BREMISCHE BÜRGERSCHAFT **Drucksache 20/330**
Landtag **24.03.20**
20. Wahlperiode

Bericht der Landesdatenschutzbeauftragten

Tätigkeitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit über den Datenschutz im Jahr 2019 im Land Bremen

Anlage(n):
1. 2. Jahresbericht Datenschutz nach der Datenschutzgrundverordnung

2. Jahresbericht
der Landesbeauftragten für Datenschutz nach der Europäischen Datenschutzgrundverordnung

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats meinen Bericht im Sinne des Artikels 59 der Europäischen Datenschutzgrundverordnung über das Ergebnis der Tätigkeit im Jahr 2019. Redaktionsschluss war der 31. Dezember 2019.

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

Inhaltsverzeichnis

1. Der DSGVO-Tanker hat Fahrt aufgenommen…

Es gibt Abkürzungen, die sind in aller Munde. CIA (Central Intelligence Agency) gehörte und gehört dazu. CIO (Chief Information Officer) sicherlich inzwischen auch. Dank der Enthüllungen Edward Snowdens über anlasslose und umfassende Überwachungen US-amerikanischer Geheimdienste wissen wir auch mit dem Kürzel NSA (National Security Agency) etwas anzufangen. Auch kommt es immer häufiger vor, dass Dinge asap (as soon as possible) erledigt werden sollen und manches einfach nur ein "lol" (laughing out loud) produziert. Wer hätte gedacht, dass auch über die Europäische Datenschutzgrundverordnung (DSGVO) schon nach 18 Monaten Geltungszeit nicht unter ihrem Langnamen gesprochen wird, sondern fast alle das Kürzel "DSGVO" verwenden?

Wie sehr manchen die DSGVO als feststehender Begriff in Fleisch und Blut übergegangen ist, zeigt sich an der gelegentlich zu vernehmenden Bezeichnung "DSGVO-Verordnung", die auf das Besondere der DSGVO verweist: Um den Schutz unserer personenbezogenen Daten zu gewährleisten hat der europäische Gesetzgeber die Rechtsform der Verordnung gewählt, also bewusst eine Direktgeltung angeordnet, die nicht auf Umsetzungsakte der Mitgliedstaaten angewiesen ist. Dies geschah erstmalig in einem Bereich, der alle Menschen in der Europäischen Union direkt in fast allen ihrer Lebenslagen betrifft. Und es handelt sich dabei nicht um irgendeinen unbedeutenden Teilaspekt, sondern um den Schutz unserer zunehmend an Bedeutung gewinnenden digitalen Grundrechte.

Nicht nur an der Bereicherung unseres Abkürzungsfundus lässt sich ablesen, dass die DSGVO das Datenschutzniveau auch im Land Bremen erhöht hat. Das sei hier behauptet, obwohl es zugegebener Maßen schwierig ist, das Datenschutzniveau zu messen. Hinweise zu seiner aktuellen Höhe finden sich zum einen im Grad des Wissens der Menschen über dieses Thema und ihren daraus abgeleiteten Handlungen und andererseits in dem Grad, zu dem die Verarbeitenden die Regelungen befolgen, die dem Schutz personenbezogener Daten dienen.

1.1 Datenschutzbewusstseinserweiternde Ereignisse

Was das Datenschutzbewusstsein der Menschen anbelangt, habe ich in den zehn Jahren, in denen ich den Stand der informationellen Selbstbestimmung im Land Bremen genauer beobachte, drei Ereignisse erlebt, die eine abrupte Erhöhung zur Folge hatten, weil sie das Thema in den gesellschaftlichen Fokus rückten. Es handelt sich um die Veröffentlichung der Straßenansichten aller bremischen Häuser im November 2010, um die genannten Enthüllungen Edward Snowdens im Juni 2013 und um den ersten Geltungstag der Europäischen Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018. Genauer gesagt sind

es die mit den Begriffen Streetview und DSGVO und dem Namen Edward Snowden verbundenen öffentlichen Diskussionen, die das Datenschutzbewusstsein ansteigen ließen.

1.1.1 Streetview

Im Sommer 2010 wurde in der Freien Hansestadt Bremen darüber gestritten, ob es spießig oder legitim sei, die Welt vom virtuellen Blick auf den eigenen Vorgarten ausschließen zu wollen (siehe hierzu 33. Jahresbericht, Ziffer 1.1 "Google Street View – oder: Wie starke Wellen vom flachen Deich gebrochen werden"). Im Zuge dieser Debatte entwickelten auch Menschen, die zuvor geglaubt hatten, sie hätten nichts zu verbergen, das Gefühl, dass es Räume gebe, die ihnen so nahe sind, dass sie nicht wollen, dass sie von beliebigen anderen angesehen werden.

1.1.2 Enthüllung der Massenüberwachungen durch die NSA

Nach den ersten Enthüllungen Edward Snowdens über die umfassenden und anlasslosen Massenüberwachungen von Smartphones und Internetkommunikation durch US-amerikanische Geheimdienste machte sich im Sommer 2013 auch die bremische Öffentlichkeit hierüber Sorgen (siehe hierzu 36. Jahresbericht, Ziffer 1. "2013: Das Informationsimperium schlägt zu(rück)"). Noch ein Jahr später konnten nach einer Erhebung des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI) 80 Prozent der repräsentativ befragten Bundesbürgerinnen und Bundesbürger den Namen Edward Snowden korrekt zuordnen und nach einer Befragung des ZDF-Politikbarometers befürworteten 82 Prozent seine Enthüllungen. Ein Viertel (DIVSI) beziehungsweise ein Fünftel (ZDF) der Befragten gab an, aufgrund der gewonnenen Erkenntnisse beim Telefonieren, Mailen und Surfen im Internet vorsichtiger geworden zu sein. Auch wenn es im Bereich des Selbstdatenschutzes sicherlich eine Lücke zwischen dem Wollen und dem Tun gibt (Intention-Behaviour-Gap), ist dies doch eine bemerkenswerte Zahl (siehe hierzu 38. Jahresbericht, Ziffer 1.1 "Das gestiegene Bedürfnis nach internetvertrauensbildenden Maßnahmen"). Die hierin zum Ausdruck kommende Tendenz setzt sich bis heute fort. Im Januar 2019 gaben laut Infratest-Dimap 60 Prozent der Befragten an, möglichst wenige Daten von sich im Internet preiszugeben und gegebenenfalls auf die Nutzung von Diensten zu verzichten, die persönliche Daten einfordern. Im November 2019 fühlten sich 70 Prozent der Nutzerinnen und Nutzer des Internets laut einer repräsentativen Umfrage des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e. V. (bitkom) von Datenmissbrauch bedroht. Diese Zahlen belegen einen weiteren Anstieg des Datenschutzbewusstseins.

1.1.3 Geltungsbeginn der Datenschutzgrundverordnung

Im Sommer 2018 diskutierte auch das Land Bremen über Klingelschilder, abgenötigte Einwilligungen, unerwünschte Werbung und Bußgeldandrohungen. Auch diese öffentliche Debatte bewirkte, dass alle darüber nachdachten, welche Informationen Unbekannte ihrer Meinung nach über sie haben dürfen und welche nicht. Die Veränderungen des Datenschutzbewusstseins im Zusammenhang mit der Datenschutzgrundverordnung (DSGVO) sind quantifizierbar: 18 Monate nach dem ersten Geltungstag der DSGVO hat sich allein die Zahl der monatlich bei der Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) eingehenden Beschwerden über Datenschutzverletzungen mehr als verdoppelt (siehe Ziffer 2.2 dieses Berichts). Dies ist ein sehr deutlicher Indikator dafür, dass die Betroffenen sensibler geworden sind. Vielleicht hat die Diskussion über die DSGVO sie sogar erst ermutigt, sich mit ihrer Beschwerde bei der LfDI zu melden.

1.1.4 Melderegistersperren

Übrigens war das Sommerloch des Berichtsjahres wieder mit einem datenschutzrechtlichen Thema gefüllt, was sicherlich ein weiteres Mal zur Erhöhung des Datenschutzbewusstseins geführt hat: Anlässlich der entsetzlichen Ermordung des Kasseler Regierungspräsidenten Walter Lübcke im eigenen Garten entspann sich eine öffentliche Diskussion darüber, warum es nach dem bestehenden Recht so schwer ist, mit der Eintragung von Melderegistersperren zu verhindern, dass Dritte von Meldeämtern Auskunft über Wohnadressen erhalten. Dies gilt für Menschen, die befürchten, Opfer von Stalking-Angriffen zu werden, ebenso wie für Kommunalpolitikerinnen und Kommunalpolitiker und andere Menschen, die gefährdet sind, weil sie sich in grundrechtskonformer Weise über gewaltbereite Gruppen äußern. Hier ergibt sich die Chance für den Bundesgesetzgeber, den Kreis der Anspruchsberechtigten für die Eintragung von Melderegistersperren deutlich zu erweitern und zusätzlich die im zweiten Bundesgesetz zur Umsetzung der Datenschutzgrundverordnung (DSGVO) normierte nur minimale Änderung des Bundesmeldegesetzes noch einmal zu korrigieren. Gegenüber den Meldepflichtigen muss in einer Weise Transparenz über die Weitergabe der Meldedaten an Stellen außerhalb der öffentlichen Verwaltung geschaffen werden, die den hohen Anforderungen der DSGVO entspricht.

Wir dürfen gespannt sein, ob es auch im Jahr 2020 wieder innerhalb und außerhalb des Sommerlochs spannende öffentliche Debatten über das Grundrecht auf informationelle Selbstbestimmung geben wird. Wie der hiermit vorgelegte zweite Jahresbericht zum Datenschutz unter der Ägide der DSGVO zeigt, gäbe es Themen genug, deren öffentliche Beratung wahrscheinlich wieder zu einem Anstieg des Datenschutzbewusstseins führen würden.

1.2 Befolgung der Datenschutzgrundverordnung

Wie steht es nun aber mit dem Grad der Befolgung der rechtlichen Regelungen durch die Verarbeitenden als dem zweiten Gradmesser des Datenschutzniveaus? Die Verdoppelung der bei der Landesbeauftragten für Datenschutz und Informationsfreiheit eingegangenen Beschwerden ist sicherlich kein Indiz dafür, dass nach dem 25. Mai 2018 so viel mehr Datenschutzverletzungen im Land Bremen passiert sind als in der Zeit davor. Im Gegenteil bestätigt sich sogar in der Aufsichtspraxis der Eindruck, dass viele, die personenbezogene Daten verarbeiten, zähneknirschend, begeistert oder einfach, weil es sein musste, die Datenschutzgrundverordnung (DSGVO) umgesetzt haben. Auch steht zu vermuten, dass der Zwang der DSGVO zur Beschreibung der Datenströme und Rechtsgrundlagen Fehler aufdeckte, die nicht selten zum Verzicht auf Verarbeitungen führten. Viele haben erkannt, dass die DSGVO zum weltweiten Standard geworden ist und es insofern vielfach schlicht klug ist, sich an diese Regelungen zu halten.

Einer der es wirklich wissen muss, nämlich Martin Selmayr, der als damaliger persönlicher Referent der EU-Kommissarin Viviane Reding zum Umfeld der Eltern der DSGVO gezählt werden muss, äußerte anlässlich des Europäischen Datenschutztages 2019 in Berlin auch vor den Ohren der versammelten Wirtschaftsverbandslobbyistinnen sinngemäß, materiell rechtlich habe sich durch die DSGVO nichts an der Lage des europäischen Datenschutzes geändert. Die Hauptänderung der DSGVO liege in der Stärkung der Rolle der europäischen Aufsichtsbehörden. Damit hat er für die DSGVO das nach Habermas entscheidende Moment der Geltungskraft von Normen adressiert: "Die soziale Geltung von Rechtsnormen bestimmt sich nach dem Grad der Durchsetzung, als der faktisch zu erwartenden Akzeptanz im Kreise der Rechtsgenossen. Anders als die konventionelle Geltung von Brauch und Sitte stützt sich freilich das gesatzte Recht nicht auf die gewachsene Faktizität eingewöhnter und tradierter Lebensformen, sondern auf die artifiziell hergestellte Faktizität der Androhung rechtsförmig definierter und vor Gericht einklagbarer Sanktionen" (Jürgen Habermas, "Faktizität und Geltung", Seite 47).

Die Geltungskraft der DSGVO, der Grad ihrer Befolgung, hat also mit der Androhung von Sanktionen und der Stärkung der Rolle der Aufsichtsbehörden zu tun. Dass es nicht bei der Androhung bleibt, zeigen die verhängten Bußgelder: So erhielt der Telekommunikationsdienstleister 1&1 Telecom GmbH vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Dezember des Berichtsjahres einen Bußgeldbescheid in Höhe von 9,5 Millionen Euro, weil beim Anruf bei der Kundenbetreuung des Unternehmens schon dann weitreichende personenbezogenen Daten von Kundinnen oder Kunden preisgegeben wurden, wenn die Anrufenden deren Namen und ihr Geburtsdatum angeben konnten. Im Oktober verhängte meine Berliner Kollegin ein Bußgeld in Höhe von rund 14,5 Millionen Euro gegen die Deutsche Wohnen SE, weil das Unternehmen für die

Speicherung personenbezogener Daten von Mieterinnen und Mietern ein Archivsystem verwendet hatte, das keine Möglichkeit vorsah, nicht mehr erforderliche Daten zu entfernen. Insofern fanden sich dort beispielsweise Gehaltsbescheinigungen, Selbstauskunftsformulare, Auszüge aus Arbeits- und Ausbildungsverträgen und Steuer-, Sozial- und Krankenversicherungsdaten.

Sowohl das Datenschutzbewusstsein als auch der Grad der Befolgung der Datenschutzregeln haben sich also durch die DSGVO erhöht. Damit ergeben sich deutliche Indizien dafür, dass meine These, wonach sich das Datenschutzniveau auch im Land Bremen deutlich erhöht hat, schwer zu bestreiten ist.

1.3 Die Höchstgeschwindigkeit ist bei weitem noch nicht erreicht

Der DSGVO-Bußgeldtanker hat im Jahr 2019 wie soeben beschrieben Fahrt aufgenommen. Leider steckt die Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) noch tief in der Bearbeitung des Beschwerdebergs und hat es im Berichtsjahr nicht geschafft, die Verfahren in das Stadium der Bußgeldreife zu bringen. Da die Verjährungsfrist für Verstöße gegen die Datenschutzgrundverordnung (DSGVO) fünf Jahre beträgt, bedeutet dies zunächst nur eine Verzögerung. Noch hat der bremische Haushaltsgesetzgeber durch die Ausstattung der LfDI mit dem für Bußgeldverhängungen erforderlichen Personal die Chance, zu bewirken, dass das Tau, an dem das bremische Beiboot am Bußgeldtanker hängt, nur sehr lang ist und nicht doch am Ende noch gekappt wird.

Neben der Verhängung von Bußgeldern haben sich die Datenschutzaufsichtsbehörden im ersten vollen Kalenderjahr der Geltung der DSGVO in vielfacher Weise auch der anderen aufsichtsbehördlichen Mittel wie Warnungen, Verwarnungen und Anordnungen von Verarbeitungsverboten und Verarbeitungsbeschränkungen, Benachrichtigungen der Betroffenen, Berichtigungen und Löschungen bedient, die die DSGVO den Aufsichtsbehörden zur Verfügung stellt. Auch die bremische Landesbeauftragte für Datenschutz und Informationsfreiheit hat diese aufsichtsrechtlichen Werkzeuge, die den Betroffenen sofort Schutz bieten und nach der DSGVO in der Regel ein Bußgeld nach sich ziehen sollen, mehrfach genutzt (siehe hierzu Ziffer 2.5 dieses Berichts).

Insgesamt zeigt sich, dass die DSGVO nach 18 Monaten nicht nur rechtlicher, sondern auch tatsächlicher Geltung begonnen hat, ihre Potenziale zu entfalten. Allen sollte deutlich geworden sein, dass dies erst der Anfang ist. Der Tanker hat sich in Bewegung gesetzt und nimmt langsam Fahrt auf. Die Höchstgeschwindigkeit ist bei weitem noch nicht erreicht …

Dr. Imke Sommer

2. Zahlen und Fakten

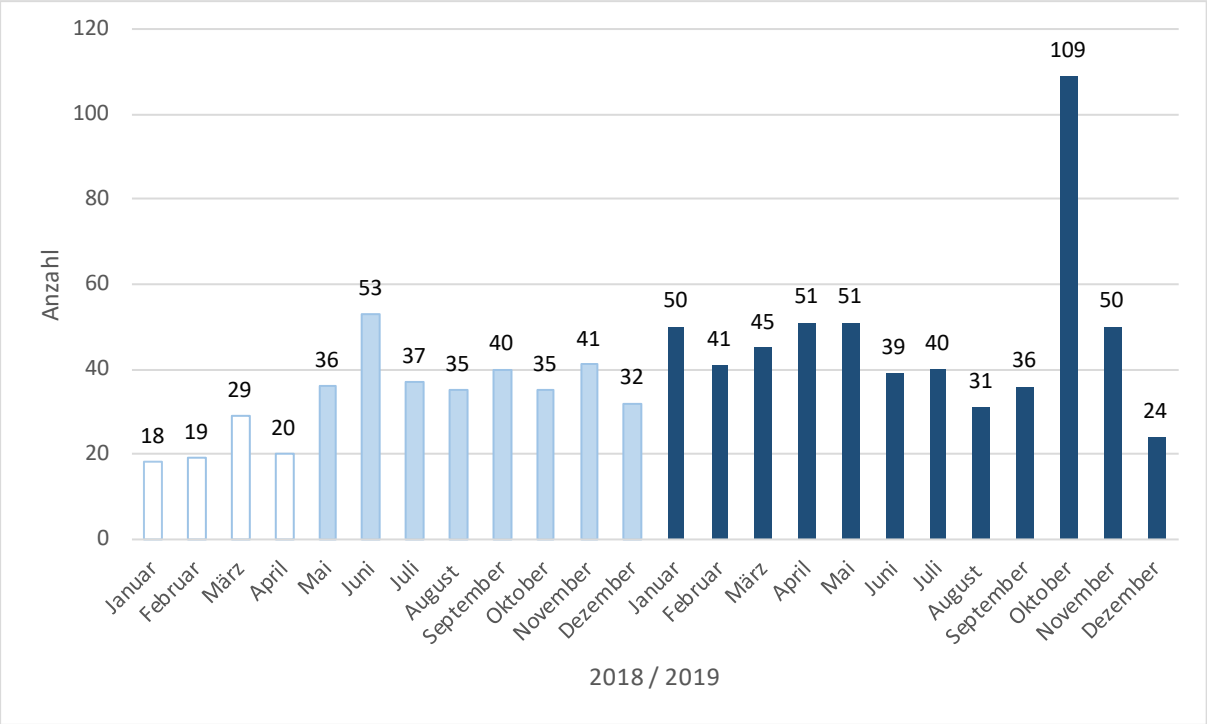
Die Datenschutzgrundverordnung macht es den Aufsichtsbehörden in Artikel 59 zur Pflicht, jährlich über ihre Tätigkeit zu berichten. Um die Transparenz und Vergleichbarkeit innerhalb der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) und für die Öffentlichkeit zu erhöhen, hat die DSK beschlossen, künftig in die jeweiligen Tätigkeitsberichte ein zusätzliches Kapitel aufzunehmen, in dem nach gemeinsam vereinbarten Kriterien Informationen zu bestimmten Kennwerten der jeweiligen Aufsichtsbehörde aufgeführt sind. Die vereinbarten Kriterien sind Beschwerden (siehe Ziffer 2.2 dieses Berichts), Beratungen (siehe Ziffer 2.3 dieses Berichts), Meldungen von Datenschutzverletzungen (siehe Ziffer 2.4 dieses Berichts), Abhilfemaßnahmen (siehe Ziffer 2.5 dieses Berichts), Europäische Verfahren (siehe Ziffer 2.6 dieses Berichts) und förmliche Begleitung von Rechtsetzungsvorhaben (siehe Ziffer 2.7 dieses Berichts).

2.1 Auswahl datenschutzrelevanter Sachverhalte, die 2019 an die Landesbeauftragte für Datenschutz und Informationsfreiheit herangetragen wurden

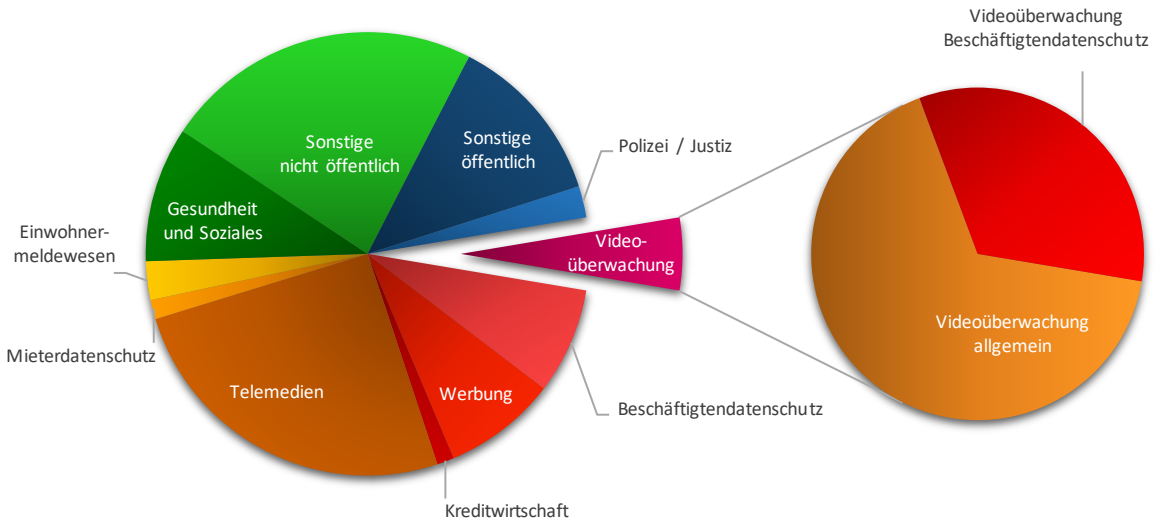
Monat	Beschwerden	Beratungs-anfragen	Meldungen Datenschutz-verletzungen	Meldungen Datenschutz-beauftragte	Vorträge
Januar	50	52	8	60	1
Februar	41	58	3	45	3
März	45	33	5	33	3
April	51	43	7	30	2
Mai	51	44	7	26	4
Juni	39	45	12	34	10
Juli	40	51	6	25	2
August	31	30	7	28	0
September	36	28	5	18	3
Oktober	109	38	5	22	0
November	50	36	11	17	4
Dezember	24	22	7	36	2
Gesamt	**567**	**480**	**83**	**374**	**34**

Nähere Angaben hierzu finden sich in den nachfolgenden Ziffern.

