BREMISCHE BÜRGERSCHAFT **Drucksache 21/1699**
Landtag 16.03.2026
21. Wahlperiode

Bericht des Landesbeauftragten für Datenschutz

8. Jahresbericht des Landesbeauftragten für Datenschutz nach der Europäischen Datenschutzgrundverordnung

Ich übersende den 8. Jahresbericht für Datenschutz nach der Europäischen Datenschutzgrundverordnung, Berichtsjahr 2025, in der Anlage.

Dr. Timo Utermark

Der Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen

8. Jahresbericht
des Landesbeauftragten für Datenschutz
nach der Europäischen Datenschutzgrundverordnung

Vorwort

Hiermit erstatte ich der Bremischen Bürgerschaft (Landtag) und dem Präsidenten des Senates meinen Bericht im Sinne des Artikels 59 der Europäischen Datenschutzgrundverordnung über das
Ergebnis der Tätigkeit im Jahr 2025. Redaktionsschluss war der 31. Dezember 2025.

Meinen Kolleginnen und Kollegen in der Dienststelle des Landesbeauftragten für Datenschutz und Informationsfreiheit, die mit außerordentlich großem Engagement und Einsatz an der Erstellung dieses Berichtes mitgewirkt haben, danke ich herzlich für Ihren unverzichtbaren Beitrag.

Bremerhaven, den 16. März 2026

Dr. Timo Utermark

Der Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

Inhaltsverzeichnis

1. Relevante Entwicklungen

Das Berichtsjahr war vor allem von der Diskussion geprägt, ob die Datenschutzaufsichtsbehörden der Länder im Bereich der nicht öffentlichen Stellen für die Aufsicht weiterhin zuständig bleiben sollten oder nicht. Um die Frage zu beantworten, ob die Betroffenen zutreffende, ihre Situation vor Ort in den Blick nehmende und für alle Rechtsbereiche auf einander abgestimmte Antworten durch die Datenschutzaufsichtsbehörden erhalten, kommt deren Organisation eine zentrale Bedeutung zu. Dabei zeigt sich sowohl bei den Fragen, ob und wie Kompetenzen bei der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Bezug auf die nicht öffentlichen Stellen zentralisiert werden können, als auch bei der Frage, wie die KI-Verordnung[1], der Data-Act[2] und die Verordnung über die Transparenz und das Targeting politischer Werbung[3] umgesetzt werden, dass bei allen diesen Fragen eine föderale Antwort den Bedürfnissen der regionalen Wirtschaft Deutschlands sowie einem effektiven Datenschutz am besten gerecht wird. Insbesondere im Bereich des Datenschutzes führen zentralstaatliche Ideen letztlich in die Irre. Der Vorteil eines föderalen Staatsaufbaus zeigt sich gerade auch darin, dass er einzelnen Ländern ermöglicht, Vorreiter in bestimmten Gebieten zu sein.

Auch in einem weiteren aus datenschutzpolitischer Sicht drängenden Problem, nämlich der Frage, wie die digitale Souveränität wieder erlangt werden kann, kommt der Einsicht, dass nur föderale Lösungen in Deutschland gelingen werden, eine entscheidende Bedeutung zu. Denn auch hier braucht es föderale Vorreiter. Dementsprechend sollte die Freie Hansestadt Bremen von ihrer föderalen Eigenständigkeit auch im Interesse des Grundrechtsschutzes der Bürgerinnen und Bürger Gebrauch machen und die digitale Souveränität im Bereich der Verwaltung vorantreiben.

Neben diesen, den Staat betreffenden, Fragen kam im Berichtsjahr ebenfalls der Entwicklung des Verhältnisses der neuen KI-Regulierung zur Datenschutzgrundverordnung eine zentrale Bedeutung zu. Dies zeigt sich beispielsweise bei dem Training von KI-Systemen durch große Konzerne der Internetwirtschaft.

---

[1] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12. Juli 2024).

[2] Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung) (ABl. L, 2023/2854, 22. Dezember 2023).

[3] Verordnung (EU) des Europäischen Parlaments und des Rates vom 13. März 2024 über die Transparenz und das Targeting politischer Werbung (ABl. L, 2024/900, 20. März 2024).

1.1 Diskussion um die Reform der datenschutzrechtlichen Aufsicht

In dem Koalitionsvertrag „Verantwortung für Deutschland“ haben die CDU/CSU und die SPD „im Interesse der Wirtschaft“ eine Reform der Datenschutzaufsicht sowie deren Bündelung bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vereinbart. Sollte die Aufsicht über die nicht öffentlichen Stellen, einschließlich „der Wirtschaft“, in großem Umfang auf die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit übertragen werden, würde dies eine tiefgreifende Neustrukturierung der Datenschutzaufsicht in Deutschland beinhalten.

Gemäß § 40 Absatz 1 Bundesdatenschutzgesetz (BDSG) liegt die Datenschutzaufsicht über nicht öffentliche Stellen nach der geltenden Gesetzeslage grundsätzlich bei den nach Landesrecht zuständigen Behörden, also in der Freien Hansestadt Bremen bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit. Gegenwärtig hat die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit lediglich über einen kleinen Teil der Wirtschaft, wie Telekommunikations- und Postdienstunternehmen sowie private Unternehmen, die unter das
Sicherheitsüberprüfungsgesetz fallen, eine datenschutzrechtliche Aufsichtszuständigkeit.

Die Landesdatenschutzbeauftragten haben sich bereits während der laufenden Koalitionsverhandlungen gegen eine weitgehende Zentralisierung der Datenschutzaufsicht gewandt. In einer Pressemitteilung vom 26. März 2025 wiesen sie darauf hin, dass gerade die kleinen und mittelständischen Unternehmen sowie Freiberuflerinnen und Freiberufler von einer regional verankerten Datenschutzaufsichtsbehörde profitierten, wie sie gegenwärtig existiere. Kleine und mittelständische Unternehmen sowie Freiberuflerinnen und Freiberufler stellten nämlich 99,2 % der Unternehmen Deutschlands. Die Datenschutzaufsicht müsse sich gerade an diesen Unternehmen ausrichten und daher föderal strukturiert bleiben.

Überdies sei eine Zentralisierung kein Beitrag zu einem Bürokratieabbau. Es müsse vielmehr eine neue Bundesbehörde aufgebaut werden, für die zusätzlich neue Mitarbeiterinnen und Mitarbeiter rekrutiert werden müssten. Dies haben erste Schätzungen in der Folgezeit bestätigt. Es würden nämlich voraussichtlich ungefähr 450 Planstellen zusätzlich auf Bundesebene benötigt, um die circa 70.000 Beschwerden jährlich zu bearbeiten, für die die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit im Falle einer Zentralisierung der Zuständigkeit für die nicht öffentlichen Stellen dann zuständig werden würde. Die Personal- und Sachkosten würden sich auf einen hohen zweistelligen Millionenbetrag belaufen.

Aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit führt der Machtzuwachs bei der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zudem zu einer zu großen institutionellen Machtfülle in einer Person. Das gegenwärtige

föderale System gewährleistet dagegen durch seinen Zwang, Kompromisse zu finden und sie wechselseitig abzustimmen, in einem hohen Maße, dass einerseits den Belangen eines effektiven Schutzes des Grundrechtes auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 Grundgesetz (GG) in Verbindung mit Artikel 1 Absatz 1 GG Rechnung getragen wird und andererseits sich in einer einzelnen Datenschutzaufsichtsbehörde keine zu große Machtfülle konzentriert.

Darüber hinaus stellt sich die Frage, ob eine weitgehende Zentralisierung der Kompetenzen der Datenschutzaufsicht über die nicht öffentlichen Stellen bei der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit rechtlich zulässig wäre.

