechtlichen Verpflichtungen der ePrivacy-Richtlinie endlich zu erfüllen und in nationales Recht umzusetzen.[7]

Der Bundesgesetzgeber gedenkt dies mit dem Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) zu tun, das sich derzeit in der Ausarbeitung befindet. Bis zum Ende des Berichtszeitraumes existierte jedoch kein abschließender Entwurf des Gesetzes.

3.2.2 ePrivacy-Verordnung

Für Rechtsklarheit sorgen könnte im Bereich des Einsatzes von Cookies und vergleichbaren Techniken die geplante ePrivacy-Verordnung. Bereits im letzten Tätigkeitsbericht wurde auf die bereits lang anhaltenden Verhandlungen im Europäischen Rat verwiesen.

Ende 2020 konnte ein Kompromissvorschlag der deutschen Ratspräsidentschaft im Rat der Europäischen Union unter den Mitgliedstaaten keine Mehrheit gewinnen. Ebenjener Vorschlag fand einen vertretbaren Ausgleich zwischen den Rechten Betroffener auf Schutz ihrer Privatsphäre sowie ihrer personenbezogenen Daten und den Interessen von Verantwortlichen. Begrüßenswert war insbesondere, dass auf eine Regelung, nach der ein Zugriff auf Informationen auf den Endgeräten von Nutzern auf Grundlage berechtigter Interessen des Verantwortlichen zulässig sein sollte, ausdrücklich verzichtet wurde. Denn in einem derart praxisrelevanten Bereich sollte der Gesetzgeber die maßgeblichen Entscheidungen darüber treffen, welche Verarbeitungstätigkeiten auch ohne Einwilligung der Nutzer zulässig sein dürfen. Dies sollte nicht der ergebnisoffenen Auslegung

[7] Elektronisch abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/TOP_10_Entschlie%C3%9Fung_DSK_BGH_Planet49.pdf.

durch Verantwortliche, Behörden und Gerichte überlassen bleiben.

Ziel sollte es vielmehr sein, dass der Gesetzgeber unter Abwägung der widerstreitenden Interessen konkret definiert, welche Verarbeitungsvorgänge aufgrund ihrer geringen Eingriffsintensität auch ohne Einwilligung zulässig sein sollen. Verarbeitungen hingegen, die erheblich in die Rechte der Nutzer eingreifen, dürfen nur zulässig sein, wenn diese aus freien Stücken und in informierter Weise ihre Einwilligung hierzu geben.

3.3 Orientierungshilfe Videokonferenzen

Ausgelöst durch die Corona-Krise ist die Nutzung von Videokonferenzdiensten in den letzten Monaten stark angestiegen und hat sich als weitere Säule der Kommunikation sowohl im Privatbereich als auch im beruflichen und schulischen Umfeld etabliert. Solche Videokonferenzen können mit zwei unterschiedlichen Betriebsmodellen (Eigenbetrieb und Online-Service) genutzt werden.

Unabhängig von den technischen Rahmenbedingungen wie Bandbreite und Betriebsmodell ist zu beachten, dass bei Videokonferenzen personenbezogene Daten verarbeitet werden.

Betroffen sind hier inhaltliche Äußerungen sowie die Übertragung von Bild und Ton der teilnehmen Personen und ggf. ihres Umfelds, wie etwa Arbeitsplatz, Wohnung oder sonstiger Aufenthaltsort (Inhaltsdaten). Ferner werden sog. Metadaten bzgl. der Durchführung der Kommunikation, Daten über berufliche Kontakte, über Arbeitszeiten und Arbeitsleistung anhand der Daten einer oder mehrerer Videokonferenzen verarbeitet (Rahmendaten). Zusätzlich können personenbezogene Daten in Text-Beiträgen der teilnehmenden Personen und den im Rahmen von Videokonferenzen sichtbar gemachten Dokumenten enthalten sein.

Zum Betrieb bzw. zur Nutzung von Videokonferenzsystemen sind somit entsprechende rechtliche als auch technische Rahmenparameter zu berücksichtigen, um die mit der Nutzung verbundenen Risiken auf ein Minimum zu reduzieren.

Vor diesem Hintergrund hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Orientierungshilfe und eine diese ergänzende Checkliste veröffentlicht, um Unternehmen, Behörden und anderen Einrichtungen Hinweise zu den Anforderungen an die Nutzung von Videokonferenzsystemen zu geben.

Die Orientierungshilfe beleuchtet im Wesentlichen die rechtlichen Anforderungen und spricht Empfehlungen aus, die dabei unterstützen, Videokonferenzsysteme rechtskonform für alle Beteiligten zu nutzen und zu betreiben.

Die Orientierungshilfe "Videokonferenzsysteme" kann unter https://www.datenschutz.saarland.de/datenschutz/datenschutzkonferenz in der Rubrik Orientierungshilfen heruntergeladen werden.

Fazit/ Empfehlung:

Die Corona-Krise hat zu einer extremen Beschleunigung der Digitalisierung geführt. Insbesondere sind hier Videokonferenzsysteme zu nennen, da sie nicht nur im beruflichen, sondern auch im privaten Umfeld große Veränderungen mit sich bringen. Dennoch muss der Schutz von personenbezogenen Daten beim Einsatz moderner Systeme mit berücksichtigt werden.

3.4 Änderung des Gesetzes zur Errichtung eines Landesamtes für IT-Dienstleistungen

Bereits zum 1. Januar 2016 wurde auf Grund landesgesetzlicher Regelungen das Landesamt für IT-Dienstleistungen (IT-DLZ) ge-

gründet, dessen Aufgabe es seitdem ist, als zentraler IT-Dienstleister die saarländischen Landesbehörden beim Einsatz ihrer Informations- und Kommunikationstechnik zu unterstützen. Hierzu gehört neben der Bereitstellung und dem Betrieb der Informations- und Kommunikations-Infrastruktur inklusive der Gewährleistung der IT-Sicherheit auch der Betrieb der in den einzelnen Landesbehörden vorhandenen Fachverfahren (§ 2 Abs. 1 Nr. 5 IT-DLZ-Gesetz).

Der technische Betrieb der Fachverfahren wird damit durch das IT-DLZ durchgeführt (§ 3 Abs. 2 IT-DLZ-Gesetz), während die inhaltliche Verantwortung bei den abgebenden Stellen verbleibt. Gerade bei Fachverfahren mit Personenbezug stellt sich damit die Frage, wie die Weitergabe personenbezogener Daten, bspw. Informationen, die sich auf im Fachverfahren beteiligte Bürgerinnen und Bürger beziehen, an das IT-DLZ datenschutzrechtlich gerechtfertigt werden kann.

Das IT-DLZ-Gesetz enthielt dazu bisher keine Regelungen. Aus datenschutzrechtlicher Sicht handelt es sich bei der Auslagerung des Betriebs von Fachverfahren an das IT-DLZ um rein technische Hilfs- und Unterstützungsaufgaben, die rechtlich eine Datenverarbeitung im Auftrag darstellt und den gesetzlichen, formalen und inhaltlichen Anforderungen des Art. 28 Datenschutz-Grundverordnung (DSGVO) genügen muss. Daher war es bisher notwendig, dass zwischen dem jeweiligen Fachressort und dem IT-DLZ für jedes einzelne Fachverfahren eine den Anforderungen des Art. 28 Abs. 3 DSGVO genügende Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag abgeschlossen werden musste, was auf Grund der Vielzahl von Einzelvereinbarungen wenig praktikabel war.

Wir hatten daher schon 2016 angeregt, datenschutzrechtliche Regelungen in das IT-DLZ-Gesetz aufzunehmen. Mit Inkrafttreten der DSGVO wurde dieser Vorschlag aufgegriffen, zumal Art. 28 Abs. 3 DSGVO, anders als nach vorheriger Rechtslage, nun nicht mehr ausschließlich einen Vertrag zwischen Verantwortlichem und Auftragsverarbeiter fordert, sondern auch „*andere*

Rechtsinstrument[e] nach dem [...] dem Recht der Mitgliedstaaten" genügen lässt, solange diese den Auftragsverarbeiter in Bezug auf den Verantwortlichen binden und bestimmte inhaltliche Anforderungen erfüllt werden.

§ 4 Abs. 1 Satz 2 IT-DLZ-Gesetz sieht nunmehr vor, dass beim Betrieb von Fachverfahren das IT-DLZ die Rolle des Auftragsverarbeiters übernimmt und bei der Verarbeitung und Nutzung der Daten an die Weisungen der jeweils für die Verarbeitung verantwortlichen Stellen gebunden ist.

Erforderlich ist damit jedoch weiterhin, dass Zweck, Art und Umfang der Datenverarbeitung i. S. von Art. 28 Abs. 3 DSGVO für jedes Fachverfahren individuell festgelegt und dem IT-DLZ durch die verantwortliche Stelle vorgegeben werden müssen. Eine entsprechende Regelung im IT-DLZ-Gesetz wäre angesichts der Heterogenität der unterschiedlichen Verfahren wenig zielführend gewesen. Die nach Art. 30 DSGVO und § 15 Abs. 1 SDSG zu fertigende Verfahrensdokumentation kann nach hiesigem Dafürhalten als eine ausreichende individuelle Festlegung angesehen werden, da durch die Freigabeerklärung nach § 15 Abs. 1 SDSG die Rahmenbedingungen des Verfahrens auch für das IT-DLZ als Auftragsverarbeiter verbindlich werden. Beabsichtigt das IT-DLZ von diesen Vorgaben abzuweichen, löst dies eine neue Pflicht zur Freigabe nach § 15 Abs. 1 Saarländischen Datenschutzgesetzes (SDSG) aus, wodurch letztlich die Zurechenbarkeit zum Verantwortlichen sichergestellt wird.

3.5 Novellierung der polizeilichen Datenverarbeitung

Eines der größeren Gesetzgebungsverfahren, das wir im Berichtszeitraum begleitet haben, war das Gesetz zur Novellierung der polizeilichen Datenverarbeitung. Die Vorgaben der Richtlinie 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder

der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 04.05.2016, S. 89) und die neuere Rechtsprechung des Bundesverfassungsgerichts, insbesondere der Entscheidung zum BKA-Gesetz vom 20. April 2016 (1 BvR 966/09, 1 BvR 1140/09), haben es erforderlich werden lassen, dass die Datenverarbeitungsgrundlagen für die saarländische Polizei an die neuen europa- und verfassungsrechtlichen Vorgaben angepasst werden. Zugleich sollten hierbei auch mit Blick auf die Modernisierung der polizeilichen Datenverarbeitung im Rahmen des Programms "Polizei 2020" die hierfür entsprechenden Rahmenbedingungen geschaffen werden.

Um dies zu erreichen, hatten sich die saarländische Landesregierung und der saarländische Gesetzgeber dafür entschieden, die bisherigen Datenverarbeitungsvorschriften für die Polizei aus dem Saarländischen Polizeigesetz (SPolG) herauszunehmen und in einem neuen Saarländischen Polizeidatenverarbeitungsgesetz (SPolDVG) eine abschließende Vollregelung der Datenverarbeitung durch die saarländische Polizei zu Zwecken der polizeilichen Gefahrenabwehr zu schaffen.

Die Landesbeauftragte für Datenschutz war seit 2018 in das Verfahren zur Erstellung des vorliegenden Gesetzentwurfs durch das Ministerium für Inneres, Bauen und Sport eingebunden worden. Eine erste ausführliche Stellungnahme zu einem sehr frühen Referentenentwurf haben wir schon im Oktober 2018 abgegeben. Danach folgten weitere Befassungen und schriftliche Stellungnahmen im Rahmen der internen und externen Anhörung. Zudem gab es mehrere Besprechungen zwischen dem Unabhängigen Datenschutzzentrum Saarland (UDZ) und dem zuständigen Referat des Ministeriums sowie dem Landespolizeipräsidium, in dem einige ausgewählte datenschutzrechtliche Implikationen der vom Ministerium vorgesehenen Regelungen erörtert und diskutiert wurden. Wenn auch im Rahmen dieser vorparlamentarischen Erörterungen über den Gesetzentwurf letztlich nicht in allen

Rechtsfragen Einvernehmen erzielt werden konnte, so erfolgte unsere Beteiligung in einem konstruktiven Austausch mit dem gemeinsamen Ziel, ein Polizeigesetz zu schaffen, das auch unter Datenschutzgesichtspunkten den europarechtlichen und verfassungsrechtlichen Anforderungen Rechnung trägt.

Allgemein ist zu der Neuregelung der polizeilichen Datenverarbeitung anzumerken, dass angesichts einer Vielzahl von Verweisungen, Weiterverweisungen und Rückverweisungen innerhalb des Gesetzes, aber auch durch Verweise auf andere Gesetze, die Lesbarkeit und Verständlichkeit einzelner Regelungen erheblich leidet, was durchaus Zweifel an der Bestimmtheit und damit Rechtsstaatlichkeit einiger Vorschriften hervorruft, jedenfalls aber in der praktischen Anwendung zu Schwierigkeiten führen wird.

Aus inhaltlicher Sicht sehr gelungen sind zunächst die Regelungen im fünften und sechsten Teil des Gesetzes, mithin die §§ 53-67. Die gesetzlichen Vorgaben orientieren sich hier eng an den europarechtlichen Vorgaben der Richtlinie und schaffen damit die rechtlichen Grundlagen, um bei der Datenverarbeitung durch die Polizei aus technischer/organisatorischer Sicht ein hohes Datensicherheitsniveau zu gewährleisten.

Zu begrüßen ist auch, dass es uns im parlamentarischen Verfahren gelungen ist, den Gesetzgeber davon zu überzeugen, dass eine unabhängige Aufsichtsbehörde, die mit effektiven und wirksamen Befugnissen ausgestattet ist, für die Gewährleistung des Datenschutzes bei der polizeilichen Datenverarbeitung unerlässlich ist. Der Gesetzentwurf sah noch vor, dass die Abhilfebefugnisse der Aufsichtsbehörde in gewissen Fällen eingeschränkt werden sollten, indem diese vor dem Erlass von Untersagungsverfügungen Einvernehmen mit dem Ministerium für Inneres, Bauen und Sport hätte herstellen müssen. Aus hiesiger Sicht wäre dies mit der vom EuGH verlangten Unabhängigkeit der Aufsichtsbehörde nicht zu vereinbaren gewesen, da hierdurch der Fach- und Rechtsaufsichtsbehörde ein entscheidender Einfluss auf die von der Aufsichtsbehörde zu ergreifenden

Maßnahmen eingeräumt geworden wäre. Die vom Landtag verabschiedete Regelung sieht nun vor, dass die der Aufsichtsbehörde gesetzlich eingeräumten Befugnisse unbeschränkt anwendbar sind, soweit datenschutzrechtliche Verstöße bei der Polizei festgestellt werden. Allein vor der Ausübung entsprechender Abhilfebefugnisse ist ein Beanstandungsverfahren durchzuführen, bei dem auch die Rechts- und Fachaufsichtsbehörde zu beteiligen ist, das zum Ziel hat, die festgestellten Verstöße auch ohne die Inanspruchnahme verwaltungsverfahrensrechtlicher Abhilfemaßnahmen zu beenden oder zu beseitigen. Die mit diesem Vorverfahren verfolgte Intention des Gesetzgebers, nämlich die Fach- und Rechtsaufsichtsbehörde in das datenschutzrechtliche Aufsichtsverfahren einzubinden und dieser die Möglichkeit zur Stellungnahme zu eröffnen, bevor eine behördliche Anordnung ergeht, um so zu einem schnellen und effektiven Abschluss des Aufsichtsverfahrens zu gelangen, unterstützen wir sehr.

Auf unsere Anregung im Rahmen der parlamentarischen Anhörung hat der Gesetzgeber auch die Benachrichtigungspflichten im Rahmen verdeckter Ermittlungsmaßnahmen präzisiert. Der Gesetzentwurf sah noch relative allgemeine Regelungen vor, die der Polizei insbesondere mit Blick auf den Umfang der Benachrichtigungsempfänger einen gewissen Spielraum eröffnete. Die nunmehr in § 10 Abs. 5 SPolDVG geregelten Benachrichtigungspflichten legen für jede verdeckte polizeiliche Maßnahme normenklar fest, welche Personen zu benachrichtigen sind und regeln auch in § 10 Abs. 7 SPolDVG die Voraussetzungen einer Zurückstellung bzw. des Absehens von einer Benachrichtigung neu.

Darüber hinaus enthält das Gesetz aber auch einige neue polizeiliche Datenverarbeitungsbefugnisse, die aus Sicht des Gesetzgebers für eine moderne polizeiliche Gefahrenabwehr erforderlich sind.

So normiert § 28 Abs. 2 SPolDVG eine umfassende Abgleichbefugnis polizeilicher Datenbanken. Diese erlaubt eine Suche nach Personen in polizeilichen Datenbanken immer schon dann,

wenn eine Person mit der Polizei in Kontakt kommt. Leider konnten wir uns mit unserer Forderung im Rahmen der parlamentarischen Anhörung, diesen Datenabgleich auf Fahndungsfälle zu beschränken, nicht durchsetzen. Die Neuregelung birgt aus unserer Sicht die Gefahr, dass Bürger Opfer von Vorverurteilungen, Stigmatisierungen und polizeilichen Folgemaßnahmen werden, wenn die Polizei bspw. im Rahmen einer allgemeinen Verkehrskontrolle, ohne dass hierfür Anlass besteht, alle polizeilichen Systeme nach (vorhandenen) Informationen über den Fahrer des Fahrzeugs abrufen darf.

Neu geregelt ist in § 28 Abs. 2 SPolDVG zudem die Befugnis zur Durchführung von sog. Zuverlässigkeitsüberprüfungen. Mit der Überprüfung der Zuverlässigkeit von Personen durch einen Abgleich mit polizeilichen Dateien soll festgestellt werden, ob sicherheitsrelevante Erkenntnisse gegen diese Personen vorliegen. Solche Überprüfungen sind 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 für ein polizeiliches Tätigwerden bietet oder eine konkrete Gefahr existiert. Insofern begrüßen wir, dass wenigstens unsere Forderung aufgegriffen wurde, dass der Betroffene zumindest im Falle eines negativen Ausgangs der Zuverlässigkeitsüberprüfung, wenn also Sicherheitsbedenken bestehen, vorher angehört werden muss und so die Möglichkeit erhält, seinen Standpunkt und eventuell entlastende Angaben in das Verfahren einzubringen.

Ebenfalls zu den neuen Befugnissen, die die Polizei durch die Neuregelung der polizeilichen Datenverarbeitung erhält, gehören die Möglichkeit zum Zugriff auf informationstechnische Systeme (sog. Quellen-TKÜ) und die Ausweitung der Einsatzmöglichkeiten der Body-Cam. Nunmehr ist es nämlich möglich, unter den erhöhten Voraussetzungen einer dringen Gefahr für Leib und Leben Body-Cams auch in Wohnungen einzusetzen. Bedauerlich ist hieran, dass der Gesetzgeber sich mit dieser Regelung von seiner ursprünglichen Intention, mit dem Einsatz der Body-Cams Übergriffen und Angriffen gegenüber

Polizeivollzugsbeamten vorzubeugen, verabschiedet hat und durch die nunmehrige Regelung, die nicht mehr nur auf den Schutz von Leib und Leben von Polizeivollzugsbeamten abstellt, der Body-Cam-Einsatz – gerade in Wohnungen bei Fällen häuslicher Gewalt – zukünftig wohl zur polizeilichen Standardmaßnahme gehören wird.