2.2 Beschwerden



Seit 25. Mai 2018 gilt die Datenschutzgrundverordnung (DSGVO). In diesem Diagramm sind die monatlichen Beschwerdezahlen seit dem Jahr 2018 dargestellt. Das durchschnittliche Monatsaufkommen hat sich damit von 21,5 Beschwerden in den vier Monaten vor Geltung der DSGVO im Jahr 2018 über 38,6 Beschwerden in den ersten acht Geltungsmonaten der DSGVO im Jahr 2018 auf 47,3 Beschwerden im Berichtsjahr 2019 erhöht. Damit hat sich das Beschwerdeaufkommen seit Geltung der DSGVO mehr als verdoppelt.



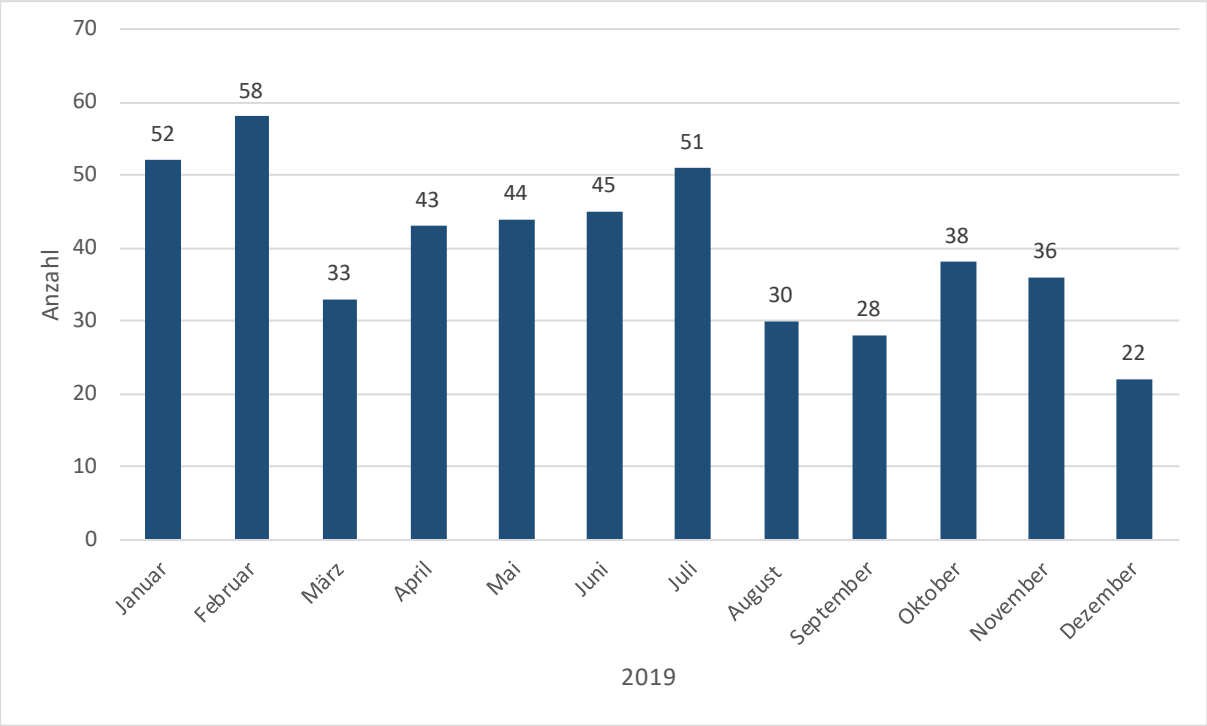
Das Diagramm zeigt die bei der Landesbeauftragten für Datenschutz und Informationsfreiheit eingegangenen Beschwerden im gesamten Jahr 2019 nach Themengebieten unterteilt. Dabei wird deutlich, dass es bei den genannten Themengebieten – wie bei der Videoüberwachung und dem Beschäftigtendatenschutz hervorgehoben – zu Überschneidungen kommen kann.

Themengebiet	AW	RW
Beschäftigtendatenschutz	44	8 %
Werbung	47	8 %
Kreditwirtschaft	7	1 %
Telemedien	144	25 %
Mieterdatenschutz	8	1 %
Einwohnermeldewesen	16	3 %

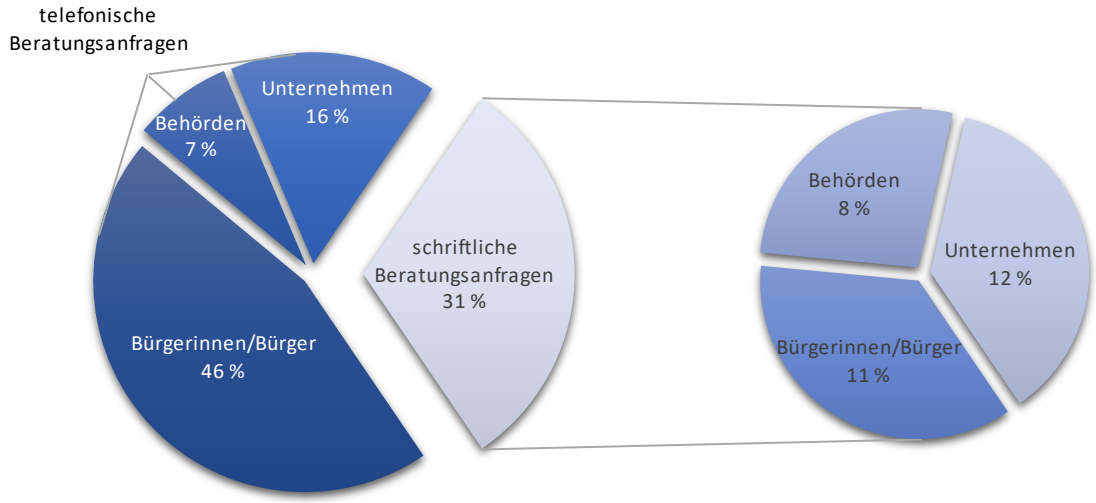
Themengebiet	AW	RW
Sonstiges (nicht öffentlich)	131	23 %
Sonstiges (öffentlich)	71	13 %
Gesundheit und Soziales	56	10 %
Polizei / Justiz	13	2 %
Videoüberwachung	30	6 %

Die Tabelle stellt die absoluten Werte (AW) und relativen Werte (RW) der unterschiedlichen Themengebiete der Beschwerden dar.

2.3 Beratungen

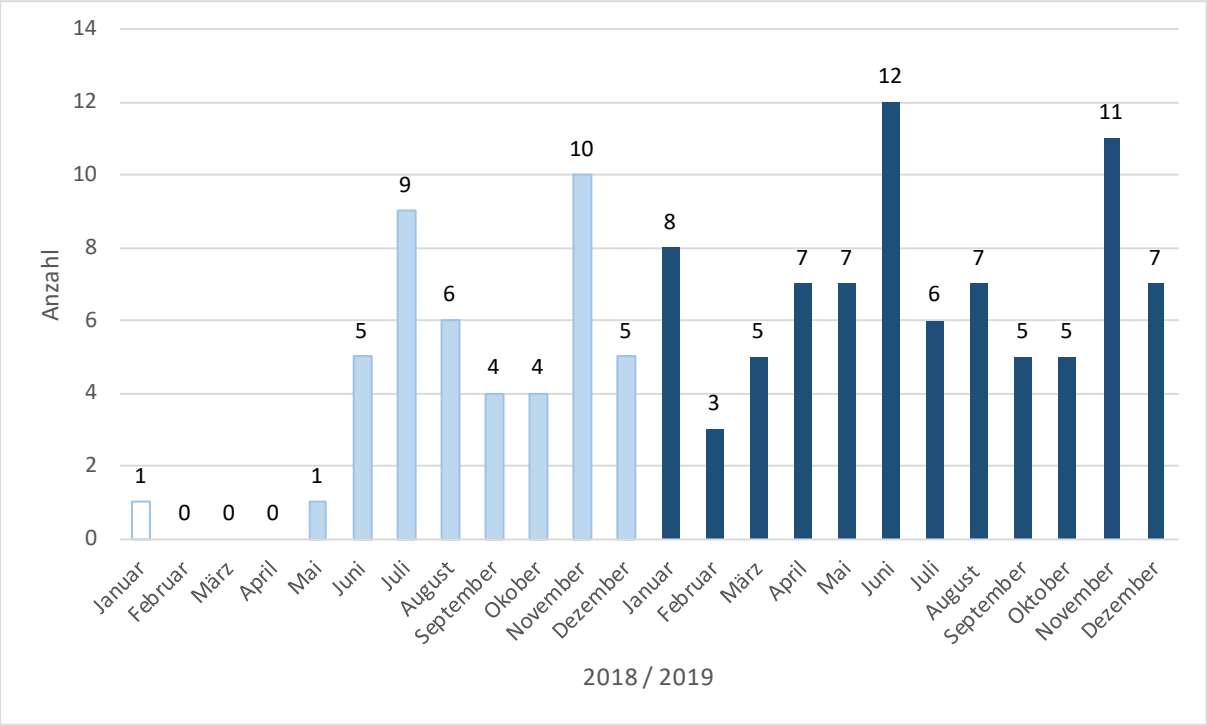


Diese Grafik gibt eine Übersicht über die Anzahl von schriftlichen und telefonischen Beratungen von Verantwortlichen und betroffenen Personen.

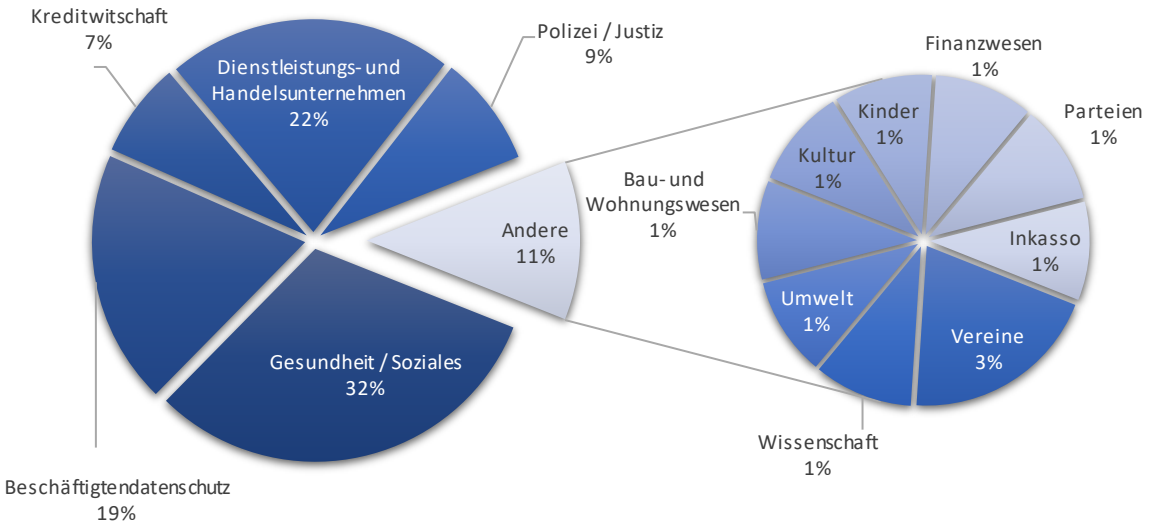


Dieses Tortendiagramm stellt die telefonischen und schriftlichen Beratungen im Jahr 2019 dar. Differenziert wird dabei zwischen telefonischen und schriftlichen Beratungsanfragen. Daneben wird danach unterschieden, wer Beratungsanfragen stellt. Dies sind zum einen die Verantwortlichen (Behörden und Unternehmen) und andererseits die von der Verarbeitung personenbezogener Daten betroffenen Grundrechtsträgerinnen und Grundrechtsträger.

2.4 Meldungen von Datenschutzverletzungen



Diese Grafik vermittelt eine Übersicht über die Anzahl schriftlicher Meldungen über Datenschutzverletzungen durch Verantwortliche oder Auftragsverarbeiter nach Artikel 33 Datenschutzgrundverordnung.



Diese Darstellung schlüsselt die gemeldeten Datenschutzverletzungen für das Jahr 2019 nach Themengebieten auf.

2.5 Abhilfemaßnahmen

Warnungen

Abhilfemaßnahmen nach Artikel 58 Absatz 2 a DSGVO: Eine

Verwarnungen

Abhilfemaßnahmen nach Artikel 58 Absatz 2 b DSGVO: Acht

Anweisungen und Anordnungen

Abhilfemaßnahmen nach Artikel 58 Absatz 2 c-g DSGVO: Fünf

Geldbußen

Abhilfemaßnahmen nach Artikel 58 Absatz 2 i DSGVO: Keine

Widerruf von Zertifizierungen

Abhilfemaßnahmen nach Artikel 58 Absatz 2 h DSGVO: Keine

2.6 Europäische Verfahren

Anzahl der Verfahren mit Betroffenheit nach Artikel 56 DSGVO

Ein Fall.

Anzahl der Verfahren mit Federführung nach Artikel 56 DSGVO

Kein Fall.

Anzahl der Verfahren gemäß Kapitel VII nach den Artikeln 60ff. DSGVO

Zwei Fälle nach Artikel 61 DSGVO.

Drei Fälle nach Artikel 64 DSGVO.

2.7 Förmliche Begleitung bei Rechtsetzungsvorhaben

Folgende Beratungen wurden im Berichtsjahr 2019 durchgeführt:

Justiz

- Bremisches Gesetz zum Schutz personenbezogener Daten im Justizvollzug (Bremisches Justizvollzugsdatenschutzgesetz – BremJVollzDSG)

Gesundheit

- Bremisches Krankenhausdatenschutzgesetz (BremKHDSG)

(Zum Redaktionsschluss noch nicht verabschiedet, daher im Fall der Kollision mit Regelungen der DSGVO Direktgeltung der DSGVO)

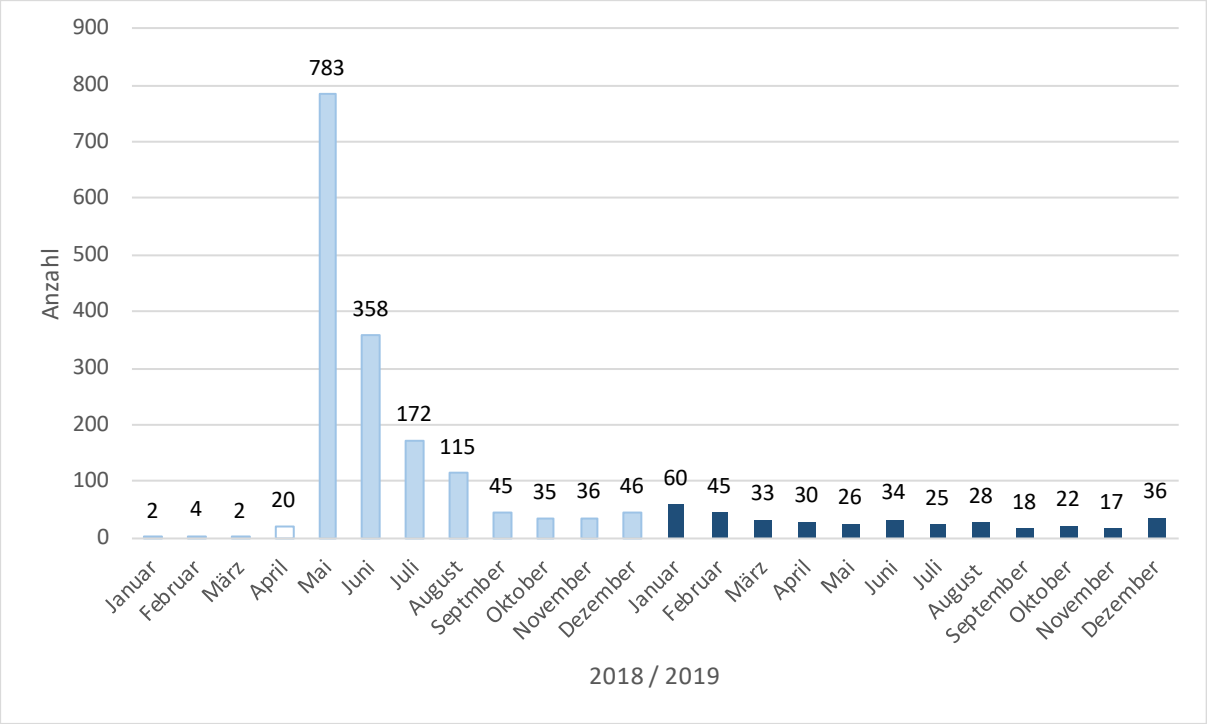
Soziales

- Bremisches Tageseinrichtungs- und Kindertagespflegegesetz (BremKTG)
- Bremisches Gesetz zur Ausführung des Betreuungsgesetzes und zur Anpassung des Landesrechts (BremAG-BtG)

Bauen und Wohnen

- Bremisches Architektengesetz (BremArchG)
- Bremisches Ingenieurgesetz (BremIngG)

2.8 Meldungen der behördlichen und betrieblichen Datenschutzbeauftragten



Nach Artikel 37 Datenschutzgrundverordnung müssen die behördlichen und betrieblichen Datenschutzbeauftragten an die zuständige Aufsichtsbehörde gemeldet werden. Diese Grafik zeigt die Zahl der jeweiligen Meldungen pro Monat.

2.9 Akkreditierung von Zertifizierungsstellen

Zur Umsetzung der Anforderungen nach den Artikeln 42 und 57 Absatz 1 Buchstabe q Datenschutzgrundverordnung (DSGVO), wonach datenschutzrechtliche Aufsichtsbehörden Zertifizierungsstellen auf Antrag akkreditieren müssen, und des § 39 Bundesdatenschutzgesetz muss die Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) mit der Deutschen Akkreditierungsstelle GmbH (DAkkS) zusammenarbeiten und jeweils eine Fachbegutachterin beziehungsweise einen Fachbegutachter für die Bereiche Recht und Informatik stellen. Nachdem die LfDI den bundesweit ersten Antrag auf Akkreditierung einer Zertifizierungsstelle erhalten (siehe hierzu 1. Jahresbericht, Ziffer 2.9) und bereits einen Informatiker zum Fachbegutachter bei der DAkkS fortgebildet hatte, steht eine entsprechende Fortbildung für eine Juristin an.

2.10 Europäisches Binnenmarkt-Informationssystem

Das europäische Binnenmarkt-Informationssystem (Internal Market Information System, IMI) ist ein Instrument, welches den Informationsaustausch zwischen den Datenschutzaufsichtsbehörden europaweit erleichtern und vereinheitlichen soll. Die Menge an zu sichtenden und zu bewertenden E-Mails übersteigt jedoch die Kapazität der Landesbeauftragten für Datenschutz und Informationsfreiheit bei Weitem. Für Verfahren nach den Artikeln 56, 60, 61, 62, 64, 65 und 66 Datenschutzgrundverordnung (DSGVO) sind im Berichtsjahr mehr als 1.200 E-Mails eingegangen. Beispielsweise nach Artikel 61 Absatz 2 DSGVO muss jede Aufsichtsbehörde alle geeigneten Mittel ergreifen, um einem Ersuchen einer anderen Aufsichtsbehörde unverzüglich und spätestens innerhalb eines Monats nach Eingang des Ersuchens nachzukommen. Um eine mögliche Zuständigkeit ermitteln zu können, muss deshalb jede E-Mail im IMI-System überprüft werden. Mit den derzeitigen Mitteln ist die Wahrnehmung dieser wichtigen Aufgabe nicht möglich.

3. Bremische Bürgerschaft – Ergebnisse der Beratungen des 1. Jahresberichts

Bericht des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit. 1. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit nach der Europäischen Datenschutzgrundverordnung und Stellungnahme des Senats.

I. Bericht

Die Bürgerschaft (Landtag) überwies in ihrer Sitzung am 8. Mai 2019 den 1. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit vom 27. März 2019 (Drucksache 19/2128) und in ihrer Sitzung am 15. August 2019 die dazu erfolgte Stellungnahme des Senats vom 25. Juni 2019 (Drucksache 20/3) an den Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zur Beratung und Berichterstattung.

Der Ausschuss stellte bei den nachfolgend aufgeführten Punkten des 1. Jahresberichts Beratungsbedarf fest:

Ziffer 2 Zahlen und Fakten

Ziffer 5 Übergreifende IT-Verfahren

Ziffer 6 Inneres

Ziffer 7 Justiz

Ziffer 8 Gesundheit und Soziales

Ziffer 10 Beschäftigtendatenschutz

Ziffer 11 Videoüberwachung

Ziffer 16 Internationales und Europa

In seinen Sitzungen am 13. November 2019 und 18. Dezember 2019 erörterte der Ausschuss die beratungsbedürftigen Punkte mit der Landesbeauftragten für Datenschutz und Informationsfreiheit sowie mit den Vertreterinnen und Vertretern der betroffenen Ressorts.

