BREMISCHE BÜRGERSCHAFT
Landtag
19. Wahlperiode

Drs. 19/2128

27.03.19

1. 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 2018. Redaktionsschluss war der 31. Dezember 2018.

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

Inhaltsverzeichnis

1. Die Datenschutzgrundverordnung kommt an

Mit der seit 25. Mai 2018 geltenden Datenschutzgrundverordnung (DSGVO) hat die Europäische Union den Grundrechtsschutz in ihren Fokus genommen. Das sollte für die Menschen im Land Bremen ein Grund mehr sein, am 26. Mai 2019, also einen Tag nach dem ersten Geburtstag der DSGVO, von ihrem Recht Gebrauch zu machen, über die Zusammensetzung des europäischen Parlamentes mitzubestimmen.

Dass die DSGVO wirkt, wo sie wirken wollte, nämlich direkt bei den Menschen in Europa, zeigt auch der unter Ziffer 2 illustrierte Anstieg der Eingangszahlen bei der bremischen Landesbeauftragten für Datenschutz und Informationsfreiheit. Allein die Anzahl der Beschwerden Betroffener und die Anzahl der Beratungsbitten sind seit dem ersten Geltungstag der DSGVO noch einmal um 79,5 Prozent beziehungsweise um 185 Prozent angestiegen. Auch Anzeigen und Meldungen von Datenschutzverletzungen erreichen die bremische Landesbeauftragte für Datenschutz und Informationsfreiheit in signifikant höherer Zahl als in der Zeit vor Geltung der DSGVO. Neben weiteren bereits bekannten Aufgaben wie der Sensibilisierung der Öffentlichkeit und der Verarbeiter weist die DSGVO den Aufsichtsbehörden auch diverse neue Aufgaben wie die Akkreditierung von Zertifizierungsstellen diverse Genehmigungspflichten und Dokumentationspflichten (unter anderem im Zusammenhang mit Datenschutzfolgeabschätzungen) und Kooperationspflichten mit den anderen europäischen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss zu.

Dass die Regelungen der DSGVO nicht nur gelten, sondern auch durchgesetzt werden, zeigen erste Bußgelder, die europäische Aufsichtsbehörden nach der DSGVO verhängt haben: Ein portugiesisches Krankenhaus erhielt eine Geldbuße in Höhe von 400.000 Euro, weil diejenigen, die das leicht erlangbare Profil "Techniker" nutzten, in den IT-Systemen auf Daten zugreifen konnten, die Ärztinnen und Ärzten vorbehalten sein müssen. Auch waren 985 "Arzt"-Profile registriert, obwohl das Krankenhaus lediglich 296 Ärztinnen und Ärzte beschäftigte. Die österreichische Aufsichtsbehörde verhängte gegen ein Sportwettencafé eine Geldbuße in Höhe von 5.280 Euro, weil dieses Café Videokameras installiert hatte, die die öffentliche Straße und öffentlich zugängliche Parkplätze vor dem Café überwachten. Noch nach der alten Rechtslage erhielt der Kfz-Fahrtendienstleister Uber für die Verletzung der Pflicht, Betroffene über eine Datenschutzverletzung zu unterrichten, von der niederländischen Aufsichtsbehörde eine Geldbuße in Höhe von 600.000 Euro und von der britischen Aufsichtsbehörde eine Geldbuße in Höhe von 385.000 Pfund. Zu den ersten von deutschen Behörden nach der DSGVO verhängten Bußgeldern gehört eines in Höhe von 20.000 Euro, das mein Kollege aus Baden-Württemberg gegen einen Social-Media-Anbieter verhängte, weil dieser die Passwörter der Nutzenden im Klartext gespeichert hatte.

Die bremische Aufsichtsbehörde muss nicht nur bei der Bußgeldverhängung ressourcenbedingt noch sehr hinterherhinken: Zum deutlichen quantitativen Anstieg der Beschwerden, Anzeigen, Meldungen von Datenschutzverletzungen und sonstigen Aufgaben kommt hinzu, dass die Verfahren nach der DSGVO erheblich länger dauern, weil jeder Einzelfall, in dem eine Verletzung datenschutzrechtlicher Vorschriften festgestellt wird, eine bußgeldrechtliche Entscheidung nach sich zieht. Auf einen solchen extremen Anstieg des Arbeitsanfalls kann die bremische Landesbeauftragte für Datenschutz und Informationsfreiheit nicht ohne zusätzliches Personal angemessen reagieren. Ohne einen entsprechenden personellen Zuwachs ist es ihr nur möglich, einen kleinen Bruchteil der ihr nach der DSGVO obliegenden Aufgaben zu erfüllen. Deshalb muss der bremische Gesetzgeber, der gemeinsam mit dem Europäischen Parlament neu gewählt werden wird, den Haushalt der Landesbeauftragten für Datenschutz und Informationsfreiheit noch deutlich aufstocken, um die seit 25. Mai 2018 geltende Anforderung des Artikel 52 Absatz 4 DSGVO zu erfüllen: "Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können".

Dr. Imke Sommer

2. Zahlen und Fakten

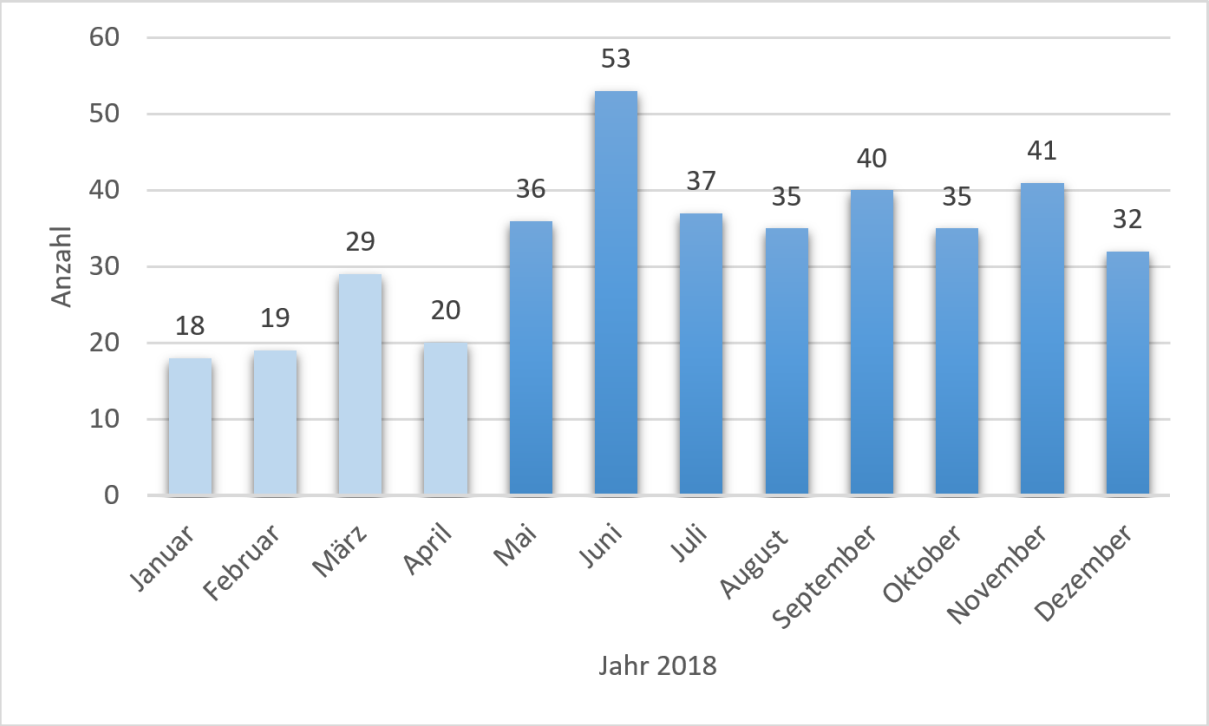
Die Datenschutzgrundverordnung macht es den Aufsichtsbehörden in Artikel 59 zur Pflicht, jährlich über ihre Tätigkeit zu berichten. Um die Transparenz und Vergleichbarkeit innerhalb der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) und für die Öffentlichkeit 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 2018 an die Landesbeauftragte für Datenschutz und Informationsfreiheit herangetragen wurden

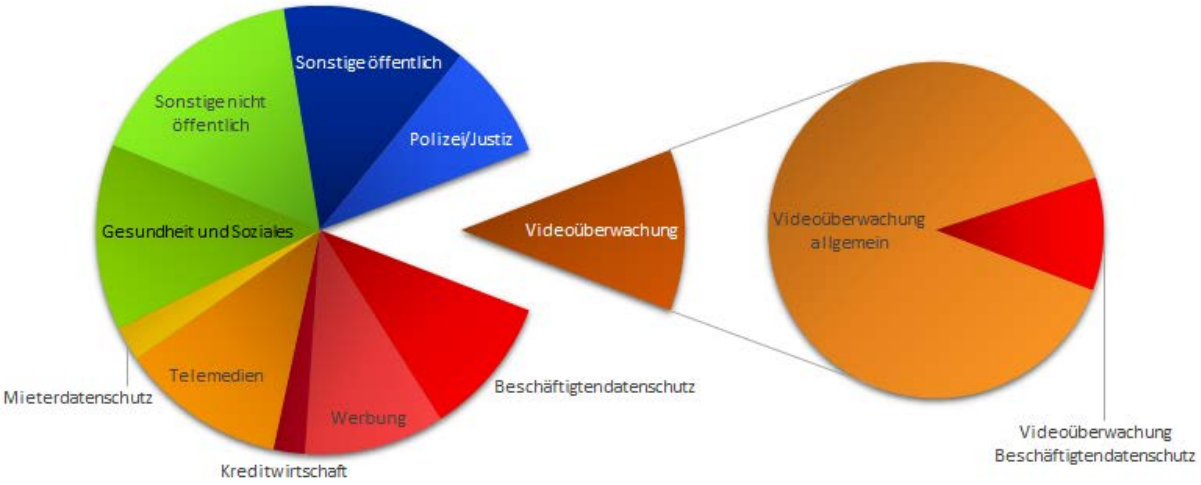
Monat	Beschwerden	Beratungs-anfragen	Datenschutz-verletzungen	Meldungen Datenschutz-beauftragte	Vorträge
Januar	18	41	1	2	5
Februar	19	33	0	4	3
März	29	67	0	2	6
April	20	88	0	20	6
Mai	36	249	1	783	4
Juni	53	129	5	358	3
Juli	37	65	9	172	1
August	35	61	6	115	4
September	40	53	3	45	8
Oktober	35	55	5	35	3
November	41	53	14	63	2
Dezember	32	32	2	46	5
Gesamt	**395**	**926**	**46**	**1.645**	**50**

Nähere Angaben hierzu finden sich in den nachfolgenden Ziffern.