Nicht durchsetzen konnten wir uns zudem mit unserer Forderung, die Voraussetzungen für die Erhebung von Telekommunikationsdaten und Nutzungsdaten von Telemedien bei Diensteanbietern an die verfassungsrechtlichen Vorgaben anzupassen. Mit Beschluss vom 27. Mai 2020 (1 BvR 1873/13) hat das Bundesverfassungsgericht strenge Vorgaben für Regelungen zum Datenabruf aufgestellt. Danach muss der Datenabruf nicht nur für sich genommen verhältnismäßig sein, sondern ist – auch aus Gründen der Normenklarheit – zudem an die in der Übermittlungsregelung begrenzten Verwendungszwecke gebunden. Diesen Anforderungen wird die gesetzliche Regelung in § 36 SPolDVG derzeit nicht gerecht, da sie die Voraussetzungen für einen Datenabruf offener gestaltet, als dies die für die Diensteanbieter geltenden Übermittlungsbefugnisse im Telekommunikationsgesetz und im Telemediengesetz vorsehen. Eine gesetzgeberische Überarbeitung und verfassungsrechtliche Ausgestaltung der Abrufbefugnisse in § 36 SPolDVG ist daher dringend geboten.

3.6 Datenschutzaufsicht im strafprozessualen Ermittlungsverfahren

Im Rahmen eines datenschutzrechtlichen Aufsichtsverfahrens wegen einer polizeilichen Maßnahme in einem laufenden Ermittlungsverfahren vertrat das Landespolizeipräsidium die Auffassung, dass aufgrund der strafprozessualen Verfahrensherrschaft der Staatsanwaltschaft sowie der Übermittlungsvoraussetzungen der §§ 474, 480 Strafprozessordnung (StPO) allein die Staatsanwaltschaft verantwortliche Stelle für die in einem Ermittlungsverfahren erfolgende Datenverarbeitung sei. Daher sei

die Aufsichtsbehörde auch nur gegenüber der Staatsanwaltschaft befugt, die aufsichtsbehördlichen Befugnisse wahrzunehmen.

Dies war für uns Anlass, uns mit Art und Umfang der datenschutzrechtlichen Aufsicht im strafprozessualen Ermittlungsverfahren näher zu beschäftigen.

3.6.1 Zuständigkeit der Landesbeauftragten für Datenschutz

Die Zuständigkeit der Landesbeauftragten für Datenschutz für die Überwachung der Einhaltung des Datenschutzes im strafprozessualen Ermittlungsverfahren ergibt sich aus einem Zusammenspiel aus verfassungsrechtlichen und europarechtlichen Vorgaben, die in der StPO umgesetzt und im Saarländischen Datenschutzgesetz (SDSG) konkretisiert werden.

In § 500 StPO hat der Bundesgesetzgeber die Aufsicht durch die jeweils zuständigen Landesbeauftragten für Datenschutz ausdrücklich angeordnet, soweit öffentliche Stellen der Länder – wozu sowohl das Landespolizeipräsidium als auch die Staatsanwaltschaft Saarbrücken gehören – personenbezogene Daten im Anwendungsbereich der StPO und damit in Strafermittlungsverfahren verarbeiten.

Zur konkreten inhaltlichen Ausgestaltung dieser Aufsicht schweigt die StPO und überlässt dies der Regelungsbefugnis der Landesgesetzgeber. Ausweislich der Gesetzesbegründung zu § 500 StPO soll so eine „*landesspezifische einheitliche Aufsicht der Staatsanwaltschaften und der übrigen öffentlichen Stellen sichergestellt*" werden (BT-Drucksache 19/4671, S. 71).

Die Zuständigkeit der Landesbeauftragten für Datenschutz ergibt sich danach aus den Vorschriften des SDSG.

Für die Datenverarbeitung durch die Polizei im Rahmen von strafprozessualen Ermittlungsverfahren folgt dies mangels einer speziellen gesetzlichen Zuständigkeitsregelung aus § 3 Abs. 1 SDSG. Die Regelungen des Saarländischen Polizeidatenverarbeitungsgesetzes (SPolDVG) können hier schon wegen der

Begrenzung auf die Gefahrenabwehr keine Anwendung finden (§ 1 Abs. 1 und 3 SPolDVG).

Bezogen auf die Datenverarbeitung durch die Staatsanwaltschaft ordnet § 2 Abs. 1 Satz 4 2. Hs. SDSG ausdrücklich an, dass die speziellen Vorschriften des Fünften Abschnitts des SDSG auch dann Anwendung finden sollen, wenn die Staatsanwaltschaft andere als Verwaltungsaufgaben wahrnimmt. Laut Antragsbegründung zur Ergänzung des Gesetzentwurfs sollte durch diese Regelung *„eine eventuelle Regelungslücke bei der Anpassung an die Datenschutz-Grundverordnung [geschlossen werden], eine datenschutzrechtliche Aufsicht und Kontrolle der* ***Ermittlungstätigkeit*** *der Staatsanwaltschaft auch weiterhin möglich sein."* (LT-Drucksache 16/380, S. 2).

3.6.2 Art und Umfang der Aufsicht

Art und Umfang der zulässigen aufsichtsbehördlichen Befugnisse, also das „Wie" der Aufsicht, ergeben sich für die Landesbeauftragte für Datenschutz im Rahmen strafprozessualer Ermittlungsverfahren wegen der Anwendungsregel des § 2 Abs. 1 Satz 4 SDSG aus § 20 SDSG. Insbesondere stellt § 20 Abs. 1 SDSG klar, dass die sich aus Art. 58 Datenschutz-Grundverordnung (DSGVO) ergebenden Einzelbefugnisse auf die Einhaltung (auch) „*anderer datenschutzrechtlicher Bestimmungen*", mithin denen der Strafprozessordnung (StPO) und des dritten Teils des Bundesdatenschutzgesetz (BDSG), erstrecken.

Weiterhin sind die öffentlichen Stellen nach § 20 Abs. 4 SDSG verpflichtet, die Landesbeauftragten für Datenschutz und deren Beauftragte bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere Auskunft auf Fragen zu erteilen sowie Einsicht in alle Vorgänge und Aufzeichnungen zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, sowie jederzeit – auch unangemeldet – ungehinderten Zutritt zu allen Diensträumen zu gewähren.

Hiergegen wurde von Seiten der Staatsanwaltschaft und der Polizei vorgetragen, dass die in §§ 474 ff. StPO geregelten Auskunfts- und Akteneinsichtsrechte den sich aus § 20 Abs. 4 SDSG

ergebenden Mitwirkungsverpflichtungen vorgingen, mit der Folge, dass die Polizei schon überhaupt nicht befugt wäre, ohne Zustimmung durch die Staatsanwaltschaft entsprechende Auskünfte zu erteilen (siehe § 480 Abs. 1 StPO) und auch die Staatsanwaltschaft grundsätzlich einen Ermessensspielraum hätte, ob sie im laufenden Ermittlungsverfahren Auskünfte in einem datenschutzrechtlichen Aufsichtsverfahren erteilt.

Im Ergebnis ist diese Sichtweise jedoch abzulehnen. Zwar handelt es sich bei der Anforderung von Informationen und Unterlagen durch die Aufsichtsbehörde und die daraufhin erfolgende Zurverfügungstellung von Informationen mit personenbezogenem Inhalt durch den Verantwortlichen im tatsächlichen Sinne um eine Weitergabe personenbezogener Daten. Im rechtlichen Sinne liegt jedoch in diesen Fällen keine Übermittlung personenbezogener Daten vor, die an den Vorgaben der §§ 474 ff. StPO zu messen wäre.

Die §§ 474 ff. StPO regeln nur die Zulässigkeit von Akteneinsicht und Auskünften aus Akten eines Strafverfahrens für sog. zweckumwandelnde, d.h. verfahrensexterne Zwecke. Eine Zweckumwandlung findet aber bei der Zurverfügungstellung personenbezogener Daten zur datenschutzrechtlichen Aufsicht gerade nicht statt. Vielmehr dient die datenschutzrechtliche Aufsicht der Überprüfung, ob die Datenverarbeitung der beaufsichtigten Stelle im Rahmen der ursprünglichen Zweckfestlegung erfolgt und ob sie diesem Zweck angemessen ist.

Für den Bereich der allgemeinen Fach- und Rechtsaufsicht ist dies im Übrigen allgemein anerkannt und unbestritten (Gieg, in: KK-StPO, 8. Aufl. 2019, § 474 Rn. 1; Radtke/Hohmann, StPO, 2011, § 474 Rn. 2; Köhler, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl. 2020, § 474 Rn. 1). Zum Ausdruck kommt dies auch in den Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV). Die Bestimmungen Nr. 183-189 RiStBV, die die gesetzlichen Vorschriften der §§ 474 ff. StPO konkretisieren, finden nach RiStBV 182 Nr. 2 keine Anwendung im Rahmen der Wahrnehmung von Aufsichts- und Kontrollbefugnissen anderer Stellen. Dies entspricht auch dem Willen des Gesetzgebers, der die

Wahrnehmung von Aufsichts- und Kontrollbefugnissen nicht den Beschränkungen der §§ 474 ff. StPO unterwerfen wollte (BT-Drs. 14/1484, S. 25 f.). Als Ausdruck eines allgemeinen Rechtsgedankens stellt dies zudem § 7 Abs. 1 SDSG deklaratorisch klar, wonach eine Verarbeitung personenbezogener Daten durch öffentliche Stellen zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen keine Zweckänderung darstellt. Auch die Datenschutzaufsicht ist eine Aufsichts- und Kontrollinstanz im vorgenannten Sinne.

Entscheidender ist aus hiesiger Sicht jedoch, dass eine Anwendbarkeit der §§ 474 ff. StPO auf Aufsichtskonstellationen jeglicher Art zudem mit dem Wesen und Funktion der Aufsicht im Allgemeinen und der datenschutzrechtlichen Aufsicht im Speziellen nicht zu vereinbaren sind. Betrachtet man mit dem Bundesverfassungsgericht (BVerfG) die Existenz einer wirksamen, unabhängigen datenschutzrechtlichen Kontrolle als notwendige Voraussetzung einer verhältnismäßigen Ausgestaltung staatlicher Befugnisse, wie sie gerade auch im strafprozessualen Ermittlungsverfahren existieren, und damit als verfassungsrechtliche Obliegenheit, wird schnell deutlich, dass eine Weitergabe personenbezogener Daten nicht an §§ 474 ff. StPO und den dort genannten Einschränkungen gemessen werden kann. Denn die Vorschriften sehen, anders als dies verfassungsrechtlich für eine wirksame Aufsicht geboten wäre, keine Übermittlungspflicht, sondern lediglich eine Übermittlungsbefugnis vor und stellen damit die Übermittlung in das Ermessen der Strafverfolgungsbehörde.

Für die datenschutzrechtliche Aufsicht im strafprozessualen Ermittlungsverfahren bedeutet dies im Ergebnis, dass die Landesbeauftragte die ihr gemäß § 20 SDSG eingeräumten Befugnisse sowohl gegenüber der Polizei als auch gegenüber der Staatsanwaltschaft geltend machen kann. Sie muss sich insbesondere nicht auf die Staatsanwaltschaft verweisen lassen, sondern kann ihre Aufsichts- und Kontrollbefugnisse unmittelbar gegenüber der Polizei ausüben, soweit diese als eigene datenschutzrechtlich verantwortliche Stelle selbst über die Zwecke und Mittel der

Verarbeitung entscheidet. Die strafprozessuale Sachleitungsbefugnis der Staatsanwaltschaft steht dem nicht entgegen (so auch: VG Hamburg, Urteil vom 23.10.2019 – 17 K 203/19 -, S. 14).

Fazit/Empfehlung:

In einem gemeinsamen Termin mit Staatsanwaltschaft und Polizei wurde die oben dargestellte Rechtslage erörtert. Es wurde sich darauf verständigt, dass in einer gemeinsamen Vereinbarung die Rahmenbedingungen der Ausübung datenschutzaufsichtsrechtlicher Befugnisse fixiert werden sollen, um so eine effektive Aufsicht sicherstellen zu können. Der Entwurf einer entsprechenden Vereinbarung findet sich derzeit in Erarbeitung durch unsere Dienststelle.

3.7 Bearbeitung polizeilicher Vorgänge bei Selbstbetroffenheit des Bearbeiters

Der länderübergreifende Arbeitskreis Sicherheit der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) befasste sich mit datenschutzrechtlichen Fragen im Zusammenhang mit polizeilichen Verfahren, bei denen ein Polizeibeamter oder ihm nahestehende Familienangehörige betroffen sind und er selbst Ermittlungen in dem Verfahren durchführt.

Die Neutralitätspflicht des Polizeibeamten steht vorliegend einer Bearbeitung solcher Verfahren durch den selbst betroffenen Beamten entgegen. Auch das Saarländische Beamtengesetz (SBG) enthält in § 57 Abs. 1 eine entsprechende Ausschlussregelung, denn danach dürfen Beamtinnen und Beamte keine Amtshandlungen vornehmen, die sich gegen sie selbst oder Angehörige richten oder die ihnen oder Angehörigen einen Vorteil verschaffen würden.

Auf unsere Bitte teilte uns das saarländische Landespolizeipräsidium insoweit auch mit, dass die Bearbeitung von Ermittlungsverfahren nach den Regelungen einer entsprechenden Handlungsanweisung in Fällen der Selbstbetroffenheit von Polizeibeamten grundsätzlich ausgeschlossen ist.

Ist in einem Ermittlungsverfahren zum Nachteil von Polizeivollzugsbeamten im Privatbereich die örtlich und sachlich zuständige Dienststelle zugleich die Dienststelle, bei der der Polizeivollzugsbeamte seinen Dienst verrichtet, so erfolgt durch eine zentrale Abteilung des Landespolizeipräsidiums eine Zuweisung des Vorgangs an eine andere ermittlungsführende Dienststelle. Auch Verkehrsunfälle, an denen Polizeibeamtinnen oder Polizeibeamte beteiligt sind, sind im Interesse einer objektiven Verkehrsunfallaufnahme grundsätzlich nicht von der eigenen Dienststelle zu bearbeiten.

Rechtlich ist demnach im Saarland die Bearbeitung polizeilicher Vorgänge bei Selbstbetroffenheit des Polizeibeamten ausgeschlossen.

Aus datenschutzrechtlicher Sicht ist aber von besonderem Belang, wie durch technisch-organisatorische Maßnahmen nicht nur sichergestellt wird, dass keine Bearbeitung durch den betroffenen Beamten/Beschäftigten erfolgt, sondern dass dieser auch keinen Zugriff auf die entsprechenden Vorgangsbearbeitungsdaten nehmen kann, um so möglicherweise an Informationen zu gelangen, die ihm als „normalen" Verfahrensbeteiligten nicht oder nicht im gleichen Umfang zustünden. Hinsichtlich der organisatorischen Umsetzung wird diesem Erfordernis durch die in der Handlungsanweisung verpflichtend vorgegebene Abgabe des Verfahrens Rechnung getragen. Zur datenschutzkonformen Umsetzung dieser Vorgabe wäre aber zudem eine technische Maßnahme erforderlich, die sicherstellt, dass der von der Sachbearbeitung ausgeschlossene Polizeibeamte keinen Zugriff auf das Verfahren erhält. Zugriffsbefugnisse sollten alleine die von der zentralen Abteilung betrauten Dienststellen erhalten.

Fazit/ Empfehlung:

Bei Selbstbetroffenheit ist dem Polizeibeamten der Vorgang zu entziehen und gleichzeitig sicherzustellen, dass für diesen Vorgang bis zum Verfahrensabschluss keine Zugriffsmöglichkeit für den betroffenen Beamten besteht.

3.8 Datenabruf für eine Sicherheitsüberprüfung

Die Sicherheitsüberprüfungsgesetze (SÜG) des Bundes und der Länder regeln die Voraussetzungen und das Verfahren zur Sicherheitsüberprüfung einer Person. Eine Person, die mit einer sicherheitsempfindlichen Tätigkeit betraut werden soll, ist vorher einer Sicherheitsüberprüfung zu unterziehen. Es handelt sich i.d.R. um Fälle, in denen eine Person in einem Sicherheitsbereich, z.B. bei der Polizei oder dem Verfassungsschutz beschäftigt werden soll.

Zweck dieser Gesetze ist es, im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, sogenannte Verschlusssachen, vor dem Zugang von Personen zu schützen, bei denen ein Sicherheitsrisiko nicht ausgeschlossen werden kann.

Bewirbt sich jemand daher bei einer Sicherheitsbehörde, muss er in die Durchführung einer Sicherheitsüberprüfung einwilligen und eine Sicherheitserklärung mit umfassenden Informationen zu Daten wie Name, Vornamen, Geburtsdatum und -ort, Staatsangehörigkeit und Wohnsitz zu seiner Person, weiteren Haushaltsangehörigen und seinen Eltern, abgeben. Verweigert die betroffene Person die Einwilligung, kann sie in einem solchen Fall nicht mit einer sicherheitsempfindlichen Tätigkeit betraut werden, was in der Praxis ein Beschäftigungsverhältnis ausschließt.

Einer an uns gerichteten Beschwerde lag folgender Sachverhalt zugrunde:

Ein Betroffener mit Wohnsitz im Saarland hatte sich für den Polizeidienst in Rheinland-Pfalz beworben. Nach bestandenem Auswahlverfahren und durchgeführter Sicherheitsüberprüfung zu seiner Person wurde er sodann durch die Hochschule der Polizei Rheinland-Pfalz informiert, dass hinsichtlich seiner Einstellung in den Polizeidienst erhebliche Sicherheitsbedenken bestehen.

Der Beschwerdeführer bestritt diesen Vorwurf und gab an, eine eidesstattliche Versicherung gegenüber der Hochschule abgegeben zu haben, um die Sicherheitsbedenken auszuräumen. Aufgrund persönlicher Recherchen habe er erst nach dem Vorhalt der Hochschule der Polizei Kenntnis erlangt, dass es sich bei der Person, gegen die Sicherheitsbedenken geäußert wurden, möglicherweise um seinen Vater handelt. Er habe seit längerer Zeit nur noch sporadisch Kontakt zu seinem Vater. Von dessen ideologischer Ausrichtung habe er bislang keine Kenntnis gehabt. Da der Rufname des Vaters mit seinem zweiten Vornamen und auch die Nachnamen identisch seien, gehe er davon aus, dass es sich um eine Verwechselung seiner Person mit der seines Vaters handelt.