Es bestehen zunächst europarechtliche Bedenken gegen eine umfassende Zentralisierung der Datenschutzaufsicht bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit noch in dieser Legislaturperiode. Zwar gibt die Datenschutzgrundverordnung (DSGVO) den Mitgliedstaaten nicht vor, wie sie ihre Datenschutzaufsicht organisieren; es kann eine oder auch mehrere Datenschutzaufsichtsbehörden geben. Doch sind die allgemeinen Vorgaben der Datenschutzgrundverordnung zu beachten. Insbesondere müsste im Rahmen einer Zentralisierung der Datenschutzaufsicht die Unabhängigkeit der bisherigen Datenschutzaufsichtsbehörden gewahrt werden. Der Europäische Gerichtshof hat in seinem Urteil vom 8. April 2014 (Aktenzeichen C-288/12) festgestellt, dass die Unabhängigkeit der Datenschutzaufsichtsbehörden verletzt würde, wenn das Mandat für Mitglieder einer Aufsichtsbehörde für den Schutz personenbezogener Daten vor dem Ablauf der regulären Amtszeit beendet werden würde. Wenn eine Datenschutzaufsichtsbehörde befürchten müsste, dass die Amtszeit der Mitglieder vorzeitig beendet würde, könnte – indem eine implizite Drohung über der Amtsausübung schwebte – nämlich die Unabhängigkeit in der Führung der Amtsgeschäfte faktisch beeinträchtigt werden. Auch wenn die Entscheidung noch zur alten Datenschutzrichtlinie ergangen ist, können die Erwägungen auf die Datenschutzgrundverordnung übertragen werden, weil die Unabhängigkeit der Datenschutzaufsichtsbehörden durch Artikel 52 Absatz 1 DSGVO ebenfalls vollständig gewährleistet ist. Zudem müsste eine Zentralisierung der Datenschutzaufsicht bei der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auch den Anforderungen genügen, die sich aus Artikel 87 Absatz 3 GG ergeben. Dieser sieht zwei unterschiedliche Erlaubnistatbestände vor, Bundesbehörden einzurichten, wobei die erste Möglichkeit, eine Bundesbehörde einzurichten, gemäß Artikel 87 Absatz 3 Satz 1 GG eines Einspruchsgesetzes und die zweite Möglichkeit gemäß Artikel 87 Absatz 3 Satz 2 GG eines Zustimmungsgesetzes bedarf, dem überdies die Mehrheit der Mitglieder des Bundestages zustimmen muss. Da gegenwärtig die genaue Ausgestaltung der Behörde der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für den Fall, dass bei ihm oder ihr die Aufsicht über die nicht öffentlichen Stellen zentralisiert würde, nicht konkretisiert ist, kann nicht abgeschätzt werden, ob die Voraussetzungen einer dieser beiden Alternativen im Falle einer Zentralisierung eingehalten werden würden.

Ungeachtet dieser Bedenken, die einer Zentralisierung der Datenschutzaufsicht über die nicht öffentlichen Stellen entgegenstehen, teilen die Datenschutzaufsichtsbehörden der Länder das Ziel, die Rechtssicherheit in Deutschland durch eine einheitlichere Anwendung der Datenschutzgrundverordnung zu erhöhen, ohne dass zusätzliche Bürokratie entsteht. Um dieses Ziel zu erreichen, haben Datenschutzaufsichtsbehörden der Länder Vorschläge zur Reform der Datenschutzaufsicht entwickelt. Diese beinhalten:

1. Eine Datenschutzaufsichtsbehörde als Ansprechpartnerin für Unternehmen und Forschende: Zentrale Zuständigkeit einer Datenschutzaufsichtsbehörde bei länderübergreifenden Sachverhalten, zum Beispiel bei Forschungsprojekten oder bei Konzernen mit mehreren Standorten.

2. Effiziente Arbeitsteilung durch Ausweitung des Eine-für-Alle-Prinzips auf die Datenschutzaufsichtsbehörden: Das Ergebnis der Prüfung von länderübergreifend oder bundesweit eingesetzten Verfahren durch eine Landesbehörde bindet die anderen Behörden.

3. Eine starke Stimme, die einheitlich entscheidet: Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes oder der Länder (Datenschutzkonferenz), in der die Datenschutzaufsichtsbehörden von Ländern und Bund vertreten sind, institutionalisieren und mit einer Geschäftsstelle zum gemeinsamen Entscheidungsgremium von Bund und Ländern formen. Rechtssicherheit durch verbindliche Mehrheitsentscheidungen in der Datenschutzkonferenz schaffen.

In die weitere Diskussion haben sich die Landesdatenschutzbeauftragten eingebracht und Vorschläge zur Bündelung und Optimierung der operativen Standards in der Datenschutzaufsicht entwickelt. Um eine Landesbehörde als Ansprechpartnerin für Unternehmen und Forschende zu schaffen, halten sie es beispielsweise im nicht öffentlichen Bereich für sinnvoll, dass bei länderübergreifenden Datenverarbeitungen durch verbundene Unternehmen oder bei Forschungsvorhaben, die Daten länderübergreifend verarbeiten, nach einer Anzeige die Zuständigkeit bei einer Datenschutzaufsichtsbehörde nur eines Landes gebündelt wird. Durch diesen nationalen „One-Stop-Shop“ würden die Zuständigkeiten damit bei einer Aufsichtsbehörde zusammengeführt.

Im Rahmen des Einer-für-Alle-Prinzips werben die Landesdatenschutzbeauftragten für eine höhere Verbindlichkeit der Prüfergebnisse der zuständigen Datenschutzaufsichtsbehörde. Soweit die zuständige Datenschutzaufsichtsbehörde ein Verfahren oder System zur Verarbeitung personenbezogener Daten geprüft hat, soll diese datenschutzrechtliche Bewertung nach Vorstellung der Landesdatenschutzbeauftragten zukünftig die anderen Datenschutzaufsichtsbehörden binden, sofern es nicht zu wesentlichen Änderungen am Verfahren oder System kommt. Im Interesse der Wirtschaft sollte gesetzlich eine bindende Übernahme der Prüfergeb-

nisse erfolgen. Demgegenüber sieht das Onlinezugangsgesetz für öffentliche Verwaltungsleistungen bislang nur vor, dass ein entwickelter digitaler Prozess von anderen nachgenutzt werden kann.

Schließlich wird in die Diskussion seitens der Landesdatenschutzbeauftragten eingebracht, dass die Datenschutzkonferenz institutionalisiert werden, sich eine Geschäftsordnung geben und eine Geschäftsstelle erhalten sollte, die bei der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit angesiedelt werden sollte. Bei der Geschäftsstelle könnte auch ein gemeinsames Meldeportal der unterschiedlichen Datenschutzaufsichtsbehörden der Länder für Betroffene, Verantwortliche und Auftragsverarbeiter eingerichtet werden, an das Beschwerden oder Meldungen von Datenschutzverletzungen nach Artikel 33 DSGVO gerichtet werden könnten. Durch ein solches Portal würden Zweifel über die zuständige Behörde bei Unternehmen, aber auch bei Bürgerinnen und Bürgern entfallen.

Die Vorschläge der Datenschutzaufsichtsbehörden der Länder gewährleisten besser als eine Zentralisierung, dass eine effektive, bundesweit einheitliche Datenschutzaufsicht geschaffen wird und die gegenwärtige Nähe der Datenschutzaufsichtsbehörden zur regionalen Wirtschaft erhalten bleibt, wie dies eine Bundesbehörde so nicht erreichen könnte. Zudem würde eine gespaltene Datenschutzaufsicht zwischen dem öffentlichen Bereich und dem nicht öffentlichen Bereich, die in Deutschland bis auf im Freistaat Bayern bisher nicht besteht, vermieden, die ebenfalls einer effektiven und einheitlichen Datenschutzaufsicht entgegenstehen könnte.

Neben dieser Strukturänderung beabsichtigt die neue Koalition auf Bundesebene, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in die Bundesbeauftragte für Datennutzung, Datenschutz und Informationsfreiheit umzubenennen. Die Datenschutzgrundverordnung sieht zwar vor, dass die Datenschutzaufsichtsbehörden auch die Aufgabe haben, mit der Überwachung der Datenschutzgrundverordnung den freien Verkehr von personenbezogenen Daten zu ermöglichen (Artikel 51 Absatz 1 DSGVO). Entsprechend der Rechtsprechung des Europäischen Gerichtshofes, wie sie bereits zur Datenschutzrichtlinie ergangen ist, dient das europäische Datenschutzrecht aber dazu, einen möglichst hohen Datenschutz zu gewährleisten. Die Datennutzung wird auf der Grundlage dieses hohen Schutzniveaus gewährleistet, das durch den nationalen Gesetzgeber nicht verringert werden kann (Europäischer Gerichtshof, Urteil vom 6. November 2003, Aktenzeichen C-101/01, Randnummer 96). Mit dem Verweis darauf, dass die Datennutzung verbessert werden muss, kann daher kein geringeres datenschutzrechtliches Schutzniveau begründet werden. Die Umbenennung weckt vor diesem Hintergrund Erwartungen, die nicht erfüllt werden können.

1.2 Verhältnis Künstliche Intelligenz und Datenschutz

1.2.1 Training von Systemen der Künstlichen Intelligenz

Das Zusammenspiel zwischen der Datenschutzgrundverordnung (DSGVO) und der KI-Verordnung bildete im Berichtsjahr eine zentrale Fragestellung. Dass die KI-Verordnung den Schutz der personenbezogenen Daten durch die Datenschutzgrundverordnung nicht einschränkt, wird in Erwägungsgrund 10 KI-Verordnung hervorgehoben. Dieser lautet:

> „Das Grundrecht auf Schutz personenbezogener Daten wird insbesondere durch die Verordnung (EU) 2016/679 […] gewahrt. […] Diese Verordnung [gemeint ist die KI-Verordnung] soll die Anwendung des bestehenden Unionsrechts zur Verarbeitung personenbezogener Daten, einschließlich der Aufgaben und Befugnisse unabhängiger Aufsichtsbehörden, die für die Überwachung und Einhaltung dieser Instrumente zuständig sind, nicht berühren. Sie lässt ferner die Pflichten der Anbieter und Betreiber von KI-Systemen […], die sich aus dem Unionsrecht [...] über den Schutz personenbezogener Daten ergeben, unberührt, soweit die Konzeption, die Entwicklung oder die Verwendung von KI-Systemen die Verarbeitung personenbezogener Daten umfasst. […]“

Dieser fortbestehende umfassende Schutz der personenbezogenen Daten durch die Datenschutzgrundverordnung muss nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit sowohl bei der Bewertung einzelner Konfliktlagen, etwa im Zusammenhang mit dem Training von Systemen der Künstlichen Intelligenz (KI), als auch bei der Ausgestaltung der Aufsichtsstruktur durch ein Ausführungsgesetz zur KI-Verordnung beachtet werden.