2.2 Beschwerden



Seit 25. Mai 2018 gilt die Datenschutzgrundverordnung. In diesem Diagramm sind die monatlichen Beschwerdezahlen für das gesamte Jahr 2018 dargestellt.



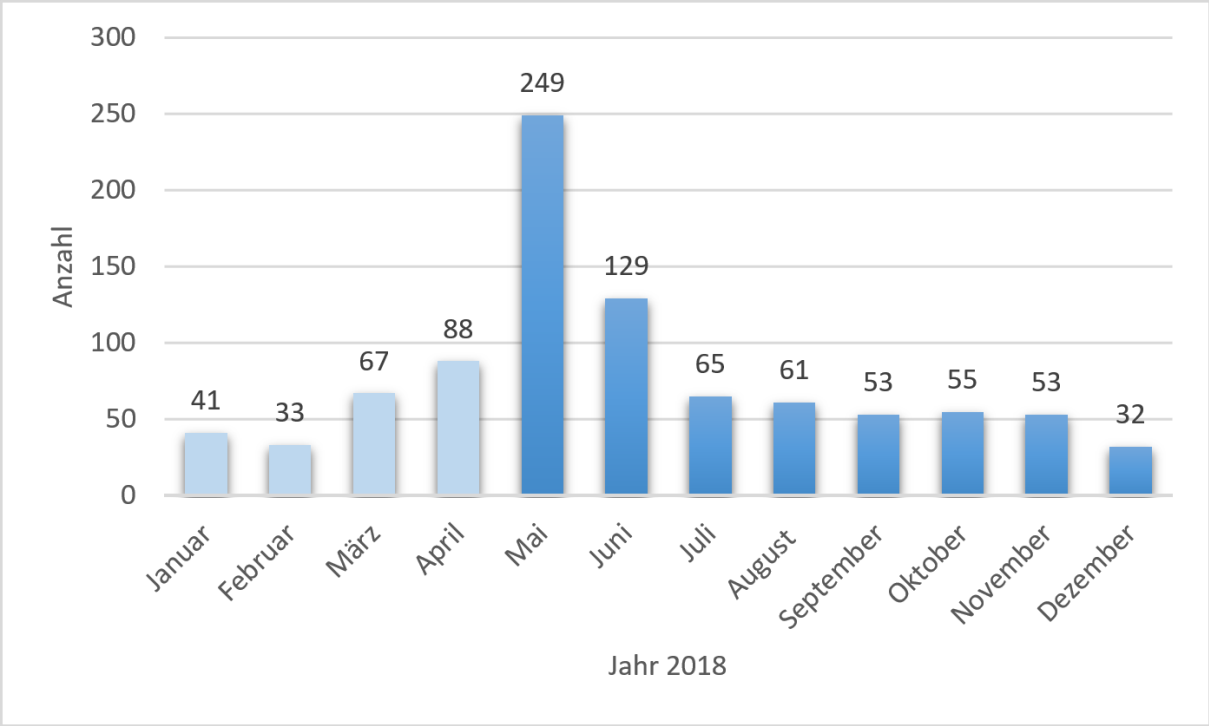
Das Diagramm zeigt die bei der Landesbeauftragten für Datenschutz und Informationsfreiheit eingegangenen Beschwerden im gesamten Jahr 2018 nach Themengebieten unterteilt. Dabei wird deutlich, dass es bei den genannten Themengebieten – wie bei der Videoüberwachung und dem Beschäftigtendatenschutz hervorgehoben – zu Überschneidungen kommen kann.

Themengebiet	AW	RW
Beschäftigtendatenschutz	40	10 %
Werbung	40	10 %
Kreditwirtschaft	9	2 %
Telemedien	47	12 %
Mieterdatenschutz	10	3 %

Themengebiet	AW	RW
Sonstiges (nicht öffentlich)	64	16 %
Sonstiges (öffentlich)	53	14 %
Gesundheit und Soziales	53	14 %
Polizei / Justiz	33	8 %
Videoüberwachung	46	11 %

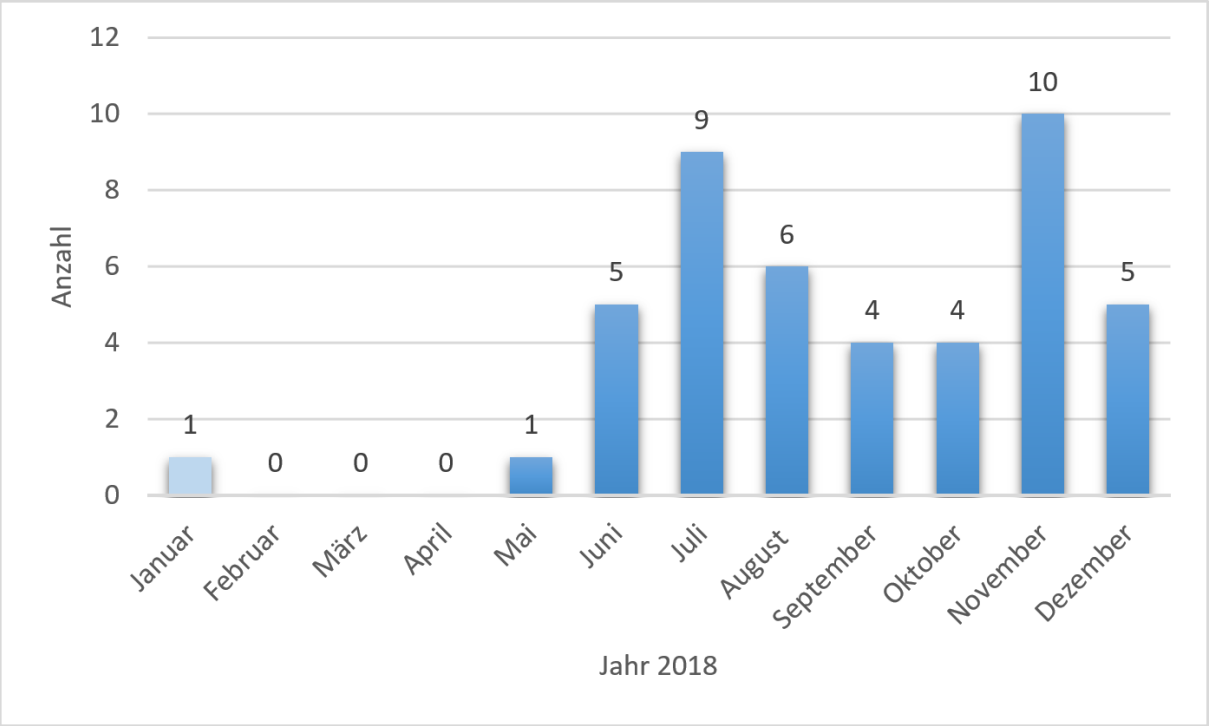
Die Tabelle stellt die absoluten Werte (AW) und relativen Werte (RW) der unterschiedlichen Themengebiete der Beschwerden dar.

2.3 Beratungen

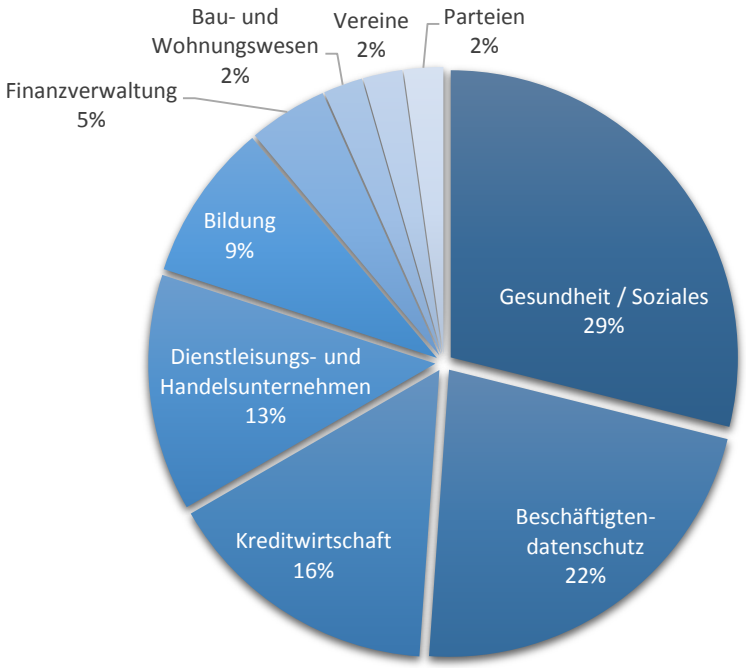


Diese Grafik gibt eine Übersicht über die Anzahl von schriftlichen und telefonischen Beratungen von Verantwortlichen und betroffenen Personen.

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 nach Themengebieten auf.

2.5 Abhilfemaßnahmen

Warnungen

Abhilfemaßnahmen nach Artikel 58 Absatz 2 a DSGVO: Keine

Verwarnungen

Abhilfemaßnahmen nach Artikel 58 Absatz 2 b DSGVO: Keine

Anweisungen und Anordnungen

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

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

Keine

Anzahl der Verfahren mit Federführung nach Artikel 56 DSGVO

Keine

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

Im Berichtsjahr waren wir an zehn Verfahren nach den Artikeln 60 ff. beteiligt.

2.7 Förmliche Begleitung bei Rechtsetzungsvorhaben

Folgende Beratungen wurden im Berichtsjahr 2018 durchgeführt:

Datenschutz

– Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG)

Inneres

– Bremischen Polizeigesetz (BremPolG)

  Trotz der an die Mitgliedstaaten gerichteten Verpflichtung, die Richtlinie (EU) 2016/680 des Europäischen Parlamentes und des Rates 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.

- Bremisches Gesetz zur Ausführung des Bundesmeldegesetzes (BremAGBMG)
- Bremisches Glücksspielgesetz (BremGlüG)
- Gesetz über die Zulassung einer öffentlichen Spielbank (SpielbankenG)
- Bremisches Hilfeleistungsgesetz (BremHilfeG)
- Verordnung zur Übermittlung von Meldedaten (MeldDÜV)
- Bremisches Wahlgesetz
- Bremische Landeswahlordnung
- Anordnung über Mitteilungen in Zivilsachen (MiZi)

Gesundheit

- Bremisches Krankenhausdatenschutzgesetz (BremKHDSG)

  Zum Redaktionsschluss noch nicht verabschiedet, daher im Falle der Kollision mit Regelungen der DSGVO Direktgeltung der DSGVO.
- Bremisches Krankenhausgesetz (BremKrhG)

  Zum Redaktionsschluss noch nicht verabschiedet, daher im Falle der Kollision mit Regelungen der DSGVO Direktgeltung der DSGVO.
- Bremisches Ausführungsgesetz zum Tiergesundheitsgesetz (BremAGTierGesG)
- Bremisches Krebsregistergesetz (BremKRG)
- Bremisches Landesgremiumgesetz

Bildung

- Bremisches Hochschulgesetz (BremHG)
- Gesetz über das Studentenwerk Bremen (StWG)
- Bremisches Schuldatenschutzgesetz (BremSchulDSG)
- Bremisches Berufsqualifikationsfeststellungsgesetz (BremBQFG)

Beschäftigte

- Bremisches Beamtengesetz (BremBG)

  Zum Redaktionsschluss noch nicht verabschiedet, daher im Falle der Kollision mit Regelungen der DSGVO Direktgeltung der DSGVO.