Der Ausschuss begrüßt, dass es in vielen Fällen, die Anlass zur Kritik gegeben haben, bereits zu einer Klärung mit den zuständigen Ressorts und Dienststellen gekommen ist beziehungsweise im Rahmen von Gesprächen zwischen den Beteiligten konstruktiv an Lösungsmöglichkeiten gearbeitet wird.

Der Ausschuss nimmt mit Blick auf Ziffer 2 des Berichts zur Kenntnis, dass sich seit Geltung der Datenschutzgrundverordnung (DSGVO) die Anzahl der bei der Landesbeauftragten monatlich eingehenden Beschwerden verdoppelt und damit der Arbeitsanfall erheblich erhöht hat. Dies liege unter anderem auch darin begründet, dass die Verantwortlichen nach der DSGVO verpflichtet seien, Datenschutzverstöße bei der Landesbeauftragten zu melden. Zusätzlich zu den bestehenden seien bei der Behörde durch die Regelungen der DSGVO weitere Aufgaben hinzugekommen, wie zum Beispiel die Akkreditierung von Zertifizierungsstellen sowie diverse Genehmigungs-, Dokumentations- und Kooperationspflichten mit anderen europäischen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss. Der Ausschuss erkennt an, dass diese Arbeitsbelastung ohne zusätzliches Personal kaum bewältigt werden kann. Durch die neu geschaffene Möglichkeit, bei bestimmten Datenschutzverstößen Bußgelder zu verhängen, bestehe jedoch die Aussicht, weitere Stellen künftig zumindest teilweise durch eingenommene Bußgelder zu refinanzieren.

Aus dem Bereich "Übergreifende IT-Verfahren" hat sich der Ausschuss mit der Problematik Blockchains und Datenschutz befasst (Ziffer 5.3). Auch wenn Blockchains aus Gründen der Datensicherheit gewisse Vorteile mit sich brächten, sei die Technologie aus Sicht der Betroffenen und aus datenschutzrechtlichen Gründen kritisch zu betrachten, da Daten irreversibel gespeichert würden und somit nicht gelöscht werden könnten. Der Ausschuss begrüßt daher, dass die bremische Verwaltung zurzeit keine Blockchains einsetzt und keine IT-Systeme aufbaut, die gegen die DSGVO oder andere datenschutzrechtliche Vorschriften verstoßen.

Im Hinblick auf die Gewährleistung der Sicherheit der Verarbeitung bei der Übertragung personenbezogener Daten per Fax (Ziffer 5.4) nimmt der Ausschuss zur Kenntnis, dass die Übermittlung per Fax inzwischen nicht mehr sicherer ist als diejenige per E-Mail. Beide

Verfahren nutzten heutzutage IP-basierte Telekommunikationsnetze, sodass die Sicherheitsstufe bei unverschlüsselter Übermittlung identisch sei.

Zum Themenbereich "Inneres" begrüßt der Ausschuss, dass die bei der Kontrolle der Antiterror- und der Rechtsextremismusdatei (Ziffer 6.1) im Einzelfall festgestellten Mängel inzwischen behoben worden sind. Die Landesdatenschutzbeauftragte kritisiert jedoch weiterhin, dass nach Ablaufen der Speicherfrist keine automatisierte Löschung der Daten erfolge, sondern eine sogenannte Löschprüfliste vorliege, die manuell abgearbeitet werde. Dies könne zu Fehlern und insbesondere zu langen Bearbeitungszeiten und damit zu verzögerten Löschungen führen.

Gleiches gelte für das polizeiliche Vorgangsbearbeitungssystem (Ziffer 6.3), das ebenfalls keine automatisierte Löschung vorsehe. Dies liegt nach Aussage des Ressortvertreters darin begründet, dass es insbesondere in polizeilichen Sachverhalten häufig einer weiteren Prüfung bedürfe, ob eine Verlängerung oder Veränderung der Speicherfrist erforderlich sei. Dies könne nicht automatisiert erfolgen.

Zur unbefugten Abfrage in den polizeilichen Informationssystemen (Ziffer 6.2) nimmt der Ausschuss zur Kenntnis, dass solche Vorkommnisse polizeiintern immer überprüft und auch geahndet werden. Grundsätzlich gäbe es für alle Informationssysteme innerhalb der Polizei Berechtigungskonzepte und nicht jede Person dürfe in jedem System Abfragen tätigen. Zudem werde jede Anfrage protokolliert und sei auch revisionsfähig. Ob eine Information der Betroffenen erfolge, deren Daten abgefragt wurden, werde unterschiedlich gehandhabt. Nach der Datenschutzgrundverordnung (DSGVO) existiere zwar eine entsprechende Informationspflicht, jedoch gelte die DSGVO nicht für den Bereich der Polizei. Hier gelte die Europäische Datenschutzrichtlinie, die Bremen aber noch nicht umgesetzt habe.

Zum Fall der unerlaubten Speicherung von Daten auf einem USB-Stick beim Auftragsverarbeiter (Ziffer 7.1) hat sich der Ausschuss berichten lassen, dass es in der konkreten Konstellation schwierig sei, Zugriffsrechte von Mitarbeiterinnen und Mitarbeitern der Forensik weiter zu beschränken, da diese sonst nicht mehr arbeitsfähig seien. Datenschutzrechtlich handele es sich um einen speziellen Fall. Ob der Vorfall weitere datenschutzrelevanten Maßnahmen beim Auftragsverarbeiter nach sich gezogen habe, konnte nicht geklärt werden.

Im Hinblick auf den Bereich "Gesundheit und Soziales" begrüßt der Ausschuss, dass bei der Bewohner- und Quartiersmanagementsoftware für Flüchtlingsunterkünfte (Ziffer 8.1) zum Teil bereits nachgebessert und das von der Landesbeauftragten kritisierte Beschäftigtenmodul inzwischen abgeschaltet worden ist. Bei der Datenspeicherung im Hinblick auf die Essensausgabe seien Veränderungen vorgenommen worden, die jedoch aus Sicht der Landesbeauftragten noch nicht zufriedenstellend seien. Ein vollständiges Löschkonzept liege

weiterhin nicht vor. Insbesondere über die Aufbewahrungsfristen beziehungsweise Speicherfristen sei noch keine Einigkeit erzielt worden. Der Ausschuss erwartet, dass hier zeitnah eine Einigung zwischen den Beteiligten und eine zufriedenstellende Lösung erzielt wird, die alle berechtigten Interessen berücksichtigt. Der Bereich der Sozialdaten ist aus Sicht des Ausschusses sehr sensibel und verdient besondere Aufmerksamkeit, speziell im Hinblick auf die Schnittstellen.

Bei der datenschutzrechtlichen Problematik im Zusammenhang mit der Übermittlung von Blutalkoholwerten vom Krankenhaus an die Polizei (Ziffer 8.2) hat der Ausschuss zur Kenntnis genommen, dass es im Krankenhausdatenschutzgesetz keine gesetzliche Grundlage für eine solche Übermittlungsbefugnis an Strafverfolgungsbehörden gibt. Mangels Einwilligung und Schweigepflichtentbindung sei die Übermittlung daher unzulässig erfolgt. Der Ausschuss geht jedoch davon aus, dass es sich um einen Einzelfall gehandelt hat und solche Datenübermittlungen nicht regelmäßig erfolgen, sondern die Krankenhäuser grundsätzlich bei der Weitergabe von Informationen die geltenden datenschutzrechtlichen Bestimmungen beachten.

Bei der Kennzeichnung von Patientenbetten im Krankenhaus mit vollständigen privaten Adressdaten (Ziffer 8.3) nimmt der Ausschuss positiv zur Kenntnis, dass diese Praxis in allen Krankenhäusern abgestellt worden ist und nicht mehr angewendet wird.

Das Thema "Datenbank Haaranalysen" (Ziffer 8.12) war bereits Gegenstand zahlreicher Jahresberichte und hat den Ausschuss im Hinblick auf die datenschutzrechtliche Problematik immer wieder beschäftigt. Auch wenn die Datenbank inzwischen konzeptionell überarbeitet worden sei, liege abschließend noch kein zufriedenstellendes Datenschutzkonzept vor, insbesondere kein Löschkonzept. Die Beteiligten arbeiteten jedoch konstruktiv an einer Lösung und seien zuversichtlich, in diesem Jahr weitere Fortschritte erzielen zu können.

Im Bereich des Beschäftigtendatenschutzes (Ziffer 10) stellten sich regelmäßig Fragen im Zusammenhang mit der Zulässigkeit von Überwachungen der Arbeitszeit, der Arbeitszeiterfassung, Zugangskontrollen beziehungsweise Zutrittskontrollen sowie deren konkreten Ausgestaltungen im Einzelfall. Als wichtig erachtet der Ausschuss in diesem Zusammenhang, dass auch bei Vorliegen von Betriebsvereinbarungen, denen der Personalrat beziehungsweise Betriebsrat zugestimmt hat, Vorgaben der DSGVO beachtet werden müssen. Durch Betriebsvereinbarungen könne lediglich gestaltend Einfluss genommen werden, nicht jedoch reduzierend.

Im Hinblick auf den Einsatz von Bodycams im Bahnhofsumfeld durch private Sicherheitsdienste (Ziffer 11.4) nimmt der Ausschuss positiv zur Kenntnis, dass diese unzulässige Praxis abgestellt worden ist, nachdem sich die Landesdatenschutzbeauftragte eingeschaltet hat. Insbesondere bei der öffentlichen Videoüberwachung im Bereich des

Bahnhofsvorplatzes werde sehr darauf geachtet, dass die installierten Kameras nur das filmten, was rechtlich erlaubt sei. Schwieriger gestalte sich die Lage bei den privat installierten Videokameras, deren Besitzern häufig nicht bewusst sei, was rechtlich erlaubt sei und was nicht. Entscheidend sei auch hier das Kriterium der Erforderlichkeit. Auch im nicht öffentlichen Bereich gäbe es legitime private Interessen, zu deren Schutz Videokameras eingesetzt werden dürften.

Zu dem Themenbereich "Internationales und Europa" nimmt der Ausschuss zur Kenntnis, dass der EU-U.S. Privacy Shield ebenso wie schon zuvor das Safe-Harbour-Abkommen aufgrund von datenschutzrechtlichen Einwänden vor den Europäischen Gerichtshof (EuGH) gebracht worden ist. Sowohl die Stellungnahme des Generalanwalts als auch eine endgültige Entscheidung stünden jedoch noch aus (Ziffer 16.1).

Durch den U.S.-amerikanischen Cloud-Act versuche die USA, sich Zugriff auf Daten von Personen aus der EU zu verschaffen, in dem sie europäische Unternehmen verpflichte, ihnen Daten zu übermitteln (Ziffer 16.2). Dieses Vorgehen werde von europäischen Datenschützer sehr kritisch beurteilt.

II. Beschlussempfehlung

Die Bürgerschaft (Landtag) nimmt den Bericht des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zur Kenntnis.

Dr. Solveig Eschen
Vorsitzende

4. Datenschutzbeauftragte

4.1 Treffen der behördlichen Datenschutzbeauftragten

Die halbjährlichen Treffen der behördlichen Datenschutzbeauftragten aus Bremen und Bremerhaven wurden im Jahr 2019 fortgesetzt. Schwerpunkte dieser Treffen waren im Frühjahr des Berichtsjahres der Umgang mit sogenannten Datenpannen, also der Verletzung des Schutzes personenbezogener Daten in den Dienststellen und die hiermit verbundene Pflicht zur Abgabe von Meldungen nach Artikel 33 Datenschutzgrundverordnung sowie im Herbst die sichere, datenschutzkonforme Kommunikation mit Hilfe von Verschlüsselungstechniken.

Beide Treffen stießen bei den Datenschutzbeauftragten auf erhebliches Interesse und wurden mit guter Resonanz angenommen. Deutlich wurde bei den Treffen erneut, dass für die Datenschutzbeauftragten bei der Wahrnehmung ihrer Aufgaben zur Umsetzung der Datenschutzgrundverordnung die Unterstützung sowohl durch ihre Dienststellen als auch durch die bremische Landesbeauftragte für Datenschutz und Informationsfreiheit unerlässlich ist.

4.2 Meldungen von Datenschutzbeauftragten nach Artikel 37 Absatz 7 Datenschutzgrundverordnung

Im Jahr 2019 erhielten wir von Verantwortlichen und Auftragsverarbeiterinnen beziehungsweise Auftragsverarbeitern weit mehr als 300 Meldungen nach Artikel 37 Absatz 7 Datenschutzgrundverordnung (DSGVO) im Hinblick auf die Benennung von behördlichen und betrieblichen Datenschutzbeauftragten oder die Beendigung dieser Funktion. Für die Abgabe der Meldungen wurden größtenteils die von uns auf unserer Homepage eingestellten Formulare genutzt.

Nach Artikel 38 Absatz 6 DSGVO hat die oder der Verantwortliche beziehungsweise die Auftragsverarbeiterin oder der Auftragsverarbeiter sicherzustellen, dass andere von der oder dem Datenschutzbeauftragten wahrzunehmende Aufgaben nicht zu einem Interessenkonflikt führen, der die Amtswahrnehmung beeinträchtigt. Auch kann sich wie bei Familienangehörigen der Firmenchefin beziehungsweise des Firmenchefs ein Interessenkonflikt aus in der Person der oder des Beauftragten liegenden Gründen ergeben. Wir wiesen einige Verantwortliche auf mögliche Interessenkonflikte hin.

Die Beendigung der Übertragung des Amts der oder des Datenschutzbeauftragten erfolgt zulässigerweise in den meisten Fällen dadurch, dass die oder der bisherige Beauftragte das Amt niederlegt oder gegenseitiges Einvernehmen hierüber besteht. Bei einigen Meldungen gingen wir Zweifeln an der Zulässigkeit der Beendigung der Funktion nach.

4.3 Benennung von Datenschutzbeauftragten im Gesundheitswesen

Mehrfach fragten Arztpraxen und Datenschutzbeauftragte solcher Praxen bei uns an, ob sich durch die Änderung des § 38 Absatz 1 Bundesdatenschutzgesetz (vergleiche Ziffer 4.5 dieses Berichts) auch für Arztpraxen die bisherige Verpflichtung ändere, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen, wenn in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. Die betreffende Verpflichtung ergibt sich aus einer Entschließung der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder aus dem Jahr 2018 (siehe hierzu 1. Jahresbericht, Ziffer 4.2)[1].

Da die Entschließung zur Interpretation des Artikels 37 Absatz 1 der Datenschutzgrundverordnung im Gesundheitswesen gefasst wurde, nicht aber mit den Bestimmungen des § 38 Absatz 1 Bundesdatenschutzgesetz in Verbindung steht, verneinten wir die an uns gerichteten Anfragen ausdrücklich. Die Entschließung der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder besteht fort. Arztpraxen, die Gesundheitsdaten verarbeiten, sind unter Berücksichtigung der darin aufgeführten Kriterien zur Benennung einer oder eines Datenschutzbeauftragten verpflichtet.

4.4 Datenschutzbeauftragter und Informationssicherheitsbeauftragter in Personalunion

Ein Datenschutzbeauftragter wandte sich an uns mit der Frage, ob die Stellen der oder des Datenschutzbeauftragten und der oder des Informationssicherheitsbeauftragten in einem Unternehmen in Personalunion wahrgenommen werden können.

Hierzu vertreten wir die Auffassung, dass die gleichzeitige Wahrnehmung der Funktionen in Personalunion nur insoweit möglich ist, als gleichgerichtete Aufgaben erfüllt werden. Dies kann zum Beispiel bei der Beratung der Unternehmensleitung im Hinblick auf die Zulässigkeit der Verarbeitung personenbezogener Daten und die damit verbundene Pflicht zur Ergreifung geeigneter technischer und organisatorischer Schutzmaßnahmen der Fall sein. Die von einer beziehungsweise einem Informationssicherheitsbeauftragten wahrzunehmenden Aufgaben weichen aber häufig von denen der oder des Datenschutzbeauftragten ab und es entsteht daraus ein Interessenkonflikt. Ein solcher Konflikt besteht unter anderem dann, wenn

[1] online unter: https://www.datenschutz.bremen.de/publikationen/jahresberichte-7242

Informationssicherheitsbeauftragte eigenständig IT-Sicherheitsleitlinien, Richtlinien und Regelungen zur Informationssicherheit oder ein IT-Sicherheitskonzepts erstellen. Solche Tätigkeiten sind mit den sich aus den Datenschutzgrundverordnung ergebenden Kontrollbefugnissen und Beratungsbefugnissen von Datenschutzbeauftragten nicht zu vereinbaren. Die Aufgabe von Informationssicherheitsbeauftragten läuft dann den datenschutzrechtlichen Bestimmungen entgegen. Dies gilt gleichermaßen auch für die Umsetzung von Leitlinien und Konzepten. Die gleichzeitige Wahrnehmung der Funktion der oder des Datenschutzbeauftragten und der oder des Informationssicherheitsbeauftragten in Personalunion sollte daher in der Regel vermieden werden.

4.5 Änderung des § 38 Bundesdatenschutzgesetz

Der Bundestag beschloss im Berichtsjahr mit Zustimmung des Bundesrats eine Änderung des § 38 Absatz 1 Satz 1 Bundesdatenschutzgesetz, wonach Verantwortliche und mit der Verarbeitung personenbezogener Daten Beauftragte eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten grundsätzlich erst dann zu benennen haben, wenn sie in der Regel mindestens zwanzig Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Bisher lag die Untergrenze bei zehn Personen. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder kritisierte die Gesetzesänderung mit ihrer Entschließung vom 23. April 2019 (siehe hierzu Ziffer 21.3 dieses Berichts). Sie wies darauf hin, dass sich die Pflicht zur Benennung einer oder eines Beauftragten seit vielen Jahren und ganz besonders bei der Umstellung auf die Datenschutzgrundverordnung (DSGVO) bewährt hat. Die Datenschutzbeauftragten sorgen für eine kompetente datenschutzrechtliche Beratung, um Datenschutzverletzungen schon im Vorfeld zu vermeiden und das Sanktionsrisiko gering zu halten. Die Aufweichung der Benennungspflicht werde die Verantwortlichen und die Auftragsverarbeiterinnen beziehungsweise Auftragsverarbeiter nicht entlasten, sondern ihnen mittelfristig schaden.

Die Änderung gilt nicht für öffentliche Stellen. Diese haben nach Artikel 37 Absatz 1 Buchstabe a DSGVO auch weiterhin auf jeden Fall eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen. Für Gerichte gilt dies nicht für die Verarbeitung personenbezogener Daten im Rahmen ihrer justiziellen Tätigkeit.

5. Übergreifende IT-Verfahren

5.1 Gewährleistung der Sicherheit der Verarbeitung bei der Übertragung personenbezogener Daten per Fax

Aufgrund zahlreicher Nachfragen von verantwortlichen Stellen, ob die Übertragung personenbezogener Daten per Fax den Anforderungen der Datenschutzgrundverordnung

(DSGVO) genügt, haben wir den nachfolgenden Text auf unserer Homepage unter dem Menüpunkt "Datenschutztipps – Orientierungshilfen und Handlungshilfen" veröffentlicht:

"Galt ein Telefax noch vor einigen Jahren als relativ sichere Methode um auch sensible personenbezogene Daten zu übertragen, so hat sich diese Situation grundlegend geändert: Sowohl bei den Endgeräten als auch den Transportwegen gab es weitreichende Änderungen. Bisher wurden beim Versand von Faxen exklusive Ende-zu-Ende-Telefonleitungen genutzt. Technische Änderungen in den Telefonnetzen sorgen jetzt dafür, dass keine exklusiven Leitungen mehr genutzt werden, sondern die Daten paketweise in Netzen transportiert werden, die auf Internet-Technologie beruhen.

Zudem kann nicht mehr davon ausgegangen werden, dass an der Gegenstelle der Faxübertragung auch ein reales Fax-Gerät existiert. Meist werden Systeme genutzt, die ankommende Faxe automatisiert in eine E-Mail umwandeln und diese dann an bestimmte E-Mail-Postfächer weiterleiten.

Aufgrund dieser Umstände hat ein Fax hinsichtlich der Vertraulichkeit das gleiche Sicherheitsniveau wie eine unverschlüsselte E-Mail (welche oftmals mit der offen einsehbaren Postkarte verglichen wird). Fax-Dienste enthalten keinerlei Sicherungsmaßnahmen um die Vertraulichkeit der Daten zu gewährleisten. Sie sind daher in der Regel nicht für die Übertragung personenbezogener Daten geeignet.

Für die Übertragung besonderer Kategorien personenbezogener Daten gemäß Artikel 9, Absatz 1 der Datenschutzgrundverordnung ist die Nutzung von Fax-Diensten unzulässig.

Für den Versand personenbezogener Daten müssen daher alternative, sichere und damit geeignete Verfahren, wie etwa Ende-zu-Ende verschlüsselte E-Mails oder – im Zweifel – auch die herkömmliche Post genutzt werden."

5.2 Modul im eHaushalt: Beteiligungsinformationssystem

Bei der Entwicklung eines Moduls für den eHaushalt, welches das Beteiligungscontrolling abbildet, wurden wir vom Senator für Finanzen über den Beginn und den weiteren Fortgang des Projekts informiert.

6. Inneres

6.1 Gemeldete Datenschutzverletzungen

Es erreichten uns Meldungen von Datenschutzverletzungen vom Senator für Inneres, von der Polizei Bremen und von der Meldebehörde Bremerhaven (siehe hierzu Ziffer 6.6.1 dieses

Berichts). Dies nahmen wir zum Anlass, mit dem Senator für Inneres einen Prozess für die Meldung nach Artikel 33 Datenschutzgrundverordnung abzustimmen.