Anlässlich der Ankündigung des Meta-Konzerns mit Pressemitteilung vom 14. April 2025, die Daten ihrer volljährigen Nutzerinnen und Nutzer, die diese bei Facebook und Instagram öffentlich zugänglich gemacht haben, für das Training einer generativen Künstlichen Intelligenz zu verwenden, ist die datenschutzrechtliche Zulässigkeit dieses Vorgehens in den Fokus einer breiteren Öffentlichkeit getreten. Meta berief sich für die Datenverarbeitung im Rahmen des Trainings auf die Rechtsgrundlage des berechtigten Interesses nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f) DSGVO.

In einem Rechtsstreit, in dem die Verbraucherzentrale Nordrhein-Westfalen nach dem Unterlassungsklagengesetz Meta darauf in Anspruch genommen hat, die Verarbeitung dieser Trainingsdaten zu unterlassen, hat das Oberlandesgericht Köln auf der Grundlage einer summarischen Prüfung bestätigt, dass sich Meta auf diese Rechtsgrundlage stützen könne (Oberlandesgericht Köln, Urteil vom 23. Mai 2025, 15 UKl 2/25). Es gelangte in seiner Begründung zu dem Ergebnis, dass die „als sehr bedeutsam einzuschätzende[n] Interessen [von Meta] am

Training der KI“ überwögen, und stützte sich zur Begründung insbesondere unter Verweis auf Erwägungsgrund 8 KI-Verordnung auch darauf, dass der Europäische Gesetzgeber in der KI-Verordnung dem Ziel hohes Gewicht eingeräumt habe, dass Europa bei der Entwicklung einer vertrauensvollen, sicheren und ethisch vertretbaren Künstlichen Intelligenz eine Führungsrolle einnehmen solle (Oberlandesgericht Köln, am angeführten Ort, Randnummer 100).

Diese Argumentation lässt aber außer Acht, dass die KI-Verordnung den Schutz der personenbezogenen Daten durch die Datenschutzgrundverordnung gerade unberührt lässt. Würde die Entwicklung von KI-Systemen, selbst bei Großkonzernen, als ein berechtigtes Interesse von einem solchen Gewicht anerkannt werden, dass die datenschutzrechtlichen Belange der Bürgerinnen und Bürger, wie in dem vom Oberlandesgericht Köln entschiedenen Fall, zurücktreten müssen, führte dies im Ergebnis dazu, dass die datenschutzrechtlichen Garantien der Datenschutzgrundverordnung durch einen zu weit gefassten Anwendungsbereich der Rechtsgrundlage des Artikels 6 Absatz 1 Unterabsatz Buchstabe f) DSGVO unterlaufen werden würden.

Im Ergebnis schließt dies nicht aus, dass auch das Training von KI-Systemen auf die Annahme von berechtigten Interessen in einzelnen Fällen als Rechtsgrundlage gestützt werden kann (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f) DSGVO). Allerdings setzt dies eine umfassende Interessenabwägung des Einzelfalls voraus, wobei in der Abwägung zu Lasten der Annahme berechtigter Interessen berücksichtigt werden muss, dass Sprachmodelle und andere generative KI-Systeme unter Umständen personenbezogene Daten wiedergeben, mit denen sie trainiert worden sind. Auf der anderen Seite sind wirtschaftsfördernde Aspekte bei kleinen und mittelständischen Unternehmen zu berücksichtigen, die dafürsprechen können, dass diese sich auf die Rechtsgrundlage der berechtigten Interessen im Sinne des Artikels 6 Absatz 1 Unterabsatz 1 Buchstabe f) DSGVO unter Umständen berufen dürfen, um personenbezogene Daten für das Trainieren von Künstlicher Intelligenz zu verarbeiten. Die KI-Verordnung betont nämlich die wirtschaftlichen Entfaltungsmöglichkeiten von kleinen und mittelständischen Unternehmen in besonderer Weise.

1.2.2 Umsetzung der KI-Verordnung in Deutschland

Welche Bedeutung dem Datenschutz im Zusammenhang mit Systemen der Künstlichen Intelligenz (KI) zukünftig zukommen wird, wird auch durch die Aufsichtsstruktur für KI-Systeme in Deutschland mitbestimmt. Das Bundesministerium für Digitales und Staatsmodernisierung hat am 11. September 2025 einen Referentenentwurf für ein Gesetz zur Durchführung der KI-Verordnung vorgelegt.

§ 2 Absatz 1 dieses Gesetzesentwurfes zur Durchführung der KI-Verordnung sieht vor, dass die Bundesnetzagentur im Grundsatz die zuständige Marktüberwachungsbehörde sein soll.

Selbst für die Hochrisiko-KI-Systeme, für die Artikel 74 Absatz 8 KI-Verordnung eine besondere Regelung hinsichtlich einer zuständigen Marktüberwachungsbehörde trifft, bestimmt § 3 Absatz 5 des Gesetzesentwurfes zur Durchführung der KI-Verordnung, dass bei der Bundesnetzagentur eine Unabhängige KI-Marktüberwachungskammer eingerichtet werden soll. Die Aufgaben dieser besonderen Marktüberwachungskammer sollen die Präsidentin oder der Präsident der Bundesnetzagentur sowie deren oder dessen beiden Vizepräsidentinnen beziehungsweise Vizepräsidenten neben ihren sonstigen Aufgaben wahrnehmen (§ 4 Absatz 1 des Gesetzesentwurfes zur Durchführung der KI-Verordnung). Nach Artikel 74 Absatz 8 KI-Verordnung muss als Marktüberwachungsbehörde demgegenüber entweder die Datenschutzaufsichtsbehörde nach der Datenschutzgrundverordnung oder der JI-Richtlinie[4] benannt werden.

Nach § 13 Absatz 1 des Gesetzesentwurfes zur Durchführung der KI-Verordnung soll zumindest ein KI-Reallabor nach Artikel 57 und Artikel 58 KI-Verordnung durch die Bundesnetzagentur betrieben werden, wobei die Einrichtung anderer KI-Reallabore hiervon unberührt bleibt. Die KI-Reallabore bieten eine kontrollierte Umgebung, um die Entwicklung, das Training, das Testen und die Validierung innovativer KI-Systeme für einen begrenzten Zeitraum vor Inverkehrbringen oder Inbetriebnahme nach einem KI-Reallabor-Plan zu erleichtern. In den KI-Reallaboren können auch Tests unter Realbedingungen durchgeführt werden (Artikel 57 Absatz 4 KI-Verordnung). Diese KI-Reallabore sind für kleine und mittelständische Unternehmen von erheblicher Bedeutung, weil ihre Einbindung nach Artikel 57 Absatz 12 KI-Verordnung zu einer Befreiung von Bußgeldern führen kann. Ebenso wird gemäß Artikel 57 Absatz 7 KI-Verordnung nach einem erfolgreichen Abschluss des KI-Reallabors die Konformität angenommen, wonach das KI-System mit der KI-Verordnung konform sei. Hierüber ist dem Anbieter des KI-Systems von der Behörde ein schriftlicher Nachweis auszustellen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz), der auch der Landesbeauftragte für Datenschutz und Informationsfreiheit angehört, hat zu diesem Gesetzesentwurf kritisch Stellung genommen. Insbesondere die Zuweisung der Zuständigkeit als Marktüberwachungsbehörde für Hochrisiko-KI-Systeme an eine unabhängige Marktüberwachungskammer der Bundesnetzagentur verstößt nach der Stellungnahme gegen Artikel 74 Absatz 8 KI-Verordnung, weil Artikel 74 Absatz 8 KI-Verordnung einen sehr engen Zusammenhang zwischen der Datenschutzaufsicht nach der Datenschutzgrundverordnung und der JI-Richtlinie und der Marktaufsichtsbehörde nach Artikel 74

[4] 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 (ABl. L 119 Seite 89, berichtigt 2018 L 127 Seite 9 und 2021 L 74 Seite 36).

Absatz 8 KI-Verordnung herstellt. Dies gewährleistet die organisatorische Anbindung an die Bundesnetzagentur nicht.