Kultur

- Gesetz über die Sicherung und Nutzung öffentlichen Archivguts im Lande Bremen (Bremisches Archivgesetz – BremArchivG)

  Bislang nicht verabschiedet, daher im Falle der Kollision mit Regelungen der DSGVO Direktgeltung der DSGVO.

- Bremisches Gesetz zur Pflege und zum Schutz der Kulturdenkmäler (Bremisches Denkmalschutzgesetz – BremDSchG)

- Gebühren- und Benutzungsordnung für die Bremer Volkshochschule, Eigenbetrieb der Stadtgemeinde Bremen

- Ortsgesetz über die Musikschule Bremen, Eigenbetrieb der Stadtgemeinde Bremen (BremMusikSchOG)

- Ortsgesetz über den Eigenbetrieb Stadtbibliothek Bremen, Eigenbetrieb der Stadtgemeinde Bremen (BremStBOG)

  Bislang nicht verabschiedet, daher im Falle der Kollision mit Regelungen der DSGVO Direktgeltung DSGVO.

Bauen und Wohnen

- Bremische Landesbauordnung (BremLBO)

- Bremisches Architektengesetz (BremArchG)

- Bremisches Ingenieurgesetz (BremIngG)

- Gesetz über die Landesvermessung und das Liegenschaftskataster (Vermessungs- und Katastergesetz)

- Verordnung über das Verfahren zum automatisierten Abruf von Daten des Liegenschaftskatasters (Liegenschaftsdaten-Abruf-Verordnung – LieDAV)

- Bremische Bauvorlagenverordnung (BremBauVorlV)

Verkehr

- (Bremisches) Landes-Carsharinggesetz (BremLCsgG)
- Straßenverkehrsgesetz (StVG)

Umwelt

- Gesetz zu dem Staatsvertrag zur Änderung des Staatsvertrags zwischen dem Land Niedersachsen und der Freien Hansestadt Bremen über die Zusammenarbeit bei Überwachungs- und Untersuchungsaufgaben im Verbraucherschutz- und Tiergesundheitsbereich
- Bremisches Wassergesetz (BremWG)
- Bremisches Gesetz über Naturschutz und Landschaftspflege (BremNatG)
- Ortsgesetz über die Begrünung von Freiflächen und Flachdachflächen in der Stadtgemeinde Bremen (Begrünungsortsgesetz Bremen – BegrünungsOG)
- Verordnung über die Übertragung staatlicher Aufgaben auf die Landwirtschaftskammer Bremen (Landwirtschaftskammer-Übertragungsverordnung – LWKÜV)

Beiräte

- Ortsgesetz über Beiräte und Ortsämter

Presse/Medien

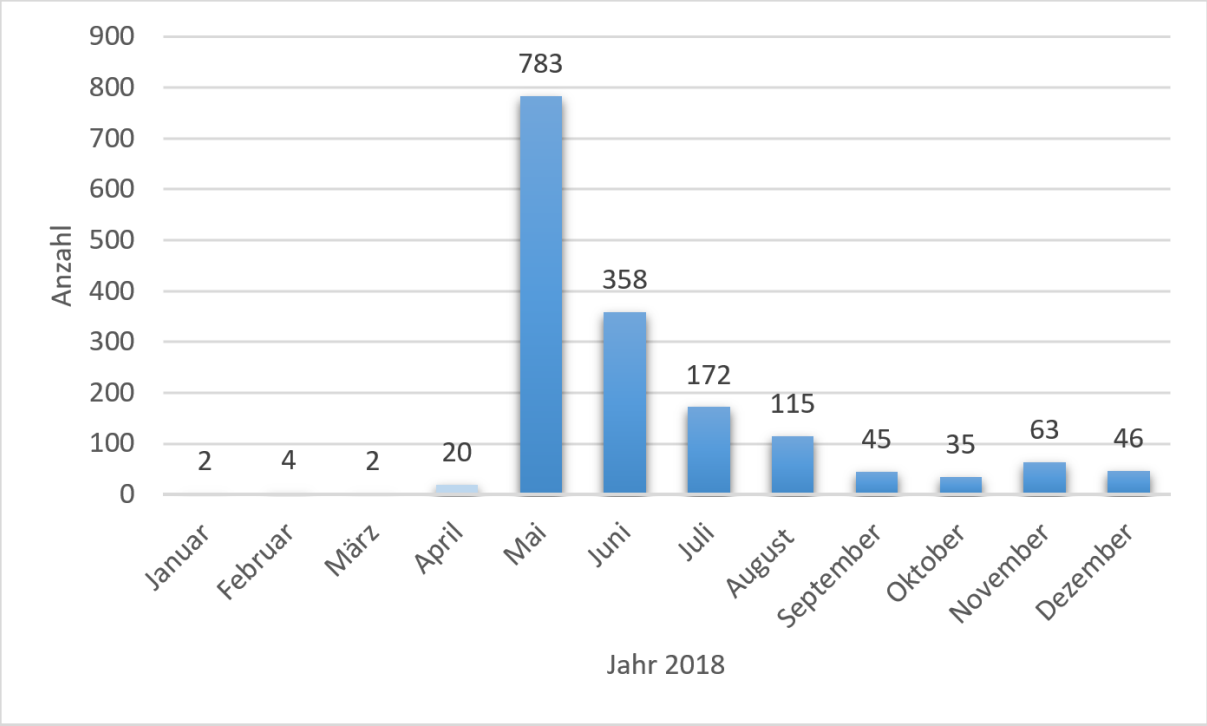
- Gesetz über die Presse (Pressegesetz)
- Bremisches Landesmediengesetz (BremLMG)

Informationsfreiheit

- Gesetz über die Freiheit des Zugangs zu Informationen für das Land Bremen (Bremer Informationsfreiheitsgesetz – BremIFG)

  Zum Redaktionsschluss noch nicht verabschiedet, daher im Falle der Kollision mit Regelungen der DSGVO Direktgeltung der DSGVO.

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

Die Datenschutzgrundverordnung ermöglicht es Unternehmen, sich nach Artikel 43 als Zertifizierungsstelle im Bereich Datenschutz akkreditieren zu lassen. Nach § 39 Bundesdatenschutzgesetz-neu wird die Akkreditierung durch die für die Zertifizierungsstelle zuständige Aufsichtsbehörde auf der Grundlage einer Akkreditierung durch die Deutsche Akkreditierungsstelle (DAkkS) erteilt. Die bremische Landesbeauftragte für Datenschutz und Informationsfreiheit hat der bundesweit erste Antrag auf Akkreditierung erreicht.

3. Bremische Bürgerschaft – Ergebnisse der Beratungen des 40. Jahresberichts

Bericht und Beschlussempfehlung des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit.

40. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit und Stellungnahme des Senats.

I. Bericht

Die Bürgerschaft (Landtag) überwies in ihrer Sitzung am 25. April 2018 den 40. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit vom 16. März 2018 (Drucksache 19/1583) und in ihrer Sitzung am 26. September 2018 die dazu erfolgte Stellungnahme des Senats vom 28. August 2018 (Drucksache 19/1801) an den Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zur Beratung und Berichterstattung.

Der Ausschuss stellte bei den nachfolgend aufgeführten Punkten des 40. Jahresberichts Beratungsbedarf fest:

Ziffer 3.5 Arbeitsgruppe "Prüfung bei Dataport"

Ziffer 4.3 Microsoft Office 365

Ziffer 5.1 Allgemeines zu den Polizeiverfahren

Ziffer 5.3 Rahmendatenschutzkonzept

Ziffer 5.4 BodyCam

Ziffer 5.5 Telekommunikationsüberwachung

Ziffer 5.7.1 Probleme der länderübergreifenden Telekommunikationsüberwachung

Ziffer 6.3 Protokollierung lesender Zugriffe bei der Staatsanwaltschaft

Ziffer 7.2 Festplattenverlust bei einer Laborarztpraxis

Ziffer 8.8 Jugendberufsagentur

Ziffer 10.3 Restaurant

Ziffer 10.4 Eiscafékette

Ziffer 11.5 Richtlinien des Europarats zu Big Data

In seiner Sitzung am 27. Oktober 2018 erörterte der Ausschuss die beratungsbedürftigen Punkte mit der Landesbeauftragten für Datenschutz und Informationsfreiheit und 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 betroffenen Ressorts und Dienststellen gekommen ist

beziehungsweise im Rahmen von Gesprächen zwischen den Beteiligten konstruktiv an Lösungsmöglichkeiten gearbeitet wird.

So sind die von der Arbeitsgruppe "Prüfung bei Dataport" (Ziffer 3.5) genannten Probleme beim User-Help-Desk inzwischen behoben worden.

Im Hinblick auf die mit dem Office-Paket "Microsoft Office 365" verbundenen datenschutzrechtlichen Risiken begrüßt der Ausschuss, dass der Senat nicht die Absicht hat, Office 365 einzuführen (Ziffer 4.3).

Hinsichtlich des polizeilichen Vorgangsbearbeitungssystems @rtus (Ziffer 5.1) wurde dem Ausschuss zugesichert, dass hier Anfang 2019 ein Konzept vorgelegt wird. Gleiches gilt für das immer noch ausstehende Rahmendatenschutzkonzept der Polizei Bremen, mit dessen Erarbeitung noch im Jahr 2018 begonnen werden soll (Ziffer 5.3).

Zu den datenschutzrechtlichen Fragen im Zusammenhang mit dem Einsatz einer BodyCam (Ziffer 5.4) hat der Ausschuss zur Kenntnis genommen, dass die durch das sogenannte Pre-Recording aufgezeichneten Bilder bei Nichtaktivierung der BodyCam automatisch überschrieben beziehungsweise gelöscht werden. Im Falle einer gezielten Aktivierung der BodyCam wird die automatische Löschfunktion hingegen deaktiviert und die Bilder stehen zum Zweck der Beweissicherung zur Verfügung. Eine Rechtsgrundlage für das Pre-Recording findet sich im Bremischen Polizeigesetz.