Zuständig für die Sicherheitsüberprüfung ist nach § 4 Abs. 1 Nr. 1 Landessicherheitsüberprüfungsgesetz Rheinland-Pfalz (LSÜG) die öffentliche Stelle, die eine Person mit einer sicherheitsempfindlichen Tätigkeit betrauen will, vorliegend demnach die Polizei Rheinland-Pfalz.

Darüber hinaus ist die betroffene Person von der zuständigen Stelle, gemäß § 8 Abs. 1 Satz 2 LSÜG nach Möglichkeit in einem persönlichen Gespräch, über das Ergebnis der abgeschlossenen Sicherheitsüberprüfung zu unterrichten.

Mitwirkende Behörde bei der Sicherheitsüberprüfung ist gemäß § 4 Abs. 5 LSÜG die Verfassungsschutzbehörde Rheinland-Pfalz. Bei der Sicherheitsüberprüfung hat die mitwirkende Behörde Erkenntnisse der Verfassungsschutzbehörden des Bundes und der Länder einzuholen und diese zusammen mit den Angaben des Betroffenen in der Sicherheitserklärung zu bewerten.

Demzufolge wurde auch die hiesige Verfassungsschutzbehörde im Wohnsitzland des Betroffen hinsichtlich möglicher Erkenntnisse zu seiner Person angefragt. Das Ministerium für Inneres, Bauen und Sport, Abteilung V, Verfassungsschutz bestätigte auf unsere Nachfrage die Anfrage der rheinland-pfälzischen Verfassungsschutzbehörde, die Durchführung einer Zuverlässigkeitsüberprüfung aufgrund der im saarländischen Bestand gespeicherten Daten sowie die anschließende Antwort an die rheinland-pfälzische Verfassungsschutzbehörde.

Der Antwort lag jedoch, wie die hiesige Verfassungsschutzbehörde einräumte, eine falsche Speicherung im Nachrichtendienstlichen Informations-System (NADIS) zugrunde. Es wurde festgestellt, dass die Ermittlungen zur Person des Vaters seinerzeit unzureichend durchgeführt wurden, was zur Verwechselung mit der Person des Beschwerdeführers führte. Die Speicherungen zur Person des Betroffenen wurden daher umgehend gelöscht und es erfolgte unmittelbar telefonisch sowie auch schriftlich eine entsprechende Richtigstellung bei der Geheimschutzbeauftragten des Innenministeriums Rheinland-Pfalz.

Der Beschwerdeführer wurde daraufhin zwischenzeitlich als Bewerber angenommen.

Der hier beschriebene Sachverhalt verdeutlicht das Erfordernis, im Rahmen einer Sicherheits- oder Zuverlässigkeitsüberprüfung dem Betroffenen rechtliches Gehör zu gewähren, bevor das Ergebnis der Sicherheitsüberprüfung anderen Stellen mitgeteilt wird. Nur so kann sichergestellt werden, dass die Bewertung auf einer aktuellen und richtigen Tatsachen- und Informationsgrundlage erfolgt. Für das Erfordernis einer vorherigen Anhörung haben wir uns mit Erfolg auch im Rahmen des Gesetzgebungsverfahrens zum Saarländischen Polizeidatenverarbeitungsgesetz eingesetzt.

Die saarländische Verfassungsschutzbehörde hat den vorliegenden Vorfall umgehend zum Anlass genommen, das Verfahren des Datenabgleichs in NADIS zur Durchführung von Zuverlässigkeitsüberprüfungen zu überarbeiten.

3.9 Bußgeldverfahren gegen Polizeibeamte wegen unzulässiger Abfragen

3.9.1 Einleitung

Gegenstand datenschutzrechtlicher Ordnungswidrigkeitenverfahren sind regelmäßig Verstöße von Polizeibediensteten gegen das geltende Datenschutzrecht in Form von unrechtmäßigen Abfragen personenbezogener Daten aus zum Zwecke der polizeilichen Aufgabenerfüllung zur Verfügung gestellten Datenbanken bzw. polizeilichen Vorgangsbearbeitungs- und Informationssystemen.

Im Rahmen der Bearbeitung dieser Sachverhalte ist zunächst zu ermitteln, welche rechtlichen Grundlagen bei der Frage, ob ein Verstoß vorliegt, im jeweiligen Einzelfall heranzuziehen sind. Maßgeblich für diese Beurteilung ist, ob die Abfrage aus einer dienstlichen Veranlassung/Motivation oder aus einem rein persönlich-privaten Interesse erfolgte.

3.9.2 Verstoß im Rahmen einer dienstlichen Motivation

In dieser Konstellation handelt der jeweilige Polizeibedienstete zwar aus einer dienstlichen Motivation heraus, er geht hierbei jedoch – bewusst oder unbewusst – über die Grenzen der datenschutzrechtlichen Zulässigkeit hinaus, d. h. er handelt nicht mehr innerhalb der ihm vorgegebenen Rechtsgrundlagen.

Im Rahmen der polizeiliche Sachbearbeitung kommt als Rechtsgrundlage für einen Abruf personenbezogener Daten allein § 30 Saarländisches Polizeigesetz (SPolG) in Betracht, der insofern abschließenden Charakter hat. Demnach müssen für einen rechtmäßigen Abruf die dort normierten Voraussetzungen erfüllt sein, namentlich die Erforderlichkeit des Datenabrufs für die Erfüllung polizeilicher Aufgaben. Soweit diesen Voraussetzungen durch den polizeilichen Sachbearbeiter nicht Rechnung getragen wird, liegt ein unbefugter Abruf i. S. d. § 27 Abs. 1 Nr. 2 Saarländisches Datenschutzgesetz (SDSG) vor, der gem. § 27

Abs. 2 SDSG mit einer Geldbuße von bis zu 50.000 EUR geahndet werden kann. Die grundsätzliche Anwendbarkeit des SDSG ergibt sich insofern aus § 2 Abs. 1 SDSG.

3.9.3 Verstoß aus privaten Interessen

Bei den im Berichtszeitraum eingeleiteten Bußgeldverfahren handelte es sich demgegenüber ausschließlich um Verstöße, die außerhalb der dienstlichen Sachbearbeitung aus rein persönlich-privaten Interessen und demnach unter Zugrundelegung einer (eigenmächtigen) Entscheidung über die Zwecke der Datenverarbeitung begangen wurden. Dabei war insbesondere zu beobachten, dass sich die Abrufe auf Daten von Personen aus dem Kreis der Kollegen bzw. Vorgesetzten bezogen. Durch die eigenmächtige Zweckbestimmung handelte der jeweilige Bedienstete nicht mehr für eine verantwortliche Stelle (die Polizei), sondern wurde selbst zum Verantwortlichen i. S. d. Art. 4 Nr. 7 Datenschutz-Grundverordnung (DSGVO), mit der Folge, dass für sein Handeln sowie die etwaige Ahndung eines Verstoßes (ggf. neben dem SDSG) die DSGVO unmittelbar anzuwenden war.

Die unbefugten Abfragen waren demnach als Verstöße gegen die Art. 5, 6 DSGVO zu werten, insbesondere, da die Verarbeitung nicht für festgelegte, eindeutige und legitime Zwecke i. S. d. Art. 5 Abs. 1 lit. b DSGVO und ohne Erfüllung der Rechtmäßigkeitsvoraussetzungen des Art. 6 DSGVO, wie beispielsweise dem Vorliegen eines berechtigten Interesses oder einer Einwilligung, erfolgt war.

Als mögliche Sanktionen sieht Art. 58 Abs. 2 DSGVO grundsätzlich die Verwarnung sowie die Verhängung von Bußgeldern vor. Aufgrund des besonderen Vertrauens, das der Polizei hinsichtlich eines ordnungsgemäßen Umgangs mit personenbezogenen Daten entgegengebracht wird, wurden in den bearbeiteten Fällen jeweils Bußgelder gem. Art. 83 Abs. 5 i. V. m. Art. 5, 6 DSGVO verhängt, wobei sich die Bußgelder im unteren bis mittleren dreistelligen Bereich bewegten, so dass der durch Art. 83

Abs. 5 DSGVO vorgegebene Bußgeldrahmen demnach bei Weitem nicht ausgeschöpft wurde.

Fazit/ Empfehlung:

Aufgrund des Umstandes, dass die durch die Bußgeldstelle bearbeiteten Fälle zufällig aufgedeckt wurden und daher von einer Vielzahl weiterer, unentdeckter Fälle auszugehen ist, ist im Hinblick auf eine Vermeidung solcher Verstöße in der Zukunft eine regelmäßige Schulung und Sensibilisierung der Polizeibediensteten dringend zu empfehlen. Daneben wird eine zumindest stichprobenartige Kontrolle der Protokolldaten der getätigten Abrufe – insbesondere im Hinblick auf die Schlüssigkeit des jeweils angegebenen Abfragegrundes bzw. -anlasses – angeraten.

3.10 Datenschutzrechtliche Zulässigkeit eines Bauschilds

Viele Bauherren dürften mitunter den Eindruck haben, dass das Recht ihnen zunächst Steine in den Weg legt, bevor diese aufeinandergesetzt werden können. Die bei der Durchführung eines Bauvorhabens einzuhaltenden Regularien beziehen sich dabei nicht nur auf das geplante oder in der Entstehung befindliche Bauwerk an sich, welches zuvörderst natürlich den planerischen und sicherheitsspezifischen Anforderungen genügen muss. Darüberhinausgehend sind mit dem Wunsch nach dem eigenen Heim und dem hierbei zu durchlaufenden Genehmigungsverfahren auch weitreichende Offenlegungspflichten von personenbezogenen Daten verbunden.

Eine dieser Offenlegungspflichten geht mit dem Baufreigabeschein (Roter Punkt) einher, welchen der Bauherr zusätzlich zur Baugenehmigung nach § 11 Abs. 4 S. 1 der Landesbauordnung (LBO) benötigt, um mit seinem Bauvorhaben beginnen zu dürfen. An der Baustelle nicht verfahrensfreier Bauvorhaben ist

hiernach ein dauerhaftes und von der öffentlichen Verkehrsfläche aus sichtbares Schild anzubringen, welches die Bezeichnung des Vorhabens, das Genehmigungsdatum, die Bauschein-Nummer und die Genehmigungsbehörde sowie Namen und Anschriften der Bauherrin oder des Bauherrn, der Entwurfsverfasserin oder Entwurfsverfassers und der Bauleiterin oder des Bauleiters enthalten muss.

Manch einem Bauherren/einer Bauherrin mag diese Offenbarungspflicht ein Dorn im Auge sein, widerspricht sie doch dem vielfachen Wunsch nach Anonymität gerade in finanziell bedeutenden und von der Nachbarschaft oftmals mit Interesse verfolgten Angelegenheiten wie dem Bau einer Immobilie.

In datenschutzrechtlicher Hinsicht ist die durch das Bauschild geforderte Datenoffenlegung jedoch nicht zu beanstanden.

In § 11 Abs. 4 S. 1 LBO trifft der Landesgesetzgeber eine Abwägung zwischen dem Daten- und Persönlichkeitsschutz der betroffenen Personen (Bauherren, Architekten, Bauleiter) und dem öffentlichen Interesse an der Kenntnis der für das Bauvorhaben verantwortlichen Personen. Sinn des Bauschilds (oder Bautafel) ist es, neben der Wahrnehmung bauordnungsrechtlicher Aufsichtsbefugnisse auch eine einfache Feststellbarkeit der verantwortlichen Personen im Falle von baustellenbezogenen Gefahren, Unfällen und Schäden zu ermöglichen.[8]

Zur Erreichung letzterer Zwecke und der damit verbundenen Transparenz des Bauvorhabens werden die datenschutzrechtlichen Positionen der betroffenen Personen während der Zeit des Bauvorhabens in zulässiger Art und Weise beschränkt.

Die Forderung der Bauaufsichtsbehörden zum Aufstellen (Anbringen) von Bauschildern mit dem betreffenden Inhalt beruht demnach gemäß Art. 6 Abs. 1 lit. e, Abs. 3 lit. b Datenschutz-Grundverordnung (DSGVO) i. V. m. § 11 Abs. 4 S. 1 LBO auf einer

[8] *Nolte*, in: Simon/Busse, Bayerische Bauordnung, 135. EL. 2019, Art. 9 Rn. 44; *Kammeyer*, in: Große-Suchsdorf, Niedersächsische Bauordnung, 10. Aufl. 2020, § 11 Rn. 27.

gesetzlichen Rechtsgrundlage (Verarbeitungsgrundlage) und steht daher im Einklang mit dem Datenschutzrecht.

3.11 Digitale Unterschrift im Bürgerbüro

Der Besuch kommunaler Bürgerämter (Bürgerbüros) geht für die Bürgerinnen und Bürger vielfach mit der Leistung einer Unterschrift einher, vor allem im Zuge der Neubeantragung oder Verlängerung von Ausweisdokumenten.

In datenschutzrechtlicher Hinsicht ist die behördliche Aufforderung zur Erteilung einer solchen Unterschrift in aller Regel nicht zu beanstanden, handeln die tätigen Ämter hierbei doch im Rahmen ihrer gesetzlichen Aufgabenzuweisung. Die eigenhändige Unterschrift der antragstellenden Person, bei Kindern ab dem vollendeten 10. Lebensjahr, ist gemäß den §§ 5 Abs. 2 Nr. 6, 9 Abs. 5 Personalausweisgesetz (PAuswG) sowie § 4 Abs. 1, Abs. 4a Satz 2 Paßgesetz (PaßG) Bestandteil der Ausweisdokumente und für deren Beantragung erforderlich.

Diese Unterschrift wird durch die Ausweisbehörden in der Regel nicht mehr auf Papier erhoben, sondern in elektronischer Form erfasst. Die antragstellende Person unterschreibt hierbei auf einem Unterschriftenpad (Signaturpad), welches die Unterschrift in digitaler Form erfasst und vorgangsbezogen abspeichert.

In seiner an unsere Behörde herangetragenen Beschwerde wandte sich ein Beschwerdeführer gegen eine in dieser Form durchgeführte Unterschrifteneinholung durch die für ihn zuständige Behörde. Seine datenschutzrechtliche Rüge bezog sich dabei jedoch weniger auf die Rechtmäßigkeit bzw. Notwendigkeit der Unterschrift an sich, sondern vielmehr auf die Art und Weise der Unterschriftenerteilung.

Durch die alleinige Nutzung eines Unterschriftenpads könne er während oder nach der Unterschriftenerteilung nicht einsehen bzw. überprüfen, auf welches Dokument und welchen Vorgang sich die Unterschrift beziehe, was letztlich einer behördlichen Aufforderung zur Abgabe einer "Blankounterschrift" gleichkomme.

Auch wenn dieser Vergleich mit einem Blankett im Ergebnis wohl zu weit gegriffen sein dürfte, so ist auch unsere Behörde der Auffassung, dass der antragstellenden Person während des Verwaltungsverfahrens eine Überprüfungsmöglichkeit eröffnet sein muss.

Bei der Einholung einer Unterschrift handelt es sich rechtlich um eine direkte Datenerhebung bei der betroffenen Person. Selbige ist gemäß Art. 13 Datenschutz-Grundverordnung (DSGVO) folglich im Zeitpunkt der Erhebung durch den Verantwortlichen (die handelnde Behörde) über die Zwecke der Datenverarbeitung zu unterrichten.

Konkret bedeutet dies, dass der betroffenen Person insbesondere erklärt werden muss, warum ihre Unterschrift unter ein Dokument erforderlich ist. Dies kann letztlich nur durch Vorlage des zu unterzeichnenden Dokuments bzw. durch Sichtbarmachung des zu unterzeichnenden Inhalts in digitaler Form geschehen. Nur auf diese Weise ist es der betroffenen Person möglich, den Aussagegehalt des Dokuments zu prüfen, welchen sie mit ihrer Unterschrift sodann mit ihrer Person verknüpft. Wenn man so will, folgt das Datenschutzrecht in diesem Punkt dem allgemeinen zivilrechtlichen Sorgfaltsgebot, dass zu unterschreibende Dokumente durch den Unterzeichner vorher zu lesen sind.

Nach Inkenntnissetzung der betroffenen Kommune über die Beschwerde wurde durch selbige zeitnah ein Verfahren vorgeschlagen, welches aus datenschutzrechtlicher Sicht vorgenannter Problematik Abhilfe verschafft. Das Verwaltungsverfahren soll in den betreffenden Bereichen angepasst und um technische Möglichkeiten ergänzt werden, welche eine Darstellbarkeit der zu unterzeichnenden Schriftstücke für die betroffene Person ermöglichen.

Verwirklicht werden soll dies durch "Spiegelung" des betreffenden Dokuments (Vorgangs) auf einen zweiten, dem Antragsteller zugewandten Bildschirm (sog. "Bürgermonitor"), auf welchem der Antragsteller die Angaben überprüfen und sodann

digital unterschreiben kann. Die erfasste digitale Unterschrift soll sodann für den Antragsteller sichtbar in das Dokument eingefügt und abgespeichert werden.

3.12 Nachweis über Masernimpfschutz

Am 1. März 2020 ist in Deutschland das Gesetz für den Schutz vor Masern und zur Stärkung der Impfprävention (Masernschutzgesetz) in Kraft getreten. Das Gesetz sieht vor, dass alle nach 1970 geborenen Personen, die in einer Gemeinschaftseinrichtung betreut werden oder in einer Gemeinschafts- oder Gesundheitseinrichtung beschäftigt sind, einen Masernschutz aufweisen müssen. Die Regelung betrifft damit unter anderem alle Kinder ab dem vollendeten ersten Lebensjahr beim Eintritt in den Kindergarten oder die Schule. Für diese muss gegenüber der jeweiligen Einrichtung (z.B. Schule, Kindertagesstätte) ein Nachweis über den Impfschutz erbracht werden.

Die entsprechenden gesetzlichen Regelungen finden sich im Infektionsschutzgesetz (IfSG), das durch oben genanntes Masernschutzgesetz geändert wurde. § 20 Abs. 8 IfSG normiert dabei die grundsätzliche Verpflichtung für den genannten Personenkreis, einen ausreichenden Impfschutz oder eine Immunität gegen Masern nachzuweisen. Nach § 20 Abs. 9 IfSG kann ein ausreichender Impfschutz durch Vorlage einer Impfdokumentation (Impfausweis oder Impfbescheinigung) nachgewiesen werden. Besteht eine Immunität gegen Masern, z. B. auf Grund einer zurückliegenden Infektion, ist diese durch eine ärztliche Bescheinigung zu belegen. Liegen gesundheitliche Gründe vor, aus denen eine Masernimpfung nicht oder noch nicht möglich ist (medizinische Kontraindikation), ist hierüber ebenfalls ein Nachweis zu erbringen (§ 20 Abs. 9 Nr. 2 IfSG).

Zu dieser Thematik haben uns im Berichtszeitraum mehrere Anfragen hinsichtlich des datenschutzkonformen Umgangs mit den betroffenen Gesundheitsdaten erreicht.