Überdies greift nach Auffassung der Datenschutzkonferenz die nahezu umfassende Zuweisung der Marktüberwachungskompetenz über KI-Systeme in die föderale Kompetenzordnung ein und verstößt damit in Teilen gegen Artikel 87 Absatz 3 Satz 1 Grundgesetz, weil der Bund nur für Bereiche, in denen ihm die Gesetzgebungskompetenz zusteht, auch selbständige Bundesbehörden errichten darf. Nach dem Gesetzesentwurf zur Durchführung der KI-Verordnung würde die Bundesnetzagentur aber auch für KI-Systeme bei der Polizei oder den Schulen zuständig sein. Hierbei handelt es sich um Gebiete, die in die Verwaltungskompetenz der Länder fallen. Da die KI-Systeme eine große Bedeutung auch für diese Teile der Länderverwaltung spielen, besteht die Gefahr, dass die Autonomie der Länder durch eine Bundesaufsicht in einem beachtlichen Umfang eingeschränkt würde, wenn das Gesetz in der geplanten Form in Kraft träte.

Schließlich drängt die Datenschutzkonferenz auf eine Klarstellung, dass auch die Landesdatenschutzbeauftragten KI-Reallabore mit einem datenschutzrechtlichen Fokus einrichten und betreiben können. Eine solche Klarstellung ist notwendig, weil die Zulassung des Betriebes von KI-Reallaboren durch andere Behörden als der Bundesnetzagentur so ausgelegt werden kann, dass dies möglicherweise zukünftig nicht zulässig ist. Gerade KI-Reallabore in der Fläche sind aber notwendig, um Innovationsförderung bei der regional geprägten deutschen Wirtschaft auch im Bereich der KI-Systeme zu gewährleisten.

Insgesamt zeigt sich aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit, dass die Zuweisung der Aufsichtszuständigkeiten an die Bundesnetzagentur statt an die Datenschutzaufsichtsbehörden zu einer weiteren Zersplitterung der Datenschutzaufsicht im Digitalbereich führt. Insofern ist grundlegende Kritik an dem Entwurf zu üben. Neben den Datenschutzaufsichtsbehörden ist dann auch die Bundesnetzagentur für weite Teile des Digitalrechtes zuständig. Es ist nicht zu erwarten, dass diese Vorschläge zu einer in sich stimmigen Aufsichtspraxis in Bezug auf die digitale Wirtschaft führen werden, und zwar unabhängig davon, ob die Zuständigkeit für die Datenschutzaufsicht über den nicht öffentlichen Bereich bei der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zentralisiert wird oder nicht.

1.3 Zuständigkeit nach dem Data Act und der Verordnung über die Transparenz und das Targeting politischer Werbung

Am 12. September 2025 ist der Data Act in Kraft getreten. Mit diesem ergeben sich zunächst neue Zuständigkeiten für den Landesbeauftragten für Datenschutz und Informationsfreiheit. Die europäische Verordnung enthält harmonisierte Vorschriften über die Verfügbarkeit von Produktdaten und verbundenen Dienstdaten (Artikel 1 Absatz 1 Data Act). Sie gibt Nutzerinnen und Nutzern von vernetzten Produkten ein Zugangsrecht zu den Daten, die sie generieren, und regelt die Voraussetzungen dafür, wann Unternehmen diese Daten untereinander austauschen müssen. Vernetzte Produkte sind Gegenstände, die Daten über ihre Nutzung oder Umgebung mittels eines Kommunikationsdienstes beispielsweise an das Internet übermitteln können (Artikel 2 Nummer 5 Data Act). Die Anwendungsbeispiele reichen von smarten Haushaltsgeräten bis zu vernetzten Industriemaschinen und -anlagen. Vernetzte Dienste sind diejenigen Dienste, die mit vernetzten Produkten so verbunden sind, dass diese nur mit Hilfe dieser vernetzten Dienste ihre Funktionen ausfüllen können (Artikel 2 Nummer 6 Data Act). Dies ist beispielsweise eine App, mit deren Hilfe Sportaktivitäten aufgezeichnet und ausgewertet werden. Der Data Act lässt dabei den Schutz personenbezogener Daten, wie er durch die Datenschutzgrundverordnung gewährleistet wird, unberührt und tritt daher, soweit es zu Kollisionen kommt, hinter der Datenschutzgrundverordnung zurück (Artikel 1 Absatz 5 Data Act).

Neben der Möglichkeit, Ansprüche aus dem Data Act, soweit sie zivilrechtlicher Natur sind, vor den Zivilgerichten geltend zu machen, oder eine Streitbeilegung unter den Voraussetzungen des Artikel 10 Data Act durchzuführen, sieht Artikel 38 Data Act auch ein Beschwerderecht vor. Soweit die Datenschutzaufsichtsbehörden in diesem Zusammenhang über den Schutz personenbezogener Daten zu entscheiden haben, sind die Datenschutzaufsichtsbehörden insofern zuständig (Artikel 37 Absatz 3 Data Act). Dies führt, weil gegenwärtig kein Ausführungsgesetz des Bundes vorliegt, dazu, dass der Landesbeauftragte für Datenschutz und Informationsfreiheit diese Zuständigkeit in der Freien Hansestadt Bremen nunmehr als zusätzliche Aufgabe wahrzunehmen hat. Soweit auch für diese Zuständigkeit im Bereich des Data Acts bei der Behörde der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit eine Bündelung erfolgen soll, führt dies nicht zu einer Vereinfachung, sondern würde zu einer weiteren Zersplitterung der Datenschutzaufsicht führen.

Zusätzliche Zuständigkeiten ergeben sich auch aus der Verordnung über die Transparenz und das Targeting politischer Werbung (TTPW-VO), die seit dem 10. Oktober 2025 gilt. Gegenstand der Verordnung über die Transparenz und das Targeting politischer Werbung sind insbesondere Transparenz- und Sorgfaltspflichten für die Erbringung politischer Werbung sowie Vorschriften über den Einsatz von Targeting- und Anzeigenschaltungsverfahren, die die Verarbeitung personenbezogener Daten bei politischer Online-Werbung umfassen (Artikel 1

Absatz 1 TTPW-VO). Zudem sind in der Verordnung Regelungen über ihre Überwachung und Durchsetzung, einschließlich der hierfür erforderlichen Zusammenarbeit und Koordinierung der zuständigen Behörden, enthalten.

Mit dem Inkrafttreten dieser Verordnung ist der Landesbeauftragte für Datenschutz und Informationsfreiheit nach Artikel 22 Absatz 1 TTPW-VO dafür zuständig geworden, die Anwendung von Artikel 18 TTPW-VO und Artikel 19 TTPW-VO zu überwachen. Artikel 18 TTPW-VO und Artikel 19 TTPW-VO regeln die speziellen Anforderungen in Bezug auf das Targeting und die Anzeigenschaltung im Zusammenhang mit politischer Werbung im Internet, wenn diese eine Verarbeitung personenbezogener Daten umfassen. Zudem wird der Landesbeauftragte für Datenschutz und Informationsfreiheit voraussichtlich die Zuständigkeit für die Überwachung von Artikel 20 TTPW-VO erhalten. Artikel 20 TTPW-VO enthält eine ausdrückliche Übermittlungspflicht, die in engem Zusammenhang mit der bereits durch die Datenschutzaufsichtsbehörden zu überwachenden Vorgaben des Artikels 19 TTPW-VO steht. Aus Gründen der Sachgerechtigkeit erscheint es daher konsequent, dass auch die Kontrolle der Anwendung von Artikel 20 TTPW-VO durch den Landesbeauftragten für Datenschutz und Informationsfreiheit wahrgenommen wird. Dieser geht weiterhin davon aus, dass der Bundesgesetzgeber die Zuständigkeit für die Überwachung dieses Artikels nicht gesondert für die Landesdatenschutzbehörden regeln wird. Daher begrüßt er, dass für die Freie Hansestadt Bremen die Aufnahme einer entsprechenden Zuständigkeitsregelung in das Bremische Ausführungsgesetz zur EU-Datenschutz-Grundverordnung in die Wege geleitet werden soll.

1.4 Digitale Souveränität

Die Bedeutung der digitalen Souveränität, um die Digitalisierung in der Freien Hansestadt Bremen zukunftsfest zu gestalten, wird von allen politischen Kräften in der Bremischen Bürgerschaft anerkannt. In der Koalitionsvereinbarung „Veränderung gestalten: sicher, sozial, ökologisch, zukunftsfest“ wurde für die laufende Legislaturperiode das Ziel benannt, die Digitalisierung in der Freien Hansestadt Bremen unter anderem im Sinne der digitalen Souveränität zu gestalten. Die digitale Souveränität müsse eine „Leitidee bei der Planung und Beschaffung von IT-Infrastruktur“ sein. Die oppositionelle Fraktion der CDU betont ebenfalls in einer Vorbemerkung zu ihrer Kleinen Anfrage „Open Source Software und digitale Souveränität in der bremischen Verwaltung“ (Bremische Bürgerschaft Drucksache 21/1160), dass es sich bei der digitalen Souveränität um ein zentrales Thema für eine moderne IT-Strategie der Freien Hansestadt Bremen handele.