6.2 Allgemeines zu Polizeiverfahren

Wir beraten die Polizei Bremen und die Ortspolizeibehörde Bremerhaven als Teil der Exekutive sowohl nach der Datenschutzgrundverordnung als auch nach der Datenschutz-Richtlinie im Bereich Strafverfolgung. Ein großes, noch zu bearbeitendes Projekt der Polizei Bremen stellt in diesem Zusammenhang weiterhin die Erstellung des Rahmendatenschutzkonzepts dar, siehe hierzu 40. Jahresbericht, Ziffer 5.3 und 38. Jahresbericht, Ziffer 5.1. Weitere Themen waren im Berichtsjahr unter anderem das polizeiliche elektronische Notizbuch "@rtus-Mobile" (mit einer Verbindung zum polizeilichen Informationssystem @rtus) sowie die weitere Begleitung der Umsetzung von PIAV, dem Polizeilichen Informations- und Analyseverbund.

6.3 Polizeiliche Videoüberwachung

Im Fokus unserer Beratungen im Zusammenhang mit der polizeilichen Videoüberwachung standen die Verbesserung der stationären Videoüberwachung (im Folgenden unter Ziffern 6.3.1 und 6.3.2 dieses Berichts) auf der rechtlichen Grundlage von § 29 Absatz 3 des Bremischen Polizeigesetzes und die mobile Videoüberwachung mittels einer am Körper getragenen Kamera (Bodycam) gemäß § 29 Absatz 5 des Bremischen Polizeigesetzes (siehe hierzu Ziffer 6.3.3 dieses Berichts).

6.3.1 Bremer Hauptbahnhof

Die polizeiliche Videoüberwachung am Bremer Hauptbahnhof wurde unter Einsatz neuer Technik zum Nordausgang Willy-Brandt-Platz und südlich um einen Bereich vom Hugo-Schauinsland-Platz über den Platz der Deutschen Einheit bis zum Breitenweg erweitert. Wir empfahlen die technisch unterstützte sofortige Unkenntlichmachung (Schwärzung), insbesondere der Abbildung öffentlich nicht zugänglicher Bereiche und von Bereichen, in denen dies aus Gründen des Beschäftigtendatenschutzes erforderlich ist. Unseren Empfehlungen wurde grundsätzlich entsprochen.

6.3.2 Bahnhof Vegesack

Am Bahnhof Vegesack wurde eine neue polizeiliche Videoüberwachungsanlage installiert. Die Erforderlichkeit dieser Neueinrichtung von Videokameras rund um den Vegesacker Bahnhofsplatz von der Straße Zur Vegesacker Fähre bis Friedrich-Klippert-Straße wurde von

der Polizei mit der steigenden Anzahl an Kriminalität und mit Tumultlagen begründet. Tumultlagen sind schwierige kriminalitätsbehaftete Situationen, in denen in relativ kurzer Zeit eine Vielzahl von Polizeibeamtinnen und Polizeibeamten aus anderen Polizeirevieren angefordert und eingesetzt werden müssen, um diese Situationen zu entschärfen und vor Ort für die Sicherheit der Bürgerinnen und Bürger zu sorgen. Nach § 29 Absatz 3 Bremisches Polizeigesetz ist eine polizeiliche Videoüberwachung öffentlich zugänglicher Orte möglich, wenn an diesen "vermehrt" Straftaten begangen werden oder wenn an ihnen aufgrund der örtlichen Verhältnisse die Begehung von Straftaten besonders zu erwarten ist. Nachdem die Polizei Bremen mit Hilfe kriminalstatistischer Zahlen begründet hatte, dass es sich aus ihrer Sicht beim Bahnhof Vegesack um einen den gesetzlichen Anforderungen entsprechenden Ort handelte, sahen wir keine Rechtsfehler, die Rechtsgrundlage als erfüllt anzusehen. Im Kontext dieser Beurteilung stellte sich allerdings die Auslegung des Tatbestandsmerkmals "vermehrt" als schwierig dar. Eine gesetzgeberische Klarstellung etwa im Zusammenhang mit der bevorstehenden Änderung des Bremischen Polizeigesetzes zur Umsetzung der Richtlinie (Europäische Union) 2016/680 wäre hier sinnvoll.

6.3.3 Bodycams in Bremen und Bremerhaven

Der Einsatz von Bodycams durch die Polizei Bremen wurde im Jahr 2019 in der Stadt Bremen erweitert. Die Ortspolizeibehörde Bremerhaven setzte solche von Polizeibeamtinnen und Polizeibeamten am Körper getragenen Videokameras im Berichtsjahr erstmalig ein. Wir sprachen in beiden Fällen datenschutzrechtliche Empfehlungen aus. Insbesondere wiesen wir darauf hin, dass Datenschutz-Folgenabschätzungen Voraussetzung für den Einsatz von Bodycams sind.

6.4 Beschwerden über die Polizei Bremen

Im Berichtszeitraum erreichten uns elf Beschwerden über die Polizei Bremen. Die meisten Beschwerden bezogen sich auf die lange Bearbeitungsdauer von Auskunfts-, Berichtigungs- oder Löschbegehren. Vier Beschwerdeführende berichteten von der aus ihrer Sicht ungerechtfertigten Verweigerung von Auskünften. Für die Bearbeitung von Beschwerden sind gesetzlich bestimmte Fristen vorgegeben.

Ausgangspunkt für Beschwerden über Polizeibehörden, die im Rahmen ihrer Strafverfolgungsaufgabe tätig werden, ist die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rats vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rats (im Folgenden JI-Richtlinie). Trotz Ablaufs der Umsetzungsfrist seit 6. Mai 2018 wurde

die JI-Richtlinie noch nicht im Bremischen Polizeigesetz umgesetzt. Wir wiesen die Polizei Bremen darauf hin, dass die Artikel 12, 14 und 16 der JI-Richtlinie als detaillierte, subjektive Rechte auch ohne mitgliedstaatliche Umsetzung unmittelbar gegen den Staat wirken und daher entsprechend der Rechtsprechung des Europäischen Gerichtshofs (Entscheidungen: van Gend & Loos-Entscheidung vom 5. Februar 1963 (26/62); Francovich-Entscheidung vom 19. November 1991 (C-6/90 und C-9/90); Mangold-Entscheidung vom 22. November 2005 (C-144/04)) direkt anwendbar sind.

6.4.1 Beschwerden über die Bearbeitungsdauer

Beschwerden über die Bearbeitungsdauer verwiesen in der Regel auf eine sehr lange Zeitspanne, die vergangen sei, bis die Bearbeitung der Beschwerden beendet worden sei. Auch von unserer Seite ist zu berichten, dass aufgrund mangelnder personeller Ressourcen drei Beschwerden aus dem Jahr 2018 und eine Beschwerde von Anfang des Jahres 2019 noch nicht abgeschlossen worden sind.

Wir wiesen die Polizei Bremen darauf hin, dass es gegen die Artikel 4, 8 und 16 der JI-Richtlinie verstoßen kann, Berichtigungen oder Löschungen zu unterlassen.

6.4.2 Beschwerden über Nichterteilung von Auskünften

Im Berichtsjahr erreichten uns vier Beschwerden über die Nichterteilung von Auskünften durch die Polizei Bremen. Beantragte Auskünfte nicht zu erteilen, kann Verstöße gegen Artikel 12 Absatz 3 und Artikel 14 der JI-Richtlinie bedeuten. Darauf wiesen wir die Polizei Bremen hin. Nachdem wir gegenüber der Polizei Bremen die Nichterteilung der Auskünfte bemängelt hatten, wurden die Auskünfte zeitnah erteilt. Wir nahmen diese Beschwerden zum Anlass, im November 2019 ein Gespräch mit der Polizei Bremen über die Verbesserung des Prozesses der Auskunftserteilung zu führen.

6.5 Nichtumsetzung der Richtlinie (EU) 2016/680

Trotz der an die Mitgliedstaaten gerichteten Verpflichtung, die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rats vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke 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 (JI-Richtlinie) bis zum 6. Mai 2018 umzusetzen, ist dies im Land Bremen bislang nicht geschehen. Die Europäische Kommission stellte im Juli des Berichtsjahres fest, dass die JI-Richtlinie in Deutschland noch nicht vollständig umgesetzt worden ist, weil es an der Umsetzung in sechs Bundesländern, zu denen auch das Land Bremen zählt, fehlt. Gleichzeitig wies die Kommission darauf hin, dass der Europäische

Gerichtshof finanzielle Sanktionen verhängen kann, wenn die Kommission eine Klage anstrengt, weil sie der Auffassung ist, dass ein Mitgliedstaat eine Richtlinie nicht in der erforderlichen Weise umgesetzt hat.

6.6 Beschwerden über Meldebehörden

Uns erreichten im Berichtsjahr 17 Beschwerden über die Meldebehörden. Einige davon standen im Zusammenhang mit Datenübermittlungen in besonderen Fällen. Zum einen handelte es sich um Beschwerden über Datenübermittlungen an eine Partei vor der Wahl im Mai 2019 zu Wahlwerbezwecken auf der Rechtsgrundlage des § 50 Absatz 1 Bundesmeldegesetz (siehe hierzu Ziffer 6.6.1 dieses Berichts). Andere Beschwerden standen im Zusammenhang mit der Nichterteilung von Auskunftssperren gemäß § 51 Bundesmeldegesetz (siehe hierzu Ziffer 6.6.2 dieses Berichts).

6.6.1 Datenübermittlungen an eine Partei

Das Bundesmeldegesetz erlaubt den Meldebehörden die Übermittlung der Namen und Adressdaten von Gruppen wahlberechtigter Bürgerinnen und Bürger auf Antrag von Parteien, die diese Daten zu Zwecken der Wahlwerbung verwenden dürfen.

Gegen solche Datenübermittlungen können die Bürgerinnen und Bürger Widerspruch einlegen. In diesen Fällen dürfen ihre Daten nicht an Parteien weitergegeben werden. Über dieses Widerspruchsrecht werden die Bürgerinnen und Bürger bei der Anmeldung des Wohnsitzes in der Meldebehörde und einmal jährlich durch ortsübliche Bekanntmachung informiert. Es erreichten uns acht Beschwerden, die sich auf die mangelnde Transparenz in der ortsüblichen Bekanntmachung bezogen. Aus dieser Bekanntmachung gehe nicht eindeutig hervor, in welchen Fällen ein Widerspruchsrecht bestehe. Wir empfahlen den Meldebehörden konkrete Formulierungen zur Verbesserung der ortsüblichen Bekanntmachung.

In der Meldebehörde in Bremerhaven kam es zu einer rechtswidrigen Übermittlung von Namen und Adressdaten von Wahlberechtigten trotz eingetragener Widersprüche. Die Meldebehörde meldete uns diese Datenschutzverletzung und informierte die Betroffenen durch öffentliche Bekanntmachung.

6.6.2 Nichterteilung von Auskunftssperren

Uns erreichten vier Beschwerden darüber, dass beantragte Einrichtungen von Auskunftssperren nach § 51 Bundesmeldegesetz von der Meldebehörde versagt worden waren. Die Beschwerdeführenden waren in Organisationen beschäftigt, die sich gegen gewaltbereite, extremistische Gruppen positionieren und mit ihrer Kritik an die Öffentlichkeit

gehen. Alle vier Verfahren sind aus unserer Sicht abgeschlossen, wobei bei einer Beschwerde die Auskunftssperre noch nicht verlängert wurde.

Die bei uns erhobenen Beschwerden zeigen, dass eine Änderung des Bundesmeldegesetzes sinnvoll ist, die klarstellt, dass Auskunftssperren in der Regel eingetragen werden müssen, wenn es sich bei der oder dem Antragstellenden um Angehörige solcher Berufsgruppen handelt, die sich aufgrund ihrer oder seiner Berufsausübung in einer Gefährdungslage befinden, weil sie oder er im Rahmen ihrer oder seiner Tätigkeit typischerweise privat oder beruflich unmittelbaren oder mittelbaren Kontakt zu gewaltbereiten Personen oder Personengruppen haben. Dies sollte auch für ehrenamtlich Tätige und für Privatpersonen gelten, die durch ihr grundrechtskonformes Verhalten zur Zielscheibe gewaltbereiter Gruppen werden können oder geworden sind, weil sie in Ausübung ihrer Grundrechte öffentlich Kritik an gewaltbereiten Personen oder Personengruppen geäußert haben.

6.7 Aktueller Stand zu Zensus 2021

Über den ersten Entwurf des Bremischen Zensusausführungsgesetzes zu dem für Mai 2021 geplanten Volkszählungsverfahren (Zensus 2021) sind wir unterrichtet worden. Aus Kapazitätsgründen war es uns jedoch bis Redaktionsschluss nicht möglich, eine Stellungnahme abzugeben.

7. Justiz

7.1 Gemeldete Datenschutzverletzungen

Insgesamt wurden von Rechtsanwälten und Notaren im Jahr 2019 bei der Landesbeauftragten für Datenschutz und Informationsfreiheit vier Verletzungen des Schutzes personenbezogener Daten nach Artikel 33 Datenschutzgrundverordnung (DSGVO) gemeldet.

Die Staatsanwaltschaft Bremen meldete einen Fall nach Artikel 33 DSGVO. Von Seiten der Gerichte erreichte uns keine Meldung. Aufgrund der richterlichen Unabhängigkeit hat die Landesbeauftragte für Datenschutz und Informationsfreiheit in großen Teilen keine Aufsicht über die Gerichte. Die Datenschutzgrundverordnung ist aber gleichwohl auch dort geltendes Recht. Folglich müssen Meldungen nach Artikel 33 DSGVO an die Aufsichtsbehörde erfolgen und der Verantwortliche muss die Verletzungen dokumentieren. Das gilt auch, wenn Verletzungen im Bereich der richterlichen Unabhängigkeit erfolgt sind. Es entspricht nicht der Lebenserfahrung, dass bei der Bearbeitung einer so großen Anzahl an Akten in der Bremer Justiz nur eine meldepflichtige Datenschutzverletzung geschehen ist, sodass wir davon ausgehen müssen, dass erforderliche Meldungen von Datenschutzverletzungen nicht erfolgten. Wir rechnen hier wie auch sonst mit einer hohen Dunkelziffer und gehen davon aus,

dass die Zahl meldepflichtiger Verletzungen des Schutzes personenbezogener Daten weitaus größer sein wird, als es sich im Berichtsjahr darstellte.

7.1.1 Versendung eines Kaufvertragsentwurfs an falsche E-Mail-Adresse

Ein Notariat versandte aufgrund eines Tippfehlers in der E-Mail-Adresse einen Kaufvertragsentwurf an eine falsche, völlig unbeteiligte fremde Person und meldete uns diese Verletzung des Schutzes personenbezogener Daten. Der richtige Empfänger wurde über diese Verletzung nach Artikel 34 Datenschutzgrundverordnung unterrichtet.

7.1.2 Versendung einer Strafakte im halboffenen Umschlag über die Behördenpost

Eine Behörde in Bremen verschickte einen halboffenen Umschlag mit einer Strafakte über die Behördenpost. Der Umschlag ließ sich 10 cm weit öffnen und die komplette Akte mit dem Namen des Beschuldigten und der Tatvorwurf waren zu lesen. In solchen Fällen handelt es sich um Verletzungen des Schutzes personenbezogener Daten, die nach Artikel 33 Datenschutzgrundverordnung (DSGVO) meldepflichtig sind. Verantwortliche müssen dann prüfen, ob die offene Versendung Risiken für die Rechte und Freiheiten natürlicher Personen zur Folge hatte und nach Artikel 34 DSGVO eine Benachrichtigung an die betroffenen Personen ergehen muss.

7.2 Unverschlüsselte E-Mail-Versendung einer Rechtsanwaltskanzlei

Eine Rechtsanwaltskanzlei versandte rechtswidrig gerichtliche Schriftsätze per unverschlüsselter E-Mail an die Gegenpartei, ohne dass die Partei wusste, dass die E-Mail-Adresse als Kontaktdatum gespeichert worden war. Für den Versand personenbezogener Daten müssen sichere und damit geeignete Verfahren, wie zum Beispiel die Post oder Ende-zu-Ende verschlüsselte E-Mails genutzt werden. Auch ein Fax hat hinsichtlich der Vertraulichkeit das gleiche Sicherheitsniveau wie eine unverschlüsselte E-Mail. Fax-Dienste enthalten auch keinerlei Sicherungsmaßnahmen, um die Vertraulichkeit der personenbezogenen Daten zu gewährleisten. Unverschlüsselte E-Mails und Fax-Dienste sind nicht für die Übertragung personenbezogener Daten geeignet (siehe hierzu Ziffer 5.1 dieses Berichts).

7.3 Aushang von Angaben über Zeuginnen und Zeugen auf Gerichtsfluren

Wir erhielten eine Beschwerde von einem in einem Verfahren geladenen Zeugen darüber, dass sein vollständiger Name mit Angabe seines Wohnorts vor dem Gerichtssaal öffentlich

ausgehängt war. Die Information über Zeit und Ort der Verhandlung durch Aushang ist aufgrund des Grundsatzes der Öffentlichkeit von Gerichtsverfahren rechtsstaatlich geboten. Wir baten das Gericht um Prüfung, ob zur Durchsetzung des Grundsatzes der Datenminimierung auf die Angabe des Wohnorts und des vollständigen Vornamens der Zeuginnen und Zeugen verzichtet werden kann.

7.4 Nichtumsetzung der Richtlinie (EU) 2016/680 für den Strafvollzug, die Strafgerichte und die Staatsanwaltschaft

Der europäische Gesetzgeber hat im Jahr 2016 die Richtlinie 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 erlassen. Diese ist anders als die Datenschutzgrundverordnung nicht direkt anwendbar und hätte vom bremischen Gesetzgeber bis zum 6. Mai 2018 in Landesrecht umgesetzt werden müssen. Die Senatorin für Justiz und Verfassung legte uns im November des Berichtsjahres 2019 einen Entwurf für ein Bremisches Justizvollzugsdatenschutzgesetz zur Stellungnahme vor. Für den Bereich der Strafgerichte und der Staatsanwaltschaft hatte der Bundesgesetzgeber die bundesrechtlichen Regelungen bereits im Jahr 2018 angepasst. Im Land Bremen bliebe die Zuständigkeit für die datenschutzrechtliche Aufsicht über die Gerichte und die Staatsanwaltschaften auch nach Erlass des Justizvollzugsdatenschutzgesetzes weiterhin ungeregelt.

8. Gesundheit

8.1 Gemeldete Datenschutzverletzungen

Im Bereich Gesundheit wurden uns im Berichtsjahr insgesamt 17 Datenschutzverletzungen gemeldet. Neben kriminellen Ursachen wie Hackerangriffen auf E-Mail-Postfächer oder Diebstählen von Patientinnen- und Patientendaten aus Arztpraxen oder Fahrzeugen waren mitunter auch technische oder organisatorische Mängel Ursache der Verstöße, welche zum Beispiel zu Fehlversendungen und damit zu unbefugten Offenlegungen führten.

8.2 Umfangreiche Beschriftung von Infusionsflaschen im Krankenhaus

Eine betroffene Person berichtete uns, dass die auf einer Station im Klinikum Bremen-Ost verwendeten Infusionsflaschen mit Namen, Geburtsdatum, Adresse, Telefonnummer, Krankenkasse sowie Krankenversicherungsnummer der Patientinnen und Patienten gekennzeichnet seien. Eine so umfassende Etikettierung ist nicht erforderlich und daher aus datenschutzrechtlicher Sicht unzulässig. Nach unserem Tätigwerden bestätigte uns das

Klinikum Bremen-Ost, künftig Infusionsflaschen lediglich mit dem Namen und der Patientennummer zu kennzeichnen.

8.3 Mängel bei Zugriffsrechten und Einwilligungserklärung eines ambulanten Pflegedienstes

Wir erhielten zwei Beschwerden über einen ambulanten Pflegedienst, welche zum einen die Zugriffs- und Berechtigungsstrukturen des Pflegedienstes und zum anderen die verwendeten Formulare zur datenschutzrechtlichen Einwilligung betrafen. Obwohl der Pflegedienst aus zwei rechtlich selbstständigen Teilen, einem Kinderkrankenpflegedienst und einem Hauspflegedienst, besteht, wurden zwischen beiden Teilen ohne Rechtsgrundlage personenbezogene Daten in den Bereichen Personalverwaltung, Buchhaltung, Qualitätssicherung und Telefonzentrale übermittelt. Inzwischen wurde ein Vertrag zur Auftragsverarbeitung geschlossen; die Mängel hinsichtlich der datenschutzrechtlichen Einwilligungserklärung wurden noch nicht vollständig ausgebessert.

8.4 Rechtswidrige Übermittlung von Patientendaten an externes Abrechnungsunternehmen

Gleich mehrere Beschwerdeverfahren betrafen die Übermittlung von Patientendaten an externe Abrechnungsunternehmen durch Arztpraxen. Wenn die Patientin oder der Patient privatversichert ist, ist eine solche Übermittlung nur zulässig, wenn die betroffene Person darin eingewilligt hat. Wir mussten allerdings feststellen, dass eine entsprechende Einwilligung nicht immer vorlag und haben in diesen Fällen die betroffenen Praxen sensibilisiert und verwarnt.

8.5 Beschwerden über Einladungsschreiben zu Mammographie-Screenings

Uns erreichten mehrere Beschwerden über die Einladungsschreiben zu Mammographie-Screenings, welche durch die dafür errichtete Zentrale Stelle Mammographie-Screening beim Gesundheitsamt Bremen verschickt werden. Die Beschwerdeführenden beklagten insbesondere, dass aus den Schreiben nicht hervorgeht, welche Rechtsgrundlage die Verwendung der Adressdaten und Geburtsdaten erlaube. Wir konnten beim Gesundheitsamt Bremen darauf hinwirken, dass aus Transparenzgründen künftig weitere Informationen zu den gesetzlichen Grundlagen für die Datenverarbeitung zu Zwecken der Einladung zu einem Mammographie-Screening in das Einladungsschreiben aufgenommen werden.