So wurde die Frage aufgeworfen, ob die Einrichtung eine Kopie des vorgelegten Nachweises anfertigen und diese aufbewahren darf. Das Gesetz spricht lediglich davon, dass der Nachweis der

Einrichtung „vorzulegen“ ist, woraus sich ein Recht auf Speicherung nicht ableiten lässt. Bei Attesten, die ausschließlich Angaben zum Masernschutz enthalten, sehen wir die Aufbewahrung einer Kopie durch die Einrichtung dennoch unkritisch. Sie sollte dann in einem verschlossenen Umschlag innerhalb der jeweiligen Akte erfolgen. Nachweisdokumente wie beispielsweise der Impfausweis, die auch andere Gesundheitsdaten enthalten, deren Kenntnis für die Einrichtung nicht erforderlich ist, sind dagegen im Hinblick auf den Grundsatz der Datenminimierung nicht zur Akte zu nehmen. Hier sollte ein Vermerk über die Vorlage des Nachweises regelmäßig ausreichen.

Weiterhin hat sich die Frage gestellt, ob im Falle einer medizinischen Kontraindikation das geforderte ärztliche Zeugnis eine konkrete Diagnose enthalten muss oder die Aussage genügt, dass eine medizinische Kontraindikation (ohne nähere Bezeichnung) vorliegt. Hier ist festzuhalten, dass gegenüber der Einrichtung eine Bescheinigung ohne genaue Angabe der Diagnose ausreicht. Die Verantwortlichen in Kindergarten oder Schule verfügen in der Regel nicht über die erforderliche medizinische Fachkenntnis, um eine Diagnose korrekt einordnen zu können. In Zweifelsfällen kann die Einrichtung das zuständige Gesundheitsamt um Einschätzung bitten.

Für bestimmte Fälle sieht das IfSG eine Benachrichtigung des zuständigen Gesundheitsamtes zwingend vor.

So ist unter bestimmten Voraussetzungen eine Betreuung bzw. ein Tätigwerden in einer Einrichtung auch dann zulässig, wenn der Nachweis über eine vorhandene Immunität, einen ausreichenden Impfschutz bzw. das Vorliegen einer medizinischen Kontraindikation gegenüber der Einrichtung nicht erbracht wird. Dies ist insbesondere bei schulpflichtigen Kindern der Fall, da hier die Schulpflicht nicht durch einen fehlenden Nachweis ausgehebelt werden soll. § 20 Abs. 9 S. 4 IfSG regelt für diese Konstellationen, dass in solchen Fällen eine Benachrichtigung an das Gesundheitsamt erfolgen muss. Zu den hierbei zu übermittelnden personenbezogenen Angaben gehören Name und Vorname, Geschlecht, Geburtsdatum, Anschrift der Hauptwohnung

oder des gewöhnlichen Aufenthaltsortes und soweit vorliegend Telefonnummer und E-Mail-Adresse.

Der Weg der Übermittlung ist gesetzlich nicht festgelegt, so dass die allgemeinen datenschutzrechtlichen Bestimmungen gelten. Dementsprechend sind gem. Art. 32 Datenschutz-Grundverordnung (DSGVO) geeignete technische und organisatorische Maßnahmen für eine sichere Übermittlung der Daten zu ergreifen. Stehen keine entsprechenden technischen Lösungen (z.B. verschlüsselte elektronische Übertragung) für die Datenübermittlung zwischen Einrichtung und Gesundheitsamt zur Verfügung, sollte der Postweg gewählt werden.

Das Gesundheitsamt fordert nach Erhalt der Daten den fehlenden Nachweis noch einmal an. Wird dieser weiterhin nicht vorgelegt oder ergibt sich daraus, dass ein Impfschutz gegen Masern erst zu einem späteren Zeitpunkt möglich ist oder vervollständigt werden kann (z. B. bei vorübergehender Kontraindikation), kann das Gesundheitsamt die von der Nachweispflicht betroffene Person zu einer Beratung laden und sie zu einer Vervollständigung des Impfschutzes auffordern.

Fazit/ Empfehlung:

Nachweise im Sinne des Masernschutzgesetzes sind der jeweiligen Einrichtung vorzulegen. In bestimmten Fällen ist das zuständige Gesundheitsamt zu beteiligen.

3.13 Aufnahme datenschutzrechtlicher Gebührentatbestände in das Allgemeine Gebührenverzeichnis

Mit Einführung der Datenschutz-Grundverordnung (DSGVO) am 25.05.2018 und Neufassung des Bundesdatenschutzgesetzes (BDSG) wurden weitreichende Untersuchungs-, Abhilfe- und

sonstige Befugnisse der Aufsichtsbehörden normiert. Im Rahmen der Wahrnehmung vorgenannter Befugnisse durch die Fachreferate des Unabhängigen Datenschutzzentrums Saarland stellte sich im Folgenden die Frage, welche Gebührensätze für die einzelnen Verwaltungsmaßnahmen konkret heranzuziehen sind. Denn auch datenschutzrechtliche Prüfungen und Kontrollen stellen Amtshandlungen dar (§ 1 Abs. 1 Satz 2 Saarländisches Gebührengesetz), für die grundsätzlich Verwaltungsgebühren zu erheben sind. Anders aber als im allgemeinen Gebührenrecht, wo die Erhebung von Verwaltungsgebühren grundsätzlich eine gebundene Entscheidung darstellt und damit für die Verwaltungsbehörde verpflichtend ist, sieht § 21 Saarländisches Datenschutzgesetz (SDSG) eine ermessensabhängige Befugnis zur Erhebung von Gebühren und Auslagen für Amtshandlungen und sonstige öffentlich-rechtliche Leistungen nach der DSGVO und dem BDSG vor. § 21 Abs. 2 i. V. m. Abs. 3 SDSG ermächtigt die Landesregierung, im Einvernehmen mit der/dem Landesbeauftragten für Datenschutz per Rechtsverordnung die gebührenpflichtigen Tatbestände und die hinsichtlich des Verwaltungsaufwands und der Bedeutung der Angelegenheit zu bemessenden Gebührensätze festzulegen.

Im Rahmen einer Überarbeitung des Allgemeinen Gebührenverzeichnisses Saarland wurden in Zusammenarbeit mit dem Ministerium für Inneres, Bauen und Sport speziell auf die in der DSGVO sowie dem BDSG normierten Befugnisse zugeschnittene Gebührentatbestände geschaffen, um eine einheitliche und rechtssichere Gebührenerhebung zu gewährleisten. In das Verzeichnis aufgenommene Tatbestände sind dabei neben Befugnissen gem. Art. 58 Abs. 3 DSGVO und Aufgaben nach § 40 Abs. 6 BDSG insbesondere die in Art. 58 Abs. 1 DSGVO festgelegten Untersuchungsbefugnisse, wie beispielsweise die Anweisung zur Bereitstellung von Informationen, die für die Aufgabenerfüllung der Aufsichtsbehörden erforderlich sind, des Weiteren die Abhilfebefugnisse gem. Art. 58 Abs. 2 DSGVO (mit Ausnahme der Verhängung von Bußgeldern, für die die Normen des Ordnungswidrigkeitsrechts anzuwenden sind), wie bei-

spielsweise Anweisungen zur Anpassung von Verarbeitungsvorgängen an das geltende Recht. Hervorzuheben ist in diesem Zusammenhang, dass gegenüber dem Verantwortlichen nur dann Gebühren anfallen, wenn tatsächlich ein Verstoß festgestellt wurde.

Des Weiteren findet gegenüber dem Beschwerdeführer grundsätzlich keine Gebührenerhebung statt, so dass jedem Bürger die Möglichkeit offensteht, Eingriffe in sein Recht auf informationelle Selbstbestimmung ohne Kostenlast der Aufsichtsbehörde zur Kenntnis zu bringen. Ausnahmen von diesem Grundsatz sind lediglich bei offenkundig unbegründeten oder exzessiven Anfragen gegeben.

3.14 Erhebung von Mieterdaten durch den Grundversorger

Die gesetzlichen Grundversorger von Elektrizität und Gas stehen gelegentlich vor dem Problem, wie sie im Falle einer Ersatzversorgung einer Immobilie an die Rechnungsdaten eines noch unbekannten Abnehmers von Strom und Gas, und damit Vertragspartners, gelangen. Oftmals führt hier der erste Weg zu dem Eigentümer der versorgten Immobilie, welcher über die Besitzverhältnisse i. d. R. Auskunft erteilen und so auch einen potentiellen Abnehmer von Strom und Gas benennen kann.

Eine solche Datenerhebung über den Eigentümer (Vermieter) einer Immobilie birgt jedoch datenschutzrechtliches Konfliktpotential und führte auch im Berichtzeitraum zu Beschwerden bei unserer Behörde.

Die Beschwerdeführer sind Eigentümer und Vermieter von Wohnimmobilien und wurden durch ein Strom- und Gasversorgungsunternehmen auf schriftlichem Wege kontaktiert. Diese Schreiben waren als "*Vertragsbestätigung*" bezeichnet und enthielten, neben allgemeinen rechtlichen Informationen zur Grundversorgung mit Strom und Gas, die jeweiligen Zählerstände sowie Zahlungsaufforderungen für zu leistende Ab-

schlagszahlungen. Sie bezogen sich jeweils auf eine Verbrauchsstelle in einem Haus (Gas-/Stromzähler) und adressierten die Beschwerdeführer als potentielle Anschlussnutzer im Rahmen der Grundversorgung.

Darüber hinaus befand sich in ihnen folgender Passus:

"*Sie sind nicht die Person, die hier Energie bezieht?*

Sollten Sie nicht der Anschlussnutzer dieser Verbrauchstelle sein (z.B. weil Sie Vermieter des betreffenden Objekts sind oder ein Eigentümerwechsel stattgefunden hat), so bitten wir Sie um Benachrichtigung per Brief oder über einer der anderen o. g. Kontaktmöglichkeiten. Bitte geben Sie den tatsächlichen Anschlussnutzer an (z. B. den Mieter oder bei Wohnungseigentumsgemeinschaften den abweichenden Eigentümer). (...) Bei abweichendem Anschlussnutzer zusätzlich: Den Namen der Person, die hier Energie bezieht, sowie Anschrift, soweit von der Verbrauchstelle abweichend. Das Datum eines eventuellen Mieter- oder Eigentümerwechsels, sowie Namen und Anschrift des vorherigen Anschlussnutzers (sofern vorhanden)."

Die Beschwerdeführer waren der Ansicht, die Verarbeitung ihrer personenbezogenen Daten sowie die mit den Schreiben bezweckte Intention der Erhebung von Mieterdaten über die jeweiligen Immobilieneigentümer laufe den datenschutzrechtlichen Bestimmungen zuwider. Letzteres vor allem deshalb, da sie als Eigentümer nicht automatisch Vertragspartner des grundversorgenden Energieunternehmens seien.

Im Ergebnis erachtete unsere Behörde die geschilderte Datenverarbeitung jedoch als rechtmäßig. Die Rechtsgrundlage für die Verarbeitung von Eigentümerdaten sowie für die Erhebung von Daten potentieller Mieter ergab sich für die Versorgungsunternehmen aus Art. 6 Abs. 1 lit. f Datenschutz-Grundverordnung (DSGVO). Hiernach ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundechte und

Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Diese Rechtsgrundlage besteht dabei unabhängig von einer vertraglichen Beziehung zu der von der Datenverarbeitung betroffenen Person und ist daher nicht mit Art. 6 Abs. 1 lit. b DSGVO zu verwechseln. Erforderlich, aber auch ausreichend, ist vielmehr ein berechtigtes Interesse rechtlicher, tatsächlicher, wirtschaftlicher oder ideeller Art.

Dieses berechtigte Interesse ergab sich für das Versorgungsunternehmen vorliegend aus seiner Stellung als Grundversorger von Strom und Gas für die betreffenden Wohneinheiten. Durch diese Stellung unterliegt der Grundversorger einem Kontrahierungszwang, d. h. er muss grundsätzlich jeden Haushaltskunden mit Strom und/oder Gas beliefern, vgl. § 36 Energiewirtschaftsgesetz (EnWG). In einer solchen Situation hat der Grundversorger ein berechtigtes Interesse daran, seinen Vertragspartner für die Lieferung von Strom und Gas – und damit den Schuldner der entsprechenden Entgeltforderung – mit Namen und Anschrift zu kennen. Dieses Interesse wird gesetzlich dadurch gesichert, indem der tatsächliche Nutzer von Strom und Gas dazu verpflichtet ist, die Entnahme von Elektrizität und Gas dem Grundversorger mitzuteilen (§ 2 Abs. 2 StromGVV[9], § 2 Abs. 2 GasGVV[10]).

Ist keine diesbezügliche Meldung erfolgt und auch kein anderweitiger Strom- und Gaslieferungsvertrag nachgewiesen, so liegen hinsichtlich Mietwohnungen vor allem zwei Konstellationen nahe. Zum einen kommt die Konstellation in Betracht, dass die jeweiligen Mieter einen entsprechenden Nachweis oder eine Mitteilung schlicht versäumt haben. Zum anderen kommt diejenige Konstellation in Frage, dass der Eigentümer der Immobi-

[9] Stromgrundversorgungsverordnung vom 26. Oktober 2006 (BGBl. I S. 2391), zuletzt geändert durch Verordnung 14. März 2019 (BGBl. I S. 333).

[10] Gasgrundversorgungsverordnung vom 26. Oktober 2006 (BGBl. I S. 2391, 2396), zuletzt geändert durch Gesetz vom 29. August 2016 (BGBl. I S. 2034).

lie im Rahmen einer dauernden oder vorübergehenden Eigennutzung selbst Strom bzw. Gas entnimmt, ohne seiner Mitteilungspflicht nachgekommen zu sein. Nach der Rechtsprechung des Bundesgerichtshofes (Urteil vom 2.7.2014 – VIII ZR 316/13) wird je nach Sachlage jedenfalls entweder der bzw. die Mieter (Besitzer der Wohnung) oder der bzw. die Eigentümer einer Wohnimmobilie per Gesetz Vertragspartner des Grundversorgers.

Die tatsächlichen Verhältnisse kann das die Grundversorgung sicherstellende Unternehmen dabei i. d. R. nur über eine Abfrage beim Eigentümer ermitteln, da es die Mieterdaten nicht auf anderem Wege gesichert in Erfahrung bringen kann; im Falle von Mehrparteienhäusern auch nicht über eine Meldeabfrage beim Einwohnermeldeamt, da diesbezüglich keine Daten zur jeweiligen Wohneinheit vorhanden sind.

Die beschwerdegegenständlichen Schreiben des Versorgungsunternehmens waren hierfür jedoch geeignet, da sie die Eigentümer dazu auffordern, im Falle eines abweichenden Anschlussnutzers (Mieters) dessen Kontaktdaten zu übermitteln.

Der Vermieter handelt auch nicht datenschutzwidrig, wenn er die entsprechenden Informationen über seine Mieter an das Versorgungsunternehmen übermittelt. Auch ihm steht in diesem Zusammenhang die Rechtsgrundlage des Art. 6 Abs. 1 lit. f DSGVO zur Seite, da er ein berechtigtes Interesse daran hat, nicht mit unberechtigten Forderungen des Grundversorgers konfrontiert zu werden und demnach diesen über den tatsächlichen Forderungsschuldner in Kenntnis setzen darf. Hierin liegt zugleich eine zulässige Zweckänderung gemäß Art. 6 Abs. 4 DSGVO, insbesondere, da die Übermittlung der Daten an den Grundversorger eng mit einem bestehenden oder vergangenen Mietverhältnis in Verbindung steht.

Die Mieter der jeweiligen Wohneinheiten haben auch keine überwiegenden schutzwürdigen Interessen daran, dass ihre Daten nicht an den Energieversorger übermittelt werden. Zum ei-

nen liegt es nahe, dass in den Fällen, in welchen nicht der Eigentümer aus der Verbrauchstelle Strom oder Gas entnimmt, eine Entnahme durch den jeweiligen Mieter erfolgt und eine entsprechende Anzeige beim Grundversorger unterblieben ist. Zum anderen handelt es sich bei dem Namen und der Anschrift nicht um Daten solcher Sensibilität, dass ihre Übermittlung nur mit Einverständnis (Einwilligung) des Mieters erfolgen dürfte.

Der Mieter hat jedenfalls kein schutzwürdiges Interesse daran, dass seine Daten allein aufgrund einer sonst zu befürchtenden berechtigten Forderungserhebung gegen seine Person nicht übermittelt werden dürfen. Im Gegenteil hat sich sein Interesse gerade darauf zu richten, die tatsächlichen Vertragsverhältnisse der Strom- und Gaslieferung aufzuklären, damit er zum einen seine evtl. bestehenden vertraglichen Pflichten erfüllen kann und zum anderen möglichst zeitnah über eine bestehende Grundversorgung Kenntnis erhält, die für ihn unter Umständen mit höheren Energiekosten verbunden ist.

Fazit/ Empfehlung:

Der Grundversorger von Elektrizität und Gas hat grundsätzlich ein berechtigtes Interesse daran, seinen Vertragspartner in Erfahrung zu bringen. Er darf hierzu sowohl bei ihm vorhandene Eigentümerdaten verarbeiten als auch weitergehende Mieterdaten durch den Eigentümer in Erfahrung bringen. Es steht daher im Ermessen des Eigentümers, ob er Daten des Mieters an den Energieversorger übermittelt. Aus datenschutzrechtlicher Sicht ist er hierzu jedenfalls befugt.

3.15 Kundendatenerhebung mittels Postkarte

Eine Verletzung datenschutzrechtlicher Bestimmungen ist nicht immer das Resultat eines bewussten Hinwegsetzens über gesetzliche Vorgaben. Im Gegenteil kann die weit überwiegende Anzahl datenbezogener Schutzverletzungen im Bereich

des fahrlässigen Handelns verortet werden. Der Verantwortliche agiert hier oftmals aus lauteren Motiven, verkennt jedoch dabei die datenschutzrechtliche Brisanz seines Handelns, was dessen Rechtswidrigkeit oftmals nach sich zieht.

Zum Glück sind viele dieser sogenannten "Datenpannen" für die betroffenen Personen mit geringen Konsequenzen verbunden. Vielfach beschränken sich die Auswirkungen auf die Offenlegung personenbezogener Daten für einen unbestimmten Personenkreis, was für die betroffenen Personen zwar unangenehm ist, jedoch in der Regel keine weitergehenden negativen Auswirkungen nach sich zieht.

Leider gibt es jedoch auch Fälle, in denen eine auf den ersten Blick vielleicht unbedeutend anmutende Datenschutzverletzung bei genauerem Hinsehen ungeahnte Folgen mit sich bringt. Besonders problematisch wird es dann, wenn Bankdaten (Kontodaten) unbefugt offengelegt werden. In diesen Konstellationen ist ein schnelles Handeln, insbesondere in Form einer vollumfänglichen Information des Betroffenen, für den Verantwortlichen das Gebot der Stunde.

Als anschauliches Beispiel dafür, wie schnell eine risikoreiche Datenschutzverletzung eintritt, kann der gut gemeinte, jedoch missglückte Versuch dienen, mit welchem ein Versorgungsunternehmen im Berichtzeitraum die Aktualisierung seiner Kundendaten durchführen wollte.