Auch der Senat der Freien Hansestadt Bremen bekennt sich ausdrücklich zu dem Ziel, die IT digital souveräner aufzustellen. In seiner Antwort auf die erwähnte Kleine Anfrage zur digitalen Souveränität in der bremischen Verwaltung (Bremische Bürgerschaft Drucksache 21/1225)

erklärte der Senat, dass er trotz der am 6. August 2024 beschlossenen Microsoft-Office-Beschaffung an dem Ziel festhalte, die Abhängigkeit von Software-Anbietern, wie Microsoft, langfristig zu reduzieren und die digitale Souveränität der Verwaltung zu stärken. Dazu solle die Open-Source-basierte Alternative openDesk, die unter anderem auf Basis der dPhoenixSuite entwickelt wird, unterstützt und ihre Einsatzfähigkeit bis zum Jahr 2029 in der bremischen Verwaltung erneut geprüft werden. Der Senat hält damit an seinem Beschluss vom 6. August 2024 fest, ein Migrationskonzept für die Komplettausstattung mit souveränen Cloud-Arbeitsplätzen bis zum Jahr 2029 zu entwickeln.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit begrüßt dieses Bekenntnis der relevanten politischen Kräfte in der Freien Hansestadt Bremen, die digitale Souveränität zu stärken. Sachgerecht wäre hierfür unter anderem die Erfahrungen, die Schleswig-Holstein mit den dort erprobten Open-Source-Arbeitsplätzen und der verstärkten Nutzung von Open Source gemacht hat, für die Freie Hansestadt Bremen zu nutzen. Auch wenn die Abhängigkeiten nur schrittweise reduziert werden können, ist die Erhöhung der digitalen Souveränität aus datenschutzpolitischen Gründen von großer Bedeutung und wird in den kommenden Jahren stärker ins Zentrum rücken. Wichtig ist im Einzelnen, dass bei den einzusetzenden Cloud-Lösungen perspektivisch die Souveränitätsanforderungen, wie sie auf der Grundlage der Deutschen Verwaltungscloud-Strategie vorgesehen sind, jeweils umgesetzt werden. Der IT-Planungsrat hat am 17. November 2020 das Papier „Deutsche Verwaltungscloud-Strategie“ veröffentlicht. Die Strategie diente dazu, gemeinsame Standards und offene Schnittstellen für Cloudlösungen in der Bundes- und Landesverwaltung zu schaffen und so eine übergreifende föderale Cloud-Infrastruktur, die interoperabel und modular sein soll, zu ermöglichen. Die föderale Struktur schafft auch im Bereich der digitalen Souveränität die Möglichkeit, dass einzelne Länder, wie die Freie Hansestadt Bremen, vorangehen.

2. Bremische Bürgerschaft – Ergebnisse der Beratungen des 7. Jahresberichtes und des 6. Jahresberichtes nach Inkrafttreten der Datenschutzgrundverordnung

2.1 Ergebnisse zum 7. Jahresbericht

Der Bericht des Ausschusses für Wissenschaft, Medien, Datenschutz, Informationsfreiheit und Digitalisierung (WMDID-Ausschuss) zum 7. Jahresbericht nach der Europäischen Datenschutzgrundverordnung des Landesbeauftragten für Datenschutz vom 28. März 2025 (Drucksache 21/1108) und zur Stellungnahme des Senates vom 16. September 2025 (Drucksache 21/1352) lag zum Redaktionsschluss noch nicht vor.

2.2 Ergebnisse zum 6. Jahresbericht

Bericht des Ausschusses für Wissenschaft, Medien, Datenschutz, Informationsfreiheit und Digitalisierung (Drucksache 21/1076).

6. Jahresbericht der Landesbeauftragten für Datenschutz nach der Europäischen Datenschutzgrundverordnung (DSGVO) und Stellungnahme des Senates.

Die Landesbeauftragte für den Datenschutz hat der Bremischen Bürgerschaft (Landtag) und dem Präsidenten des Senates den Bericht im Sinne des Artikels 59 der Europäischen Datenschutzgrundverordnung über das Ergebnis ihrer Tätigkeit im Jahr 2023 am 18. März 2024 (Drucksache 21/341) vorgelegt. Der Senat hat der Bremischen Bürgerschaft (Landtag) seine Stellungnahme hierzu am 3. September 2024 (Drucksache 21/739) übermittelt. Entsprechend Ziffer 11 des Einsetzungsbeschlusses des Ausschusses für Wissenschaft, Medien, Datenschutz, Informationsfreiheit und Digitalisierung hat die Präsidentin der Bremischen Bürgerschaft den Bericht der Landesbeauftragten für Datenschutz sowie die Stellungnahme des Senates dem Ausschuss unmittelbar zugeleitet.

Der Ausschuss stellte bei den nachfolgend aufgeführten Punkten des 6. Jahresberichtes Beratungsbedarf fest:

Ziffer 2.3 Beratungen

Ziffer 4 Geldbußen

Ziffer 4.8 Unbefugte Abfragen von Polizistinnen und Polizisten

Ziffer 6.2 Videoüberwachung

Ziffer 6.2.2 Bremer Freimarkt und Weihnachtsmarkt 2023

Ziffer 6.2.3 Drohneneinsatz durch die Polizei zu repressiven Zwecken

Ziffer 6.2.4 Drohneneinsatz durch die Feuerwehr Bremerhaven

Ziffer 6.2.5 Evaluierung Videoüberwachung öffentlicher Plätze

Ziffer 6.3 Einsatz von KI bei Auswertung kryptierender Messenger

Ziffer 6.4 Zuverlässigkeitsüberprüfungen

Ziffer 6.8 Behördlicher Datenaustausch zwecks Beantwortung parlamentarischer Anfragen

Ziffer 7.2 Datenschutzrechtliche Anforderungen an den digitalen Versand anwaltliche Schreiben

Ziffer 7.4 Novellierung des bremischen Richtergesetzes

Ziffer 8.2 Hackerangriff auf den Klinikverbund Gesundheit Nord

Ziffer 9.5 Akteneinsichtsrecht von Abgeordneten der Bremischen Bürgerschaft bei Sozialbehörden

Ziffer 10.3 Nutzung der iCloud an bremischen Schulen

Ziffer 10.4 Noten in Klassen

Ziffer 11.3 Überarbeitung der Orientierungshilfe für Mietinteressentinnen und Mietinteressenten

Ziffer 16.5 Unterlassene Auskunft nach Artikel 15 Datenschutzgrundverordnung

In seinen Sitzungen am 15. Januar 2025 und 19. Februar 2025 erörterte der Ausschuss die beratungsbedürftigen Punkte mit dem 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 Klärungen mit den zuständigen Ressorts und Dienststellen gekommen ist beziehungsweise im Rahmen von Gesprächen zwischen den Beteiligten konstruktiv an Lösungsmöglichkeiten gearbeitet wird.

Der Ausschuss bewertet die steigenden Beratungszahlen (Ziffer 2.3) auch als positives Zeichen. Dadurch rückten neue Datenschutzthemen ins Blickfeld, die bisher unter Umständen

nicht bekannt gewesen seien. Wichtig sei auch, dass die Beratungen durch die Landesdatenschutzbehörde kostenlos blieben. Datenschutzbeauftragte aus anderen Bundesländern meldeten inzwischen erhöhten Bedarf an personellen Ressourcen an. Dieses Thema habe in Bremen allerdings aufgrund der längeren Zeit ohne Besetzung der Amtsleitung keine Priorisierung erfahren.

Der Ausschuss diskutierte, nach welchen Maßstäben die Höhe der Geldbußen (Ziffer 4) durch den Landesbeauftragten für Datenschutz und Informationsfreiheit festgelegt wird. Dazu berichtete der Landesbeauftragte für Datenschutz und Informationsfreiheit, dass der Ausgangspunkt für ein Bußgeld die Kriterien nach der Datenschutzgrundverordnung seien. Da es sich um europäische Gesetzgebung handele, müsse es eine Vergleichbarkeit in ganz Europa geben. Bei Datenschutzverstößen durch Unternehmen gebe der Europäische Datenschutzausschuss (EDSA) Leitlinien vor, welche die Spannbreiten für die unterschiedlichen Verstöße unter Berücksichtigung des Unternehmensumsatzes auflisteten, um einen Ausgleich von Wettbewerbsvorteilen zu bewirken. Die Festsetzung der Bußgelder habe weitgehend vor Gericht Bestand. Der Ausschuss begrüßt den Umstand, dass es für die Verhängung von Bußgeldern klare und einheitliche Richtlinien gebe.