8.6 Datenschutzverletzungen durch Versandapotheke

Mehrere Personen beschwerten sich bei uns über eine in Bremen ansässige Online-Versandapotheke. Die Beschwerden betrafen unzureichend gewährte Auskunfts- beziehungsweise Löschersuchen und fehlversandte Abrechnungen. Durch unser Tätigwerden konnten wir unter anderem erreichen, dass im Anmeldebereich der Online-Apotheke Kundendaten mithilfe einer Zwei-Faktor-Authentisierung zukünftig stärker geschützt werden.

9. Soziales

9.1 Gemeldete Datenschutzverletzungen

Im Bereich Soziales haben uns Verantwortliche insgesamt neun Datenschutzverletzungen gemeldet.

9.1.1 Abfotografieren und Verbreitung einer Bewohnerliste einer Flüchtlingsunterkunft

Das Sozialamt Bremerhaven meldete uns einen Vorfall aus einer Flüchtlingsunterkunft. Eine Bewohnerin habe eine Liste mit Angaben zu Name, Vorname, Geburtsdatum, Herkunftsland, Ankunft, Zimmernummer und Aufenthaltsstatus aller Bewohnerinnen und Bewohnern der Unterkunft abfotografiert und im Internet verbreitet. Diese Meldung nahmen wir zum Anlass, die Zugriffsberechtigungsstrukturen in Bezug auf die Bewohnerdaten zu überprüfen. Das Sozialamt Bremerhaven teilte uns mit, dass die Angaben auf der Liste nun begrenzt und die Zugriffe beschränkt wurden.

9.1.2 Diebstahl eines Tourenplans aus dem Dienstwagen eines Pflegedienstes

Ein Pflegedienst meldete uns den Diebstahl eines Tourenplans mit Namen, Adressen und den zu erledigenden pflegerischen Aufgaben von zehn Personen aus einem Dienstwagen. Die betroffenen Kundinnen und Kunden wurden über den Vorfall informiert und auf damit einhergehende Gefahren hingewiesen. Der Pflegedienst stellt inzwischen auf Tourenpläne in digitaler Form um, welche gegebenenfalls per Fernzugriff gesperrt werden können.

9.2 Unzulässige Veröffentlichung der Kandidatinnen für das Jugendschöffenamt

Durch einen Hinweis wurden wir darauf aufmerksam, dass das Jugendamt im Zuge der Wahl der Jugendschöffinnen und Jugendschöffen eine Liste mit allen Kandidatinnen und Kandidaten

in das Transparenzportal der Freien Hansestadt Bremen gestellt hatte. Trotz der gesetzlichen Pflicht, die Liste in Papierform in zwei Sozialzentren für jedermann einsehbar auszulegen, war eine Veröffentlichung im Internet nicht erforderlich und auch nicht von der gesetzlichen Grundlage gedeckt, die die "öffentlichen Auslage" anordnet. Nach entsprechender Sensibilisierung wurde die Liste umgehend aus dem Transparenzportal entfernt.

9.3 Datenschutzverletzungen durch Integrationsfachdienst

Im Rahmen eines Beschwerdeverfahrens überprüften wir die Datenverarbeitung durch einen Integrationsfachdienst, dessen gesetzliche Aufgabe darin besteht, behinderten Menschen Hilfestellungen bei dem Zugang zum Arbeitsmarkt zu leisten. Hierbei stellten wir einige Mängel fest: Dem Integrationsdienst waren die Rechtsgrundlagen der eigenen Datenverarbeitung nicht bekannt, betroffene Personen wurden nicht ausreichend über die Verarbeitung Ihrer personenbezogenen Daten informiert und sensible Daten wurden unverschlüsselt auf dem unsicheren E-Mail-Weg versandt. Der Integrationsfachdienst zeigte sich kooperativ und setzte unsere Anforderungen weitestgehend um.

9.4 Anforderung eines vollständigen MDK-Gutachtens bei Antragstellung für Betreutes Wohnen

Im Rahmen der Antragstellung für das Betreute Wohnen verlangen die zuständigen Sozialbehörden auf Grundlage einer landesweiten Rahmenrichtlinie die Vorlage eines vollständigen Gutachtens des Medizinischen Dienstes der Krankenkassen (MDK). Schwärzungen wurden in dem uns berichteten Fall nicht gestattet. Eine solche umfangreiche Übermittlung von Gesundheits- und Sozialdaten der Antragstellerinnen beziehungsweise Antragsteller ist nach unserer Auffassung nicht mit dem Grundsatz der Datenminimierung gemäß Artikel 5 Absatz 1 Buchstabe c Datenschutzgrundverordnung vereinbar. Wir teilten der Senatorin für Soziales unsere Bedenken im Januar 2019 mit; eine Beantwortung steht zu Redaktionsschluss noch aus.

9.5 Bewohner- und Quartiersmanagementsoftware für Flüchtlingsunterkünfte

Im 40. Jahresbericht, Ziffer 8.9, berichteten wir über die Software zum Management der Unterkünfte und schilderten im 1. Jahresbericht, Ziffer 8.1, die noch offenen Punkte. Inzwischen wurde das Beschäftigtenmodul abgeschaltet. Die übrigen Punkte hinsichtlich der Speicherung der Essensausgabe bei jeder einzelnen Person, der Freitexteingabe und der Löschung von nicht mehr erforderlichen Daten wurden noch nicht bearbeitet.

9.6 Datenbank Haaranalysen

Uns liegt weiterhin kein datenschutzkonformer Lösungsvorschlag für die Themen Anonymisierung, Zugriffsstruktur und Auswertungen vor.

10. Bildung

10.1 Gemeldete Datenschutzverletzungen

Im Bereich Schulen und Bildung gab es im Jahr keine Meldungen von Verantwortlichen nach Artikel 33 der Datenschutzgrundverordnung. Es erreichten uns jedoch diverse telefonische Anfragen von Betroffenen.

10.2 Verbot eines Beschwerdeportals über Lehrerinnen und Lehrer

Die Landesbeauftragte für Datenschutz und Informationsfreiheit erließ ein Verbot eines vom Landesverband Bremen der Partei Alternative für Deutschland auf ihrer Internetpräsenz betriebenen Beschwerdeportals über das Verhalten von Lehrerinnen und Lehrern in den Schulen. Dies wurde rechtskräftig. Wir erreichten dadurch, dass das Portal bereits wenige Tage nach Inbetriebnahme abgeschaltet wurde. In einem Beschluss des Verwaltungsgerichts Schwerin vom 2. Dezember 2019 im Rahmen eines einstweiligen Rechtsschutzverfahrens über ein vergleichbares Verbot des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (Aktenzeichen 1 B 1568/19 SN), findet sich eine rechtliche Einschätzung solcher Beschwerdeportale, die die unserem Verbot zugrundeliegende Auffassung bestätigt.

10.3 Unzulässigkeit offener E-Mail-Verteiler

Auch in der Elternvertretungsarbeit ist es in der Regel unzulässig, offene E-Mail-Verteiler zu nutzen. Dies gilt sowohl für die Nutzung des Adressfelds als auch für die sogenannte Carbon Copy oder CC-Funktion. Dabei ist es unerheblich, ob der Inhalt der versandten E-Mails personenbezogene Daten enthält, da die E-Mail-Adressen selbst personenbezogene Daten sind.

10.4 Problem des Aushangs personenbezogener Daten in Schulräumen

Die Landesbeauftragte für Datenschutz und Informationsfreiheit erreichte ein Hinweis, dass in einem als Wahlraum genutzten Schulraum Aushänge mit personenbezogenen Daten von Schülerinnen und Schülern offen sichtbar gewesen seien. Aushänge mit personenbezogenen Daten in Schulräumen sind (soweit sie überhaupt zulässig sind) vor jeder Öffnung für Außenstehende zu entfernen oder anderweitig unkenntlich zu machen.

10.5 Private Fotoaufnahmen bei Schulveranstaltungen

Uns erreichen immer wieder Anfragen zur Zulässigkeit der Anfertigung von Fotoaufnahmen und Videoaufnahmen durch Privatpersonen bei (schul-) öffentlichen Veranstaltungen in Schulen. Die Anfertigung von Aufnahmen für rein private Zwecke ist in der Regel nicht datenschutzrechtswidrig, weil sie durch die sogenannte Haushaltsausnahme vom Anwendungsbereich der Datenschutzgrundverordnung ausgenommen sind. Unzulässig kann aber die Veröffentlichung solcher Aufnahmen sein, auch wenn sie durch Privatpersonen erfolgt.

10.6 Kein Microsoft Office 365 in (Privat-) Schulen

In öffentlichen Schulen in der Freien Hansestadt Bremen wird nach unserer Kenntnis wie in der bremischen Verwaltung insgesamt (siehe hierzu 1. Jahresbericht, Ziffern 3 und 5.1 und 40. Jahresbericht, Ziffer 4.3) auch aufgrund datenschutzrechtlicher Bedenken auf die Nutzung von Microsoft Office 365 weiterhin verzichtet. Die Möglichkeit einer datenschutzkonformen Verwendung konnte bislang nicht dargelegt werden (siehe hierzu Ziffer 11.13 dieses Berichts). Daher sollten auch die bremischen Privatschulen im Zusammenhang mit der Verarbeitung personenbezogener Daten andere Angebote nutzen.

11. Beschäftigtendatenschutz

11.1 Gemeldete Datenschutzverletzungen

Insgesamt wurden im Bereich Beschäftigtendatenschutz im Jahr 2019 bei der Landesbeauftragten für Datenschutz und Informationsfreiheit 16 Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung gemeldet. Vielfach erreichten uns zudem zusätzlich telefonische Anfragen, insbesondere von Betroffenen und Personalvertretungen. Bedauerlicherweise schrecken letztere nach unserer Erfahrung häufig davor zurück, Datenschutzverletzungen unter Nennung der Verantwortlichen bei uns zwecks aufsichtsrechtlicher Verfolgung zu melden, da sie selbst bei anonymer Meldung Repressalien seitens der jeweiligen Arbeitgeberinnen oder Arbeitgeber befürchten.

11.2 Aufzeichnung von Anrufen durch ein Callcenter

Die Aufzeichnung von eingehenden Anrufen durch den Arbeitgeber in einem Callcenter zum Zweck der späteren Auswertung zur Schulung der Beschäftigten verstößt in der Regel gegen Datenschutzrecht, weil die Aufzeichnung für die Schulung der Beschäftigten nicht erforderlich ist. Angesichts des Beschäftigungskontexts kommt auch eine Einwilligung als

Rechtsgrundlage im Regelfall nicht in Betracht (siehe zu den besonderen Anforderungen an die Erteilung einer Einwilligung durch Beschäftigte auch Ziffer 11.8 dieses Berichts).

11.3 Unzulässigkeit der Kenntlichmachung des Herkunftslands

Uns erreichte eine telefonische Beratungsanfrage, ob es zulässig sei, dass ein Verantwortlicher verlangt, dass Flüchtlinge Namensschilder tragen, auf denen zusätzlich die Flagge ihres Herkunftslands abgebildet ist, wenn sie in einem von diesem Verantwortlichen betriebenen Supermarkt tätig sind. Dies ist unzulässig. Auch von Beschäftigten mit Außenkontakt darf die Arbeitgeberin oder der Arbeitgeber nicht verlangen, ihr Herkunftsland während der Arbeitszeit offenzulegen, insbesondere nicht durch das Tragen entsprechender Schilder oder Kennzeichnungen auf der Kleidung. Dies gilt auch für Hilfskräfte. Angesichts des Beschäftigungskontexts ist aus unserer Sicht auch eine wirksame Einwilligung nicht denkbar (siehe zu den besonderen Anforderungen an die Erteilung einer Einwilligung durch Beschäftigte auch Ziffer 11.8 dieses Berichts).

11.4 Unzulässige Weitergabe von persönlichen Passwörtern in Behörde

Uns erreichte die Information, dass in der bremischen Verwaltung Bedienstete die für ihr persönliches Konto angelegten Passwörter für Vertretungstätigkeiten zum Beispiel in Abwesenheitsfällen weitergegeben hatten und dies auf Anweisung oder zumindest mit Wissen der Dienstvorgesetzten erfolgt war. Dieses Vorgehen ist unter anderem aus Gründen des Beschäftigtendatenschutzes unzulässig. Eine Rechtsgrundlage besteht nicht, die Weitergabe ist auch nicht einwilligungsfähig.

11.5 Aufforderung zur Einrichtung eines Zugriffs auf dienstliche E-Mail-Postfächer

Die Aufforderung an Bedienstete, für eventuelle Vertretungsfälle die Möglichkeit eines Vertretungszugriffs auf die personalisierten dienstlichen E-Mail-Postfächer einzurichten, ist unter anderem aus Gründen des Beschäftigtendatenschutzes unzulässig. Dies gilt unabhängig von der Frage, ob das Konto privat genutzt werden darf. Die geltenden Vorschriften in der Freien Hansestadt Bremen enthalten keine Rechtsgrundlage, insbesondere auch nicht die Verwaltungsvorschrift zu Kommunikation und Dokumentenverwaltung in der Freien Hansestadt Bremen (VV KommDok). Eine Einwilligung als Rechtsgrundlage ist angesichts des Beschäftigtenkontexts nur in Ausnahmefällen denkbar und könnte allenfalls die Bedenken im Hinblick auf den Beschäftigtendatenschutz ausräumen.

11.6 Fund vertraulicher Personalunterlagen in einem Behördendrucker

In einem Behördendrucker wurden durch einen anderen Nutzer als die Person, die den Ausdruck veranlasst hatte, vertrauliche Unterlagen in einer Personalsache aufgefunden. Im Umgang mit Personalunterlagen muss auch beim Ausdruck der Datenschutz durchgehend gewährleistet werden. Ausdrucke sollten daher direkt am Arbeitsplatz der oder des Zugriffsberechtigten erfolgen. Sofern dies nicht möglich ist, ist die Funktion des sogenannten sicheren Druckens zu verwenden, bei der der Ausdruck erst erfolgt, wenn sich die oder der Berechtigte am Drucker legitimiert.

11.7 Zurücksetzung des Passworts einer Mitarbeiterin oder eines Mitarbeiters bei Abwesenheit

Uns erreichte eine Beratungsbitte einer Personalvertretung zur Frage des Zugriffs auf passwortgeschützte Beschäftigtenkonten bei insbesondere längerer oder unvorhergesehener Abwesenheit. Ein solcher Zugriff unter Überwindung des Passwortschutzes ist ohne vorherige Zustimmung der oder des Betroffenen nur in Ausnahmefällen zulässig. Die Arbeitgeberin beziehungsweise der Arbeitgeber hat grundsätzlich für solche Fälle technische und organisatorische Vorkehrungen zu treffen. Sofern der Zugriff unvermeidbar ist, ist dieser auf das Mindestmaß zu beschränken, genau zu dokumentieren und im Anschluss für einen erneuerten Passwortschutz zu sorgen. Die oder der Betroffene ist unverzüglich zu informieren.

11.8 Fotos von Beschäftigten in Infomaterial und Werbematerial

Immer wieder erreichen uns Beschwerden und Anfragen zur Abbildung von Beschäftigten in Materialien der Arbeitgeberin beziehungsweise des Arbeitgebers oder auf Internetpräsenzen. Diese sind datenschutzrechtlich hochproblematisch und können allenfalls in bestimmten Konstellationen erlaubt sein, sofern eine wirksame Einwilligung vorliegt. Die Einwilligung ist in aller Regel schriftlich einzuholen und muss auch sonst den strengen Anforderungen des § 26 Absatz 2 Bundesdatenschutzgesetz genügen. Diese Norm verdeutlicht, dass für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit zu berücksichtigen ist sowie die Umstände, unter denen die Einwilligung erteilt wurde. Erforderlich ist neben der Berücksichtigung der Besonderheiten des Einzelfalls, dass eindeutig dargelegt und klar begrenzt ist, welche Nutzung von welchem Bildmaterial der Arbeitgeberin beziehungsweise dem Arbeitgeber zu welchem Zweck gestattet ist. Zudem muss die Arbeitgeberin oder der Arbeitgeber darlegen, dass Beschäftigten, die keine Einwilligung erteilen, keine Nachteile drohen und dass dies den Beschäftigten deutlich gemacht wurde. Auch müssen die Beschäftigten darauf hingewiesen worden sein, dass sie ihre Einwilligung jederzeit widerrufen können.

11.9 Grenzen des Einsatzes von Ortungssystemen in Firmenfahrzeugen

Uns erreichten mehrere Anfragen von Beschäftigten und von Personalvertretungen bezüglich der Zulässigkeit des Einsatzes von Ortungssystemen in Dienstfahrzeugen, zum Beispiel in Fahrzeugen von Fahrdiensten für Senioren oder Menschen mit Behinderungen. Eine kontinuierliche Echtzeitbeobachtung des Standorts der Fahrzeuge ist auch wegen des dadurch erzeugten lückenlosen Überwachungsdrucks ebenso wenig zulässig wie eine längerfristige Speicherung der erfassten Ortungsdaten, die die Erstellung von Bewegungsprofilen ermöglicht. Ein Einsatz von Ortungssystemen wie dem Global Positioning System (GPS) oder ähnlicher Technologie in den Beschäftigten zur Nutzung überlassenen Firmenfahrzeugen darf nicht zur Verhaltenskontrolle genutzt werden. Der Einsatz muss also von einem anderen legitimen Interesse der Arbeitgeberin beziehungsweise des Arbeitgebers abgedeckt und auf das für diesen Zweck erforderliche Maß begrenzt sein. Soweit mit den zulässig erhobenen Daten ein Missbrauch für Zwecke der Verhaltenskontrolle möglich wäre, sind hiergegen technische und organisatorische Vorkehrungen zu treffen.

11.10 Bedingungen für die Zulässigkeit elektronischer Zugangssysteme

In einer Behörde in Bremerhaven erfasste ein elektronisches Zugangssystem mithilfe der personalisierten elektronischen Schlüssel die genauen Zutrittszeiten der Beschäftigten, wobei es möglich war, die gesicherten Türen mit einem anderen Schlüsselinhaber beziehungsweise einer anderen Schlüsselinhaberin ohne Nutzung des eigenen Schlüssels zu passieren. Die Speicherdauer der erfassten Daten betrug mehrere Monate. Eine solche Datenverarbeitung ist unzulässig. Insbesondere für eine Prävention oder Verfolgung von Straftaten ist die Datenerhebung nicht geeignet.

11.11 Enge Grenzen der Videoüberwachung in Arbeitsräumen

Uns erreichten mehrere Anfragen zum Einsatz von Videoüberwachungssystemen an Orten, an denen sich auch Beschäftigte aufhalten, zum Beispiel Anfragen zum Einsatz von Kameras in Zugangsbereichen zu Seniorenwohnheimen, in Lagerräumen eines Supermarkts, im von mehreren Unternehmen gemeinsam genutzten Eingangsbereich eines Bürogebäudes durch eines dieser Unternehmen, in den für Besucherinnen und Besucher zugänglichen Bereichen sowie im Kassenbereich der Geschäftsräume einer Wohnungsgenossenschaft und in Spielhallen. Ein Einsatz von Videoüberwachung im Arbeitsumfeld darf nicht zur Verhaltenskontrolle genutzt werden. Der Einsatz muss also von einem anderen legitimen Interesse der Arbeitgeberin oder des Arbeitgebers abgedeckt und einschließlich der Speicherdauer auf das für diesen Zweck erforderliche Maß begrenzt sein. Soweit mit zulässig erhobenen Daten ein Missbrauch für Zwecke der Verhaltenskontrolle möglich wäre, sind hiergegen technische und organisatorische Vorkehrungen zu treffen. Die Videoüberwachung

muss den Beschäftigten gegenüber offengelegt werden, einschließlich des genauen Umfangs der erfassten Daten, der Zugriffsmöglichkeiten sowie des Ob und Wie und der Dauer der Speicherung.

11.12 Keine Legalisierung durch Betriebsvereinbarung

Uns erreichen häufig Beratungsbitten von Personalvertretungen zu von der Arbeitgeberin beziehungsweise vom Arbeitgeber vorgelegten Betriebsvereinbarungen, mit denen Rechtsgrundlagen für ansonsten unzulässige Datenverarbeitungen geschaffen werden sollen, und von Beschäftigten, gegenüber denen sich die Arbeitgeberin beziehungsweise der Arbeitgeber für die Rechtfertigung der Verarbeitung von personenbezogenen Daten allein auf bestehende Betriebsvereinbarungen beruft. Soweit Datenverarbeitungen gegen die datenschutzrechtlichen Grundprinzipien verstoßen, ist eine Legalisierung durch Abschluss einer Betriebsvereinbarung nicht möglich, die Datenverarbeitungen bleiben auch bei Abschluss der Vereinbarung unzulässig.

11.13 Umfrage zur Nutzung von Microsoft Office 365

Mit dem Büroanwendungspaket Office 365 folgt Microsoft dem Trend, die Verarbeitung und Speicherung von Daten auf externe Anbieter zu übertragen. Neben bekannten Problemen, welche durch die Nutzung von sogenannten Cloud-Diensten entstehen (wie beispielsweise die Möglichkeit Dritter, auf die Daten zuzugreifen oder die Übermittlung der Daten in datenschutzrechtlich unsichere Drittländer), gibt es auch gravierende Probleme beim Schutz von Beschäftigtendaten bei der Nutzung bestimmter Module. In diesem Zusammenhang befragten wir im Berichtsjahr in einem ersten Schritt die (gemessen an der Zahl der Beschäftigten) 33 größten Unternehmen des Landes Bremen danach, ob und in welcher Form sie Microsoft Office 365 nutzen, unter anderem nach der Office Edition und den eingesetzten Modulen. Der Fragebogen kann auf der Homepage der Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) eingesehen werden.[2] Die Auswertung der Rückmeldungen ergab, dass knapp ein Drittel der angefragten Unternehmen diese Software im Einsatz hat; die von der LfDI aufgrund der Auswertungsmöglichkeiten besonders problematischen Module Microsoft Graph und Delve werden von vier Unternehmen verwendet.