Kern der diesbezüglichen Datenverarbeitung war eine Postkarte, welche der Jahresverbrauchsabrechnung an die Kunden beigelegt war. Auf dieser Postkarte konnten die Kunden in hierfür vorgefertigten Feldern, neben den Daten zur Person und zur Rechnungseinheit, auch Bankdaten für die Nutzung eines SEPA-Lastschriftmandats eintragen.

Damit die Datenerhebung für die Kunden kostenneutral war, enthielt die Postkarte den Frankiervermerk "*Entgelt zahlt Empfänger*", was aus Sicht der Kunden jedoch bedeutete, dass man die "Postkarte" auch als solche behandeln, d. h. unverschlossen auf den Postweg geben sollte. Insbesondere mit Blick auf die

Kontodaten war dies mit nicht unerheblichen Risiken verbunden und widersprach den Bestimmungen der Datenschutz-Grundverordnung (DSGVO).

Gemäß Art. 32 DSGVO trifft den Verantwortlichen bei jedweder Verarbeitung personenbezogener Daten die Pflicht, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Verarbeitungsrisiko angemessenes Schutzniveau zu gewährleisten. Dies impliziert es zuvörderst, die Datenverarbeitung vor unbefugter Kenntnisnahme von außen zu schützen.

Zur Erfüllung dieser "Kardinalpflicht" ist das beschriebene Erhebungsverfahren von Kundendaten mittels Postkarte offensichtlich ungeeignet, da es einem unbestimmten Personenkreis die Möglichkeit eröffnet, die Kontodaten der Kunden unbemerkt auf dem Postweg einzusehen.

Die Kenntnis von Name, Geburtsdatum, Anschrift und Kontodaten (IBAN, BIC) kann unter Umständen bereits ausreichen, dass Dritte im Wege eines Lastschriftmissbrauchs oder durch einen unbefugten Kauf auf Rechnung, diese Daten zu Lasten des Betroffenen nutzen.

In ihren Art. 33 und 34 sieht die Datenschutz-Grundverordnung für Fälle vorliegender Art (sog. "Datenpannen") einen zweistufigen Schutzmechanismus vor. Auf der ersten Stufe ist gemäß Art. 33 Abs. 1 DSGVO die zuständige Aufsichtsbehörde binnen 72 Stunden über den Vorfall zu informieren, es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.

Ist ein solches Risiko vorhanden und wird es als hoch eingestuft – was in Fällen einer Datenschutzverletzung betreffend Bank- und Kontodaten oder Datenkategorien nach Art. 9 Abs. 1 DSGVO (bspw. Gesundheitsdaten) in der Regel der Fall ist – so hat der Verantwortliche gemäß Art. 34 Abs. 1 DSGVO die betroffenen Personen unverzüglich, d. h. ohne schuldhaftes Zögern, über die Datenschutzverletzung zu benachrichtigen. Diese

Benachrichtigungspflicht der betroffenen Personen ist kein bloßer Formalismus, sondern wesentlicher Bestandteil einer Risiko- bzw. Schadensminimierung.

Gerade in Bezug auf Bank- und Kontodaten tritt die wichtige Funktion von Art. 34 Abs. 1 DSGVO deutlich zutage, da in diesen Fällen nur die betroffenen Personen oftmals in der Lage sind, einen drohenden Schaden zu verhindern. Die Benachrichtigung soll demnach eine an die betroffene Person gerichtete Empfehlung zur Minderung etwaiger nachteiliger Auswirkungen der Verletzung enthalten (vgl. Art. 34 Abs. 2 i. V. m. Art. 33 Abs. 3 lit. d DSGVO, Erwägungsgrund 86 DSGVO).

Der Verantwortliche sollte die betroffenen Personen im Zuge der Benachrichtigung über die Datenschutzverletzung demnach dahingehend sensibilisieren, dass diese sich im Falle des Bemerkens ungewöhnlicher Kontobewegungen oder Kontoabbuchungen unverzüglich mit dem kontoführenden Kreditinstitut (Bank) in Verbindung setzten sollen, da insbesondere für die Widerspruchmöglichkeit gegen eine unberechtigte Buchung (Lastschrift) Fristen gewahrt werden müssen.

In vorliegender Angelegenheit wurde das betroffene Versorgungsunternehmen unmittelbar nach der Benachrichtigung durch unsere Behörde tätig. Das Erhebungsverfahren der Kundendaten wurde dahingehend geändert, dass nunmehr eine mit Klebelaschen zu verschließende Postkarte zum Einsatz gelangt. Hierdurch kann den Kunden weiterhin eine kostenfreie postalische Übersendung ihrer Daten zur Verfügung gestellt werden, die zu übersendenden Daten werden jedoch, in gleicher Form wie bei einem verschlossenen Briefumschlag, gegen unbefugte Kenntnisnahme von außen geschützt.

Fazit/ Empfehlung:

Datenpannen, bei denen besonders sensible Daten betroffen sind, verpflichten nicht nur zur Meldung an die Aufsichtsbehörde. Regelmäßig ist auch eine Benachrichtigung der betroffenen Person erforderlich.

3.16 Branchenpool Energieversorger

Großes Medienecho hat im abgelaufenen Berichtszeitraum ein Ansinnen der einflussreichsten Wirtschaftsauskunfteien erfahren, einen speziellen Datenpool über Strom- und Gaskunden aufzubauen.

Im Kern ging es darum, die für die Energieversorger wenig ertragreichen sog. Bonus-Hopper zu entlarven und diesen keine Neukundenrabatte zu gewähren. Das Geschäft der Energieversorger ist nämlich so aufgebaut, dass Neukunden einen besonders attraktiven und von den Anbietern subventionierten Tarif erhalten, um dadurch neue Kunden an sich binden zu können. Eine nicht gerade unbeachtliche Zahl an Kunden nutzt dieses Modell in rechtlich nicht zu beanstandender Weise aus und wechselt jährlich den Stromanbieter – mit dem Ziel, jedes Jahr aufs Neue einen günstigen Tarif abschließen zu können. Für die Stromversorger geht die Rechnung insoweit nicht auf, als sich so keine Bestandskunden gewinnen lassen, die nach einem Jahr automatisch in einen teuren Tarif wechseln.

Innerhalb der Datenbank der Auskunfteien sollten branchenweit Vertragsdaten der Kunden von Energieversorgern gesammelt werden (z.B. Vertragsdauer). Hierbei handelt es sich um sog. Positivdaten, die keine Aussage über die Zahlungsmoral beinhalten. Die damit verbundene Befürchtung der Aufsichtsbehörden war, dass dadurch die Anbieter in die Lage versetzt werden, wechselwillige Verbraucher zu identifizieren und entsprechende Anträge auf Abschluss eines Storm- bzw. Gaslieferungsvertrags ablehnen zu können.

Dies hätte zur Konsequenz gehabt, dass vollkommen vertragstreue Kunden künftig mit Nachteilen bei der Strombelieferung hätten rechnen müssen. Anstatt treue Bestandskunden mit Rabattgewährungen zu belohnen, sollte vielmehr an Lockangeboten für Neukunden festgehalten werden, wobei diese Angebote jedoch nicht mehr jedem, sondern nur noch potentiellen Nichtwechselkunden angeboten werden sollten. Dies beißt sich insoweit mit der bisherigen Praxis, als es grundsätzlich originäre Aufgabe der Auskunfteien ist, die Marktteilnehmer vor schwarzen Schafen unter den Verbrauchern zu schützen, die sich nicht vertragstreu verhalten und sich in der Vergangenheit durch eine schlechte Zahlungsmoral ausgezeichnet haben.

Zwar wurde dieses Szenario von Seiten der betroffenen Auskunfteien dementiert. Dennoch hat sich der Arbeitskreis Auskunfteien der Datenschutzbeauftragten des Bundes und der Länder mit der Thematik unter Einbeziehung der Auskunfteienvertreter befasst. Diese teilten darin mit, dass die geplante Datenverarbeitung zu den Energieversorgungskunden so ausgestaltet sei, dass Rückschlüsse auf eine etwaige Wechselneigung ausgeschlossen sind.

Ungeachtet dessen vertreten die Aufsichtsbehörden die Auffassung, dass erhebliche Zweifel an der Zulässigkeit der Verarbeitung von Positivdaten durch Wirtschaftsauskunfteien im Bereich der Energieversorgungsbranche bestehen. Entsprechende Branchenpools zur Identifizierung von wechselwilligen Kunden sind mit den datenschutzrechtlichen Vorgaben nicht in Einklang zu bringen.

Darüber hinaus hätte das beabsichtigte Vorgehen auch eine mögliche Signalwirkung für andere Vertragstypen und Branchen mit der Folge des Entstehens von Vertragsdatenbanken. Der gläserne Kunde wäre damit greifbar nahe.

Fazit/ Empfehlung:

Die Verarbeitung von Positivdaten (z.B. Vertragsdauer) zur Identifizierung von "Bonus-Hoppern" ist unzulässig. Wechselwillige Kunden müssen auch künftig nicht damit rechnen, von attraktiven Neukundenangeboten ausgeschlossen zu werden.

3.17 Bonitätsabfragen durch Unternehmen

Wirtschaftsauskunfteien wie die Creditreform, die Schufa oder Crif Bürgel, sammeln in umfangreichem Maße Informationen über Verbraucher und Unternehmen. Diese Daten umfassen neben Anschriftendaten auch Angaben über negatives Zahlungsverhalten, beispielsweise wenn ein Verbraucher in der Vergangenheit seinen vertraglichen Pflichten in finanzieller Sicht nicht nachgekommen ist. Anhand dieser Informationen erstellen Auskunfteien einen sogenannten Score-Wert, mithilfe dessen potentielle Vertragspartner einschätzen können, ob eine ausreichende Kreditwürdigkeit vorliegt. Hierdurch werden sie in die Lage versetzt entscheiden zu können, ob sie einem Kunden einen Kredit oder auch einen Kauf auf Rechnung anbieten können. Bei einem negativen Score-Wert erhalten Verbraucher wie auch Unternehmen im äußersten Falle überhaupt keine Kredite mehr, was existentielle Auswirkungen für die Betroffenen zur Folge haben kann.

Da im Rahmen einer solchen Bonitätsabfrage bei der Auskunftei durch den möglichen Vertragspartner eines Kunden personenbezogene Daten verarbeitet werden, sind die datenschutzrechtlichen Vorgaben zu beachten. Rechtsgrundlage für diese Verarbeitung kann Art. 6 Abs. 1 lit. f Datenschutz-Grundverordnung (DSGVO) sein. Danach ist die Verarbeitung zulässig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen erforderlich ist, sofern nicht die schutzwürdigen Interessen der Betroffenen der Datenverarbeitung entgegenstehen. Berechtigt ist das Interesse an der Bonitätsabfrage regelmäßig dann, wenn für das abfragende Unternehmen ein kreditorisches Ausfallrisiko

besteht. Wird beispielsweise eine Ware erst versandt, nachdem der Kunde die Rechnung gezahlt hat, ist es grundsätzlich nicht mehr erforderlich, die Zahlungsmoral des Kunden zu durchleuchten. Anders kann dies freilich bei einem Mobilfunkvertrag aussehen. In einem solchen Falle darf das Telekommunikationsunternehmen prüfen, ob der Vertragspartner in der Lage ist, die monatlichen Rechnungen auch begleichen zu können.

Im Berichtszeitraum sind wir wieder vermehrt auf Sachverhalte gestoßen, in denen die Bonitätsabfragen unzulässig erfolgt sind.

In einem konkreten Fall erfuhr ein Betroffener im Rahmen einer bei einer Auskunftei geltend gemachten Selbstauskunft nach Art. 15 DSGVO, dass ein Unternehmen über seine Person eine Bonitätsabfrage eingeholt hatte. Bei dem Unternehmen handelte es sich um einen ehemaligen Vertragspartner des Betroffenen, wobei das Vertragsverhältnis unternehmensseitig gekündigt worden war. Dem Betroffenen schien die Bonitätsabfrage anlasslos zu sein, weshalb er Beschwerde bei der Aufsichtsbehörde einreichte.

Auf Nachfrage teilte das Unternehmen u.a. mit, dass der Beschwerdeführer in der Vergangenheit wiederholt negative Kommentare auf einem privaten Blog des Geschäftsführers des Unternehmens abgegeben habe. Aufgrund dessen begann der Geschäftsführer über den Beschwerdeführer zu recherchieren und stieß auf Jahrzehnte alte Zeitungsberichte, die den Beschwerdeführer mit mehreren Gerichtsverfahren in Verbindung brachten. Dies brachte das Unternehmen auf die Idee, eine Bonitätsabfrage über den Beschwerdeführer einzuholen, obwohl dieser während des bestehenden Vertragsverhältnisses keinerlei negative Zahlungsmoral aufgewiesen hatte. Dass das Unternehmen auf diesem Wege auf negative Zahlungsinformationen des Beschwerdeführers gestoßen ist, muss als reiner Zufallsfund bezeichnet werden. Jedenfalls nahm das Unternehmen diesen Umstand zum Anlass, das Vertragsverhältnis ordentlich zu kündigen.

Ein berechtigtes Interesse für die beschriebene Abfrage bestand mangels drohendem Zahlungsausfalls jedoch weder während des laufenden Vertrages noch nach der Kündigung. Im Rahmen der grundgesetzlich geschützten Privatautonomie wäre es dem Unternehmen ohnehin möglich gewesen, dass Dauerschuldverhältnis nicht weiter zu verlängern. Jedenfalls bedurfte es hierzu keiner Bonitätsabfrage des Beschwerdeführers.

Weiterhin fiel auf, dass es keine unternehmensinternen Vorgaben hinsichtlich der datenschutzkonformen Einholung von Bonitätsauskünften gab. Vielmehr wurden entsprechende Abfragen situativ vorgenommen. Um dies zu vermeiden, wurde mit dem Unternehmen ein datenschutzkonformer Prozess hinsichtlich der künftigen Einholung von Bonitätsabfragen abgestimmt. Es wurde dabei festgelegt, dass in einem mehrstufigen Prozess zu prüfen ist, ob ein berechtigtes Interesse an der Bonitätsauskunft besteht.

In einem weiteren Fall erfuhr ein Betroffener im Rahmen einer Selbstauskunft nach Art. 15 DSGVO, dass ein Unternehmen eine Bonitätsabfrage über seine Person eingeholt hatte, mit dem er nach eigenen Angaben jedoch in keinerlei Geschäftsbeziehung stehe. Das Unternehmen nahm gegenüber der Aufsichtsbehörde dahingehend Stellung, dass es sich bei dem Betroffenen um eine ehemalige Aushilfskraft eines Schwesterunternehmens handele. Dessen Lebensgefährte sei ein ehemaliger Mitarbeiter des Unternehmens, mit dem man sich in einer zivil- und strafrechtlichen Auseinandersetzung wegen Betruges im Zusammenhang mit arbeitsvertraglichen Pflichten befinde. Vor diesem Hintergrund sah man sich veranlasst, im Umfeld des Lebensgefährten über potentielle Tatmotive zu recherchieren. Insofern habe man auch die wirtschaftliche Lage des Beschwerdeführers unter die Lupe nehmen wollen, um mögliche Zusammenhänge herleiten zu können. Weitere Erläuterungen, inwiefern die Bonität des Beschwerdeführers hierfür erforderlich gewesen sein soll, wurden nicht vorgetragen. Ein berechtigtes Interesse lag demzufolge nicht vor. Das Unternehmen hat den datenschutzrechtlichen Verstoß schließlich eingeräumt.

Hinsichtlich der beiden datenschutzrechtlichen Verstöße wurden Bußgeldverfahren nach Maßgabe von Art. 83 DSGVO eingeleitet.

Fazit/ Empfehlung:

Bonitätsabfragen sind nur bei Vorliegen eines berechtigten Interesses des abfragenden Unternehmens zulässig. Das berechtigte Interesse besteht grundsätzlich in der Vermeidung von Zahlungsausfällen und kann daher nur dann geltend gemacht werden, wenn ein kreditorisches Ausfallrisiko (Kreditverträge, Rechnungskauf etc.) gegeben ist. In einigen Fällen werden Bonitätsdaten zweckwidrig abgefragt. Verbraucher sollten daher stets prüfen, welche Unternehmen über ihre Person eine Bonitätsauskunft einholen. Dies können sie über eine kostenfreie Selbstauskunft nach Art. 15 DSGVO, welche gegenüber den Auskunfteien geltend gemacht werden kann, in Erfahrung bringen.

3.18 Kreditwirtschaft

3.18.1 Videoüberwachung in Banken

Die Regellöschfrist bei Videoüberwachung beträgt grundsätzlich 48 bis 72 Stunden. Jedoch ist in Banken eine Sondersituation anzuerkennen, die für verschiedene Bereiche eine darüberhinausgehende Speicherdauer rechtfertigt. Dabei sind jedoch die einzelnen Bereiche einzeln zu betrachten, die besonderen Situationen darzulegen und unter Berücksichtigung der vorgetragenen Aspekte eine angemessene Speicherdauer festzulegen.

Für den Bereich des Foyers wurde seitens der Banken geltend gemacht, dass ein Zugang auch außerhalb der Öffnungszeiten möglich sei. Der unbefugte Zugriff auf Schließfächer an Feiertagen, die Ausspähung im Vorfeld eines Überfalls und die Mani-

pulation an den Schließanlagen könnten oftmals erst Tage später festgestellt werden. Vor diesem Hintergrund wird die seitens der Kreditwirtschaft für erforderlich erachtete Speicherdauer von einer Woche zur Sicherstellung von Beweisen und zur Strafverfolgung von den Aufsichtsbehörden akzeptiert.

Im Bereich der Geldautomaten ist bei der Bemessung der Speicherdauer zudem die Beweislastumkehr zu Lasten der Kreditinstitute zu berücksichtigen, wonach das Kreditinstitut im Falle des Bestreitens nachweisen muss, dass der Kunde eine Transaktion am Geldautomaten getätigt hat. Vor diesem Hintergrund erscheint eine Speicherdauer orientiert an dem Zeitraum, in dem eine Transaktion bestritten werden kann, akzeptabel. Danach sind die Rechnungsabschlussperiode von 3 Monaten, plus eine Woche Versandlaufzeit, plus sechs Wochen Einwendungsfrist des Kunden nach Zugang zu Grunde zu legen, welches insgesamt eine Speicherfrist von 142 Tagen ergibt.

Eine Videoüberwachung mit in Geldausgabeautomaten eingebauten Kameras im öffentlichen Raum ist allerdings nur zulässig, wenn die Aufzeichnung erst bei Bedienung des Automaten beginnt.

Für den Schalterbereich sehen die Banken zur Sicherung von Beweisen und zur Strafverfolgung sowie mit Blick auf geltende Unfallverhütungsvorschriften eine Speicherdauer von 30 Tagen vor, welche zu diesem Zeitpunkt von den Aufsichtsbehörden noch nicht als nachvollziehbar erachtet wird und eine weitere Darlegung seitens der Bankenverbände erfordert.