Mit Blick auf Ziffer 4.8 ließ sich der Ausschuss berichten, dass unbefugte Abfragen von Polizistinnen und Polizisten nicht gänzlich vermeidbar seien. Hintergrund sei, dass die Auskunftssysteme allen Polizistinnen und Polizisten zur Erledigung ihrer Aufgaben zur Verfügung stehen müssten und ein Genehmigungsverfahren aufgrund der Masse nicht umsetzbar sei. Es würden jedoch regelmäßig Sensibilisierungen für die Notwendigkeit der klaren dienstlichen Begründbarkeit der Maßnahmen erfolgen und es gebe eine randomisierte verpflichtende Abfrage, zu welchem Verfahren die Eingabe gewesen sei. Intern erfolge eine Stichprobenkontrolle durch den Datenschutzbeauftragten, welcher die Rechtmäßigkeit der Abfragen überprüfe. Das Aufdecken der Fälle sei ein Ausdruck, dass die polizeiinternen Maßnahmen wirkten, was der Ausschuss als positiv bewertet.

Der Ausschuss kritisierte zu Ziffer 6.2.2 (Bremer Freimarkt und Weihnachtsmarkt 2023), dass bei einem Vor-Ort-Termin auf dem Freimarkt das Schwenken der Kameras möglich gewesen sei, wodurch sich der Erfassungsbereich der Vorrichtungen erheblich erweitert habe. Das Schwenken von Kameras bei Veranstaltungen sei nicht grundsätzlich ausgeschlossen und müsse anhand des Einzelfalles nach dem Bremischen Polizeigesetz bewertet werden. Im konkreten Fall habe es eine Absprache zwischen dem Landesbeauftragten für Datenschutz und Informationsfreiheit und der Polizei gegeben, die das Bewegen der Geräte untersagt habe. Das Schwenken der Kameras sei aufgetreten, da sich ein Polizist fälschlicherweise mit seinem persönlichen Account angemeldet habe und nicht mit dem dafür vorgesehenen Funktionsaccount. Der Ausschuss bewertet es als positiv, dass das Anmelden mit einem persönlichen Account künftig technisch ausgeschlossen sei.

Zum Thema „Drohneneinsatz durch die Polizei zu repressiven Zwecken“ (Ziffer 6.2.3) ließ sich der Ausschuss berichten, dass die verwendete Drohne im lokalen Datenmodus Aufnahmen speichere, zur Station zurückkehre und anschließend von der Polizei vor Ort ausgelesen werde. Nach Auffassung des Ausschusses ist es erfreulich, dass eine Schnittstelle, bei der eine Datenübertragung nach außen stattfinde, nicht mehr existiere. Für eine repressive polizeiliche Nutzung sei die Verwendung im lokalen Datenmodus ausreichend, da in erster Linie Tatortaufnahmen aus der Luft angefertigt werden müssten. Im Bereich der Gefahrenabwehr sei nach Auffassung des Senators für Inneres und Sport eine Liveübertragung erstrebenswert, ebenso beim Einsatz durch die Feuerwehr, um unmittelbare taktische Maßnahmen ableiten zu können. Bei der anstehenden Novelle des Bremischen Polizeigesetzes strebe der Senator für Inneres und Sport an, einen solchen Einsatzzweck im präventiv-polizeilichen Bereich zu schaffen.

Hinsichtlich Ziffer 6.2.5 (Evaluierung Videoüberwachung öffentlicher Plätze) bittet der Ausschuss um einen weiteren Bericht zum aktuellen Stand der Überwachungsgesamtrechnung.

Der Ausschuss bewertet es als konstruktiv, dass bei der Auswertung kryptierender Messenger unter Einsatz von Künstlicher Intelligenz (Ziffer 6.3) die polizeiliche Arbeit bei der Aufklärung von Straftaten erfolgreich gewesen sei und ein enger Draht ohne Dissens zwischen den Behörden bestehe. Die „EncroChat“-Verfahren liefen am Landgericht, ohne dass es zu Problemen bei der Beweisverwertung gekommen sei. Weiter ließ sich der Ausschuss berichten, dass es seit dem vergangenen Jahr eine KI-Verordnung gebe, aber kein dazugehöriges Ausführungsgesetz. Die Novellierung des Bremischen Polizeigesetzes werde demgemäß keine Regelungen zum Einsatz von Künstlicher Intelligenz beinhalten.

Zum Thema Zuverlässigkeitsprüfungen (Ziffer 6.4) nimmt der Ausschuss positiv zur Kenntnis, dass der Senator für Inneres und Sport aufgrund der Anregung des Landesbeauftragten für Datenschutz und Informationsfreiheit plane, im Rahmen der Novellierung des Bremischen Polizeigesetzes Bedingungen zur Durchführung von Zuverlässigkeitsprüfungen durch Ortspolizeibehörden gesetzlich festzulegen, wobei darauf geachtet werde, datenschutzrechtliche Begriffe präziser zu formulieren.

Zu den datenschutzrechtlichen Anforderungen an den digitalen Versand anwaltlicher Schreiben (Ziffer 7.2) ließ sich der Ausschuss berichten, dass es in dem Fall, bei dem es um den Versand von Gesundheitsdaten ging, ein Bußgeld gegeben habe. Ein Gerichtsverfahren sei nicht notwendig gewesen, da zwischen der Betroffenen und Rechtsanwaltskammer Einigkeit bestanden habe. Der Ausschuss begrüßt, dass es zwischen dem Landesbeauftragten für Datenschutz und Informationsfreiheit und der Rechtsanwaltskammer Gespräche gebe, wie die Kommunikation in Zukunft rechtssicher ablaufen könne. Die Kritik des Landesbeauftragten für Datenschutz und Informationsfreiheit, die Senatorin für Justiz und Verfassung habe sich in

ihrer Stellungnahme zugunsten der Hanseatischen Rechtsanwaltskammer Bremen ausgesprochen, obwohl der Landesbeauftragte für Datenschutz und Informationsfreiheit zuständig sei, nimmt der Ausschuss zur Kenntnis.

Zu Ziffer 7.4 (Novellierung des bremischen Richtergesetzes) diskutierte der Ausschuss das Thema der Zuverlässigkeitsüberprüfungen. Dazu ließ sich der Ausschuss berichten, dass bei Bewerbungsverfahren von hauptamtlichen Richterinnen und Richtern sowie Staatsanwältinnen und Staatsanwälten anhand von Internetrecherchen durch die senatorische Behörde geprüft werde, ob öffentliche Informationen zu extremistischen Bestrebungen vorlägen. Bei ehrenamtlichen Richterinnen und Richtern könne eine solche Prüfung durch die Dienststellenleitung erfolgen.

Zum Hackerangriff auf den Klinikverbund Gesundheit Nord gGmbH (Ziffer 8.2) ließ sich der Ausschuss berichten, dass die Löschung von Gesundheits- und Beschäftigtendaten innerhalb der Fristen nicht rechtskonform abgelaufen sei. Dabei sei es nicht um Bank- und Sozialversicherungsdaten gegangen, da die Beschäftigtendaten nicht aus Personalakten stammten, sondern aus Teambesprechungen. Von dem Hackerangriff sei zwar nicht das Krankenhausinformationssystem des Klinikverbundes Gesundheit Nord gGmbH getroffen gewesen, jedoch das zuvor genutzte Dateiablagesystem. Theoretisch hätten diese Daten bei der rechtssicheren Archivierung der Patientinnen- und Patientenakten gelöscht werden können, wobei es sich vermutlich um ein deutschlandweites Problem handle.

Der Ausschuss hinterfragte kritisch, ob die Gesundheit Nord gGmbH Beschäftigen und Patientinnen und Patienten in ausreichender Form über den Abfluss ihrer Daten informiert habe. Aufgrund der großen Datenmenge sei nicht zu überblicken gewesen, wer konkret in welcher Form geschädigt gewesen sei. Die Benachrichtigung der Betroffenen sei deswegen über öffentliche Berichte in sämtlichen großen deutschen Zeitungen erfolgt. Die Gesundheit Nord gGmbH habe die Beschäftigten über einen Unternehmensnewsletter per Mail angeschrieben und es sei eine Hotline für Beschäftigte und Patientinnen und Patienten eingerichtet worden. Dieses Vorgehen habe nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit der Benachrichtigungspflicht in Artikel 34 DSGVO entsprochen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit erhob kein Bußgeld, da die Gesundheit Nord gGmbH den Verstoß von sich aus gemeldet habe. Auch Schadensersatzansprüche habe es nicht gegeben.

Der Ausschuss begrüßt den Umstand, dass der Schaden mithilfe der Polizei und des Bundeskriminalamtes habe begrenzt werden können. Positiv hervorzuheben ist, dass die Gesundheit Nord gGmbH die Verstöße unter Einbindung des Landesbeauftragten für Datenschutz und Informationsfreiheit umfassend beseitigt und aufgearbeitet habe.

Zum Thema Akteneinsichtsrecht von Abgeordneten der Bremischen Bürgerschaft bei Sozialbehörden (Ziffer 9.5) berichtete der Landesbeauftragte für Datenschutz und Informationsfreiheit, nach seiner Einschätzung sei das Vorgehen plausibel gewesen. Der Datenschutz sei auch im parlamentarischen Raum relevant, so habe auch der Europäische Gerichtshof aktuell zur Anwendbarkeit der Datenschutzgrundverordnung auf das Parlament geurteilt.