Bei der länderübergreifenden Kooperation im Bereich der Telekommunikationsüberwachung (Ziffern 5.5 und 5.7.1) bestehen nach wie vor zahlreiche datenschutzrechtliche Mängel. Da das derzeit in Kooperation mit Niedersachsen genutzte Rechenzentrum jedoch 2020 ausläuft, wird es aller Voraussicht nach nicht mehr zu einer Behebung der Mängel kommen. Dies sieht der Ausschuss kritisch und teilt die Auffassung der Landesbeauftragten für Datenschutz, dass trotz des begrenzten Betriebszeitraums Ziel sein muss, allen datenschutzrechtlichen Belangen vollumfänglich Rechnung zu tragen. Mit Blick auf die Zukunft begrüßt es der Ausschuss, dass sich – in Kenntnis der bestehenden Mängel – die Bemühungen aller Beteiligten darauf konzentrieren, im TKÜ-Nordverband ein neues länderübergreifendes Rechen- und Dienstleistungszentrum aufzubauen, das datenschutzkonform betrieben wird.

Im Bereich Justiz sieht es der Ausschuss als problematisch an, dass nach wie vor beim von der Staatsanwaltschaft Bremen verwendeten Informationstechnikverfahren "web-sta" keine Protokollierung des lesenden Zugriffs erfolgt, obwohl dies schon seit längerem von der Landesbeauftragten kritisiert wird (Ziffer 6.3). Lesende Zugriffsrechte können von den Berechtigten auch für rechtswidrige Zwecke missbraucht werden, sodass es aus Sicht des Ausschusses dringend erforderlich ist, einem potenziellen Missbrauch durch entsprechende technische Maßnahmen vorzubeugen, zumal diese auch verfügbar sind. Die

Staatsanwaltschaft daraufhin mitgeteilt, dass die erforderlichen Veränderungen im Fachverfahren nunmehr beauftragt worden sind und nach erfolgreicher Umsetzung aller notwendigen Prozesse mit einem Einsatz gegen Ende 2019 gerechnet werden kann.

Im Fall des Festplattenverlusts bei einer Laborpraxis (Ziffer 7.2) hat der Ausschuss zur Kenntnis genommen, dass der europäische Gesetzgeber in der inzwischen in Kraft getretenen Datenschutzgrundverordnung die Transparenzanforderungen für die Betroffenen deutlich erhöht hat und auch für wissenschaftliche Zwecke gespeicherte Daten nun anonymisiert gespeichert werden müssen.

Bei der Berichterstattung zur Jugendberufsagentur (Ziffer 8.8) geht es um die Beteiligung Bremens an einem Pilotprojekt zum Aufbau eines "Kerndatensystems Jugendliche" bei der Bundesagentur für Arbeit, einer gemeinsamen Datenbank für alle Partner aller Jugendberufsagenturen im Bundesgebiet. Gegen die Umsetzung dieses Projekts hat die Landesbeauftragte für Datenschutz erhebliche Bedenken geäußert. Der Ausschuss wurde darüber informiert, dass das Projekt inzwischen aufgrund der vorgetragenen datenschutzrechtlichen Bedenken gestoppt worden ist und eine bundeseinheitliche Regelung angestrebt wird. Ferner arbeitet das Ressort an einer kleinen Lösung, um Daten über potenziell unterstützungsbedürftige Jugendliche austauschen zu können.

Zum Thema Videoüberwachung (Ziffern 10.3 und 10.4) wurde dem Ausschuss berichtet, dass die im Bericht angesprochenen problematischen Kameras inzwischen abgebaut und auch die sonstigen von der Landesbeauftragten geforderten Maßnahmen umgesetzt worden sind.

Vor dem Hintergrund der Richtlinie des Europarats zum Schutz der Einzelnen bei der Datenverarbeitung in einer Big-Data-Welt (Ziffer 11.5) beschäftigte sich der Ausschuss mit der Frage, wie von staatlicher Seite mit dem Thema "Künstliche Intelligenz" umgegangen wird und künftig umgegangen werden soll. Dabei wurde deutlich, dass es bei der Entscheidung für oder gegen den Einsatz von künstlicher Intelligenz unabdingbar ist, die dahinterstehenden Algorithmen und Vorannahmen für alle transparent zu machen. Diese Veröffentlichungspflicht muss sowohl für öffentliche wie nicht öffentliche Datenverarbeiter gelten. Der Ausschuss ist sich einig, die Entwicklung in diesem für die Zukunft wichtigen Bereich weiter kritisch zu begleiten und beabsichtigt, eine Anhörung zum Thema "Künstliche Intelligenz" durchzuführen.

II. Beschlussempfehlung

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

Susanne Grobien

Vorsitzende

4. Datenschutzbeauftragte

4.1 Kurzpapier Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern

Die Konferenz der Datenschutzbehörden des Bundes und der Länder veröffentlichte das Kurzpapier Nummer 12 zum Thema "Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern". Das Dokument ist im Internetangebot der Landesbeauftragten für Datenschutz und Informationsfreiheit abrufbar. [1]

4.2 Benennung von Datenschutzbeauftragten durch Arztpraxen, Apotheken und sonstige Angehörige von Gesundheitsberufen

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fasste einen Beschluss zur Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Absatz 1 Buchstabe c Datenschutzgrundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs, der im Internetangebot der Landesbeauftragten für Datenschutz und Informationsfreiheit abrufbar ist. [2]

4.3 Pflicht zur Bestellung von Datenschutzbeauftragten bei Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung

Nach Artikel 35 Absatz 2 Datenschutzgrundverordnung (DSGVO) holt die oder der Verantwortliche bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat der oder des Datenschutzbeauftragten ein, sofern eine solche oder ein solcher benannt wurde. § 38 Absatz 1 Bundesdatenschutzgesetz in Verbindung mit Artikel 37 Absatz 4 DSGVO legt hierzu ergänzend fest, dass dem Bundesdatenschutzgesetz unterliegende Verantwortliche, die eine Datenschutz-Folgenabschätzung durchzuführen haben, unabhängig von der Anzahl

[1] https://www.datenschutz.bremen.de/datenschutztipps/kurzpapiere_der_datenschutzkonferenz-13713

[2] https://www.datenschutz.bremen.de/publikationen/konferenzentschliessungen-7501

der mit der Verarbeitung befassten Personen stets eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen haben.

5. Übergreifende IT-Verfahren

5.1 Microsoft Office 365

Das als "Deutschland-Cloud" bekannt gewordene Treuhändermodell von Microsoft und T-Systems (siehe 40. Jahresbericht, Ziffer 4.3), welches die datenschutzrechtlich sichere Nutzung von Microsoft Office 365 sicherstellen sollte, wird nicht weiter fortgeführt. Die bremische Verwaltung hat im Ausschuss der Bremischen Bürgerschaft für Wissenschaft, Medien, Datenschutz und Informationsfreiheit bereits zugesichert, dass diese Office-Variante nicht eingesetzt werden wird (siehe Ziffer 3. dieses Berichts).

5.2 Begleitung des Projekts eHaushalt

5.3 Blockchains und Datenschutz

Der große Trend "Blockchain" hat auch uns in Form allgemeiner Anfragen erreicht. Wir vertreten dabei grundsätzlich die Auffassung, dass insbesondere die Artikel 16 (Recht auf Berichtigung) und Artikel 17 (Recht auf Löschen) der Datenschutzgrundverordnung (DSGVO) nur schwer mit der Integrität und Vertraulichkeit der Blockchain in Einklang zu bringen sind.

5.4 Gewährleistung der Sicherheit der Verarbeitung bei der Übertragung personenbezogener Daten per Fax und E-Mail

Nach Ermittlung des Schutzbedarfs der zu übermittelnden Daten und einer Analyse der Risiken der Verarbeitung sind für Übertragungsverfahren Sicherheitsmaßnahmen wie beispielsweise die in Artikel 32 Absatz 1 Buchstabe a Datenschutzgrundverordnung (DSGVO) explizit genannte Verschlüsselung zu ermitteln und umzusetzen. Hierbei ist zu beobachten, dass die Übermittlung per Fax inzwischen wie die Übermittlung durch eine unverschlüsselte E-Mail bewertet werden muss, weil beide Verfahren inzwischen IP-basierte Telekommunikationsnetze nutzen.

6. Inneres

6.1 Kontrolle der Antiterrordatei und der Rechtsextremismusdatei

Im Jahr 2018 haben wir Kontrollen der Antiterrordatei und der Rechtsextremismusdatei durchgeführt.

6.2 Unbefugte Abfragen in den polizeilichen Informationssystemen

6.2.1 Gegen Entgelt

6.2.2 Aus Neugier

6.2.3 In einem Bewerbungsverfahren

6.3 Beschwerden wegen nicht erfolgter Löschung

Im Jahr 2018 wurden bei uns zehn Beschwerden in Bezug auf die Ausübung von Betroffenenrechten gegenüber der Polizei Bremen, insbesondere wegen nicht erfolgter Löschung in den polizeilichen Verfahren, erhoben.

6.4 Verschlüsselung beim Projekt Online-Wache

6.5 Alternierende Telearbeit bei der Polizei

6.6 Kontrollen beim Migrationsamt Bremen und bei der Ausländerbehörde Bremerhaven

In Bezug auf das Schengener Informationssystem II (SIS II) und das Visainformationssystem (VIS) haben wir Kontrollen beim Migrationsamt Bremen und bei der Ausländerbehörde Bremerhaven durchgeführt.

7. Justiz

7.1 Unerlaubte Speicherung von Daten auf einen USB-Stick beim Auftragsverarbeiter

Im letzten Jahresbericht (siehe hierzu 40. Jahresbericht, Ziffer 8.9) haben wir über die Software zum Management der Unterkünfte berichtet. Die noch offenen Punkte hinsichtlich der Speicherung der Essensausgabe bei jeder einzelnen Person, dem Beschäftigtenmodul, der Freitexteingabe und der Löschung von nicht mehr erforderlichen Daten wurden bisher nicht bearbeitet.

8.9 Laptopdiebstahl in einem Kindergarten (Meldung des Verantwortlichen)

8.10 Falsche Sortierung von Rezepten bei einer Versandapotheke (Meldung des Verantwortlichen)

8.11 Verwendung von Kundennamen und Aktenzeichen bei der Überweisung von Nachbarschaftshilfen

8.12 Datenbank Haaranalysen

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

9. Bildung

9.1 Toilettenkontrolle in einer Schule

In einer Grundschule überwachten ältere Schülerinnen und Schüler in der großen Pause in jedem Einzelfall, ob die Toilette sauber verlassen wurde.

9.2 Erhebung von Daten aus einer Chatgruppe von Schülerinnen und Schülern durch die Lehrerin

9.3 Voraussetzungen für die Weitergabe von Notenspiegeln an die Eltern

10. Beschäftigtendatenschutz

10.1 Unzulässige Überwachung der Arbeitszeit durch eine Hochschule

10.2 Ausdruck eines privaten Chats aus dem Facebook-Account eines Lehrers aus dem Dienstrechner

10.3 Ausdruck des privaten digitalen Verhaltens von Kundinnen und Kunden, die gleichzeitig Beschäftigte sind

10.4 Telefonaufzeichnung der Anrufe durch ein Call Center

Nach der Datenschutzgrundverordnung sind Datenverarbeitungen im Zusammenhang mit Vertragsabschlüssen oder aufgrund besonderer gesetzlicher Verpflichtungen grundsätzlich zulässig, ohne dass es einer gesonderten Einwilligung der oder des Betroffenen bedürfte. Wir erhielten Anhaltspunkte dafür, dass das eine oder andere Kreditinstitut die Unsicherheit seiner Kundinnen und Kunden über die neuen Datenschutzregeln dazu genutzt haben könnte, sich unter Vorspiegelung der Notwendigkeit der Abgabe einer datenschutzrechtlichen Einwilligungserklärung weitergehende Möglichkeiten zur Auswertung und Nutzung der Kundendaten zu verschaffen. Mangels personeller Ressourcen konnten wir diesen Hinweisen bislang bedauerlicherweise nicht nachgehen.