Generell gilt es bei der Videoüberwachung zu beachten, dass ein strenges Zugriffs- und Berechtigungskonzept vorzusehen ist und Hinweispflichten mit differenzierten Angaben umzusetzen sind, so dass klar erkennbar ist, in welchem Bereich welche Speicherdauer gilt.

Fazit/ Empfehlung:

Hinsichtlich der Speicherdauer von Videoaufnahmen in einer Bank ist nach den überwachten Bereichen und dem jeweiligen Zweck der Überwachung zu unterscheiden. Für den Bereich des Foyers wird eine Speicherdauer von einer Woche und für den der Geldausgabeautomaten von 142 Tagen akzeptiert.

3.18.2 Übermittlung der IBAN-Nummer des Überweisenden

Bereits seit einigen Jahren wird immer wieder diskutiert, ob im Rahmen einer Überweisung die Übermittlung der IBAN des Überweisenden an den Zahlungsempfänger zulässig ist.

Im Jahr 2015 wurde seitens der Aufsichtsbehörden die Position vertreten, dass dies nicht zulässig ist, da insbesondere weder Art. 248 § 8 Nr. 1 Einführungsgesetz zum Bürgerlichen Gesetzbuch (EGBGB) noch § 675r des Bürgerlichen Gesetzbuchs (BGB) eine entsprechende Rechtsgrundlage darstellten. Art. 248 § 8 Nr. 1 EGBGB bestimmte damals, dass dem Zahlungsempfänger weitere mit dem Zahlungsvorgang übermittelte Angaben mitzuteilen sind. Die neue Fassung der Norm sieht nunmehr vor, dass alle weiteren mit dem Zahlungsvorgang übermittelten Angaben mitzuteilen sind [siehe auch Art. 58 Abs. 1 lit. a der Zweiten Zahlungsdiensterichtlinie (RL (EU) 2015/2366)]. Daher diskutierten die Aufsichtsbehörden im Berichtszeitraum, ob die Übermittlung der IBAN an den Zahlungsempfänger nunmehr aufgrund einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 lit. c Datenschutz-Grundverordnung (DSGVO) zulässig ist.

Im Ergebnis halten die Aufsichtsbehörden weiterhin an ihrer Position aus dem Jahr 2015 fest, dass keine bankaufsichtsrechtliche Pflicht besteht, dem Übertragungsempfänger die IBAN des Überweisenden zu übermitteln. Dies ergibt sich letztlich auch mit Blick auf eine in diesem Zusammenhang eingeholte Stellungnahme der BaFin, welche aus der zitierten Vorschrift eben-

falls keine dahingehende Verpflichtung herleitet. Die regelmäßige automatische Übermittlung insbesondere durch Abdruck auf dem Kontoauszug ist daher weder nach Art. 6 Abs. 1 S. 1 lit. c DSGVO noch nach Art. 6 Abs. 1 S. 1 lit. f DSGVO erforderlich. Eine Ausweisung im Bereich des Online-Bankings auf ein gezieltes Auswählen hin wird indessen vorläufig akzeptiert.

Fazit/ Empfehlung:

Die regelmäßige automatische Übermittlung der IBAN-Nummer des Überweisenden durch bspw. Abdruck auf dem Kontoauszug des Zahlungsempfängers ist unzulässig.

3.18.3 Einwilligungserklärungen der Sparkassen

Die Sparkassen verwenden Einwilligungsformulare über die Analyse verschiedener Daten zur Person sowie von Zahlungsverkehrsdaten.

In diesem Zusammenhang gab es einerseits einige Beschwerden von Kundinnen und Kunden, die monierten, dass die Formulare vorangekreuzt seien oder sie unter Hinweis auf die Erforderlichkeit der Einwilligung für die Fortführung des Geschäftsverhältnisses zu einer entsprechenden Willenserklärung bewegt worden seien.

Andererseits hatten auch die Aufsichtsbehörden gegenüber dem Deutschen Sparkassen und Giroverband einige Kritikpunkte hinsichtlich der Gestaltung der Einwilligungserklärungen geltend gemacht. Zwischenzeitlich hat man sich auf eine Neugestaltung des Formulars geeinigt, die zum einen eine Trennung der Einwilligung über die Analyse von Daten bei Nutzung digitaler Angebote der Sparkasse beinhaltet. Zum anderen wurde hinsichtlich dieser Analyse sichergestellt, dass keine sensitiven Daten verwendet werden. Neben einer kleineren Ergän-

zung wurde weiterhin festgelegt, dass die Reichweite der Einwilligungserklärung in den Datenschutzhinweisen erläutert wird.

Nach wie vor gibt es jedoch vereinzelte Beschwerden im Hinblick auf die Freiwilligkeit der Einwilligung. So wurde auch im Berichtszeitraum vorgetragen, dass die von den Sparkassen vorgelegten Formulare in allen Abschnitten bereits durch die Sparkasse vorangekreuzt seien und dass den Kunden eine Einwilligung unter Hinweis darauf, dass Vorschriften des Geldwäschegesetzes oder die Aufrechterhaltung der Geschäftsbeziehung eine solche erforderten, nahegelegt würde. Die betroffenen Sparkassen versicherten indessen, keine vorangekreuzten Formulare zu verwenden und dass ein individuelles Ankreuzen nur nach entsprechender Erörterung unter Betonung der Freiwilligkeit auf Wunsch der Kundin/des Kunden erfolge. Auf Nachfrage der Aufsichtsbehörde wurde seitens der betroffenen Sparkassen bestätigt, dass entsprechende Schulungen und eine dahingehende Sensibilisierung der Mitarbeiterinnen und Mitarbeiter der Sparkassen erfolgten.

Fazit/ Empfehlung:

Die Einwilligungsformulare der Sparkassen wurden entsprechend der von den Aufsichtsbehörden formulierten Anforderungen umgestaltet. Es gilt weiterhin darauf zu achten, dass Felder nicht vorangekreuzt sind und auf die Freiwilligkeit der Einwilligung hingewiesen wird.

3.18.4 Personalausweiskopien nach der Neufassung des § 8 Abs. 1 GwG

Unter der bis Juni 2017 geltenden Rechtslage vertraten die Aufsichtsbehörden die Auffassung, dass die Anfertigung von Kopien von Personalausweisen durch Banken bei der Überprüfung der Identität natürlicher Personen nur unter Schwärzung nicht erforderlicher Angaben zulässig war. Nachdem jedoch

durch eine Änderung des Geldwäschegesetzes (GwG) zum Juli 2017 in § 8 Abs. 2 Satz 2 nunmehr festgelegt war, dass *vollständige* Kopien der Dokumente zur Überprüfung der Identität anzufertigen sind, war die Vorgabe von Schwärzungen nicht mehr aufrechtzuerhalten. Vor dem Hintergrund einer neuerlichen Gesetzesänderung im Berichtszeitraum wurde diese Frage jedoch erneut diskutiert.

Die neue Formulierung des § 8 Abs. 2 GwG sah nun unter Streichung des Wortes „vollständig" nur noch die Anfertigung von Kopien vor, ohne dass aus der Gesetzesbegründung die Beweggründe für diese Änderung ersichtlich sind. Der materiell-rechtliche Gehalt der Änderung ist lediglich dahingehend ersichtlich, dass eine Erweiterung der Regelung auf den Fall des Vor-Ort-Auslesens von Personendaten getroffen wurde. Auch das vor diesem Hintergrund um Stellungnahme gebetene Bundesministerium der Finanzen führte in einem Schreiben an die Aufsichtsbehörden aus, dass eine materiell-rechtliche Änderung mit der Streichung des Wortes „vollständig" nicht verbunden und auch nicht beabsichtigt gewesen sei.

Der Wortlaut der neuen Vorschrift dürfte jedoch aus hiesiger Sicht durchaus eine neuerliche Berücksichtigung des Grundsatzes der Datenminimierung nach Art. 5 Abs. 1 lit. a Datenschutz-Grundverordnung (DSGVO) und eine Beschränkung der Kopie auf die notwendigen Angaben erlauben. Mit Blick darauf, dass eine dahingehende gesetzgeberische Änderung nicht beabsichtigt war, wird auf eine entsprechende dahingehende Forderung zu diesem Zeitpunkt indessen verzichtet. Eine abschließende gemeinsame Positionierung der Aufsichtsbehörden stand zum Zeitpunkt der Berichtsfassung noch aus.

Fazit/ Empfehlung:

Ob vollständige Personalausweiskopien nach dem neu gefassten § 8 Abs. 2 GwG weiterhin zulässig sind, ist umstritten. Eine abschließende Positionierung der Aufsichtsbehörden steht noch aus.

3.18.5 Love Scamming - Übermittlung personenbezogener Daten bei Verdacht auf Betrug

Der Datenschutzbeauftragte einer Sparkasse wandte sich an hiesige Behörde mit der Frage, ob eine Übermittlung personenbezogener Daten von Kunden durch Banken an die Polizei in Fällen des Verdachts auf Betrug im Zusammenhang mit dem sog. „Love Scamming" aus datenschutzrechtlicher Sicht auch ohne Einwilligung des Kunden bzw. der betroffenen Person zulässig ist. Es handelt sich dabei um solche Fälle, in denen Betrüger die betroffene Person mittels vorgetäuschter Liebe zur Überweisung von Geldbeträgen bewegen.

Eine gesetzliche Verpflichtung – vergleichbar mit bspw. Meldepflichten nach dem Geldwäschegesetz – ist für den Fall des Verdachts auf „Love Scamming" zunächst nicht ersichtlich. Eine solche kann sich hingegen aus § 161 Strafprozessordnung (StPO) ergeben, jedoch nur, wenn sich die Ermittlungsbehörden mit einem entsprechenden Auskunftsverlangen an die Bank wenden.

Soweit ein solches Verlangen jedoch nicht vorliegt, kommt als Rechtfertigungstatbestand für Datenweitergaben von der Bank an Ermittlungsbehörden die Wahrung berechtigter Interessen gemäß Art. 6 Abs. 1 lit. f Datenschutz-Grundverordnung (DSGVO) in Betracht. So erkennt Erwägungsgrund 50 Satz 8 der DSGVO die Übermittlung personenbezogener Daten zu Strafverfolgungszwecken als ein berechtigtes Interesse an. Dabei müssen das Interesse an der Übermittlung und der Beitrag zur Wahrung der öffentlichen Sicherheit die Interessen des Betroffenen an seiner informationellen Selbstbestimmung jedoch

überwiegen. Daneben ist § 24 Abs. 1 Nr. 1 Bundesdatenschutzgesetz (BDSG) zu berücksichtigen, welcher bestimmt, dass die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch nichtöffentliche Stellen zulässig ist, wenn sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.

Demnach ist – ebenso wie unter Heranziehung von Art. 6 Abs. 1 lit. f DSGVO – seitens des Verantwortlichen eine Interessenabwägung vorzunehmen, in deren Rahmen durchaus problematisch erscheint, dass die betroffene Person nicht die verdächtige Person ist und die Notwendigkeit des geltend gemachten Schutzes ihres Vermögens selbst möglicherweise nicht anerkennt. Dabei ist auch zu berücksichtigen, dass im geltend gemachten Zusammenhang sehr private Umstände der betroffenen Person eine Rolle spielen. Insoweit ist ebenfalls von Belang, welche personenbezogenen Daten im Einzelfall an die Polizei übermittelt werden sollen und als erforderlich für den geltend gemachten Zweck zu sehen sind.

Fazit/ Empfehlung:

Ob eine Übermittlung personenbezogener Daten durch die Bank an die Polizei bei Verdacht auf Betrug im Rahmen des sog. „Love Scammings“ zulässig ist, richtet sich nach einer in diesem Zusammenhang vorzunehmenden Interessenabwägung.

3.19 Versicherungswirtschaft

Im Bereich der privaten Versicherungswirtschaft können von den sogenannten Stammdaten (Name, Anschrift, Geburtsdatum, E-Mail-Adresse etc.) bis hin zu Gesundheitsdaten nach Art. 9 Datenschutz-Grundverordnung (DSGVO) alle Kategorien von

personenbezogenen Daten betroffen sein. Entsprechend breit gestreut sind auch die Beschwerden gegen Versicherungsunternehmen, wobei es auch hier spezielle Themenbereiche gibt, die jedes Jahr erneut auftauchen. An dieser Stelle ist etwa die Einwilligungs- und Schweigepflichtentbindungserklärung zu nennen.

3.19.1 Einwilligungs- und Schweigepflichtentbindungserklärung

In der privaten Versicherungswirtschaft kann es etwa zur Risikoprüfung oder zur Beurteilung der Leistungspflicht erforderlich sein, Gesundheitsdaten zu verarbeiten. Offensichtlich ist dies zum Beispiel bei Kranken- und Lebensversicherungen. Hier schreibt § 213 Versicherungsvertragsgesetz (VVG) vor, dass Versicherer für die Erhebung von Gesundheitsdaten u.a. eine Einwilligung der betroffenen Person benötigen. Gleichzeitig handelt es sich um Daten, die durch § 203 Strafgesetzbuch (StGB) und Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO) einem besonderen Schutz unterliegen, so dass diese Daten durch den Versicherer bei Dritten, wie etwa Ärzten und Krankenhäusern, nur erhoben werden dürfen, wenn die betroffene Person neben der Einwilligung auch eine Entbindung von der Schweigepflicht erteilt hat. Dieses gesetzliche Konstrukt führt sodann regelmäßig sowohl zu Beschwerden von betroffenen Personen als auch zu Fragen auf Seiten der Dritten, bei denen diese Daten angefragt werden. Im Kern geht es dabei in der Regel um die Frage, ob und inwieweit die vorgelegten Erklärungen den gesetzlichen Vorgaben entsprechen und zulässig sind, sowie die Frage, ob und inwieweit die Erhebung personenbezogener Gesundheitsdaten für die Beurteilung des zu versichernden Risikos oder der Leistungspflicht erforderlich ist. Gerade letztere Frage ist stets anhand des konkreten Einzelfalls zu beurteilen.

3.19.2 Digitale Versicherung

Immer mehr Versicherungsunternehmen bieten an, Versicherungen auch digital abzuschließen. Dies bedingt aber, dass die

versicherungsrechtlichen Anforderungen in Einklang zu bringen sind mit dem Interesse des Versicherungsnehmers, seine Daten zu schützen. So obliegt es den Versicherungen etwa nach § 7 Versicherungsvertragsgesetz (VVG) und der dazugehörigen Verordnung über Informationspflichten bei Versicherungsverträgen den Versicherungsnehmer auch über sensiblere Informationen, wie zum Beispiel Einzelheiten zur Beitragszahlung, zu informieren. Werden solche Informationen auch online zur Verfügung gestellt, bedingt dies auf Seiten der technischen und organisatorischen Maßnahmen auch angepasste Lösungen. Wenn beispielsweise eine (teilweise) Verschleierung der Informationen nicht möglich ist und diese im Klartext angezeigt werden müssen, dann ist dies etwa bei dem Online-Registrierungsprozess und der Online-Authentifizierung durch weitergehende Schutzmaßnahmen (wie etwa eine Zweifaktorauthentifizierung, einen individualisierte Registrierungslink etc.) auszugleichen.

3.20 Direktmarketing

Unverlangte Werbebotschaften gaben auch im zurückliegenden Berichtszeitraum häufig Anlass für an unsere Dienststelle gerichteten Beschwerden. Eine Vielzahl dieser Beschwerden wäre bereits dadurch vermeidbar gewesen, wenn die werbenden Unternehmen transparenter über Herkunft und Umstände der für Zwecke des Direktmarketings verwendeten personenbezogenen Daten informiert oder auf geltend gemachte Auskunftsansprüche der Werbeadressaten nach Art. 15 Datenschutz-Grundverordnung (DSGVO) fristgerecht reagiert hätten.

Fehleinschätzungen der datenschutzrechtlichen Bedingungen bei der Datenverarbeitung im Kontext des Direktmarketings sind dabei gerade nicht nur mittelständischen Betrieben zuzuschreiben, sondern auch großen Unternehmen.

Vor diesem Hintergrund kann den Verantwortlichen auch die aktualisierte Fassung der Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwe-

cke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung[11] als Hilfestellung bei der Ausgestaltung der diesbezüglichen Datenverarbeitungsprozesse dienen.

3.20.1 Telefonische und E-Mail-gestützte Kundengewinnung

Kundenakquise oder -bindung und die damit verbundene Verarbeitung personenbezogener Daten für Zwecke des Direktmarketings ist für viele Verantwortliche ein wesentliches Element ihrer Geschäftstätigkeit. Obschon im Hinblick auf Erwägungsgrund 47 der Datenschutz-Grundverordnung (DSGVO) Direktwerbung als berechtigtes Verarbeitungsinteresse anzusehen ist, sind von werbetreibenden Verantwortlichen für unterschiedliche Formen von Werbeansprachen spezifische Zulässigkeitsvorbehalte zu beachten.

Beschwerden zu Direktmarketingmaßnahmen thematisieren nach wie vor zumeist telefonische oder E-Mail-gestützte Marketingmaßnahmen, denen kein geschäftlicher Kontakt zwischen Adressat und Absender der Werbebotschaft vorausgeht. Solche Werbemaßnahmen kann das werbende Unternehmen insbesondere auch nicht auf seine berechtigten Interessen im Sinne des Art. 6 Abs. 1 lit. f DSGVO stützen, da die datenschutzrechtliche Zulässigkeit durch den wettbewerbsrechtlichen Einwilligungsvorbehalt nach § 7 Abs. 2 oder 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG) determiniert wird. Dementsprechend muss das werbende Unternehmen darlegen können, dass die Marketingmaßnahme auf eine wirksame Einwilligung des Werbeadressaten gestützt werden kann.[12] In der Prüfpraxis ist allerdings oftmals festzustellen, dass viele Unternehmen diese engen Zulässigkeitsvoraussetzungen nicht berücksichtigen.

[11] Derzeitige Fassung mit Stand 8. Oktober 2018; abrufbar unter https://www.datenschutz.saarland.de/themen/werbung.

[12] Verwaltungsgericht des Saarlandes, Urteil vom 29. Oktober 2019 – 1 K 732/19.

So wurden wir aufgrund einer Beschwerde auf ein Unternehmen aufmerksam, welches über einen Adresshändler berufsgruppenspezifische Kontaktdaten bezogen hat und den Adressaten zunächst eine postalische Werbebotschaft übersandte. Dieses Anschreiben enthielt unter anderem den Hinweis, dass, sofern seitens der Adressaten kein Opt-out erklärt wird, in einem nächsten Schritt eine Werbeansprache per E-Mail erfolgt. Seitens des Unternehmens wurde dabei die Ansicht vertreten, dass die ohnehin im Internet abrufbaren E-Mail-Adressen der Adressaten eine derartige Datenverwendung auch ohne Einwilligung der Betroffenen ermögliche. Eine derartige Rechtsauffassung war im Hinblick auf den wettbewerbsrechtlichen Einwilligungsvorbehalt nach § 7 Abs. 3 UWG nicht überzeugend und die Verarbeitung personenbezogener Daten der Empfänger der Werbemails somit nicht nach Art. 6 Abs. 1 lit. f DSGVO legitimiert.