Der Ausschuss bewertet es als positiv, dass die Senatorin für Kinder und Bildung bezüglich der Nutzung der iCloud an bremischen Schulen (Ziffer 10.3) inzwischen eine Datenschutzfolgenabschätzung vorgelegt habe, welche im nächsten Schritt durch den Landesbeauftragten für Datenschutz und Informationsfreiheit geprüft werde.

Im Rahmen der Diskussion zu Ziffer 10.4 (Noten in Klassen) verdeutlichte sich, dass Noten in jeder Klassenstufe personenbezogene Daten seien, deren Veröffentlichung im Klassenzimmer in allen Fällen rechtswidrig sei.

Zu Ziffer 11.3 (Überarbeitung der Orientierungshilfe für Mietinteressentinnen und Mietinteressenten) nimmt der Ausschuss zur Kenntnis, dass dem Senat eine rechtssichere Handreichung weitergeleitet werde, sobald der Abstimmungsprozess zwischen den Datenschutzbeauftragten der Länder und des Bundes abgeschlossen sei.

Weiter diskutierte der Ausschuss, ob es eine Empfehlung an den Gesetzgeber gebe, wie mit dem Spannungsfeld zwischen der Durchmischung von Stadtteilen und den Datenschutzrechten der Mietinteressentinnen und Mietinteressenten umgegangen werden könne. Nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit sei es möglich, nach der Wohnungsbesichtigung, gewisse Daten von Mietinteressentinnen und Mietinteressenten zum Zwecke der sozialen Durchmischung von Stadtteilen zu erheben. Dies sei allerdings an enge Bedingungen geknüpft, Voraussetzung sei ein schlüssiges wohnungspolitisches Konzept.

Der 6. Jahresbericht der Landesbeauftragten für Datenschutz nach der Europäischen Datenschutzgrundverordnung ist gemeinsam mit dem Bericht und Antrag des Ausschusses für Wissenschaft, Medien, Datenschutz, Informationsfreiheit und Digitalisierung und der Stellungnahme des Senates von der Bremischen Bürgerschaft (Landtag) in ihrer Sitzung am 26. und 27. März 2025 behandelt worden. Zudem hat der Landesbeauftragte für Datenschutz und Informationsfreiheit entsprechend der Bitte des Ausschusses für Wissenschaft, Medien, Datenschutz, Informationsfreiheit und Digitalisierung in dessen Sitzung am 11. Juni 2025 einen mündlichen Bericht zu den Videoüberwachungen unter der Überschrift „Aktueller Stand der begonnenen Überwachungsgesamtrechnung“ erstattet (siehe hierzu Ziffer 5.5 dieses Berichtes).

3. Geldbußen

3.1 Allgemeines

Im Berichtsjahr 2025 lag der Schwerpunkt der datenschutzaufsichtsbehördlichen Verfahren zur Festsetzung von Geldbußen gemäß Artikel 83 Datenschutzgrundverordnung auf gegen Unternehmen festgestellten datenschutzrechtlichen Verstößen aus den Jahren 2022 und 2023.

3.1.1 Fakten

Im Berichtsjahr ergingen seitens des Landesbeauftragten für Datenschutz und Informationsfreiheit 15 Bescheide zur Verhängung von Geldbußen gegen Unternehmen und natürliche Personen, die insgesamt 101 Geldbußen enthielten. Die Anzahl der verhängten Geldbußen divergiert mit der Anzahl der Bescheide, weil gegen eine verantwortliche Stelle in einem Bescheid mehrere Geldbußen verhängt werden können. Insgesamt wurden im Berichtsjahr Geldbußen in Höhe von 75.077 € verhängt. Im Berichtsjahr verteilten sich die Geldbußen nach Artikel 83 Datenschutzgrundverordnung wie folgt: sechs Bescheide gegen natürliche Personen und neun Bescheide gegen Unternehmen. Von den 15 erlassenen Bescheiden wurden 14 im Berichtsjahr rechtskräftig. Ein Bescheid aus dem vorherigen Berichtsjahr befindet sich zu Redaktionsschluss im Einspruchsverfahren. In 26 Fällen hat der Landesbeauftragte für Datenschutz und Informationsfreiheit von der Verhängung einer Geldbuße in diesem Berichtsjahr abgesehen oder das Verfahren über Geldbußen eingestellt.

3.1.2 Musterrichtlinien für das Verfahren über Geldbußen

Am 16. Juni 2025 hat sich die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder auf eine Festlegung zu „Musterrichtlinien für das Verfahren über Geldbußen der Datenschutzaufsichtsbehörden (MRiDaVG)“ verständigt. Neben der Zuständigkeit (Nummern 6 und 7), der Zusammenarbeit mit der Staatsanwaltschaft (Nummer 18) und den Mitteilungen nach dem Abschluss des Verfahrens über Geldbußen (Nummern 20 bis 23) steht Teil 3 „Verfahren über Geldbußen“ (Nummern 8 bis 17) im Mittelpunkt dieser Musterrichtlinien. Die Themen in Teil 3 reichen von der Entscheidung über die Einleitung oder Fortführung eines Verfahrens über Geldbußen (Nummer 9), dem Absehen von der Einleitung eines Verfahrens über Geldbußen (Nummer 8), Adressierung bei Verfahren über Geldbußen gegen juristische Personen und Personengesellschaften (Nummer 12), Auskunftsersuchen an öffentliche und nicht öffentliche Stellen (Nummer 13) bis hin zur Einstellungsverfügung (Nummer 16) oder dem Inhalt des Bescheides (Nummer 17). Mit der Musterrichtlinie für das Verfahren über Geldbußen der Datenschutzbehörde ist ein bedeutender Schritt in Richtung auf eine einheitliche Ausübung der Aufsichtspraxis in ganz Deutschland getan worden.

3.1.3 Neue Bußgeldzuständigkeit durch die europäische Verordnung über die Transparenz und das Targeting politischer Werbung

Seit 10. Oktober 2025 gibt es für den Landesbeauftragten für Datenschutz und Informationsfreiheit eine neue Bußgeldzuständigkeit aufgrund der Verordnung über die Transparenz und das Targeting politischer Werbung (siehe hierzu Ziffern 1.3 und 12.3 dieses Berichtes), insbesondere betrifft dies politische Wahlwerbung im Internet, die sich an europäische Bürgerinnen und Bürger richtet.

3.2 GPS-Tracking durch ehemaligen Lebenspartner

Der Landesbeauftragte für Datenschutz und Informationsfreiheit setzte im Berichtsjahr zehn Geldbußen gegen einen Mann fest, der die Bewegungsaktivitäten seiner ehemaligen Lebenspartnerin mittels GPS-Tracker (GPS – Global Positioning System, übersetzt: Globales Positionsbestimmungssystem) überwachte. Dazu befestigte er heimlich zwei GPS-Tracker an ihrem Auto. Immer wenn das Auto fortbewegt wurde, wurden die Bewegungsaktivitäten aufgezeichnet und konnten später in einem Online-Portal angesehen werden. Anhand der so erstellten Bewegungsprotokolle konnten die GPS-Koordinaten, das Datum, die Uhrzeit und die Geschwindigkeit einzelner Bewegungen des Wagens nachvollzogen werden und somit auch Rückschlüsse auf das Privatleben der betroffenen ehemaligen Lebensgefährtin gezogen werden. Die Erhebung und Speicherung von Standort-, Bewegungs- und Zeitdaten eines genutzten Fahrzeuges, die über das Ortungssystem anfallen, sowie deren Auswertung stellen legitimationsbedürftige Datenverarbeitungen dar.

Eine heimliche GPS-Überwachung aufgrund einer privat durchgeführten Beweiserhebung ist grundsätzlich verboten, weil dies einen schwerwiegenden Eingriff in das allgemeine Persönlichkeitsrecht der GPS-überwachten Personen darstellt. Grundrechtsbeeinträchtigende Ermittlungsmaßnahmen dürfen nur unter strengen gesetzlichen Voraussetzungen von den zuständigen Ermittlungsorganen, wie Polizei oder Staatsanwaltschaft, durchgeführt werden.

3.3 Unbefugte Abfragen unter Ausnutzung der beruflichen Stellung

Auch im Jahr 2025 (siehe hierzu 7. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 3.4) ahndete der Landesbeauftragte für Datenschutz und Informationsfreiheit mehrere Fälle des unberechtigten Zugriffes auf personenbezogene Daten durch Personen, die aufgrund ihrer beruflichen Stellung Zugang zu diesen Daten hatten. Privatmotivierte unbefugte Abfragen durch Beschäftigte öffentlicher Stellen sind in hohem Maße dazu geeignet, das Vertrauen der Allgemeinheit in den Umgang öffentlicher Stellen mit personenbezogenen Daten zu beeinträchtigen und das Ansehen der öffentlichen Verwaltung empfindlich zu schädigen.