12.2 Meldungen über unbeabsichtigte Offenlegungen von Kontoinformationen

Aus dem Finanzdienstleistungssektor meldeten uns Verantwortliche beispielsweise, dass Girokontoauszugsinformationen, welche regelmäßig detaillierte Informationen zu den Lebensumständen der Kontoinhaber, etwa zu Arbeitsverhältnissen, Wohn- und Versicherungsverhältnissen, Vereinsmitgliedschaften, Einkaufsgewohnheiten, Spenden et cetera enthalten, aufgrund fehlerhafter Briefkuvertierung, Fehladressierung und technischer Fehler beim Online-Banking, in falsche Hände gelangt seien.

12.3 Missverstandener Datenschutz: Kundenbeschwerden nach Mitarbeiterwechsel bei Finanzdienstleister

Mehrere Beschwerden erreichten uns im Berichtszeitraum, nachdem es zu einem Wechsel des Kundenbetreuers eines Finanzdienstleistungsunternehmens gekommen war und sich der neue Kundenbetreuer bei den Kunden vorgestellt hatte. Den Kundinnen und Kunden war offensichtlich nicht bewusst, dass das Finanzdienstleistungsunternehmen als solches ihr Vertragspartner und damit für ihre personenbezogenen Daten verantwortlich war, nicht aber ein bestimmter Mitarbeiter.

13. Werbung und Adresshandel

13.1 Unverlangte Werbung aufgrund angeblicher Teilnahme an einem Preisausschreiben

13.2 Unerwünschte Werbung von Reiseunternehmen ohne Einwilligung

13.3 Werbe-E-Mail von Ticketunternehmen ohne Einverständnis

13.4 Durchsetzung des Löschungsanspruchs

13.5 Durchsetzung des Auskunftsanspruchs

13.6 Angebliche Gewinnbenachrichtigung trotz fehlender Teilnahme an einem Gewinnspiel

13.7 Verbot, die Einwilligung zur Verarbeitung von personenbezogenen Daten von einem Dienstleistungsangebot abhängig zu machen

14. Gewerbe und Mieterdatenschutz

14.1 Umsetzung Prostituiertenschutzgesetz

Das Prostituiertenschutzgesetz soll nach seiner ausdrücklichen Zielsetzung eine Verbesserung der Arbeitsbedingungen von Prostituierten bewirken. Die vor diesem Hintergrund eingeführte Gesundheitsberatungs- sowie Anmeldepflicht und Anmeldenachweis-Mitführungspflicht für Prostituierte führte wegen der hierfür vorgeschriebenen Informationserfassung und Informationsverarbeitung zu erheblichen datenschutzrechtlichen Sorgen bei den Betroffenen. Da derartige Informationen einen hohen Schutzbedarf haben und ihre Verarbeitung wegen des erheblichen Gefährdungspotenzials für die Betroffenen viele datenschutzrechtlichen Fragen aufwirft, hätten wir die technische und organisatorische Ausgestaltung der Verarbeitungsprozesse gerne begleitet, mussten hiervon jedoch aus Kapazitätsgründen absehen.

14.2 Kontrolle des Umgangs mit Kundendaten im Fitnessstudio

In Zeiten digitaler Vermessung der körperlichen Leistungsfähigkeit wächst der Umfang der Verarbeitung personenbezogener Daten, insbesondere auch sensibler Gesundheitsdaten, in Fitnessstudios stetig an. Wie sich bei einer punktuellen Kontrolle eines Fitnessstudios zeigte, war dort das Bewusstsein um die Geltung von Datenschutzregeln und die Einsicht in die Notwendigkeit datenschutzrechtlicher Maßnahmen wenig ausgeprägt.

14.3 Geschäftsmasche einer "Datenschutzauskunfts-Zentrale"

Anfang Oktober 2018 erhielten viele bremische Unternehmen und Gewerbetreibende eine als eilig gekennzeichnete Fax-Nachricht einer dubiosen "(DAZ) Datenschutzauskunfts-Zentrale" aus Oranienburg mit der Aufforderung, einen mitübersandten Fragebogen zwecks Umsetzung der Datenschutzgrundverordnung (DSGVO) auszufüllen und umgehend zurückzusenden. Mit der DSGVO hatte dies jedoch nichts zu tun, vielmehr sollte auch hier die bestehende Unsicherheit über die DSGVO ausgenutzt werden, um der oder den Angeschriebenen einen kostenpflichtigen Vertrag unterzujubeln. Wir baten die zuständige Staatsanwaltschaft um strafrechtliche Ermittlungen.

14.4 Orientierungshilfe zur Mieterselbstauskunft

Die Orientierungshilfe zur datenschutzkonformen "Einholung von Selbstauskünften bei Mietinteressentinnen" und ein Musterformular "Selbstauskunft zur Vorlage bei der Vermieterin oder dem Vermieter" können von Vermietern und anderen Interessierten von unserer Internetseite[3] heruntergeladen und genutzt werden.

14.5 Belegeinsicht auch durch einen Bevollmächtigten des Mieters bei der Nebenkostenabrechnung

15. Verkehr und Umwelt

15.1 Datenschutzrechtliche Fragestellungen im Zusammenhang mit der Gasumstellung

15.2 Beschwerden zum Bike-Sharing

16. Internationales und Europa

16.1 EU-U.S. Privacy Shield

Obwohl die Europäische Kommission (EU-Kommission) den Datenschutzschild, welcher von der Europäischen Union und den Vereinigten Staaten von Amerika (EU-U.S. Privacy Shield) 2016 verabschiedet worden ist, bereits zum zweiten Mal überprüft hat, bleiben die datenschutzrechtlichen Einwände weiterhin bestehen (siehe 40. Jahresbericht, Ziffer 14.3).

16.2 Inkrafttreten des U.S.-amerikanischen CLOUD Act

Mit dem sogenannten CLOUD Act (Clarifying Lawful Overseas Use of Data Act) haben die Vereinigten Staaten von Amerika (USA) ein Instrument geschaffen, welches Unternehmen dazu verpflichtet, auch außerhalb der USA gespeicherte Daten an US-Behörden zu übermitteln, ohne die betroffenen Personen informieren zu müssen. Dies hat zur Folge, dass amerikanische Firmen einmal mehr entscheiden müssen, ob sie amerikanisches oder europäisches Recht einhalten.

[3] www.datenschutz.bremen.de/datenschutztipps/orientierungshilfen_und_handlungshilfen-7136

16.3 Angemessenheitsentscheidung der Kommission zu Japan

Im September 2018 hat die Europäische Kommission (EU-Kommission) das Verfahren zur Annahme der Angemessenheitsentscheidung für Japan eingeleitet. Ein erfolgreicher Abschluss dieses Verfahrens hätte zur Folge, dass Japan datenschutzrechtlich nicht mehr als unsicheres Drittland anzusehen und der Datentransfer dorthin ohne besondere Genehmigung möglich ist. Derzeit werden die notwendigen Schritte für die Verabschiedung der Angemessenheitsentscheidung gestartet.[4]

17. Telemedien

17.1 Urteil des Europäischen Gerichtshofes zu Facebook-Fanseiten

Am 5. Juni 2018 entschied der Europäische Gerichtshof (EuGH), dass Betreiber von Fanseiten bei Facebook für den Datenschutz mitverantwortlich sind. Einzelheiten sind der Entschließung "Die Zeit der Verantwortungslosigkeit ist vorbei: EuGH bestätigt gemeinsame Verantwortung von Facebook und Fanpage-Betreibern" vom 6. Juni 2018 (siehe Ziffer 19.3 dieses Berichts) und dem Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden zu Facebook Fanpages vom 5. September 2018 (siehe Ziffer 19.5 dieses Berichts) sowie unserer Stellungnahme vor dem Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit[5] zu entnehmen.

17.2 Keine Anwendbarkeit des Telemediengesetzes für nicht öffentliche Stellen

Seit Geltung der Datenschutzgrundverordnung werden die Vorschriften über den Datenschutz im Telemediengesetz für nicht öffentliche Stellen verdrängt und sind nicht mehr anwendbar. Einzelheiten sind der Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (siehe hierzu Ziffer 19.3 dieses Berichts) vom 26. April 2018 zu entnehmen.

---

[4] Die Angemessenheitsbeschlüsse der EU-Kommission finden sich unter: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_de

[5] https://sd.bremische-buergerschaft.de/sdnetrim/UGhVM0hpd2NXNFdFcExjZZMwBU_9iwv8ufCZSMg7pOFDaLfcNR-fSZ6Iw4D3pGek/ Vorlage_VL-449_2018.pdf

17.3 Anpassung der Landesgesetze an medienrechtliche Vorschriften der DSGVO

Bei der Anpassung des Bremischen Landesmediengesetzes und des Bremischen Pressegesetzes wurde die in Artikel 85 Absatz 1 Datenschutzgrundverordnung enthaltene Öffnungsklausel für einen Ausgleich zwischen dem Recht auf Datenschutz und dem Recht auf Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, nicht beachtet.

18. Beiräte

18.1 Novellierung des Ortsgesetzes über Beiräte und Ortsämter

Der § 6 Absatz 4 des Ortsgesetzes über Beiräte und Ortsämter gewährt Einwohnerinnen und Einwohnern das Recht, Anträge an die Beiräte zu stellen. Durch die Novellierung des Gesetzes wird dieses Recht davon abhängig gemacht, dass sich die Einwohnerinnen und Einwohner damit einverstanden erklären, dass ihre Namen in den Protokollen auch im Internet veröffentlicht werden dürfen. Dies hat zur Folge, dass die Erklärungen nicht als freiwillig im Sinne der Datenschutzgrundverordnung (DSGVO) angesehen werden können, weil sie gegen das vorrangig und unmittelbar anwendbare Koppelungsverbot (Artikel 7 Absatz 4 DSGVO) verstoßen, sodass die Einhaltung dieser Anforderung von den Ortsämtern gegenüber den Bürgerinnen und Bürgern nicht verlangt werden darf und eine Veröffentlichung der Namen auf dieser rechtlichen Grundlage nicht zulässig ist.