Fazit/ Empfehlung:

Telefonischen oder E-Mail-gestützten Maßnahmen zum Direktmarketing mit dem Ziel der Kundengewinnung müssen wirksame Einwilligungen der Werbeadressaten zugrunde liegen.

3.20.2 Kooperation im Direktmarketing

Die Vorgehensweise, dass Unternehmen vorgefertigte Blanko-Werbebotschaften an Partnerunternehmen (Adresseigner) übermitteln, damit diese den eigenen Kundenbestand in fremden Namen bewerben, ist üblich und begegnet grundsätzlich keiner datenschutzrechtlichen Kritik. Das Unternehmen, in dessen Namen geworben wird, erhält dabei zwar keine Kundendaten von dem die Werbung aussendenden Partnerunternehmen, allerdings kann sich auch ohne Zugriff auf Kundendaten eine datenschutzrechtliche Verantwortlichkeit für beide Akteure ergeben.

Während das werbende Unternehmen durch eine Vorgabe von Selektionsmerkmalen (bspw. Alter, Geschlecht, Wohnort etc.)

den Zweck der Kundengewinnung durch zielgruppenspezifische Werbeansprache verfolgt, nutzt der Adresseigner die ihm vorliegenden Adressdatenbestände gegen Entgelt für fremde Werbezwecke. Trotz vermeintlich unterschiedlicher Zwecke kann im Kontext des Direktmarketings von einer gemeinsamen datenschutzrechtlichen Verantwortlichkeit im Sinne des Art. 26 Datenschutz-Grundverordnung (DSGVO) ausgegangen werden.[13] Ausreichend für die Annahme einer die gemeinsame Verantwortlichkeit bedingenden gemeinsamen Entscheidung über Zwecke und Mittel kann dabei sein, dass ein Akteur die Datenverarbeitung beispielsweise durch Vorgabe von Rahmenbedingungen organisiert und koordiniert; dabei ist unbeachtlich, ob dass die Werbemaßnahme initiierende Unternehmen auf die zu verarbeitenden personenbezogenen Daten des Adresseigners zugreifen kann oder diesem Anleitungen oder Anweisungen zur konkreten Datenverarbeitung vorgibt.[14] Ist von einer gemeinsamen datenschutzrechtlichen Verantwortlichkeit auszugehen, haben die gemeinsam Verantwortlichen nach Art. 26 Abs. 1 Satz 2 DSGVO in einer für den Adressaten der Werbung transparenten Form festzulegen, wer von ihnen welche in der DSGVO geregelten Verpflichtungen erfüllt; dies gilt insbesondere für die Betroffenenrechte und die Informationspflichten nach Art. 13 und 14 DSGVO.

Fazit/ Empfehlung:

Greifen Unternehmen für Marketingmaßnahmen nicht auf eigene, sondern auf Adressbestände Dritter zurück, ist bei Vorliegen einer gemeinsamen Verantwortlichkeit im Sinne des Art. 26 Abs. 1 DSGVO eine Vereinbarung nach Art. 26 Abs. 1 Satz 2 DSGVO obligatorisch.

[13] Schlussantrag des Generalanwalts Bobek vom 19. Dezember 2018, C-40/17, Rdnr. 105.

[14] 3. Leitsatz der Entscheidung des Europäischen Gerichtshofs vom 10. Juli 2018, C-25/17.

3.21 Auskunftsersuchen bei Identitätsdiebstahl

Immer wieder kommt es zu sogenannten Identitätsdiebstählen. Dabei liegt in leicht unterschiedlichen Variationen ein bestimmter Sachverhalt zugrunde: Die Identität einer Person wird genutzt, um bei einem Online-Versandhändler ein Kundenkonto anzulegen oder es wird ein bereits existierendes Kundenkonto einer Person genutzt, um Waren auf deren Kosten zu bestellen. Die Waren werden entweder an deren Anschrift oder eine andere, ggf. ihr unbekannte Adresse versendet. Nachdem der Inhaber der Identität von diesen kriminellen Aktivitäten Kenntnis erlangt hat, verlangt er nunmehr vom Online-Versandhändler Auskunft nach Art. 15 Datenschutz-Grundverordnung (DSGVO) zu allen Daten, die zu diesem Konto und den dazugehörigen Bestellungen geführt werden, also auch die Daten, die der Datendieb als Besteller angegeben hat (z.B. E-Mail-Adresse oder abweichende Lieferadressen). Der Online-Versandhändler verweigert die Auskunft mit dem Hinweis auf laufende Ermittlungen der Strafverfolgungsbehörden.

Die Frage, wie mit derartigen Auskunftsersuchen im Hinblick auf die Daten des Datendiebs umzugehen ist, beschäftigten im Berichtszeitraum nicht nur die Arbeitskreise der Datenschutzkonferenz (DSK), sondern auch die Key-Provisions-Subgroup des Europäischen Datenschutzausschusses (EDSA).

Das Recht auf Auskunft nach Art. 15 DSGVO bezieht sich immer auf die personenbezogenen Daten, bei denen es sich nach der Definition des Art. 4 Nr. 1 DSGVO um alle Informationen handelt, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dies ist unproblematisch, insofern es sich um Daten des Identitätsinhabers handelt (also etwa um dessen Name, Adresse oder Bankverbindung etc.). Soweit es sich aber um Daten des Datendiebs (z.B. E-Mail-Adresse oder abweichende Lieferadresse) handelt, könnte eingewendet werden, dass es sich um die Daten eines Dritten und nicht die des Identitätsinhabers handelt. Allerdings muss man an dieser Stelle konstatieren, dass der Datendieb diese Informationen mit dem Ziel hinzugefügt hat, dass diese Daten dem Identitätsinhaber

zugerechnet werden und hat damit den Personenbezug zu dem Identitätsinhaber hergestellt. Folglich handelt es sich zumindest auch um Daten des Identitätsinhabers, die insofern auch zu beauskunften sind.

Diese Diskussion ist auf europäischer Ebene jedoch noch im Gange und die Bewertung des EDSA bleibt abzuwarten.

3.22 Einsicht in die Patientenakte

Im 28. Tätigkeitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit[15] wurde das Thema der Einsichtnahme in die Patientenakte aufgegriffen. Von Interesse ist hierbei insbesondere das Verhältnis des datenschutzrechtlichen Auskunftsanspruchs gemäß Art. 15 Datenschutz-Grundverordnung (DSGVO) zu dem in § 630g Bürgerliches Gesetzbuch (BGB) normierten Recht auf Einsichtnahme in die Patientenakte, auch weil Art. 15 Abs. 3 DSGVO einen Anspruch auf eine kostenlose Kopie der personenbezogenen Daten begründet, während nach § 630g BGB die Kosten für die Kopie der Behandlungsdokumentation dem Patienten in Rechnung gestellt werden dürfen.

Das Unabhängige Datenschutzzentrum Saarland stellt bisher bei der Bearbeitung von Anfragen oder Beschwerden in diesem Zusammenhang darauf ab, welches Anliegen der betroffene Patient im konkreten Fall verfolgt.

Im Berichtszeitraum erging nun ein erstes Urteil zur Frage der kostenlosen Kopie der Patientenakte (Landgericht Dresden, Urteil vom 29.5.2020 – 6 O 76/20). Darin heißt es, der Klägerin stehe als Patientin *neben* der spezialgesetzlichen Regelung des § 630g BGB auch ein Anspruch aus Art. 15 Abs. 3 DSGVO zu. Dabei komme es nicht darauf an, für welchen Zweck (im vorliegenden Fall zivilrechtliche Haftungsansprüche) der Auskunftsanspruch geltend gemacht wird. Weiter führt das Gericht aus: *„Die Regelung des § 630 g BGB hat nicht Vorrang vor den Bestimmungen des Art. 15 Abs. 3 DSGVO. Ein Vorrangverhältnis als*

[15] Vgl. 28. Tätigkeitsbericht 2019, Kapitel 4.21, S. 119 ff.

lex spezialis kann eine Regelung auf nationaler Ebene bezüglich einer europarechtlichen Regelung nicht enthalten. Die DSGVO sieht eine Öffnung für anderslautende nationale Regelungen nicht vor. Mithin ist einem Auskunftsverlangen, welches statt auf § 630 g BGB auf Art. 15 Abs. 3 DSGVO gestützt wird, vollumfänglich zu entsprechen."

Die interessante Frage nach der vollständigen Deckungsgleichheit der beiden Anspruchsgrundlagen lässt das Gericht offen.

Im Ergebnis lässt sich festhalten, dass das Gericht die BGB-Vorschrift nicht als vorrangige spezielle Regelung gegenüber dem Auskunftsrecht nach DSGVO einordnet, sondern von zwei nebeneinander existierenden Anspruchsgrundlagen ausgeht. Diese Auffassung deckt sich mit der des Unabhängigen Datenschutzzentrums Saarland. Die weitere Entwicklung in dieser Thematik bleibt abzuwarten.

Fazit/ Empfehlung:

Patienten haben neben dem Recht auf Akteneinsicht nach dem BGB auch einen datenschutzrechtlichen Anspruch auf Auskunft über den Inhalt der Behandlungsdokumentation.

3.23 Betriebsvereinbarung zum Einsatz von GPS

Ein großes Logistikunternehmen führte zur besseren Einsatzplanung der Fahrzeugflotte ein GPS-System zur Ortung der Fahrzeuge ein. Weder wurden die Beschäftigten des Unternehmens hierüber ausreichend informiert noch wurde der Betriebsrat beteiligt. Das Resultat dieser intransparenten Einführung eines möglichen Überwachungsinstruments für die Beschäftigten war eine Beschwerde beim Unabhängigen Datenschutzzentrum (UDZ) des Saarlandes als zuständiger Datenschutzaufsichtsbehörde.

In einer ersten Stellungnahme war man sich der datenschutzrechtlichen Brisanz eines GPS-Ortungssystems nicht ganz bewusst. So konnte erst nach genauerer Recherche festgestellt werden, dass das System in der Lage war, das Fahrverhalten der Fahrer, Geschwindigkeitsüberschreitungen und das Verlassen von bestimmten Routen zu dokumentieren. All diese Möglichkeiten waren für den vorgesehenen Zweck des Ortungssystems gar nicht erforderlich, denn eigentlich sollten lediglich Routen zeitlich optimiert und Ausfälle durch den nächstgelegenen Fahrer kompensiert werden.

Dieses Vorgehen verstößt gegen die Vorgaben des Art. 25 Datenschutz-Grundverordnung (DSGVO), der den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen regelt. So hätte das Unternehmen im Vorfeld der Einführung nur die zur Zweckerreichung erforderlichen Felder freischalten lassen dürfen und die nicht erforderlichen Felder des Systems sperren lassen können.

In einer Besprechung mit den Verantwortlichen des Unternehmens trafen wir auf eine sehr große Kooperationsbereitschaft. Man beteuerte, dass man nicht die Absicht verfolgt hätte, seine Beschäftigten zu kontrollieren, sondern lediglich ein Mittel zur besseren Logistikdisposition einsetzten wollte.

Aufgrund der vorgetragenen datenschutzrechtlichen Bedenken folgte das Unternehmen unseren Empfehlungen und konfigurierte das GPS-System datenschutzkonform, erstellte in Zusammenarbeit mit dem Betriebsrat eine entsprechende Betriebsvereinbarung als Rechtsgrundlage für die Datenverarbeitung durch das GPS-System und informierte die Beschäftigten transparent über das eingesetzte GPS-Ortungssystem. Uns als Aufsichtsbehörde wurden die Ergebnisse vorgelegt, so dass man nunmehr von einem datenschutzkonformen Zustand beim Einsatz des GPS-Ortungssystems im Unternehmen ausgehen kann.

Fazit/ Empfehlung:

Der Abschluss einer Betriebsvereinbarung bei Anwendungen, die zur Leistungs- und Verhaltenskontrolle von Beschäftigten geeignet sind, stellt eine transparente und datenschutzkonforme Lösungsmöglichkeit dar.

3.24 Parteien und E-Mail-Verteiler

Beschwerden im Bereich der Parteienarbeit betreffen häufig das gleiche Problem: offene E-Mail-Verteiler.

Parteifunktionäre und deren Mitarbeiter informieren ihre Mitglieder aufgrund des dynamischen Politikgeschehens gerne auf schnellem Wege per E-Mail. Dabei werden E-Mails mit aktuellem politischem Inhalt oder auch mit internen Parteiangelegenheiten an eine Vielzahl von Empfängern versendet.

In diesem Zusammenhang kommt es häufiger vor, dass die E-Mail-Adressen der Empfänger für alle anderen sichtbar im CC-Feld hinterlegt werden. Dies führt zwangsläufig dazu, dass sämtliche Empfänger Kenntnis von allen E-Mail-Adressen erhalten.

Aus datenschutzrechtlicher Sicht ist dieses Vorgehen problematisch. Die E-Mail-Adressen der Empfänger sind mit wenigen Ausnahmen grundsätzlich als personenbezogene Daten zu qualifizieren. Die Empfänger wiederum sind im Verhältnis zueinander als Dritte zu bezeichnen. Durch das Setzen der E-Mail-Adressen in das CC-Feld werden somit personenbezogene Daten an eine Vielzahl Dritter übermittelt.

Diese Datenverarbeitung kann auf keine Rechtsgrundlage gestützt werden. Insbesondere können die Parteimitglieder über aktuelle parteiliche Themen auch informiert werden, ohne dass ihre E-Mail-Adresse anderen Mitgliedern gegenüber offenbart wird. Die beschriebene Datenverarbeitung lässt sich leicht vermeiden, indem die E-Mail-Adressen der Empfänger in das BCC-Feld gesetzt werden und damit nicht sichtbar sind.

Kritisch ist das Vorgehen aber auch deshalb, da in diesem Zusammenhang durch die E-Mail-Adresse Rückschlüsse auf die Parteizugehörigkeit ermöglicht werden. Die Verarbeitung personenbezogener Daten, aus denen die politische Meinung hervorgeht, ist nach Art. 9 Datenschutz-Grundverordnung (DSGVO) nur unter erschwerten Bedingungen zulässig, da es sich hierbei um besonders sensible und schützenswerte Daten handelt.

Aufgrund des hohen Schutzbedarfs dieser Daten ist davon auszugehen, dass eine entsprechende Datenschutzverletzung zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt. In diesen Fällen ist der Verantwortliche nach Art. 33 DSGVO verpflichtet, die Datenschutzverletzung innerhalb von 72 Stunden, nachdem die Verletzung bekannt wurde, an die örtlich zuständige Aufsichtsbehörde zu melden.

Die Datenschutzverletzung als solche sowie die unterbliebene Meldung nach Art. 33 DSGVO sind grundsätzlich bußgeldbewehrt. Im laufenden Berichtszeitraum wurde ein Bußgeldverfahren eingeleitet, welches jedoch bis Redaktionsschluss noch nicht abgeschlossen war.

Fazit/ Empfehlung:

Bei der Versendung von E-Mails an eine Vielzahl von Empfängern ist unbedingt darauf zu achten, dass die E-Mail-Adressen lediglich in das BCC-Feld, also nicht sichtbar für alle Empfänger, gesetzt werden. Sofern Parteien eine entsprechende Datenschutzverletzung durch Verwendung des CC-Feldes unterläuft, haben sie diese gemäß Art. 33 DSGVO innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde zu melden.

3.25 Historische Dorfchroniken

Gerade ortsverbundene Personen haben häufig ein Interesse daran, die Chronik ihres Dorfes und damit der Geschichte ihrer Bürgerinnen und Bürger für sich und ihre Mitmenschen sowie

für die Nachwelt festzuhalten. Zu diesem Zweck sammeln sie umfangreich Materialien über die Geschichte des Dorfes, wobei nicht nur über die Vergangenheit berichtet werden soll, sondern auch Ereignisse bis in die Gegenwart beschrieben und bebildert werden.

Nicht selten stellen die datenschutzrechtlichen Vorgaben die Verantwortlichen vor nicht unerhebliche Fragestellungen. Schließlich werden im Rahmen der Erstellung einer Dorfchronik personenbezogene Daten von einer Vielzahl von Betroffenen verarbeitet, die einer breiten Öffentlichkeit zur Verfügung gestellt werden sollen. In diesem Kontext wird oft darauf verwiesen, dass es mangels Kenntnis des aktuellen Aufenthaltsorts der betroffenen Personen nicht möglich sei, diese nach ihrem Einverständnis in die Verarbeitung ihrer personenbezogenen Daten zu bitten.

So erreichten uns im abgelaufenen Berichtszeitraum wieder vermehrt Anfragen, was bei der historischen Datenverarbeitung zu beachten ist.

Im Hinblick auf die Tätigkeit heimatkundlicher Vereine ist festzuhalten, dass in diesem Zusammenhang häufig Daten bereits verstorbener Personen verarbeitet werden, auf die die Datenschutz-Grundverordnung (DSGVO) keine Anwendung findet (Erwägungsgrund (ErwGr) 27 zur DSGVO).

Soweit aber eine Verarbeitung personenbezogener Daten lebender Personen erfolgt, ist zu klären, ob die Arbeit heimatkundlicher Vereine dem Bereich der wissenschaftlichen Forschung zugeordnet werden kann. Unter den Begriff der Forschungszwecke ist beispielsweise auch die Forschung im Bereich der Genealogie, also der Ahnenforschung, zu subsumieren (ErwGr 160). In diesem Zusammenhang sieht die DSGVO diverse Ausnahmeregelungen vor. Dies betrifft neben der Lockerung des Zweckbindungsgrundsatzes (Art. 5 Abs. 1 lit. b DSGVO), der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) und der Informationspflichten (Art. 14 Abs. 5 DSGVO) insbesondere auch die Einschränkung der Betroffenenrechte im Sinne der Art. 15, 16,

18 und 21 DSGVO zugunsten der historischen Forschung (§ 27 Abs. 2 Bundesdatenschutzgesetz – BDSG).

Eine Veröffentlichung personenbezogener Forschungsergebnisse darf allerdings grundsätzlich nur mit Einwilligung der betroffenen Person erfolgen; ausnahmsweise ist die Veröffentlichung personenbezogener Daten von lebenden Personen auch ohne deren Einwilligung zulässig, wenn die Veröffentlichung für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist (§ 27 Abs. 4 BDSG). Der Gesetzgeber sieht also eine Privilegierung für die Forschungstätigkeit von Historikern vor. Danach hat das Recht auf informationelle Selbstbestimmung dann zurückzutreten, wenn die Veröffentlichung der personenbezogenen Daten für die vollständige und korrekte Darstellung oder das Verständnis der Forschungsergebnisse zwingend erforderlich ist und deshalb nicht darauf verzichtet werden kann. Aus dem Begriff „unerlässlich" folgt, dass ohne die Veröffentlichung personenbezogener Daten die Darstellung der Forschungsergebnisse ohne Nutzen oder unverständlich sein muss.