Das Ziel, verantwortliche Stellen im Umgang mit Microsoft Office 365 im ersten Schritt für die datenschutzrechtlichen Probleme zu sensibilisieren, ist näher gerückt, aber – wie manche Rückmeldungen gezeigt haben – noch nicht erreicht. Das Thema wird die LfDI im kommenden Jahr weiter beschäftigen.

[2] online unter: https://www.datenschutz.bremen.de/sixcms/media.php/13/Fragebogen.pdf

12. Videoüberwachung

12.1 Beschwerden

30 Beschwerden, die wir im Berichtsjahr erhielten, bezogen sich auf die Videoüberwachung: Sie nehmen somit einen erheblichen Anteil an den uns zugegangenen Eingaben ein. Mitteilungen der oder des für die Überwachung Verantwortlichen nach Artikel 33 Datenschutzgrundverordnung im Hinblick auf die Verletzung des Schutzes personenbezogener Daten erhielten wir indes nur in einem Fall, der die polizeiliche Videoüberwachung betrifft und über den wir unter Ziffer 6.1 dieses Berichts informieren.

12.2 § 4 Bundesdatenschutzgesetz auf Videoüberwachungen zu privaten Zwecken nicht anwendbar

Das Bundesverwaltungsgericht entschied in seinem Urteil vom 27. März 2019 (Aktenzeichen 6 C 2.18), dass § 4 Bundesdatenschutzgesetz (BDSG) mangels mitgliedstaatlicher Gesetzgebungskompetenz auf private Stellen nicht anwendbar sei. Rechtsgrundlage für Videoüberwachungen durch nicht öffentliche Stellen selbst und in deren Auftrag Verarbeitende könnten nur die Regelungen der Datenschutzgrundverordnung (DSGVO) sein. Zwar prüfte das Gericht im der Entscheidung zugrundeliegenden Fall, in dem es um die Videoüberwachung innerhalb einer zahnärztlichen Praxis ging, die Rechtsgrundlagen in Artikel 6 Absatz 1 DSGVO. Es stellt sich jedoch die Frage, ob nicht in dem Fall der Videoüberwachung in einer ärztlichen Praxis als Rechtsgrundlage allenfalls auf Artikel 9 DSGVO zurückgegriffen werden kann, da von der Videoüberwachung insbesondere Patientinnen und Patienten und damit Gesundheitsdaten als besondere Kategorien personenbezogener Daten betroffen sind.

13. Wirtschaft und Gewerbe

13.1 Gemeldete Datenschutzverletzungen

Es wurden uns im Berichtszeitraum aus den verschiedensten Wirtschaftssektoren Datenschutzverletzungen gemeldet. Etliche Meldungen erfolgten aufgrund erfolgreicher Schadsoftware-Attacken auf Unternehmensnetzwerke mit Abfluss personenbezogener Daten, andere aufgrund Diebstahls oder Verlusts mobiler Endgeräte, wiederum andere aufgrund individuellen Augenblicksversagens von Beschäftigten etwa bei der Auswahl des Versandfelds für Newsletter "offener Verteiler", bei der Kuvertierung von Schreiben und so weiter.

13.2 Kopiergeschäfte

In Kopiergeschäften werden Tag für Tag große Mengen personenbezogener Daten mit Informationen aus allen Lebensbereichen betroffener Personen digital verarbeitet, etwa Zeugnisse, Rechnungsnachweise, Lohnbescheinigungen, Personenstandsurkunden, Kontoauszüge, Ausweisdokumente und so weiter. All diese Daten landen auf den Speichermedien der Digitalkopierer / Multifunktionsgeräte. Zwar bieten mittlerweile viele Gerätehersteller technische Lösungen an, um insbesondere eine automatische Löschung von Daten unmittelbar nach Auftragserledigung sicherzustellen. Nicht selten handelt es sich aber lediglich um optionale, mit Zusatzkosten verbundene Geräteausstattungserweiterungen. In ganz besonderem Maße hängt daher die Frage des Datenschutzes bei Kopierläden von der Sensibilität der Geschäftsinhaberin beziehungsweise des Geschäftsinhabers ab. Dass diese jedoch nicht immer im wünschenswerten Maße vorhanden ist, zeigte uns eine Beschwerde im Berichtszeitraum. Für flächendeckende Beratungsbesuche und Kontrollbesuche fehlen uns allerdings leider die Ressourcen.

13.3 Telefonbelästigung

Auch in diesem Berichtszeitraum erhielten wir wieder Eingaben über ungewollte tagtägliche Telefonanrufe. Zumeist geht es um angebliche Vertragsabschlüsse und hieraus resultierende angebliche Zahlungsforderungen. Dieses Mal schienen die Anrufe vermeintlich von einem Bremer Telefonanschluss zu stammen. Die genannte Rufnummer (0421/36583000) war allerdings keinem Telekommunikationsteilnehmer zugeordnet, wie ein Rückruf ergab. Derartige Manipulationen der Rufnummer sind angesichts der technischen Möglichkeiten heutzutage leider keine Seltenheit. Freilich verstoßen sie gegen das Telekommunikationsgesetz. Für die Verfolgung (auch) von Rufnummernmanipulationen ist die Bundesnetzagentur zuständig. Auf deren Webseite finden sich zu diesem Thema zahlreiche Informationen einschließlich eines Beschwerdeformulars[3]. Außerdem kann bei der Staatsanwaltschaft Strafanzeige gegen Unbekannt wegen Betrugsversuchs erstattet werden, wenn das Bestehen einer Zahlungsforderung vorgetäuscht wird.

Wir hingegen können in solchen Fällen leider nichts unternehmen, da wir nach geltender Rechtslage im Bereich des Telekommunikationsverkehrs weder als Verwaltungsbehörde noch als Ordnungswidrigkeitsbehörde gesetzliche Ermittlungsbefugnisse besitzen.

[3] online unter: www.bundesnetzagentur.de/rufnummernmissbrauch

13.4 Änderung der Datenverarbeitungsbefugnis der Industrie- und Handelskammern

Der Paragraf 9 des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern (IHKG) enthält die grundlegenden Vorschriften zum Umgang der Industrie- und Handelskammern mit personenbezogenen Informationen der kammerangehörigen Gewerbetreibenden.

Das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU) hat (auch) hier Veränderungen gebracht: Bislang waren die Kammern auf direkte Datenerhebungen bei den Kammerangehörigen beschränkt, nunmehr dürfen sie – durchaus sachgerecht – die für ihre Aufgaben notwendigen Informationen zu Kammerangehörigen unter bestimmten Voraussetzungen auch aus allgemein zugänglichen Quellen beziehungsweise bei nicht öffentlichen Stellen erheben (vergleiche § 9 Absatz 1 IHKG-neu). Das Widerspruchsrecht der Kammerangehörigen gegen Datenübermittlungen der Kammern an nicht öffentliche Stellen wurde erweitert, nämlich nunmehr auf die Angaben Name, Firma, Anschrift und Wirtschaftszweig. Weitere Neuerung: Hat die oder der Gewerbetreibende der Datenübermittlung nicht widersprochen, so erfolgt diese durch die Kammer gleichwohl lediglich dann, wenn sich die informationsabfragende nicht öffentliche Stelle gegenüber der Kammer verpflichtet hat, die Informationen ausschließlich zweckgemäß zu verarbeiten (§ 9 Absatz 5 IHKG-neu).

13.5 Vertragsstreitigkeiten

Als Datenschutzaufsichtsbehörde sind wir nicht befugt, über das Zustandekommen und Bestehen von Verträgen beziehungsweise von vertraglichen Ansprüchen zu entscheiden. Diese zivilrechtlichen Fragen kann und darf verbindlich nur das zuständige Zivilgericht klären. Gleichwohl wandten sich auch in diesem Berichtszeitraum wieder einige Bürgerinnen und Bürger an uns, weil sie im Streit mit einem Unternehmen um das Zustandekommen eines Vertrags beziehungsweise einer vertraglichen Zahlungsforderung lagen und der Auffassung waren, das Unternehmen dürfe ihre Daten nicht ohne ihre Einwilligung speichern und schon gar nicht an einen Rechtsdienstleister übermitteln.

Nach geltendem Datenschutzrecht dürfen (tatsächliche / vermeintliche) Vertragspartnerinnen und Vertragspartner im Zusammenhang mit einem (tatsächlichen / vermeintlichen) Vertragsschluss jeweils im vertragserforderlichen Umfang personenbezogene Daten des anderen Vertragsteils verarbeiten. Ebenso darf ein Vertragsteil personenbezogene Daten des anderen Vertragsteils zur Geltendmachung einer aus seiner Sicht bestehenden Vertragsforderung im notwendigen Umfang (grundsätzlich Kontaktdaten und Vertragsdaten) an einen Rechtsdienstleister zwecks Rechtsdurchsetzung übermitteln. Solche

Rechtsdienstleister sind insbesondere Rechtsanwältinnen und Rechtsanwälte oder auch Inkassounternehmen. Einer Einwilligung des (tatsächlichen / vermeintlichen) Vertragspartners hierzu bedarf es grundsätzlich nicht.

Solange um einen Vertrag beziehungsweise Ansprüche hieraus gestritten wird, hat selbstverständlich auch kein Vertragsteil einen Anspruch auf Datenlöschung. Ist der Vertragsstreit beendet, also der eigentliche Zweck der Datenverarbeitung erreicht, greifen nachfolgend regelmäßig gesetzliche Aufbewahrungsfristen für Unterlagen einschließlich personenbezogener Daten und schließen zeitweilig noch einen Löschanspruch aus.

14. Kreditwirtschaft

14.1 Gemeldete Datenschutzverletzungen

Die Zahl der Meldungen über Datenschutzvorfälle im Kreditwesenssektor lag im Berichtszeitraum lediglich im einstelligen Bereich. Gemeldet wurde uns etwa der Fehlversand von Kontoauszügen beziehungsweise sonstigen Bankinformationen, daneben insbesondere die Durchführung von Mailingaktionen mit offen einsehbarem E-Mail-Adressatenkreis.

14.2 Verfrühte Schufa-Meldung

Die Darlehensvertragsverhandlungen eines Kreditinstituts mit einem Kunden waren so weit gediehen, dass "nur noch" die Unterschrift des Kunden unter den Verträgen fehlte. Für den Kunden wurden in Erwartung der Unterzeichnung bereits entsprechende Kreditkonten eingerichtet. Damit war die automatische Meldung über eine erfolgte Kreditvergabe bei der Schufa Holding AG verbunden. Da der Kunde mit Vertragsmodalitäten jedoch nicht einverstanden war, sah er von einer Unterzeichnung des Kreditvertrags ab. Die Schufa Holding AG hatte jedoch zwischenzeitlich bereits den Kredit als erteilt gespeichert, wovon der Kunde aufgrund Einsichtnahme in den zu seiner Person gespeicherten Datensatz bei der Schufa Holding AG Kenntnis erhielt. Ein aufsichtsbehördliches Einschreiten war veranlasst.

14.3 Augen auf bei Wahl des E-Mail-Adressfeldes

Gleich drei Mal hintereinander hatten Mitarbeiterinnen und Mitarbeiter eines ortsansässigen Kreditinstituts beim Versand eines Veranstaltungs-Newsletters die personifizierten E-Mail-Adressen der Privat- und Geschäftskunden nicht im verdeckten Sendefeld "BCC" eingetragen, sondern das offene Sendefeld "CC" genutzt. Damit wurden jeder einzelnen Empfängerin beziehungsweise jedem einzelnen Empfänger des Newsletters die personifizierten E-Mail-Adressen aller angeschriebenen weiteren Empfängerinnen und Empfänger offengelegt. Da uns das Institut selbst diese drei Fälle pflichtgemäß als Datenschutzvorfälle gemeldet und im

Übrigen durchaus vorbildlich auf die Vorfälle reagiert hatte, konnten wir es bei einer Verwarnung bewenden lassen.

14.4 Fehlkuvertierung von Mahnungen

Entsprechend der gesetzlichen Verpflichtung zur Meldung bestimmter Datenschutzvorfälle informierte uns ein ortsansässiges Institut im Berichtszeitraum, dass in das Briefkuvert eines Mahnschreibens wegen fälliger Zahlungen vier weitere Mahnschreiben an andere Kundinnen und Kunden geraten seien. So seien dem Adressaten des Mahnschreibens Informationen zu Name sowie Adresse und ausstehendem Zahlungsbetrag der säumigen anderen vier Kundinnen und Kunden bekannt geworden. Wir sprachen eine förmliche Verwarnung aus.

14.5 Fehlversand eines Kontoauszugs

Nachdem bei einem neueröffneten Girokonto über einen längeren Zeitraum keine Umsatzinformationen durch die Kontoinhaberin abgerufen worden waren, wurden die Kontoauszüge durch das kontoführende Kreditinstitut erstellt und postalisch versandt. Versandadresse war aber nicht die Wohnanschrift der Kundin und Kontoinhaberin, sondern diejenige des seit kurzem getrenntlebenden Partners der Kontoinhaberin. Grund hierfür war, dass zwischen den beiden Kundendatensätzen der ehemaligen Partner eine technische Verknüpfung nicht wie vorgeschrieben mitarbeiterseits gelöst worden war, sodass die Adressaktualisierung bei dem Partner automatisch zu einer fehlerhaften Adressumschreibung im Datensatz der Kundin geführt hatte. Wir sprachen eine förmliche Verwarnung aus.

14.6 Erweiterung der Datenverarbeitungsbefugnis durch erschlichene Einwilligungen?

Wie bereits berichtet (siehe hierzu 1. Jahresbericht, Ziffer 12.1) hatten wir Anhaltspunkte dafür, dass Kreditinstitute die Unsicherheit ihrer Kundinnen und Kunden im Zusammenhang mit den Neuregelungen der Datenschutzgrundverordnung dazu ausgenutzt haben könnten, sich weitergehende Möglichkeiten zur Auswertung und Nutzung der Kundendaten zu verschaffen, indem sie bei Kundinnen und Kunden individuell Einwilligungserklärung einholten unter Vortäuschung der Notwendigkeit der Abgabe zur Fortsetzung der Geschäftsbeziehung. Die in diesem Zusammenhang eigentlich notwendige flächendeckende Kontrolle bei ortsansässigen Kreditinstituten konnten wir allerdings mangels personeller Ressourcen leider (weiterhin) nicht vornehmen.

15. Werbung und Versicherung

15.1 Gemeldete Datenschutzverletzungen

Sowohl im Bereich der Werbung als auch im Bereich der Versicherungen wurden der Landesbeauftragten für Datenschutz und Informationsfreiheit keine Meldungen von Verletzungen des Schutzes personenbezogener Daten zugesandt. Es entspricht nicht der allgemeinen Lebenserfahrung, dass es in diesen Bereichen zu keinen meldepflichtigen Verletzungen des Schutzes personenbezogener Daten gekommen ist.

15.2 Versendung von Kundenzufriedenheitsabfragen trotz fehlender Einwilligung zur Werbung

Ein Unternehmen versandte über 3.000 Kundenzufriedenheitsanfragen per E-Mail, obwohl die Kundinnen und Kunden nicht in den Erhalt von Werbung eingewilligt hatten. Nach ständiger Rechtsprechung fallen Kundenzufriedenheitsabfragen unter den Werbebegriff, da sie zumindest auch dazu dienen, Kundinnen und Kunden zu binden und künftige Geschäftsabschlüsse zu fördern. Aufgrund unserer rechtlichen Ausführungen stellte das Unternehmen diese Praxis ein und versendet nunmehr nur noch Kundenzufriedenheitsabfragen, wenn eine wirksame Einwilligung zum Erhalt von Werbung vorliegt.

15.3 Auskunftsrechte betroffener Personen wurden ignoriert

Im Berichtsjahr erreichten uns Informationen, dass verschiedene Unternehmen den Auskunftsanspruch Betroffener nach Artikel 15 Datenschutzgrundverordnung nicht beachtet hatten. Die gewünschten Auskünfte wurden in diesen Fällen erst aufgrund unserer Aufforderungen erteilt.

15.4 Recht auf Löschung von bestimmten Daten auch bei Aufbewahrungspflichten

Uns erreichten Beschwerden darüber, dass die Daten Betroffener auf deren Antrag hin nicht gelöscht worden waren. Häufig gaben die verantwortlichen Unternehmen an, dass sie die Daten aufgrund der gesetzlichen Aufbewahrungsfristen nach Handelsgesetzbuch oder steuerrechtlichen Vorschriften nicht hätten löschen dürfen. Diese Aufbewahrungspflichten gelten jedoch nur für bestimmte Daten, wie die Stammdaten oder Rechnungsdaten. Alle anderen personenbezogenen Daten sind zu löschen. Für die zwingend aufzubewahrenden Daten muss als milderes Mittel eine Einschränkung der Verarbeitung erfolgen, da diese Daten nicht mehr im laufenden Geschäftsbetrieb von allen Mitarbeiterinnen und Mitarbeitern benötigt

werden. Unter der Einschränkung der Verarbeitung versteht die Datenschutzgrundverordnung die Markierung der Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

15.5 Werbebriefe mit Adressen in der eigenen Handschrift der Adressaten

Zwei Reiseunternehmen mit Sitz in Bremen versandten per Post eine Vielzahl von Werbeschreiben an Menschen im ganzen Bundesgebiet. Dazu erreichten uns 34 Beschwerden im Jahr 2019. Auf diesen Anschreiben wurden meist eingescannte handschriftlich ausgefüllte Adressdaten und Unterschriften der Betroffenen abgedruckt, die diese auf Teilnahmekarten von Gewinnspielen ausgefüllt hatten. Zum Teil lag die Teilnahme an den Gewinnspielen bereits mehr als zehn Jahre zurück. In mehreren Fällen waren die oder der Angeschriebene bereits verstorben, sodass die Angehörigen beim Lesen der Schreiben mit der Handschrift der oder des Verstorbenen konfrontiert wurden. Bei den Gewinnspielen waren weder das werbende Unternehmen genannt noch war angegeben worden, dass die Adressdatensätze an andere Unternehmen weitergegeben werden sollten. Damit war die Weitergabe der personenbezogenen Daten an die Reiseunternehmen rechtswidrig, die angaben, diese bei einem Anbieter im Nicht-EU-Ausland gekauft zu haben. Auch die Verwendung der Daten durch die bremischen Reiseunternehmen erfolgte ohne Rechtsgrundlage.

15.6 Einwilligung zur Datenübertragung bei Anpassung eines Versicherungsvertrags

Bei einer Anpassung des Versicherungsvertrags verlangte ein Maklerunternehmen eine Einwilligungserklärung für die Weiterleitung sämtlicher Daten der Versicherungsnehmerinnen und Versicherungsnehmer für eine Vielzahl anderer Unternehmen. Aufgrund der fehlenden Differenzierung war dies rechtswidrig. Nur soweit es für einen bestimmten Vertrag erforderlich ist, dürfen Datenübermittlungen stattfinden. Auch fehlt bei "Einwilligungen auf Vorrat" ohne Informationen über die konkrete Verarbeitung ein konstitutives Geltungselement, sodass diese keine Rechtsgrundlagen für die Verarbeitung personenbezogener Daten sein können.

16. Bauen und Wohnen

16.1 Gemeldete Datenschutzverletzungen

Im Bereich Bauen und Wohnen erreichten uns im Berichtsjahr zwei Meldungen von Datenschutzverletzungen durch Verantwortliche und 19 Beschwerden Betroffener.

16.2 Weitergabe personenbezogener Daten durch Hausverwaltung

In zwei Fällen wandten sich Miteigentümerinnen einer Wohnungseigentümergemeinschaft an uns, um sich darüber zu beschweren, dass die Hausverwaltung ihre über Namen und Wohnadressen hinausgehenden Kontaktdaten wie Telefonnummer und E-Mail-Adresse an die Wohnungseigentümergemeinschaft und damit an alle übrigen Miteigentümerinnen und Miteigentümer weitergegeben hatte, indem diese von ihnen verfasste und an die Hausverwaltung adressierte Schreiben weitergeleitet hatte. Ob die Weiterleitung von Schreiben mit über Namen und Adressen hinausgehenden Kontaktdaten zulässig ist, wenn kein Beschluss der Wohnungseigentümergemeinschaft hierzu vorliegt, sollte aus unserer Sicht unter den Aufsichtsbehörden bundesweit einheitlich beantwortet werden. Die von uns dazu initiierte Umfrage unter den Aufsichtsbehörden ist noch nicht abgeschlossen.

17. Verkehr und Umwelt

17.1 Gemeldete Datenschutzverletzungen

Im Bereich Verkehr und Umwelt meldete im Jahr 2019 ein Verantwortlicher eine Datenschutzverletzung. 23 Betroffene erhoben bei uns datenschutzrechtliche Beschwerden.

17.2 Unzulässiges Frageblatt der Führerscheinstelle

Uns erreichte eine Beschwerde darüber, dass die Führerscheinstelle Personen, die einen Antrag auf Verlängerung eines Führerscheins für Lastkraftwagen stellten, zusätzlich zu den in der Fahrerlaubnisverordnung verlangten Nachweisen über die gesundheitliche Eignung einen weiteren Fragebogen vorlegte. Mit diesem wurden bestimmte chronische Erkrankungen erfragt, die eine Auswirkung auf die Fahreignung haben können. Aussagen über diese chronischen Erkrankungen sind zugleich Gegenstand der vorgeschriebenen ärztlichen Untersuchung, wobei das ärztliche Attest der Fahrerlaubnisbehörde gegenüber nur das Ergebnis der Untersuchung dokumentiert. Personen, die diesen Fragebogen nicht vollständig ausfüllten, wurde eine Vorladung angekündigt. Die Fachaufsichtsbehörde war mit uns der Auffassung, dass diese Datenerhebung unzulässig war. Seit dem Frühjahr 2019 wird der Fragebogen nicht mehr verwendet.