19. Die Entschließungen der Datenschutzkonferenzen im Jahr 2018

19.1 Facebook-Datenskandal – Neues Europäisches Datenschutzrecht bei Sozialen Netzwerken durchsetzen!

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26. April 2018)

Im März 2018 wurde in der Öffentlichkeit bekannt, dass über eine von November 2013 bis Mai 2015 mit Facebook verbundene App nach Angaben des Unternehmens Daten von 87 Millionen Nutzern weltweit, davon 2,7 Millionen Europäern und etwa 310.000 Deutschen erhoben und an das Analyseunternehmen Cambridge Analytica weitergeben wurden. Dort wurden sie offenbar auch zur Profilbildung für politische Zwecke verwendet.

Aus diesem Anlass hat der national zuständige Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ein Bußgeldverfahren gegen Facebook eingeleitet. Er steht dabei in engem Austausch mit seinen europäischen Kollegen, insbesondere mit dem Information Commissioner's Office in Großbritannien sowie der Artikel-29-Gruppe. Der Datenskandal um Facebook und Cambridge Analytica wirft ein Schlaglicht auf den Umgang mit Millionen Nutzerdaten. Zudem dokumentieren die Vorgänge um Cambridge Analytica, dass Facebook über Jahre hinweg den Entwicklern von Apps den massenhaften Zugriff auf Daten von mit den Verwendern der Apps befreundeten Facebook-Nutzenden ermöglicht hat. Das geschah ohne eine Einwilligung der Betroffenen. Tatsächlich ist der aktuell diskutierte Fall einer einzelnen App nur die Spitze des Eisbergs. So geht die Zahl der Apps, die das Facebook-Login-System nutzen, in die Zehntausende. Die Zahl der davon rechtswidrig betroffenen Personen dürfte die Dimension des Cambridge-Analytica-Falls in dramatischer Weise sprengen und dem Grunde nach alle Facebook-Nutzenden betreffen. Das Vorkommnis zeigt zudem die Risiken für Profilbildung bei der Nutzung sozialer Medien und anschließendes Mikrotargeting, das offenbar zur Manipulation von demokratischen Willensbildungsprozessen eingesetzt wurde.

Die Datenschutzkonferenz fordert aus diesen offenbar massenhaften Verletzungen von Datenschutzrechten Betroffener folgende Konsequenzen zu ziehen:

- Soziale Netzwerke müssen ihre Geschäftsmodelle auf die neuen europäischen Datenschutzregelungen ausrichten und ihrer gesellschaftliche Verantwortung nachkommen. Dazu gehört auch, angemessene Vorkehrungen gegen Datenmissbrauch zu treffen.

- Facebook muss den wahren Umfang der Öffnung der Plattform für App-Anbieter in den Jahren bis 2015 offenlegen und belastbare Zahlen der eingestellten Apps sowie der von dem Facebook-Login-System betroffenen Personen nennen. Ferner gilt es Betroffene über die Rechtsverletzungen zu informieren.

- In Zukunft muss Facebook sicherstellen, dass die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) rechtskonform umgesetzt werden: Die Vorstellung von Facebook zur Einführung der automatischen Gesichtserkennung in Europa lässt erhebliche Zweifel aufkommen, ob das Zustimmungsverfahren mit den gesetzlichen Vorgaben insbesondere zur Einwilligung vereinbar ist. Wenn Facebook die Nutzenden dazu drängt und es ihnen wesentlich leichter macht, der biometrischen Datenverarbeitung zuzustimmen, als sich ihr zu entziehen, führt dies zu einer unzulässigen Beeinflussung des Nutzers.

- Die Reaktionen auf datenschutzwidriges Verhalten sind dabei nicht allein auf den Vollzug des Datenschutzrechts beschränkt, sondern betreffen auch das Wettbewerbs- und

Kartellrecht. Die Forderung nach einer Entflechtung des Facebook-Konzerns wird in dem Maße zunehmen, wie sich dieser durch die systematische Umgehung des Datenschutzes wettbewerbswidrige Vorteile auf dem Markt digitaler Dienstleistungen zu verschaffen versucht. Es bedarf europäischer Initiativen, um monopolartige Strukturen im Bereich der sozialen Netzwerke zu begrenzen und Transparenz von Algorithmen herzustellen.

Weil Datenverarbeitungsprozesse zunehmend komplexer und für Betroffene intransparenter werden, kommt der Datenschutzaufsicht eine elementare Rolle zu. Ihre fachliche Expertise ist gefragt, sie muss organisatorisch und personell in der Lage sein, beratend und gestaltend tätig zu sein. Ein starkes Datenschutzrecht und effektive Aufsichtsbehörden vermindern gemeinsam die Risiken für die Bürgerinnen und Bürger in der digitalen Gesellschaft. Sollten Facebook und andere soziale Netzwerke nicht bereit sein, den europäischen Rechtsvorschriften zum Schutz der Nutzenden nachzukommen, muss dies konsequent durch Ausschöpfung aller vorhandenen aufsichtsbehördlichen Instrumente auf nationaler und europäischer Ebene geahndet werden.

19.2 Zuverlässigkeitsüberprüfungen bei öffentlichen und privaten Veranstaltungen nur im erforderlichen Maß und nach einem rechtsstaatlichen und transparenten Verfahren

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26. April 2018)

Zunehmend werden im Rahmen von öffentlichen und privaten Veranstaltungen Personen, die in unterschiedlichen Funktionen auf einem Veranstaltungsgelände tätig werden wollen oder sonst Zutritt zu Sicherheitszonen begehren (beispielsweise Anwohner), durch Sicherheitsbehörden auf ihre Zuverlässigkeit überprüft. Auch bei privaten Veranstaltungen fordern die Polizeien die Veranstalter bisweilen dazu auf, dafür zu sorgen, dass alle im Rahmen der Veranstaltung Tätigen einer solchen Prüfung unterzogen werden. In den meisten Fällen ist alleinige Grundlage für diese Maßnahmen immer noch die Einwilligung der Betroffenen.

Bereits vor mehr als zehn Jahren haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 25./26. Oktober 2007 darauf hingewiesen, dass allein die Einwilligung der Betroffenen in eine Zuverlässigkeitsüberprüfung keine legitimierende Grundlage für solche tiefen Eingriffe in das Recht auf informationelle Selbstbestimmung darstellen kann. Die wiederholten Forderungen nach Schaffung gesetzlicher Grundlagen haben seitdem die Gesetzgeber nur weniger Bundesländer aufgegriffen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert die Gesetzgeber und die Verantwortlichen deshalb erneut nachdrücklich auf, für ein rechtsstaatliches und transparentes Verfahren solcher Zuverlässigkeitsüberprüfungen zu sorgen, das auf das absolut erforderliche Maß beschränkt bleibt, sowohl was den Umfang der Überprüfung als auch den betroffenen Personenkreis betrifft. Dabei sind insbesondere folgende Rahmenbedingungen zu beachten:

Zuverlässigkeitsüberprüfungen nur aufgrund einer spezifischen Rechtsgrundlage

Die Gesetzgeber werden aufgefordert, bereichsspezifische Rechtsgrundlagen zu schaffen, die den Grundsatz der Verhältnismäßigkeit beachten und aus denen sich die Voraussetzungen und der Umfang der Überprüfungen klar und für die Bürgerinnen und Bürger erkennbar ergeben.

Zuverlässigkeitsüberprüfungen nur im erforderlichen Maß

Anwendung, Umfang, Kreis der betroffenen Personen und die Datenverarbeitung sind auf das Erforderliche zu beschränken. Generell dürfen Zuverlässigkeitsüberprüfungen nur bei solchen Veranstaltungen eingesetzt werden, die aufgrund ihrer spezifischen Ausprägung infolge einer belastbaren Gefahrenprognose als besonders gefährdet bewertet werden. Korrespondierend müssen die personenbezogenen Daten, die in den zum Abgleich herangezogenen Dateien und Informationssystemen gespeichert sind, nicht nur eine ausreichende Qualität haben, es dürfen auch nur hinreichend gewichtige Delikte in die Überprüfung einbezogen werden. Zudem müssen die Kriterien, die zur Annahme von Sicherheitsbedenken führen, einen konkreten Bezug zu den abzuwehrenden Gefahren haben.

Zuverlässigkeitsüberprüfungen nur in einem transparenten Verfahren

Die Rechte und Freiheiten der betroffenen Personen müssen durch ein transparentes Verfahren gewährleistet werden. Dazu müssen insbesondere Anhörungsrechte der betroffenen Personen rechtlich verankert werden. Im praktischen Verfahren kann im Einzelfall auch die Einrichtung einer Clearingstelle sinnvoll sein. Zudem sollten zumindest die Datenschutzbeauftragten der Verantwortlichen frühzeitig vorab beteiligt werden, damit eine datenschutzrechtliche Beratung für eine datensparsame Ausgestaltung und Beschränkung des konkreten Verfahrens stattfinden kann.

19.3 Zur Anwendbarkeit des Telemediengesetzes für nicht öffentliche Stellen ab dem 25. Mai 2018

(Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26. April 2018)

Der Kommissionsentwurf[6] zur ePrivacy-Verordnung vom Januar 2017 sieht vor, dass diese Verordnung, welche die ePrivacy-Richtlinie[7] ersetzen soll, gemeinsam mit der Datenschutzgrundverordnung (DSGVO) ab dem 25. Mai 2018 in Kraft tritt und Geltung erlangt. Die ePrivacy-Verordnung soll die DSGVO im Hinblick auf die elektronische Kommunikation präzisieren und ergänzen.[8] Das Gesetzgebungsverfahren zur ePrivacy-Verordnung verzögert sich jedoch erheblich, sodass voraussichtlich nicht mehr mit einem Inkrafttreten im Jahr 2018 zu rechnen ist.[9]

Damit ergeben sich Fragen zur Anwendbarkeit nationalen Rechts neben der DSGVO. Der Gesetzgeber hat das Telemediengesetz (TMG) bisher nicht an die DSGVO angepasst, sodass die datenschutzrechtlichen Vorschriften des TMG (Abschnitt 4) voraussichtlich ab dem 25. Mai 2018 unverändert in Kraft sein werden.[10] Für die Rechtsanwender stellt sich wegen des Anwendungsvorrangs der DSGVO daher die Frage, ob die datenschutzrechtlichen Regelungen des TMG weiterhin anwendbar sein werden.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vertritt hierzu folgende Position:

---

[6] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10. Januar 2017, COM/2017/010 final - 2017/03 (COD).

[7] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31. Juli 2002, 37 und Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. L 337 vom 18. Dezember 2009, 11.

[8] Erwägungsgrund 5 der ePrivacy-Verordnung (E), s. Fn. 1.

[9] Insofern gilt nach dem 25. Mai 2018 die ePrivacy-Richtlinie weiter; siehe dazu auch den Entwurf einer legislativen Entschließung des Europäischen Parlaments zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), worin im Gegensatz zum Kommissionsentwurf kein konkretes Datum zum Inkrafttreten mehr genannt ist.