Bei der Beurteilung, ob ein Ereignis der Zeitgeschichte vorliegt, ist der Begriff nach § 23 Abs. 1 Nr. 1 Kunsturhebergesetz (KUG) heranzuziehen. Danach können grundsätzlich alle vergangenen Geschehnisse erfasst sein, weshalb der Begriff der Unerlässlichkeit zum Schutz der Betroffenen eng auszulegen ist. Es muss also zwischen dem Interesse am Persönlichkeitsschutz und dem öffentlichen bzw. wissenschaftlichen Interesse an der Veröffentlichung personenbezogener Daten abgewogen werden. Das Interesse am Persönlichkeitsschutz kann auch danach variieren, in welcher Fülle personenbezogene Daten über eine natürliche Person veröffentlicht werden sollen. Die Entscheidung hierüber obliegt dem Forschungsinstitut bzw. hier dem Verantwortlichen der Datenverarbeitung im Sinne des Art. 4 Nr. 7 DSGVO. Eine allgemeine Aussage über die Zulässigkeit ist daher nicht möglich.

Es spricht jedoch vieles dafür, dass die Veröffentlichung einer Dorfchronik grundsätzlich nur nach vorheriger Einwilligung der

betroffenen Personen erfolgen sollte. So ist bereits fraglich, ob die Darstellung von Familienzusammenhängen unter den Begriff der Zeitgeschichte im Sinne des Art. 23 Abs. 1 Nr. 1 KUG fallen. Zum Begriff des Zeitgeschehens gehören sämtliche Angelegenheiten von öffentlichem Interesse. Dies mag zwar gegebenenfalls für die Familiendarstellung einer historisch bedeutsamen Familie gelten, nicht jedoch für die gemeine (Arbeiter-) Familie. Selbst in der Annahme, dass die vorgenannten Voraussetzungen erfüllt wären, kann regelmäßig nicht davon ausgegangen werden, dass eine Veröffentlichung der Forschungsergebnisse unerlässlich ist, so dass die betroffenen Personen frei entscheiden können, ob ihre privaten Daten einer breiten Öffentlichkeit mitgeteilt werden.

Fazit/ Empfehlung:

Die Erhebung und die Speicherung der Informationen im Zusammenhang mit der historischen Forschung sind grundsätzlich auch ohne die Einwilligung der betroffenen Personen denkbar. Demgegenüber bedarf es für die Veröffentlichung der Forschungsergebnisse im Regelfall einer Einwilligung der noch lebenden Personen.

3.26 Datenverarbeitung im Bestattungswesen

Im Rahmen einer Beschwerde teilte eine betroffene Person mit, dass ein Bestattungsunternehmen ihrer Bitte um Löschung ihrer personenbezogenen Daten ebenso wenig nachgekommen sei wie einem Widerspruch gegen die sie betreffende Datenverarbeitung.

Der Beschwerdeführer hatte das Unternehmen mit der Bestattung seiner verstorbenen Mutter beauftragt. Im Kern ging es dem Beschwerdeführer um den Umstand, dass Daten seiner Mutter sowie von ihm selbst, u.a. seine Mobilfunknummer, an das örtliche Pfarramt weitergegeben wurden. Dieser Umstand

war in seinen Augen nicht nachvollziehbar, da seine Mutter vor Jahrzehnten bereits aus der Kirche ausgetreten sei. Insoweit machte er auch eine Verletzung des Schutzes der personenbezogenen Daten seiner verstorbenen Mutter geltend.

Ungeachtet dessen, dass die datenschutzrechtlichen Vorgaben nach Maßgabe des Erwägungsgrundes 27 zur Datenschutz-Grundverordnung (DSGVO) auf personenbezogene Daten Verstorbener keine Anwendung findet, war zu klären, weshalb die Daten des Beschwerdeführers ohne dessen Einwilligung an das Pfarramt weitergegen wurden.

Entgegen den Ausführungen des Beschwerdeführers teilte das Unternehmen mit, dass die Mutter bis zu ihrem Tode ausweislich der vorliegenden Sterbeurkunde Kirchenmitglied gewesen sei. Die Übermittlung der Telefonnummer der Hinterbliebenen an die Pfarrgemeinde erfolge regelmäßig, damit diese Kontakt mit der Familie aufnehmen und seelsorgerisch tätig werden könne. Dies sei schließlich auch im Interesse der Hinterbliebenen, um die Trauer über den Tod eines Angehörigen besser bewältigen zu können.

Auch wenn eine seelsorgerische Betreuung nach allgemeiner Lebenserfahrung für bestimmte Personen durchaus hilfreich sein dürfte, obliegt es jedoch dem Einzelnen darüber zu entscheiden, ob er entsprechende Hilfe in Anspruch nehmen möchte. Gerade bei konfessionslosen Hinterbliebenen ist fraglich, inwiefern diese Interesse an einer Unterstützung durch eine Kirchenorganisation haben.

Da auch die zur Verfügung gestellten Datenschutzinformationen des Unternehmens keine entsprechenden Hinweise auf die Datenübermittlung an die Pfarrämter enthielten und insofern die Hinterbliebenen auch nicht mit der Weitergabe ihrer Daten an ein Pfarrämter rechnen mussten, war die vorliegende Datenverarbeitung nicht zu legitimieren.

Das Bestattungsunternehmen sicherte zu, für derartige Datenübermittlungen künftig die ausdrückliche Einwilligung der Hinterbliebenen einzuholen. Aufgrund der Geringfügigkeit des

Verstoßes wurde das Unternehmen gemäß Art. 58 Abs. 2 lit. b DSGVO verwarnt.

Im Übrigen wurde dem Beschwerdeführer mitgeteilt, dass sein geltend gemachter Löschungsanspruch unbegründet war, da zwischen ihm als Auftraggeber und dem Bestattungsunternehmen ein zivilrechtlicher Vertrag über die Durchführung der Bestattung der verstorbenen Mutter zustande gekommen war. Das Unternehmen war auf der Grundlage dieses Vertrages nach Art. 6 Abs. 1 lit. b DSGVO berechtigt und darüber hinaus nach Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit den einschlägigen handels- und steuerrechtlichen Aufbewahrungsfristen sogar verpflichtet, die Daten des Beschwerdeführers zu verarbeiten bzw. zu speichern. Im Falle einer vorzeitigen Löschung hätte das Unternehmen mithin rechtswidrig gehandelt.

3.27 Videoüberwachung

Videoüberwachungsmaßnahmen nehmen in der Gesamtheit des an die Aufsichtsbehörden adressierten Beschwerdevolumens seit Jahren regelmäßig einen erheblichen Anteil ein. Da der datenschutzrechtliche Regelungsrahmen hinsichtlich der für die kameragestützte Datenverarbeitung Verantwortlichen keine Unterscheidung trifft, gelten für multinationale Konzerne, mittelständische Unternehmen, Handwerksbetriebe oder Privatpersonen beim Einsatz von Kameras im Wesentlichen dieselben Vorgaben und Pflichten.

Selbst für den Fall, dass sich der durchschnittliche Kamerabetreiber überhaupt über Bedeutung und Implikationen der Datenschutz-Grundverordnung (DSGVO) für den eigenen Kameraeinsatz bewusst ist, führen die komplexen Zulässigkeitsvoraussetzungen häufig zu einer Überforderung der Verantwortlichen bei der Rechtsanwendung. Vor dem Hintergrund, dass Kamerasysteme am Markt in jeder Preiskategorie und Ausgestaltung zur Befriedigung jedweden individuellen Überwachungsbedürfnisses zur Verfügung stehen, ist eine Vielzahl datenschutzwidriger oder zumindest nicht vollständig daten-

schutzkonformer Überwachungsmaßnahmen nicht nur wahrscheinlich, sondern dem an die Aufsichtsbehörden adressierten Beschwerdevolumen mittelbar ableitbar.

Um den Kamerabetreibern eine Hilfestellung zum datenschutzgerechten Einsatz von Videoüberwachungsmaßnahmen zu geben, wurden daher sowohl seitens des Europäischen Datenschutzausschusses als auch der Datenschutzkonferenz im Berichtszeitraum Orientierungshilfen veröffentlicht.[16]

3.28 Videoüberwachung durch Privatpersonen

Zwar sehen sowohl die Datenschutz-Grundverordnung (DSGVO) als auch das deutsche Verfahrensrecht grundsätzlich eine effiziente und zügige Gestaltung des Beschwerdeverfahrens vor, dies ist jedoch gerade bei den die Videoüberwachungsmaßnahmen betreffenden Verfahren in der Praxis eher Ausnahme denn Regel. Neben der großen Anzahl an diesbezüglichen Beschwerden bedingt oftmals eine fehlende Kooperationsbereitschaft der Kamerabetreiber überlange Verfahrensdauern. Gerade im Bereich der von Privatpersonen im Umfeld selbstgenutzter Grundstücke betriebenen Überwachungsmaßnahmen ist häufig eine komplette Verweigerung der Zusammenarbeit festzustellen, die – mangels effektiver Möglichkeit zur Sachverhaltsaufklärung im nicht-gewerblichen Bereich – eine Anordnung der Informationserteilung durch Bescheid nach Art. 58 Abs. 1 lit. a DSGVO und eine Verhängung von Zwangsgeldern im Sinne des § 20 Saarländisches Verwaltungsvollstreckungsgesetz erforderlich machen.

Da die Beitreibung der Zwangsgelder durch die zuständigen Finanzämter oftmals mehrere Monate in Anspruch nimmt, können mangels belastbarer Informationen zur Ausgestaltung der beschwerdegegenständlichen Überwachung keine weitergehenden aufsichtsbehördlichen Befugnisse ergriffen werden. Vermeintlich verordnungswidrige Überwachungsmaßnahmen

[16] Abrufbar unter https://www.datenschutz.saarland.de/themen/videoueberwachung.

werden sodann zum Leidwesen der Beschwerdeführer monatelang perpetuiert.

Unter Berücksichtigung der Reyneš-Entscheidung des Europäischen Gerichtshofs[17] und der Leitlinien des Europäischen Datenschutzausschusses[18] sind gerade auch von Privatpersonen betriebene Überwachungsmaßnahmen, die über das selbstgenutzte Grundstück hinausgehen, grundsätzlich nach den Vorgaben des Datenschutzrechts zu beurteilen. Für Beschwerden im nachbarschaftlichen Kontext droht dabei aufgrund zumeist vorausgehender latenter oder offen ausgetragener Konflikte zwischen Beschwerdeführer und Kamerabetreiber die Gefahr einer emotionalen Aufladung des gesamten aufsichtsbehördlichen Verfahrens und einer Marginalisierung des datenschutzspezifischen Gehalts des Anliegens bis hin zur reinen Instrumentalisierung der Aufsichtsbehörde für persönliche Zwecke. Hier gilt es perspektivisch diesem zeit- und ressourcenaufwändigen Beschwerdekomplex durch geeignete Mechanismen zu begegnen.

Bisweilen hochemotional wird es in den Fällen, in denen der Anlagenbetreiber lediglich sein eigenes Grundstück überwacht, der erfasste Bereich jedoch mit einem Geh- und Fahrrecht zugunsten eines Dritten (in der Regel der Nachbar) belastet ist. Überwacht werden dabei Zugangswege, welche dem betroffenen Nachbarn dazu dienen, sein Anwesen zu erreichen. Hintergrund einer solchen Videoüberwachung ist meistens ein schwelender Nachbarschaftsstreit, der unter anderem auf verbale Anfeindungen in der Vergangenheit, zerstörte Pflanzen auf dem Grundstück bis hin zu Lärmbelästigungen beruhen kann.

Einer derartigen Videoüberwachung stehen regelmäßig schutzwürdige Interessen des betroffenen Nachbarn entgegen, da dieser bei jedem Betreten und Verlassen des Anwesens gefilmt

[17] EuGH, Urteil vom 11. Dezember 2014 – C-212/13.

[18] Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte.

wird und somit auch eine Profilbildung ermöglicht wird. Der damit verbundene Eingriff in den Schutz personenbezogener Daten ist deshalb besonders eingriffsintensiv, als hierdurch die Privatsphäre des Überwachten beeinträchtigt wird. Demgegenüber liegen die geltend gemachten Überwachungsinteressen des Anlagenbetreibers bei objektiver Bewertung häufig nicht vor und können folglich den Einsatz der Videoüberwachung in diesen Fällen nicht legitimeren. Allenfalls dann, wenn in dem überwachten Bereich eine hohe Gefährdungslage gegenüber der Aufsichtsbehörde objektiv nachvollziehbar, beispielsweise durch Vorlage gestellter Strafanzeigen, dargelegt werden kann, ist eine Videoüberwachung gegen den Willen des betroffenen Nachbarn überhaupt denkbar. Ansonsten muss es der überwachte Nachbar nicht hinnehmen, in seinem häuslichen Umfeld zum Objekt einer Videoüberwachung gemacht zu werden (so auch Saarländisches OLG, Urteil vom 02.10.2019, Az. 5 U 15/19).

Soweit im 28. Tätigkeitbericht im Hinblick auf den Einsatz von Dash-Cams in Fahrzeugen ein unbeantwortetes Gesprächsangebot an das Landespolizeipräsidium thematisiert wurde, ist mittlerweile diesbezüglich ein verstetigter Austausch entstanden. Mitarbeiter hiesiger Dienststelle werden sich an zeitnah stattfindenden Schulungs- und Sensibilisierungsveranstaltungen für die Mitarbeiter der Verkehrspolizei beteiligen und im Übrigen die interbehördliche Zusammenarbeit forcieren.

3.29 Videoüberwachung im kommerziellen Bereich

Im kommerziellen Zusammenhang wurde im Berichtszeitraum gegenüber einem Gastronomiebetrieb ein Bußgeld in Höhe von knapp 10.000 € verhängt. Dem Verfahren lag dabei zugrunde, dass mit einer in Relation zur Betriebsfläche beträchtlichen Anzahl an Kameras während der Öffnungszeiten verordnungswidrig Gast- und Mitarbeiterbereiche sowie das Umfeld des Betriebs überwacht wurden. Derartige exzessive Kameraeinsätze und das Fehlen dokumentierter, eindeutiger Überwachungszwecke stellen dabei im Zusammenhang mit Beschwerden zu Überwachungsmaßnahmen in der Gastronomie keine Ausnahme dar.

Im Hinblick auf Videoüberwachungsmaßnahmen im Bereich des Beschäftigtendatenschutzes stellen Einwilligungserklärungen nach § 26 Abs. 2 Bundesdatenschutzgesetz (BDSG) der betroffenen Mitarbeiter aus Sicht der Arbeitgeber häufig noch den Goldstandard dar. Soweit für eine Überwachungsmaßnahme präventive und repressive Zwecke im Hinblick auf vermeintlich durch Mitarbeiter begangene Schadenshandlungen angeführt werden, sind allerdings zumeist Zweifel an der Freiwilligkeit der individuellen Einwilligungserklärungen durchgreifend.[19] Diese stellen daher regelmäßig keine belastbare Legitimationsgrundlage für eine kameragestützte Verarbeitung von Beschäftigtendaten dar. Wird ein Kameraeinsatz mit stattgefundenen oder drohenden Straftaten oder Pflichtverletzungen der Mitarbeiter begründet und auf § 26 Abs. 1 Satz 1 und 2 BDSG gestützt, bedingt dies die Substantiierung einer dahingehenden Gefährdungslage und eine Beschränkung der Überwachung auf das räumlich oder zeitlich erforderliche Maß. Demgegenüber sind in der Prüfpraxis nach wie vor häufig beliebig ausgedehnte Überwachungsmaßnahmen ohne verbindliche Festlegung von Einsatzzwecken anzutreffen.

3.29.1 Videoüberwachung in der Arztpraxis

Auch Arztpraxen schrecken mitunter nicht davor zurück, ihre Patienten während der Öffnungszeiten mithilfe von Überwachungskameras zu kontrollieren. In den bei der Aufsichtsbehörde eingeleiteten Verwaltungsverfahren wurden in den betreffenden Arztpraxen neben dem Anmeldebereich teilweise auch die Flure zu den Behandlungszimmern erfasst. Nachvollziehbare Belege, welche die Videoüberwachung als solche legitimieren könnten, konnten in der Regel nicht vorgelegt werden. Vielmehr wurde pauschal auf eine allgemeine Gefahrenlage in Arztpraxen hingewiesen. So diene die Überwachung dieser Bereiche unter anderem dem Schutz der Belegschaft vor übergriffigen Patienten, dem Schutz vor Diebstählen und dem Einbruchsschutz.

[19] VG Hannover, Beschluss vom 13. August 2019 – 10 B 1883/19.

Dabei wird außer Acht gelassen, dass mit der Videoüberwachung in Grundrechtspositionen der überwachten Personen eingegriffen wird. Dies wirkt vor dem Hintergrund der Überwachung einer Arztpraxis umso schwerer, als dort regelmäßig behandlungsbedürftige Patienten überwacht und damit auch Gesundheitsdaten erhoben werden.

An die Zulässigkeit von Überwachungsmaßnahmen in Arztpraxen sind daher besonders hohe Hürden zu stellen. Insbesondere ist die Videoüberwachung zur Verhinderung von Straftaten nur dann erforderlich, wenn in Bezug auf die beobachteten Räume eine erheblich über das allgemeine Lebensrisiko hinausgehende Gefährdungslage besteht (vgl. Bundesverwaltungsgericht, Urteil vom 27.03.2019 – 6 C 2/18).

Da die genannten Voraussetzungen in den von uns geprüften Fällen nicht erfüllt waren, wurden die Anlagenbetreiber aufgefordert, die Videoüberwachung während der Öffnungszeiten zu deaktivieren. Zum Zwecke des Einbruchsschutzes konnten die Überwachungskameras während der Nachtzeiten aktiv geschaltet werden. Dem wurde seitens der Anlagenbetreiber auch nachgekommen.

Fazit/ Empfehlung:

Arztpraxen dürfen während der Öffnungszeiten wegen des damit verbundenen gravierenden Grundrechtseingriffs nur in absoluten Ausnahmefällen videoüberwacht werden. Pauschale Hinweise auf eine allgemeine Gefahrenlage im Zusammenhang mit dem Betrieb einer Arztpraxis reichen hierfür nicht aus.

Anlagenverzeichnis

Anhang 1: Verzeichnis wichtiger Rechtsgrundlagen

BDSG – Bundesdatenschutzgesetz: Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), zuletzt geändert durch Gesetz vom 20.11.2019 (BGBl. I S. 1626).

BGB – Bürgerliches Gesetzbuch: In der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, ber. S. 2909 und 2003 I S. 738), zuletzt geändert durch Gesetz vom 22.12.2020 (BGBl. I S. 3256).

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 21.12.2020 (BGBl. I S. 3136).

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

SPolG – Saarländisches Polizeigesetz: Vom 26. März 2001 (Amtsbl. S. 1074), zuletzt geändert durch Gesetz vom 6./7. Oktober 2020 (Amtsbl. I S. 1133).

SPolDVG – Saarländisches Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei: Vom 6./7. Oktober 2020 (Amtsbl. I S. 1133).

TMG – Telemediengesetz: Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Gesetz vom 19.11.2020 (BGBl. S. 2456).

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