17.3 E-Scooter-Sharing in Bremen

Im Verlaufe von Gesprächen mit vier Anbietern von E-Scooter-Verleihsystemen, an denen wir auf Einladung des Senators für Umwelt, Bau und Verkehr teilnahmen, stellte sich heraus, dass die meisten Anbieter nur vage Angaben zur Einhaltung datenschutzrechtlicher Vorschriften machen konnten und sich verschiedene Mängel abzeichneten. Da die meisten Interessenten

ihren Hauptsitz nicht in Bremen haben, halten wir eine datenschutzrechtliche Prüfung gemeinsam mit den für diese Anbieter federführenden Aufsichtsbehörden für sinnvoll, die bisher an unseren hierfür erforderlichen personellen Kapazitäten gescheitert ist.

18. Telemedien

18.1 Gemeldete Datenschutzverletzungen

Im Bereich Telemedien wurden im Jahr 2019 fünf Datenschutzverletzungen gemeldet. Dabei handelt es sich vornehmlich um Meldungen von international tätigen Unternehmen.

Im Fall eines Bremer Unternehmens wurde durch eine sogenannte SQL-Injektion (Ausnutzung einer Sicherheitslücke im Zusammenhang mit SQL-Datenbanken) eine Liste mit Backend-Mitarbeiterinnen und Backend-Mitarbeiter abgerufen und in einem Forum veröffentlicht.

18.2 Verwendung von Trackingtools und Analysetools auf Webseiten

Diverse Unternehmen nutzen zahlreiche Trackingtools und Analysetools, um Informationen über die Besucherinnen und Besucher ihrer Webseiten zu erhalten. Dabei werden meistens Tools verwendet, die Daten wie IP-Adressen, Browsertypen, Auflösung des Gerätes et cetera an Dritte übermitteln. Mit Hilfe dieser Daten kann es, sofern sie mit den Daten aus anderen Quellen zusammengeführt und analysiert werden, gelingen ein Profil der Nutzerinnen und Nutzern zu erstellen. Die Nutzung der meisten handelsüblichen Analysetools von Drittanbietern ist deswegen ohne hinreichende Einwilligung nicht möglich.

18.2.1 Präsentationswebseite der Freien Hansestadt Bremen

Wir erhielten Beschwerden darüber, dass auf einer Webseite der Freien Hansestadt Bremen zur Außendarstellung eine Vielzahl unterschiedlicher Tracking- und Analysetools verwendet wurde, die personenbezogene Daten an Dritte weiterleiten. Nachdem wir uns an den Betreiber gewandt hatten, beendete dieser die Nutzung von Cookies von Fremdanbietern.

18.2.2 Gesundheitswebseite mit Forum und Selbsttests

Eine Gesundheitswebseite mit Forum und Selbsttests, welche mit einer anonymen Nutzungsmöglichkeit warb, nutzte eine Vielzahl von Trackingtools und Analysetools. Wir kontaktierten das Unternehmen und baten um Stellungnahme. Die Selbsttests zu Themen wie Alkoholismus und Depressionen wurden sofort entfernt. Der Vorgang ist damit noch nicht abgeschlossen. Zu dieser Thematik verabschiedete die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder eine Entschließung (siehe hierzu Ziffer 21.7 dieses Berichts).

18.3 Datenschutzerklärungen auf Webseiten

Immer wieder werden uns fehlende oder fehlerhafte Datenschutzerklärungen auf Webseiten gemeldet. Die Bezeichnung "Datenschutzerklärung" ist eine im deutschen Raum übliche Umschreibung für die Informationspflicht nach Artikel 13 und 14 der Datenschutzgrundverordnung (DSGVO).

Die Information muss nach Artikel 12 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form erfolgen. Darüber hinaus muss sie mindestens den Namen und die Kontaktdaten der oder des Verantwortlichen, gegebenenfalls der oder des Datenschutzbeauftragten, Zwecke der Datenverarbeitung, die Rechtsgrundlage für die Verarbeitung, die Rechte der Betroffenen der Verarbeitung und die zuständige Aufsichtsbehörde beinhalten.

19. Internationales und Europa

19.1 EU-U.S. Privacy Shield und Standardverträge

Mit dem EU-U.S. Privacy Shield und den sogenannten Standardverträgen gibt es Instrumente, den Datentransfer in die Vereinigten Staaten von Amerika (USA) rechtlich zu ermöglichen. Mit Inkrafttreten des CLOUD Act (Clarifying Lawful Overseas Use of Data Act, siehe hierzu 1. Jahresbericht, Ziffer 16.2) ist von den USA ein Gesetz geschaffen worden, welches Grundsätze des europäischen Datenschutzes ignoriert. Die oben genannten Transfermöglichkeiten sind daher mit besonderer Vorsicht zu betrachten. Zwar wurde das EU-U.S. Privacy Shield trotz weiterhin bestehender datenschutzrechtlicher Einwände (siehe 1. Jahresbericht, Ziffer 16.1 und 40. Jahresbericht, Ziffer 14.3) bei der dritten jährlichen Überprüfung der Generaldirektion Justiz und Verbraucher der Europäischen Kommission als gültiges Transferinstrument zunächst bestätigt. Die Rechtmäßigkeit von Standarddatenschutzklauseln nach Artikel 46 Absatz 2 Buchstabe c Datenschutzgrundverordnung, welche die Datenübermittlung in Drittländer regeln, wird aber derzeit vor dem Europäischen Gerichtshof verhandelt. Sollte das Gericht die Standarddatenschutzklauseln für ungültig erklären, wäre auch deshalb mit erheblichen Einschränkungen des internationalen Datentransfers zu rechnen, weil die Aussagen der Entscheidung auch Auswirkungen auf das Privacy Shield haben könnten.

19.2 Brexit

Der geplante Austritt Großbritanniens aus der Europäischen Union wirkt sich auch auf den Datentransfer dorthin aus. Es ist zwar ein Übergangszeitraum geplant, in welchem weiterhin Datentransfers stattfinden dürfen, dennoch ist Großbritannien bis zu einer möglichen

Angemessenheitsentscheidung der Europäischen Kommission ab Zeitpunkt des Austritts als datenschutzrechtlich unsicheres Drittland anzusehen. Zur Übermittlung personenbezogener Daten müssen verantwortliche Stellen die Maßnahmen nach Kapitel V der Datenschutzgrundverordnung beachten.

20. Die Beschlüsse des Europäischen Datenschutzausschusses

Der Europäische Datenschutzausschuss (EDSA) ist die Organisationsform, in der die datenschutzrechtlichen Aufsichtsbehörden in Europa gemeinsam handeln. Hierzu beschließt der EDSA unter anderem Leitlinien, Empfehlungen und bewährte Verfahren zur Datenschutzgrundverordnung[4] und trifft verbindliche Beschlüsse in Einzelfällen.

21. Die Entschließungen der Datenschutzkonferenzen im Jahr 2019

21.1 Hambacher Erklärung zur Künstlichen Intelligenz – Sieben datenschutzrechtliche Anforderungen

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 3. April 2019)

Systeme der Künstlichen Intelligenz (KI) stellen eine substanzielle Herausforderung für Freiheit und Demokratie in unserer Rechtsordnung dar. Entwicklungen und Anwendungen von KI müssen in demokratisch-rechtsstaatlicher Weise den Grundrechten entsprechen. Nicht alles, was technisch möglich und ökonomisch erwünscht ist, darf in der Realität umgesetzt werden. Das gilt in besonderem Maße für den Einsatz von selbstlernenden Systemen, die massenhaft Daten verarbeiten und durch automatisierte Einzelentscheidungen in Rechte und Freiheiten Betroffener eingreifen. Die Wahrung der Grundrechte ist Aufgabe aller staatlichen Instanzen. Wesentliche Rahmenbedingungen für den Einsatz von KI sind vom Gesetzgeber vorzugeben und durch die Aufsichtsbehörden zu vollziehen. Nur wenn der Grundrechtsschutz und der Datenschutz mit dem Prozess der Digitalisierung Schritt halten, ist eine Zukunft möglich, in der am Ende Menschen und nicht Maschinen über Menschen entscheiden.

I. Künstliche Intelligenz und Datenschutz

"Künstliche Intelligenz" (auch "KI" oder "Artificial Intelligence" – "AI") wird derzeit intensiv diskutiert, da sie neue Wertschöpfung in vielen Bereichen von Wirtschaft und Gesellschaft verspricht. Die Bundesregierung hat eine KI-Strategie veröffentlicht, mit dem Ziel, Deutschland

[4] online unter https:// https://edpb.europa.eu/our-work-tools/consistency-findings_de

an die Weltspitze der Entwicklung von KI zu bringen. "AI made in Germany" soll gleichzeitig dafür sorgen, dass auch bei weitreichendem Einsatz Künstlicher Intelligenz die Grundwerte und Freiheitsrechte, die in Deutschland und der Europäischen Union (EU) gelten, weiterhin die prägende Rolle für unser Zusammenleben spielen. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßen diesen Ansatz der grundrechtsverträglichen Gestaltung von KI ausdrücklich.

Eine allgemein anerkannte Definition des Begriffs der Künstlichen Intelligenz existiert bisher nicht. Nach dem Verständnis der Bundesregierung geht es bei KI darum, "technische Systeme so zu konzipieren, dass sie Probleme eigenständig bearbeiten und sich dabei selbst auf veränderte Bedingungen einstellen können. Diese Systeme haben die Eigenschaft, aus neuen Daten zu "lernen" […]."[5]

KI-Systeme werden beispielsweise bereits in der Medizin unterstützend in Forschung und Therapie eingesetzt. Schon heute sind neuronale Netze in der Lage, automatisch komplexe Tumorstrukturen zu erkennen. KI-Systeme können auch genutzt werden, um Depressionserkrankungen anhand des Verhaltens in sozialen Netzwerken oder anhand der Stimmmodulation beim Bedienen von Sprachassistenten zu erkennen. In den Händen von Ärzten kann dieses Wissen dem Wohl der Erkrankten dienen. In den falschen Händen jedoch, kann es auch missbraucht werden.

Auch zur Bewertung von Bewerbungsunterlagen wurde bereits ein KI-System eingesetzt, mit dem Ziel, frei von menschlichen Vorurteilen zu entscheiden. Allerdings hatte das Unternehmen bislang überwiegend männliche Bewerber eingestellt und das KI-System mit deren erfolgreichen Bewerbungen trainiert. In der Folge bewertete das KI-System Frauen sehr viel schlechter, obwohl das Geschlecht nicht nur kein vorgegebenes Bewertungskriterium, sondern dem System sogar unbekannt war. Dies offenbart die Gefahr, dass in Trainingsdaten abgebildete Diskriminierungen nicht beseitigt, sondern verfestigt werden.

Anhand dieser Beispiele wird deutlich, dass mit KI-Systemen häufig personenbezogene Daten verarbeitet werden und diese Verarbeitung Risiken für die Rechte und Freiheiten von Menschen birgt. Sie zeigen auch, wie wichtig es ist, Entwicklung und Einsatz von KI-Systemen politisch, gesellschaftlich und rechtlich zu begleiten. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder verstehen die folgenden Anforderungen als einen konstruktiven Beitrag zu diesem zentralen gesellschaftspolitischen Projekt.

II. Datenschutzrechtliche Anforderungen an Künstliche Intelligenz

[5] Bundestagsdrucksache 19/1982, Die Datenethikkommission der Bundesregierung hebt ergänzend als wichtige Grundlagen für KI die Mustererkennung, das maschinelle Lernen und Methoden der heuristischen Suche, der Inferenz und der Handlungsplanung hervor.

Für die Entwicklung und den Einsatz von KI-Systemen, in denen personenbezogene Daten verarbeitet werden, beinhaltet die Datenschutzgrundverordnung (DSGVO) wichtige rechtliche Vorgaben. Sie dienen dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen. Auch für KI-Systeme gelten die Grundsätze für die Verarbeitung personenbezogener Daten (Artikel 5 DSGVO). Diese Grundsätze müssen gemäß Artikel 25 DSGVO durch frühzeitig geplante technische und organisatorische Maßnahmen von den Verantwortlichen umgesetzt werden (Datenschutz durch Technikgestaltung).

1. KI darf Menschen nicht zum Objekt machen

Die Garantie der Würde des Menschen (Artikel 1 Absatz 1 Grundgesetz, Artikel 1 Grundrechtecharta) gebietet, dass insbesondere im Fall staatlichen Handelns mittels KI der Einzelne nicht zum Objekt gemacht wird. Vollständig automatisierte Entscheidungen oder Profiling durch KI-Systeme sind nur eingeschränkt zulässig. Entscheidungen mit rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung dürfen gemäß Artikel 22 DSGVO nicht allein der Maschine überlassen werden. Wenn der Anwendungsbereich des Artikel 22 DSGVO nicht eröffnet ist, greifen die allgemeinen Grundlagen des Artikel 5 DSGVO, die insbesondere mit den Grundsätzen der Rechtmäßigkeit, Zurechenbarkeit und Fairness die Rechte des Einzelnen schützen. Betroffene haben auch beim Einsatz von KI-Systemen den Anspruch auf das Eingreifen einer Person (Intervenierbarkeit), auf die Darlegung ihres Standpunktes und die Anfechtung einer Entscheidung.

2. KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben

Auch für KI-Systeme gilt, dass sie nur zu verfassungsrechtlich legitimierten Zwecken eingesetzt werden dürfen. Zu beachten ist auch der Grundsatz der Zweckbindung (Artikel 5 Absatz 1 Buchstabe b DSGVO). Zweckänderungen sind mit Artikel 6 Absatz 4 DSGVO klare Grenzen gesetzt. Auch bei KI-Systemen müssen erweiterte Verarbeitungszwecke mit dem ursprünglichen Erhebungszweck vereinbar sein. Das gilt auch für die Nutzung personenbezogener Daten zu Trainingszwecken von KI-Systemen.

3. KI muss transparent, nachvollziehbar und erklärbar sein

Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Artikel 5 Absatz 1 Buchstabe a DSGVO). Dies erfordert insbesondere eine transparente Verarbeitung, bei der die Informationen über den Prozess der Verarbeitung und gegebenenfalls auch über die verwendeten Trainingsdaten leicht zugänglich und verständlich sind (Artikel 12 DSGVO). Entscheidungen, die auf Grundlage des Einsatzes von KI-Systemen erfolgen, müssen nachvollziehbar und erklärbar sein. Es genügt nicht die Erklärbarkeit im Hinblick auf das Ergebnis, darüber hinaus muss die Nachvollziehbarkeit im Hinblick auf die

Prozesse und das Zustandekommen von Entscheidungen gewährleistet sein. Nach der DSGVO ist dafür auch über die involvierte Logik ausreichend aufzuklären. Diese Transparenz-Anforderungen sind fortwährend zu erfüllen, wenn KI-Systeme zur Verarbeitung von personenbezogenen Daten eingesetzt werden. Es gilt die Rechenschaftspflicht des Verantwortlichen (Artikel 5 Absatz 2 DSGVO).

4. KI muss Diskriminierungen vermeiden

Lernende Systeme sind in hohem Maße abhängig von den eingegebenen Daten. Durch unzureichende Datengrundlagen und Konzeptionen kann es zu Ergebnissen kommen, die sich als Diskriminierungen auswirken. Diskriminierende Verarbeitungen stellen eine Verletzung der Rechte und Freiheiten der betroffenen Personen dar. Sie verstoßen unter anderem gegen bestimmte Anforderungen der Datenschutzgrundverordnung, etwa den Grundsatz der Verarbeitung nach Treu und Glauben, die Bindung der Verarbeitung an legitime Zwecke oder die Angemessenheit der Verarbeitung.

Diese Diskriminierungsneigungen sind nicht immer von vornherein erkennbar. Vor dem Einsatz von KI-Systemen müssen deshalb die Risiken für die Rechte und Freiheiten von Personen mit dem Ziel bewertet werden, auch verdeckte Diskriminierungen durch Gegenmaßnahmen zuverlässig auszuschließen. Auch während der Anwendung von KI-Systemen muss eine entsprechende Risikoüberwachung erfolgen.

5. Für KI gilt der Grundsatz der Datenminimierung

Für KI-Systeme werden typischerweise große Bestände von Trainingsdaten genutzt. Für personenbezogene Daten gilt dabei auch in KI-Systemen der Grundsatz der Datenminimierung (Artikel 5 Absatz 1 Buchstabe c DSGVO). Die Verarbeitung personenbezogener Daten muss daher stets auf das notwendige Maß beschränkt sein. Die Prüfung der Erforderlichkeit kann ergeben, dass die Verarbeitung vollständig anonymer Daten zur Erreichung des legitimen Zwecks ausreicht.

6. KI braucht Verantwortlichkeit

Die Beteiligten beim Einsatz eines KI-Systems müssen die Verantwortlichkeit ermitteln und klar kommunizieren und jeweils die notwendigen Maßnahmen treffen, um die rechtmäßige Verarbeitung, die Betroffenenrechte, die Sicherheit der Verarbeitung und die Beherrschbarkeit des KI-Systems zu gewährleisten. Der Verantwortliche muss sicherstellen, dass die Grundsätze nach Artikel 5 DSGVO eingehalten werden. Er muss seine Pflichten im Hinblick auf die Betroffenenrechte aus Artikel 12 fortfolgende DSGVO erfüllen. Der Verantwortliche muss die Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO gewährleisten und somit auch Manipulationen durch Dritte, die sich auf die Ergebnisse der Systeme auswirken, verhindern.

Beim Einsatz eines KI-Systems, in dem personenbezogene Daten verarbeitet werden, wird in der Regel eine Datenschutz-Folgenabschätzung gemäß Artikel 35 DSGVO erforderlich sein.

7. KI benötigt technische und organisatorische Standards

Um eine datenschutzgerechte Verarbeitung sicherzustellen, sind für Konzeption und Einsatz von KI-Systemen technische und organisatorische Maßnahmen gemäß Artikel 24 und 25 DSGVO zu treffen, wie zum Beispiel Pseudonymisierung. Diese erfolgt nicht allein dadurch, dass der Einzelne in einer großen Menge personenbezogener Daten scheinbar verschwindet. Für den datenschutzkonformen Einsatz von KI-Systemen gibt es gegenwärtig noch keine speziellen Standards oder detaillierte Anforderungen an technische und organisatorische Maßnahmen. Die Erkenntnisse in diesem Bereich zu mehren und Best-Practice-Beispiele zu entwickeln ist eine wichtige Aufgabe von Wirtschaft und Wissenschaft. Die Datenschutzaufsichtsbehörden werden diesen Prozess aktiv begleiten.

III. Die Entwicklung von KI bedarf der Steuerung

Die Datenschutzaufsichtsbehörden überwachen die Anwendung des Datenschutzrechts, setzen es durch und haben die Aufgabe, bei der Weiterentwicklung für einen effektiven Grundrechtsschutz einzutreten. Angesichts der hohen Dynamik in der Entwicklung der Technologien von künstlicher Intelligenz und der vielfältigen Einsatzfelder zeichnen sich die Grenzen der Entwicklung noch nicht ab. Gleichermaßen sind die Risiken der Verarbeitung personenbezogener Daten in KI-Systemen nicht pauschal einzuschätzen. Auch ethische Grundsätze sind zu beachten. Wissenschaft, Datenschutz-aufsichtsbehörden, die Anwender und besonders die Politik sind gefordert, die Entwicklung von KI zu begleiten und im Sinne des Datenschutzes zu steuern.

21.2 Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten!

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 3. April 2019)

Unternehmen haften im Rahmen von Artikel 83 Datenschutzgrundverordnung (DSGVO) für schuldhafte Datenschutzverstöße ihrer Beschäftigten, sofern es sich nicht um einen Exzess handelt. Dabei ist nicht erforderlich, dass für die Handlung ein gesetzlicher Vertreter oder eine Leitungsperson verantwortlich ist. Zurechnungseinschränkende Regelungen im nationalen Recht würden dem widersprechen.

Diese Haftung für Mitarbeiterverschulden ergibt sich aus der Anwendung des sogenannten funktionalen Unternehmensbegriffs des europäischen Primärrechts. Der funktionale Unternehmensbegriff aus dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV)

besagt, dass ein Unternehmen jede wirtschaftliche Einheit unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung ist. Erwägungsgrund 150 der DSGVO weist für die Verhängung von Geldbußen wegen Datenschutzverstößen gegen Unternehmen klarstellend darauf hin. Nach der Rechtsprechung zum funktionalen Unternehmensbegriff haften Unternehmen für das Fehlverhalten sämtlicher ihrer Beschäftigten. Eine Kenntnis der Geschäftsführung eines Unternehmens von dem konkreten Verstoß oder eine Verletzung der Aufsichtspflicht ist für die Zuordnung der Verantwortlichkeit nicht erforderlich. Handlungen von Beschäftigten, die bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden können (Exzesse), sind ausgenommen.

Die alten nationalen Haftungsregeln wurden bisher nicht europarechtskonform der neuen Rechtslage angepasst. Unzutreffend verweist § 41 Absatz 1 des neuen Bundesdatenschutzgesetzes (BDSG) auf zurechnungseinschränkende Regelungen im OWiG. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) haben bereits im Rahmen des Gesetzgebungsverfahrens zum neuen Bundesdatenschutzgesetz darauf aufmerksam gemacht, dass diese Bestimmungen den Vorgaben der DSGVO zur Verantwortlichkeit für Datenschutzverstöße widersprechen.

Die DSK begrüßt insoweit, dass der Koalitionsvertrag vorsieht, das Sanktionsrecht für Unternehmen generell im deutschen Recht so zu ändern, dass "die von Fehlverhalten von Mitarbeiterinnen und Mitarbeitern profitierenden Unternehmen stärker sanktioniert werden". Diese gebotene Modernisierung des deutschen Unternehmenssanktionsrechts entspräche dann auch dem europäischen Kartellrecht und dem etablierten internationalen Standard.