[10] Siehe zum Anpassungsbedarf aufgrund der Geltungserlangung der DSGVO: Gesetzentwurf der Fraktionen der CDU/CSU und SPD zum Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) mit Verweis auf eine Äußerung der Bundesregierung im Rechtsetzungsverfahren zum 2. TMG-Änderungsgesetz, Bundestagsdrucksache 18/12356 vom 16. Mai 2017, Seite 28.

1. Im Verhältnis zum nationalen Recht kommt ab dem 25. Mai 2018 die DSGVO für sämtliche automatisierte Verarbeitungen personenbezogener Daten vorrangig zur Anwendung, es sei denn nationale Vorschriften sind aufgrund einer Kollisionsregel, eines Umsetzungsauftrages oder einer Öffnungsklausel der DSGVO vorrangig anwendbar.

2. Die DSGVO enthält in Artikel 95 eine Kollisionsregel zum Verhältnis der DSGVO zur ePrivacy-Richtlinie, wonach natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union durch die DSGVO keine zusätzlichen Pflichten auferlegt werden, soweit sie besonderen in der ePrivacy-Richtlinie festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

3. Die Vorschrift des Artikels 95 DSGVO findet keine Anwendung auf die Regelungen im 4. Abschnitt des TMG. Denn diese Vorschriften stellen vorrangig eine Umsetzung der durch die DSGVO aufgehobenen Datenschutzrichtlinie[11] dar und unterfallen – da sie auch nicht auf der Grundlage von Öffnungsklauseln in der DSGVO beibehalten werden dürfen – demgemäß dem Anwendungsvorrang der DSGVO. Hiervon betroffen sind damit auch etwaige unvollständige Umsetzungen der ePrivacy-Richtlinie in diesem Abschnitt, welche jedenfalls isoliert nicht mehr bestehen bleiben können.

4. Damit können die §§ 12, 13, 15 TMG bei der Beurteilung der Rechtmäßigkeit der Reichweitenmessung und des Einsatzes von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen, ab dem 25. Mai 2018 nicht mehr angewendet werden.

5. Eine unmittelbare Anwendung der ePrivacy-Richtlinie für die unter Ziffer 4 genannten Verarbeitungsvorgänge kommt nicht in Betracht (keine horizontale unmittelbare Wirkung von Richtlinien).

6. Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Diensteanbieter von Telemedien kommt folglich nur Artikel 6 Absatz 1, insbesondere Buchstaben a), b) und f) DSGVO in Betracht. Darüber hinaus sind die allgemeinen Grundsätze aus Artikel 5 Absatz 1 DSGVO, sowie die besonderen Vorgaben zum Beispiel aus Artikel 25 Absatz 2 DSGVO einzuhalten.

7. Verarbeitungen, die unbedingt erforderlich sind, damit der Anbieter den von den betroffenen Personen angefragten Dienst zur Verfügung stellen kann, können

[11] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23. November 1995, 31.

gegebenenfalls auf Artikel 6 Absatz 1 Buchstabe b) oder Buchstabe f) DSGVO gestützt werden.[12]

8. Ob und inwieweit weitere Verarbeitungstätigkeiten rechtmäßig sind, muss durch eine Interessenabwägung im Einzelfall auf Grundlage des Artikel 6 Absatz 1 Buchstabe f) DSGVO geprüft werden.

9. Es bedarf jedenfalls einer vorherigen Einwilligung beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und bei der Erstellung von Nutzerprofilen. Das bedeutet, dass eine informierte Einwilligung im Sinne der DSGVO[13], in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung vor der Datenverarbeitung eingeholt werden muss, das heißt zum Beispiel bevor Cookies platziert werden beziehungsweise auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.

Diese Auffassung steht im Einklang mit dem europäischen Rechtsverständnis zu Artikel 5 Absatz 3 der ePrivacy-Richtlinie.[14] Im überwiegenden Teil der EU-Mitgliedsstaaten wurde die ePrivacy-Richtlinie vollständig in nationales Recht umgesetzt[15] oder die Aufsichtsbehörden fordern schon heute ein "Opt-in" entsprechend Artikel 5 Absatz 3 der Richtlinie. Da die Verweise in der ePrivacy-Richtlinie auf die Datenschutzrichtlinie gemäß Artikel 94 Absatz 2 DSGVO als Verweise auf die DSGVO gelten, muss eine Einwilligung im Sinne der ePrivacy-Richtlinie europaweit ab dem 25. Mai 2018 den Anforderungen an eine Einwilligung nach der DSGVO genügen. Um in Zukunft einen einheitlichen Vollzug europäischen Datenschutzrechts zu gewährleisten, muss sichergestellt werden, dass auch Verantwortliche in Deutschland diese datenschutzrechtlichen Anforderungen umsetzen.

Dieses Papier wird unter Berücksichtigung der Entwicklungen auf europäischer Ebene fortgeschrieben.

---

[12] Siehe zur Frage der Erforderlichkeit und zum dafür maßgeblichen Merkmal der Funktion *Artikel-29-Datenschutzgruppe*, Workingpaper 194 – Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht vom 7. Juni 2012, die in der englischen Version noch deutlicher herausstellt, dass es darauf ankommt, ob eine Verarbeitung für die "Auslieferung" [delivery] des explizit nachgefragten Dienstes erforderlich ist, Seite 3.

[13] Siehe zur Einwilligung *Artikel-29-Datenschutzgruppe*, WP 259 – Guidelines on Consent under Regulation 2016/679 vom 28. November 2017.

[14] *Artikel-29-Datenschutzgruppe*, Workingpaper 194 – Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht vom 7. Juni 2012.

[15] European Commission, Directorate-General of Communications Networks, Content & Technology, ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation vom 31. Januar 2015, Contract number: 30-CE-0629642/00-85, SMART 2013/0071, doi: 10.2759/411362.

19.4 Die Zeit der Verantwortungslosigkeit ist vorbei: EuGH bestätigt gemeinsame Verantwortung von Facebook und Fanpage-Betreibern

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. Juni 2018)

Die unabhängigen Datenschutzbehörden des Bundes und der Länder begrüßen das Urteil des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018, das ihre langjährige Rechtsauffassung bestätigt.

Das Urteil des EuGHs zur gemeinsamen Verantwortung von Facebook und den Betreibern einer Fanpage hat unmittelbare Auswirkungen auf die Seitenbetreiber. Diese können nicht mehr allein auf die datenschutzrechtliche Verantwortung von Facebook verweisen, sondern sind selbst mitverantwortlich für die Einhaltung des Datenschutzes gegenüber den Nutzenden ihrer Fanpage.

Dabei müssen sie die Verpflichtungen aus den aktuell geltenden Regelungen der Datenschutz-Grundverordnung (DS-GVO) beachten. Zwar nimmt das Urteil Bezug auf die frühere Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr, doch die vom EuGH festgestellte Mitverantwortung der Seitenbetreiber erstreckt sich auf das jeweils geltende Recht, insbesondere auf die in der DS-GVO festgeschriebenen Rechte der Betroffenen und Pflichten der Verarbeiter.

Im Einzelnen ist Folgendes zu beachten:

- Wer eine Fanpage besucht, muss transparent und in verständlicher Form darüber informiert werden, welche Daten zu welchen Zwecken durch Facebook und die Fanpage-Betreiber verarbeitet werden. Dies gilt sowohl für Personen, die bei Facebook registriert sind, als auch für nicht registrierte Besucherinnen und Besucher des Netzwerks.

- Betreiber von Fanpages sollten sich selbst versichern, dass Facebook ihnen die Informationen zur Verfügung stellt, die zur Erfüllung der genannten Informationspflichten benötigt werden.

- Soweit Facebook Besucherinnen und Besucher einer Fanpage durch Erhebung personenbezogener Daten trackt, sei es durch den Einsatz von Cookies oder vergleichbarer Techniken oder durch die Speicherung der IP-Adresse, ist grundsätzlich eine Einwilligung der Nutzenden erforderlich, die die Anforderung der DS-GVO erfüllt.

– Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage-Betreibern ist in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtung der DS-GVO erfüllt. Diese Vereinbarung muss in wesentlichen Punkten den Betroffenen zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen können.

Für die Durchsetzung der Datenschutzvorgaben bei einer Fanpage ist die Aufsichtsbehörde zuständig, die für das jeweilige Unternehmen oder die Behörde zuständig ist, die die Fanpage betreibt. Die Durchsetzung der Datenschutzvorgaben im Verantwortungsbereich von Facebook selbst obliegt primär der irischen Datenschutzaufsicht im Rahmen der europäischen Zusammenarbeit.

Die deutschen Aufsichtsbehörden weisen darauf hin, dass nach dem Urteil des EuGHs dringender Handlungsbedarf für die Betreiber von Fanpages besteht. Dabei ist nicht zu verkennen, dass die Fanpage-Betreiber ihre datenschutzrechtliche Verantwortung nur erfüllen können, wenn Facebook selbst an der Lösung mitwirkt und ein datenschutzkonformes Produkt anbietet, das die Rechte der Betroffenen wahrt und einen ordnungsgemäßen Betrieb in Europa ermöglicht.

19.5 Beschluss der DSK zu Facebook Fanpages

(Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 5. September 2018)

Mit Urteil vom 5. Juni 2018 hat der Gerichtshof der Europäischen Union (EuGH), Aktenzeichen C-210/16, entschieden, dass eine gemeinsame Verantwortlichkeit von Facebook-Fanpage-Betreiberinnen und -Betreibern und Facebook besteht. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Entschließung vom 6. Juni 2018 deutlich gemacht, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen – insbesondere für die Betreiberinnen und Betreiber einer Fanpage – ergeben.

Bei einer gemeinsamen Verantwortlichkeit fordert die Datenschutzgrundverordnung (DSGVO) unter anderem eine Vereinbarung zwischen den Beteiligten, die klarstellt, wie die Pflichten aus der DSGVO erfüllt werden.

Seit dem Urteil des EuGHs sind drei Monate vergangen. Zwar hat Facebook einige Änderungen in seinem Angebot – zum Beispiel bezüglich der Cookies – vorgenommen, doch weiterhin werden auch bei Personen, die keine Facebook-Nutzerinnen und -Nutzer sind, Cookies mit Identifikatoren gesetzt, jedenfalls, wenn sie über die bloße Startseite einer Fanpage hinaus dort einen Inhalt aufrufen.

Auch werden nach wie vor die Fanpage-Besuche von Betroffenen nach bestimmten, teilweise voreingestellten Kriterien im Rahmen einer sogenannten Insights-Funktion von Facebook ausgewertet und den Betreiberinnen und Betreibern zur Verfügung gestellt.