Die DSK fordert den Bundesgesetzgeber daher nochmals auf, in den Beratungen des Entwurfs des Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DSGVO) und zur Umsetzung der Richtlinie (EU) 2016/680 die §§ 30, 130 OWiG klarstellend vom Anwendungsbereich auszunehmen und damit dem europäischen Recht anzupassen.

21.3 Keine Abschaffung der Datenschutzbeauftragten

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 23. April 2019)

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) spricht sich gegen eine Abschaffung oder Verwässerung der die Datenschutzgrundverordnung ergänzenden nationalen Regelungen der Pflicht zur Benennung einer oder eines Datenschutzbeauftragten aus.

Nach § 38 Bundesdatenschutzgesetz müssen zum Beispiel Unternehmen und Vereine Datenschutzbeauftragte benennen, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Diese Pflicht hat sich seit vielen Jahren bewährt und ist deshalb auch bei der Datenschutzreform im deutschen Recht beibehalten worden.

Die Datenschutzbeauftragten sorgen für eine kompetente datenschutzrechtliche Beratung, um Datenschutzverstöße schon im Vorfeld zu vermeiden und das Sanktionsrisiko gering zu halten. Dies hat sich ganz besonders bei der Umstellung auf die Datenschutzgrundverordnung bewährt.

Auch beim Wegfall der nationalen Benennungspflicht von Datenschutzbeauftragten bleiben die Pflichten des Datenschutzrechts bestehen. Verantwortliche verlieren jedoch interne Beraterinnen und Berater zu Fragen des Datenschutzes. Der Wegfall mag kurzfristig als Entlastung empfunden werden. Mittelfristig geht interne Kompetenz verloren.

Eine Aufweichung dieser Benennungspflicht, insbesondere für kleinere Unternehmen und Vereine, wird diese daher nicht entlasten, sondern ihnen mittelfristig schaden.

21.4 Digitalisierung der Verwaltung datenschutzkonform und bürgerfreundlich gestalten!

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 12. September 2019)

Die Bundesregierung will die in der Verwaltung geführten Register modernisieren und plant in diesem Zusammenhang einen einfacheren Zugriff auf dort gespeicherte personenbezogene Daten. Nach Auffassung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) darf dieses Vorhaben nicht zur Einführung von einheitlichen, verwaltungsübergreifenden Personenkennzeichen beziehungsweise Identifikatoren führen. Vielmehr muss der Schutz der Grundrechte und Grundfreiheiten, insbesondere das Recht auf Schutz personenbezogener Daten, Priorität haben. Ebenso wichtig ist es, den Bürgerinnen und Bürgern die besseren Dienstleistungen verbunden mit einer deutlich höheren Transparenz anzubieten.

Bundesregierung nimmt Modernisierung der Register in Angriff

Die Bundesregierung hat mit dem Onlinezugangsgesetz ein umfangreiches Digitalisierungsprogramm für die Verwaltung in Deutschland gestartet. Bund und Länder sind verpflichtet, ihre Verwaltungsleistungen künftig auch elektronisch über Verwaltungsportale anzubieten. Es sollen Nutzerkonten bereitgestellt werden, über die sich Nutzende für die im

Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich identifizieren können.

In diesem Zusammenhang hat sich der Nationale Normenkontrollrat (NKR) für eine Modernisierung der deutschen Registerlandschaft ausgesprochen und empfohlen, dass bestimmte Basisdaten von Bürgern und Unternehmen nur einmal mitgeteilt werden müssen ("Once Only"-Prinzip). Der NKR hat darüber hinaus angeregt, datenschutzkonforme Identifikationsnummern für Personen, Unternehmen sowie Gebäude, Wohnungen und Flurstücke zu schaffen und zu nutzen und ein "Datencockpit" einzurichten, bei dem die Bürgerinnen und Bürger alle staatlichen Datenflüsse im Auge haben können.

Die Einführung solcher Identifikationsnummern für Personen wird aktuell unter Federführung des Bundesministeriums des Innern, für Bau und Heimat (BMI) von der Bundesregierung verfolgt. Der IT-Planungsrat hat in seiner 28. Sitzung am 12. März 2019 den vom BMI vorgelegten "Leitlinien für eine Modernisierung der Registerlandschaft" zugestimmt sowie den "Vorschlag für die Verbesserung des Identitätsmanagements als Teil der Registermodernisierung" zur Kenntnis genommen und das angestrebte Vorhaben begrüßt.

Datenschutzfreundliche und transparente Gestaltung für Bürgerinnen und Bürger

Bereits die Schaffung einheitlicher und verwaltungsübergreifender Personenkennzeichen beziehungsweise. Identifikatoren und einer entsprechenden Infrastruktur zum Datenaustausch bergen die Gefahr, dass personenbezogene Daten in großem Maße leicht zusammengetragen, verknüpft und zu einem umfassenden Persönlichkeitsprofil vervollständigt werden könnten. Die Datenschutzkonferenz weist darauf hin, dass das Bundesverfassungsgericht schon seit Jahrzehnten der Einführung und Verarbeitung derartiger Personenkennzeichen sehr enge Schranken auferlegt, da sie massiv in den Schutzbereich des Rechts auf informationelle Selbstbestimmung betroffener Bürgerinnen und Bürger eingreifen. Bereits die Möglichkeit einer umfassenden Katalogisierung von Bürgerinnen und Bürgern durch den Staat gefährdet das Persönlichkeitsrecht, da sie bei den Menschen zu einer vorauseilenden Anpassung ihres Verhaltens führen kann. Auch die Grundsätze der europäischen Datenschutzgrundverordnung und deren Regelungen zur datenschutzgerechten Gestaltung setzen einheitlichen und verwaltungs-übergreifenden Personenkennzeichen enge Grenzen und verlangen geeignete Garantien für die Wahrung der Rechte und Freiheiten der betroffenen Personen.

Insbesondere im Hinblick auf die geplante Verwendung modernisierter Register für zukünftige Zensus-Erhebungen und geplante / modernisierte Zugriffsrechte der Sicherheitsbehörden bedarf es eines besonderen Schutzes der betroffenen Personen. Den hohen Risiken für das Recht auf informationelle Selbstbestimmung muss in einem umfassenden regulatorischen, vor

allem aber technischen und organisatorischen Konzept begegnet werden. Nur so können die vom deutschen und europäischen Verfassungsrecht geforderten Garantien gewahrt werden.

Die Modernisierung der Register muss zwingend von Beginn an auch dafür genutzt werden, den Bürgerinnen und Bürgern die Nutzung der im Online-Zugangsgesetz vorgesehenen Dienstleistungen durch Nutzung einmal hinterlegter Daten zu erleichtern. Von besonderer Bedeutung ist es darüber hinaus, den Bürgerinnen und Bürgern ein im Vergleich zur gegenwärtigen Situation deutlich höheres Maß an Transparenz zu gewährleisten. Ein "Datencockpit", wie es der NKR bereits vorgeschlagen hat, muss es den Bürgerinnen und Bürgern erlauben, jederzeit nachzuvollziehen, welches Register welche Daten über sie vorhält, welche Behörden darauf zugegriffen haben und mit welchen anderen Daten diese verknüpft wurden. Gleichzeitig muss gewährleistet sein, dass ausschließlich den betroffenen Bürgerinnen und Bürgern der Zugriff möglich ist. Auf dieser Grundlage muss die Digitalisierung der Verwaltung dazu genutzt werden, das informationelle Machtgefälle zwischen Staat und Bürgerinnen und Bürgern weitgehend aufzuheben und ihnen die Inanspruchnahme ihrer Rechte deutlich zu erleichtern.

Dazu muss nach Auffassung der Datenschutzkonferenz die dezentrale Registerstruktur erhalten bleiben. Die Nutzung von einheitlichen, verwaltungs-übergreifenden Personenkennzeichen beziehungsweise. Identifikatoren zur direkten Identifizierung von Bürgerinnen und Bürgern lehnt die Datenschutzkonferenz ab. Sie fordert alternative Methoden zur eindeutigen Identifizierung. Neben Abgleichen über den jeweiligen Datensatz des Registers kämen dafür allenfalls sektorspezifische Personenkennziffern in Betracht, die eine eindeutige Identifizierung erlauben, einseitigen staatlichen Abgleich von Daten verhindern, ein Höchstmaß an Transparenz beispielsweise durch ein Datencockpit ermöglichen, das Risiko von Missbrauch und Kompromittierung verringern und die Eindeutigkeit von Registern gewährleisten.

21.5 Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. November 2019)

Auf der Grundlage der Hambacher Erklärung vom 3. April 2019 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in einem Positionspapier Anforderungen an KI-Systeme erarbeitet, deren Umsetzung die DSK für eine datenschutzkonforme Gestaltung von KI-Systemen empfiehlt. Die in der Hambacher Erklärung festgelegten rechtlichen Rahmenbedingungen werden damit im Hinblick auf technische und

organisatorische Maßnahmen konkretisiert, die auf die unterschiedlichen Phasen der Lebenszyklen von KI-Systemen bezogen sind.

Die Phasen des Lebenszyklus eines KI-Systems – Designs des KI-Systems, Veredelung von Rohdaten zu Trainingsdaten, Training der KI-Komponenten, Validierung der Daten und KI-Komponenten sowie des KI-Systems, Einsatz des KI-Systems und die Rückkopplung von Ergebnissen – werden am Maßstab von Gewährleistungszielen untersucht. Um aus rechtlichen Anforderungen KI-spezifische technische und organisatorische Maßnahmen abzuleiten und zu systematisieren, werden die Gewährleistungsziele Transparenz, Datenminimierung, Nichtverkettung, Intervenierbarkeit, Verfügbarkeit, Integrität und Vertraulichkeit verwendet.

Für die Verarbeitung von personenbezogenen Daten, bei der KI-Systeme zum Einsatz kommen, gelten die in der Datenschutzgrundverordnung (DSGVO) formulierten Grundsätze. Mit dem Positionspapier wird Verantwortlichen im Umfeld von KI ein Handlungsrahmen für die datenschutzrechtlichen Vorgaben an die Hand gegeben, an dem sie sich bei der Planung und dem Betrieb von KI-Systemen orientieren können. Das Positionspapier soll verdeutlichen, dass der Einsatz von KI-Systemen und der Datenschutz keine zwingenden Gegensätze sind. Die Chancen und neuen Möglichkeiten des Einsatzes von KI-Systemen werden durch einen modernen Datenschutz nicht verhindert. Das Positionspapier soll die Entwicklung und den Einsatz von KI auch unter Nutzung personenbezogener Daten konstruktiv begleiten. Damit wird Handlungssicherheit gesteigert und sichergestellt, dass die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere das Recht auf informationelle Selbstbestimmung, auch in dem dynamischen, von KI-Systemen geprägten Umfeld gewahrt werden.

Die DSK legt dieses Positionspapier[6] auch vor, um den Dialog mit den relevanten Akteuren aus Politik, Wirtschaft, Wissenschaft und Gesellschaft wie den Verbrauchervereinigungen auf dieser Grundlage weiter zu intensivieren.

21.6 Gesundheitseinrichtungen müssen unabhängig von ihrer Größe den Schutz von Patientendaten gewährleisten

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. November 2019)

Die Datenschutzkonferenz weist nachdrücklich darauf hin, dass die Sicherheit von Patientendaten in der medizinischen Behandlung nach der Datenschutzgrundverordnung

[6] online unter: https://www.datenschutz.bremen.de/sixcms/media.php/13/Positionspapier%20Task%20Force%20KI%2020191015.pdf

flächendeckend gewährleistet sein muss. Der effektive Schutz von Gesundheitsdaten darf nicht von der Größe der Versorgungseinrichtung abhängen.

In der jüngeren Vergangenheit häufen sich Vorfälle, in denen der Schutz von Patientendaten in der stationären Versorgung gefährdet ist. So wurden im Juli 2019 eine Reihe von Einrichtungen eines Trägers in Rheinland-Pfalz und dem Saarland Opfer eines Befalls mit Schadsoftware. Die durch diese erfolgte Verschlüsselung von Daten im IT-Verbund der Trägergesellschaft hat zu weitreichenden Beeinträchtigungen des Krankenhausbetriebs geführt. Im September 2019 wurde bekannt, dass weltweit mehr als 16 Millionen Datensätze, darunter 13.000 von in deutschen Gesundheitseinrichtungen behandelten Patienten, offen im Internet zugänglich waren. Ursache hierfür waren nach den bislang bekannt gewordenen Informationen insbesondere unzureichende technische und organisatorische Vorkehrungen zum Schutz dieser Daten.

Der Einsatz von Informations- und Kommunikationstechnik in der Gesundheitsversorgung ist im Zeitalter der digitalisierten Medizin unabdingbar. Allerdings müssen die in diesem Zusammenhang rechtlich gebotenen und nach dem Stand der Technik angemessenen Vorkehrungen zu einem effektiven Schutz der Daten von Patientinnen und Patienten flächendeckend getroffen werden. Dazu sind alle in diesem Zusammenhang tätigen Einrichtungen unabhängig von ihrer Größe aufgrund der Datenschutzgrundverordnung verpflichtet.

Die Datenschutzkonferenz fordert vor dem Hintergrund einer zunehmenden Digitalisierung der Gesundheitsversorgung und angesichts der damit einhergehenden Gefährdungen ausdrücklich dazu auf, auch in finanzieller Hinsicht sicherzustellen, dass alle Einrichtungen des Gesundheitswesens die zum Schutz der Patientendaten nach dem Stand der Technik gesetzlich gebotenen Vorkehrungen ergreifen können.

21.7 Gesundheitswebseiten und Gesundheits-Apps – Keine Weitergabe sensibler Daten an unbefugte Dritte!

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. November 2019)

Mit zunehmender Sorge beobachtet die Datenschutzkonferenz, dass Betreiber von Gesundheitswebseiten und Gesundheits-Apps auch sensible personenbezogene Daten der Nutzerinnen und Nutzer ohne erkennbare Verarbeitungsgrundlage an Dritte weiterleiten. Unter anderem geschieht dies durch Tracking – und Analyse-Tools (also Programme, die das Surfverhalten beobachten und analysieren), von deren Einsatz die betroffenen Personen keine Kenntnis haben.

So wurde im September 2019 durch die Studie einer Nichtregierungsorganisation bekannt, dass zahlreiche Betreiber von Gesundheitswebseiten, die ihren Besuchern Informationen zu Depression und anderen psychischen Krankheiten anbieten, personenbezogene Nutzungsdaten ohne adäquate Einbindung der Nutzerinnen und Nutzer an andere Stellen weitergeleitet haben sollen. Teilweise soll dabei sogar die Teilnahme an Depressions-Selbsttests erfasst worden sein. Auch von 44 analysierten deutschen Webseiten besäßen weit über die Hälfte solche integrierten Bausteine, die dies ermöglicht hätten. Im Oktober 2019 wurden Recherchen veröffentlicht, wonach eine in Deutschland ansässige Diagnostik-App ebenfalls Tracking- und Analyse-Dienste nutze und in diesem Zusammenhang sensible Gesundheitsdaten wie zum Beispiel körperliche Beschwerden ohne vorherige Information und Legitimation der Nutzer an Dritte weiterleite.

Zu den Datenempfängern gehören häufig neben sonstigen Tracking-Dienstleistern große Unternehmen wie Facebook, Google und Amazon, die vorrangig eigene Geschäftsinteressen verfolgen. Die Verknüpfung der weitergeleiteten Daten mit anderen Informationen begründet das Risiko, dass für jede Nutzerin und jeden Nutzer ein personenbezogenes Gesundheitsprofil entsteht, von dessen Existenz und Umfang die betroffenen Personen nichts wissen.

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder prüfen im Rahmen ihrer Aufgaben und Möglichkeiten derartige Hinweise und werden Datenschutzverletzungen gegebenenfalls sanktionieren. Zugleich ist der Gesetzgeber aufgerufen, im Zusammenhang mit der bevorstehenden Einführung digitaler Gesundheitsanwendungen in die Regelversorgung den Schutz der Vertraulichkeit sensibler Gesundheitsdaten sicherzustellen. Beispielsweise wäre es nicht hinzunehmen, wenn die Nutzung einer von der Regelversorgung erfassten Gesundheits-App zwingend an gesetzlich nicht vorgesehene Weiterleitungen von Gesundheitsdaten gekoppelt würde.

Die Datenschutzkonferenz fordert die Betreiber von Gesundheitswebseiten und Gesundheits-Apps auf, die berechtigten Vertraulichkeitserwartungen ihrer Nutzerinnen und Nutzer zu respektieren. Unabhängig von den allgemeinen datenschutzrechtlichen Anforderungen an die Weitergabe personenbezogener Gesundheitsdaten sind dabei insbesondere folgende Anforderungen zu beachten:

- Leiten Betreiber von Gesundheitswebseiten und Gesundheits-Apps personenbezogene Nutzungsdaten an andere Stellen weiter, sind sie für diese Datenweitergabe verantwortlich, selbst wenn sie – wie etwa bei der Einbindung von Social Plugins – keinen eigenen Zugriff auf die weitergeleiteten Daten haben.

- Als Verantwortliche sind Betreiber insoweit verpflichtet, die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu beachten. Die eingangs beschriebene Weiterleitung von Gesundheitsdaten kann nach Artikel 9

Absatz 1, 2 Buchstabe a Datenschutzgrundverordnung ausnahmsweise nur auf Grundlage einer vor der Datenverarbeitung eingeholten ausdrücklichen Einwilligung zulässig sein, die auch den übrigen Wirksamkeitsvoraussetzungen einer datenschutzrechtlichen Einwilligung genügen muss.

- Insbesondere unterliegt die Einwilligung in die Verarbeitung von Gesundheitsdaten strengen Transparenzanforderungen: Unter anderem muss sie konkret benennen, wer für die Verarbeitung verantwortlich ist und welche Kategorien personenbezogener Daten, wie beispielsweise Gesundheitsdaten, Informationen über die sexuelle Orientierung oder zum Sexualleben verarbeitet werden. Auch die Zwecke der Datenverarbeitung und die Empfänger von weitergeleiteten Daten sind konkret zu benennen. Diese Informationen müssen die Nutzerinnen und Nutzer in die Lage versetzen, sich über die Konsequenzen ihrer erteilten Einwilligung bewusst zu werden.

- Im Rahmen der Regelversorgung wäre die einwilligungsbasierte Weiterleitung von Nutzerdaten an Tracking- oder Analyse-Dienstleister oder sonstige Dritte, die nicht Teil der Gesundheitsversorgung sind, allenfalls zulässig, wenn dies gesetzlich geregelt würde. Gegen eine solche gesetzliche Regelung bestünden allerdings im Hinblick auf das Erfordernis der freiwilligen Einwilligung erhebliche Bedenken.

Im Übrigen weist die Datenschutzkonferenz darauf hin, dass sich aus dem dargestellten Sachverhalt erneut die dringende Notwendigkeit ergibt, möglichst zeitnah eine ePrivacy-Verordnung zu verabschieden. Darin müssen die Bedürfnisse des elektronischen Datenverkehrs mit den Erfordernissen der Grundrechte auf Privatheit und auf Datenschutz in Einklang gebracht werden. Es sind insbesondere Regelungen erforderlich, die einen hohen Schutz sensibler Daten effektiv sicherstellen.

21.8 Keine massenhafte automatisierte Aufzeichnung von Kfz-Kennzeichen für Strafverfolgungszwecke!

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. November 2019)

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist auf den Missstand hin, dass seit einiger Zeit eigentlich für Zwecke der polizeilichen Gefahrenabwehr eingerichtete automatisierte Kennzeichenerfassungssysteme auch für Zwecke der Strafverfolgung eingesetzt werden. Sie erfassen dabei massenhaft und teilweise längerfristig Kfz-Daten unabhängig von der Beschuldigteneigenschaft der betroffenen Personen.

Im Rahmen der Gefahrenabwehr fahndet die Polizei auf Grundlage des jeweiligen Landespolizeigesetzes nach einzelnen Kraftfahrzeugkennzeichen. Nur im Fall einer Übereinstimmung von Kennzeichen und gesuchtem Fahrzeug kommt es zu einer Speicherung des einzelnen Kraftfahrzeugkennzeichens. Kfz-Kennzeichen, nach denen nicht polizeilich gefahndet wird, werden nach ihrer Erfassung unverzüglich gelöscht.

Demgegenüber wird im Bereich der Strafverfolgung – gestützt auf gerichtliche Beschlüsse oder staatsanwaltliche Anordnungen – nicht nur nach einzelnen Kraftfahrzeugen punktuell gefahndet. Vielmehr werden teilweise zusätzlich die Kennzeichen sämtlicher Fahrzeuge, die eine Straße mit einem Erfassungsgerät passieren, über einen längeren Zeitraum hinweg unterschiedslos erfasst und langfristig gespeichert. Als Rechtsgrundlage für solche Strafverfolgungsmaßnahmen wird in der Regel § 100h der Strafprozessordnung (StPO) herangezogen. Dieser erlaubt zwar, zur Observation beschuldigter Personen bestimmte technische Mittel einzusetzen, sofern Gegenstand der Strafverfolgung eine Straftat von erheblicher Bedeutung ist. Gegen andere Personen sind solche Maßnahmen nur ausnahmsweise zulässig. Eine umfassende Datenverarbeitung, wie sie die Aufzeichnung der Kennzeichen aller ein Erfassungsgerät passierender Kraftfahrzeuge über einen längeren Zeitraum bedeutet, führt jedoch dazu, dass sämtliche Verkehrsteilnehmende im Erfassungsbereich Ziel von Ermittlungsmaßnahmen sind und insoweit Bewegungsprofile entstehen können. Eine Ausweitung des Betroffenenkreises in dieser Größenordnung ist durch keinerlei Tatsachen begründbar und nicht zu rechtfertigen. Sie kann deshalb insbesondere nicht auf § 100h StPO gestützt werden.