Der EuGH hat unter anderem hervorgehoben, dass "die bei Facebook unterhaltenen Fanpages auch von Personen besucht werden können, die keine Facebook-Nutzer sind und somit nicht über ein Benutzerkonto bei diesem sozialen Netzwerk verfügen. In diesem Fall erscheint die Verantwortlichkeit des Betreibers der Fanpage hinsichtlich der Verarbeitung der personenbezogenen Daten dieser Personen noch höher, da das bloße Aufrufen der Fanpage durch Besucher automatisch die Verarbeitung ihrer personenbezogenen Daten auslöst."

Offizielle Verlautbarungen vonseiten Facebooks, ob und welche Schritte unternommen werden, um einen rechtskonformen Betrieb von Facebook-Fanpages zu ermöglichen, sind bisher ausgeblieben. Eine von Facebook noch im Juni 2018 angekündigte Vereinbarung nach Artikel 26 DSGVO (Gemeinsam für die Verarbeitung Verantwortliche) wurde bislang nicht zur Verfügung gestellt. Die deutschen Datenschutzaufsichtsbehörden wirken daher auf europäischer Ebene auf ein abgestimmtes Vorgehen gegenüber Facebook hin.

Auch Fanpage-Betreiberinnen und -Betreiber müssen sich ihrer datenschutzrechtlichen Verantwortung stellen. Ohne Vereinbarung nach Artikel 26 DSGVO ist der Betrieb einer Fanpage, wie sie derzeit von Facebook angeboten wird, rechtswidrig.

Daher fordert die DSK, dass nun die Anforderungen des Datenschutzrechts beim Betrieb von Fanpages erfüllt werden. Dazu gehört insbesondere, dass die gemeinsam Verantwortlichen Klarheit über die derzeitige Sachlage schaffen und die erforderlichen Informationen den betroffenen Personen (= Besucherinnen und Besucher der Fanpage) bereitstellen.

Eine gemeinsame Verantwortlichkeit bedeutet allerdings auch, dass Fanpage-Betreiberinnen und -Betreiber (unabhängig davon, ob es sich um öffentliche oder nicht öffentliche Verantwortliche handelt) die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und dies nachweisen können. Zudem können Betroffene ihre Rechte aus der DSGVO bei und gegenüber jedem Verantwortlichen geltend machen (Artikel 26 Absatz 3 DSGVO).

Insbesondere die im Anhang aufgeführten Fragen müssen deshalb sowohl von Facebook als auch und von Fanpage-Betreiberinnen und -Betreibern beantwortet werden können.

Anhang: Fragenkatalog

1. In welcher Art und Weise wird zwischen Ihnen und anderen gemeinsam Verantwortlichen festgelegt, wer von Ihnen welche Verpflichtung gemäß der DSGVO erfüllt? (Artikel 26 Absatz 1 DSGVO)

2. Auf Grundlage welcher Vereinbarung haben Sie untereinander festgelegt, wer welchen Informationspflichten nach Artikeln 13 und 14 DSGVO nachkommt?

3. Auf welche Weise werden die wesentlichen Aspekte dieser Vereinbarung den betroffenen Personen zur Verfügung gestellt?

4. Wie stellen Sie sicher, dass die Betroffenenrechte (Artikel 12 fortfolgende DSGVO) erfüllt werden können, insbesondere die Rechte auf Löschung nach Artikel 17 DSGVO, auf Einschränkung der Verarbeitung nach Artikel 18 DSGVO, auf Widerspruch nach Artikel 21 DSGVO und auf Auskunft nach Artikel 15 DSGVO?

5. Zu welchen Zwecken und auf welcher Rechtsgrundlage verarbeiten Sie die personenbezogenen Daten der Besucherinnen und Besucher von Fanpages? Welche personenbezogenen Daten werden gespeichert? Inwieweit werden aufgrund der Besuche von Facebook-Fanpages Profile erstellt oder angereichert? Werden auch personenbezogene Daten von Nicht-Facebook-Mitgliedern zur Erstellung von Profilen verwendet? Welche Löschfristen sind vorgesehen?

6. Zu welchen Zwecken und auf welcher Rechtsgrundlage werden beim Erstaufruf einer Fanpage auch bei Nicht-Mitgliedern Einträge im sogenannten Local Storage erzeugt?

7. Zu welchen Zwecken und auf welcher Rechtsgrundlage werden nach Aufruf einer Unterseite innerhalb des Fanpage-Angebots ein Session-Cookie und drei Cookies mit Lebenszeiten zwischen vier Monaten und zwei Jahren gespeichert?

8. Welche Maßnahmen haben Sie ergriffen, um Ihren Verpflichtungen aus Artikel 26 DSGVO als gemeinsam für die Verarbeitung Verantwortlicher gerecht zu werden und eine entsprechende Vereinbarung abzuschließen?

19.6 Der Vorschlag der EU-Kommission für eine E-Evidence-Verordnung führt zum Verlust von Betroffenenrechten und verschärft die Problematik der sogenannten Vorratsdatenspeicherung

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 7. November 2018)

Mit ihrem Vorschlag für eine E-Evidence-Verordnung (Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM (2018) 225 final)) möchte die EU-Kommission eine Alternative zum förmlichen Rechtshilfeverfahren schaffen und den Ermittlungsbehörden einen schnelleren Zugang zu Kommunikationsdaten ermöglichen. Die Strafverfolgungsbehörden der EU-Mitgliedstaaten sollen die Befugnis erhalten, Anbieter von Telekommunikations- und Internetdienstleistungen in anderen Mitgliedstaaten der Europäischen Union (EU) und auch in Staaten außerhalb der EU (Drittstaaten) unmittelbar zur Herausgabe von Bestands-, Zugangs-, Transaktions- und Inhaltsdaten zu verpflichten.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) weist hierzu auf die kritische Stellungnahme des Europäischen Datenschutzausschusses hin (https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-commission-proposals-european-production-and_de). Diese stellt bereits das Vorliegen einer Rechtsgrundlage in Frage. Mit Besorgnis sieht die DSK vor allem auch die vorgeschlagene Abkehr vom Grundsatz der doppelten beziehungsweise beiderseitigen Strafbarkeit.

Erstmals im Bereich der internationalen Zusammenarbeit in Strafsachen soll die Herausgabe von Daten nicht mehr davon abhängig sein, ob die verfolgte Tat dort, wo die Daten ersucht werden, überhaupt strafbar ist. Im Ergebnis könnten Unternehmen mit Sitz in Deutschland also zur Herausgabe von Daten an Ermittlungsbehörden in anderen EU-Mitgliedstaaten verpflichtet werden, obwohl die verfolgte Tat in Deutschland überhaupt keine Straftat ist. Das könnte zum Beispiel ein in Deutschland erlaubter Schwangerschaftsabbruch sein oder eine politische Meinungsäußerung, wenn diese im ersuchenden Staat strafbewehrt ist.

Zu befürchten ist hierbei auch, dass Drittstaaten die Regelung der EU als Blaupause für eigene Regelungen heranziehen werden. Provider in EU-Mitgliedstaaten würden sich dann vermehrt Herausgabeanordnungen von Drittstaaten ausgesetzt sehen, mit denen möglicherweise Straftaten aus einer völlig anderen Rechtstradition verfolgt werden.

Kritisch sieht die DSK auch, dass im Regelfall jegliche Information und Beteiligung der Justizbehörden des Staates, in dem der Provider seinen Sitz hat, unterbleibt und damit ein wichtiges verfahrensrechtliches Korrektiv fehlt. Ob die Rechtmäßigkeit eines Ersuchens

überprüft wird, hängt im vorgeschlagenen Verfahren ausschließlich vom Verhalten der Provider ab. Nur wenn sich das Unternehmen weigert, Daten zu übermitteln, muss der ersuchende Staat bei den Behörden vor Ort um Vollstreckungshilfe bitten. Nur dann können diese noch in das Verfahren eingreifen. Werden Daten herausgegeben, erlangen die zuständigen Justizbehörden hiervon jedoch keine Kenntnis. Der Vorschlag sieht keine Informationspflicht gegenüber den Behörden am Sitz des Unternehmens vor. Provider verfolgen aber in der Regel wirtschaftliche Interessen und unterliegen in ihren Entscheidungen anderen Verpflichtungen als die Justizbehörden Hierdurch werden Betroffene deutlich schlechter gestellt.

Provider als Adressaten eines Ersuchens sehen sich künftig nicht mehr den Justizbehörden des eigenen Staates gegenüber, sondern müssen sich mit den Behörden des anordnenden Staates auseinandersetzen. Den Betroffenen wiederum steht, wenn überhaupt, nur ein Rechtsbehelf im ersuchenden Mitgliedsstaat zu, dessen Rechtsordnung ihnen in der Regel aber fremd ist.

Ein besonderes Verfahren ist vorgesehen, wenn sich Provider mit Sitz in Drittstaaten darauf berufen, dass die angeordnete Übermittlung gegen das dortige Recht verstößt. Für diesen Fall sieht der Vorschlag eine gerichtliche Überprüfung im anordnenden Staat vor. Wenn das Gericht zu der Auffassung gelangt, dass tatsächlich ein Rechtskonflikt vorliegt, muss es die zuständigen Behörden im Zielstaat der Anordnung beteiligen. Das Ergebnis der Konsultation ist für das Gericht verbindlich. Diese Regelung ist ausdrücklich zu begrüßen. Denn auch hier wird eine Blaupause geschaffen für die Frage, welche Rechte europäische Unternehmen in der umgekehrten Situation haben sollten, wenn sie aus Drittstaaten auf der Grundlage von deren Gesetzen (wie zum Beispiel US-CLOUD-Act) zu einer Übermittlung verpflichtet werden und welche Verbindlichkeit eine Konsultation der zuständigen Behörden in Europa für Gerichte in Drittstaaten haben sollte.

Besonders kritisch ist jedoch, dass in Deutschland Telekommunikationsdienstleister verpflichtet sind, unter anderem sämtliche Verkehrsdaten für zehn Wochen zu speichern. Aus diesen Daten lassen sich genaue Schlüsse auf das Privatleben der Betroffenen, insbesondere deren Kontakt- und Interessenprofil ziehen. Die Problematik dieser sogenannten Vorratsdatenspeicherung verschärft sich deutlich, wenn ausländische Strafverfolgungsbehörden einen direkten Zugriff auf derartige Informationen erhalten.

Die DSK appelliert daher an alle im Gesetzgebungsverfahren Beteiligten, den Vorschlag für eine E-Evidence-Verordnung zu stoppen!

20. Die Europäische und die Internationale Datenschutzkonferenz

Die Entschließungen der Europäischen Datenschutzkonferenz des Jahres 2018 sind auf der Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit abrufbar[16]. Informationen und Entschließungen der 40. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre, welche am 23. Oktober 2018 in Brüssel stattgefunden hat, finden sich ebenfalls auf der Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit[17].

[16] https://www.bfdi.bund.de/DE/Infothek/Entschliessungen/EuDSK/_functions/EuDSK_table.html

[17] https://www.bfdi.bund.de/DE/Infothek/Entschliessungen/IntDSK/_functions/IntDSK_table.html