Das Abfragen von personenbezogenen Daten in behördlichen Systemen stellt gemäß Artikel 4 Ziffer 2 Datenschutzgrundverordnung (DSGVO) eine Verarbeitung von personenbezogenen Daten dar. Durch dieses Abfragen ohne berechtigten Anlass wird gegen das Erfordernis der Rechtmäßigkeit der Datenverarbeitung gemäß Artikel 5 Absatz 1 Buchstabe a) DSGVO sowie gegen das der Zweckbindung gemäß Artikel 5 Absatz 1 Buchstabe b) DSGVO verstoßen, soweit keine der in Artikel 6 Absatz 1 Unterabsatz 1 DSGVO genannten Bedingungen zum Zeitpunkt der Abfrage erfüllt sind. Insofern sind diese Abfragen von personenbezogen Daten in behördlichen Systemen ohne berechtigten Anlass bußgeldbewehrte Ordnungswidrigkeiten gemäß Artikel 83 Absatz 1, Absatz 2 und Absatz 5 Buchstabe a) DSGVO.

Die Beschäftigten sind auch Verantwortliche gemäß Artikel 4 Ziffer 7 DSGVO, insoweit die Beschäftigten allein (oder gemeinsam mit anderen) über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Dafür sprechen Wortlaut, Systematik sowie Sinn und Zweck der Datenschutzgrundverordnung (siehe hierzu Amtsgericht Stuttgart, Urteil vom 22. November 2023, Aktenzeichen 31 OWi 315 Js 18340/23 Randnummer 71 fortfolgende und Oberlandesgericht Stuttgart, Beschluss vom 25. Februar 2025, Aktenzeichen 2 ORbs 16 Ss 336/24 Randnummer 6 fortfolgende).

In drei Fällen wurden gegen natürliche Personen Geldbußen wegen des Ausnutzens der Zugriffsberechtigung für den Online-Service zur Einholung von Melderegisterauskünften „OLMERA“ verhängt.

Eine Mitarbeiterin des Gesundheitsamtes Bremerhaven tätigte über einen beträchtlichen Zeitraum von über einem Jahr wiederholt Melderegisterabfragen ohne dienstliche Gründe. Als dies dem Gesundheitsamt Bremerhaven auffiel, meldete es den Vorfall dem Landesbeauftragten für Datenschutz und Informationsfreiheit. Nach dem Ergebnis der Ermittlungen konnte festgestellt werden, dass die Mitarbeiterin Personen aus ihrem familiären und beruflichen Umfeld abfragte. Dazu gab sie Vor- und/oder Nachnamen sowie Anschriften dieser Personen im System ein. Ferner erhielt sie durch Eingabe der Adresse einer Justizvollzugsanstalt den Zugriff auf personenbezogene Daten von 86 dort gemeldeten Insassen. Das Vorliegen einer Rechtsgrundlage nach Artikel 6 Absatz 1 Unterabsatz 1 DSGVO konnte von dem Gesundheitsamt Bremerhaven ausgeschlossen werden.

Eine weitere unbefugte Melderegisterabfrage, die der Landesbeauftragte für Datenschutz und Informationsfreiheit ebenfalls mit einer Geldbuße sanktionierte, wurde von einer Mitarbeiterin einer Krankenkasse getätigt. Diese versuchte, die aktuelle Anschrift ihres ehemaligen Ehemannes und dessen Lebensgefährtin unter Angabe ihrer Vor- und Zunamen abzufragen. Die Abfrage blieb aufgrund der eingetragenen Auskunftssperre erfolglos. Allerdings stellt bereits das Abfragen personenbezogener Daten eine Datenverarbeitung dar, ein Erfolg der Abfragen wird nicht vorausgesetzt.

Ähnlich verhielt es sich in einem anderen Fall. Eine weitere unbefugte und deshalb mit einer Geldbuße sanktionierte Melderegisterabfrage wurde von einem Polizisten über seine Kollegin begangen. Hier griff der Schutzmechanismus der Auskunftssperre der Polizistin (siehe hierzu Ziffer 2.2 dieses Berichtes), sodass diese Abfrage auffiel und dieser Fall von der Ortspolizeibehörde Bremerhaven an den Landesbeauftragten für Datenschutz und Informationsfreiheit gemeldet wurde. Aus den Protokolldaten des Melderegisters ergab sich kein dienstlicher Abfrageanlass, der einem dienstlichen Sachverhalt zugeordnet werden konnte, obwohl der Polizist die Melderegisterabfrage unter seiner dienstlichen Nutzerkennung durchführte. Das Abfragen von Vor- und Nachnamen der Kollegin im Melderegister stellt gemäß Artikel 4 Ziffer 2 DSGVO eine Verarbeitung personenbezogener Daten dar. Durch dieses Abfragen ohne berechtigten Anlass wurde gegen die Rechtmäßigkeit der Datenverarbeitung gemäß Artikel 5 Absatz 1 Buchstabe a) DSGVO sowie gegen die Zweckbindung gemäß Artikel 5 Absatz 1 Buchstabe b) DSGVO verstoßen, weil keine der in Artikel 6 Absatz 1 Unterabsatz 1 DSGVO genannten Bedingungen zum Zeitpunkt der Abfrage erfüllt waren.

Aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit sind die Beschäftigten öffentlicher Stellen in der Freien Hansestadt Bremen auch zukünftig zu ihrer besonderen Pflichtenwahrung und Vorbildwirkung anzuhalten.

4. Datenschutzbeauftragte und Allgemeines öffentliche Stellen

4.1 Microsoft 365 und das Ziel der digitalen Souveränität

Der Einsatz der Office-Anwendung Microsoft 365 bringt datenschutzrechtlich weiterhin Risiken mit sich. Es handelt sich dabei um einen Cloud-Dienst, bei dem personenbezogene Daten auf Servern verarbeitet werden, die teilweise in Drittländern, und zwar in erster Linie den Vereinigten Staaten von Amerika, stehen oder von amerikanischen Unternehmen administriert werden. Selbst wenn Microsoft Rechenzentren innerhalb der Europäischen Union nutzt, behält der Konzern oft Zugriffsrechte aus den Vereinigten Staaten von Amerika, beispielsweise zu Wartungszwecken oder Sicherheitsanalysen. Verantwortliche können häufig nicht exakt nachvollziehen, welche Daten wann und wo verarbeitet oder gespiegelt werden. Dies hat eine Verletzung des Transparenzprinzips nach Artikel 5 Absatz 1 Buchstabe a) Datenschutzgrundverordnung (DSGVO) und Unsicherheiten bei der Rechenschaftspflicht (Artikel 5 Absatz 2 DSGVO) zur Folge. Personenbezogene Daten müssen nach dem Grundsatz der „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz“ gemäß Artikel 5 Absatz 1 Buchstabe a) DSGVO auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Der Verantwortliche ist nach Artikel 5 Absatz 2 DSGVO für die Einhaltung dieses Grundsatzes verantwortlich und muss dessen Einhaltung nachweisen.

Neben dieser Problematik der unklaren Datenflüsse und der Intransparenz sind die möglichen Datentransfers in Drittländer aus Sicht des Datenschutzes problematisch (siehe hierzu 30. Tätigkeitsbericht des niedersächsischen Datenschutzbeauftragten, Ziffer G 6.1). Der aktuelle Angemessenheitsbeschluss zwischen der Europäischen Union und den Vereinigten Staaten von Amerika, das Data Privacy Framework, ermöglicht rechtlich die Datenübertragung in die Vereinigten Staaten von Amerika zwar; amerikanische Gesetze, wie der U.S. CLOUD Act oder der Foreign Intelligence Surveillance Act, verpflichten Anbieter jedoch dazu, Daten an amerikanische Behörden herauszugeben, auch, wenn diese physisch in Deutschland oder der Europäischen Union liegen, was im Widerspruch zu den Vorgaben der Datenschutzgrundverordnung stehen kann. Zudem steht eine abschließende gerichtliche Klärung, ob der Angemessenheitsbeschluss nichtig ist, noch aus (siehe hierzu Ziffer 16.3 dieses Berichtes).

Es ist überdies unklar, ob Telemetriedaten, einschließlich Diagnosedaten, vollständig unter das Data Privacy Framework fallen. Telemetriedaten, einschließlich Diagnosedaten, werden durch Fernmessung regelmäßig von Microsoft erhoben und können, obwohl sie pseudonymisiert werden, personenbeziehbare Informationen enthalten, wie beispielsweise Benutzer-IDs oder IP-Adressen. Somit kann die oder der Verantwortliche möglicherweise keine vollständige Kontrolle über die Verarbeitung gewährleisten, was zu einem Verstoß gegen Artikel 5 Absatz 1 Buchstabe f) DSGVO und Artikel 28 DSGVO führen kann. Nach dem in Artikel 5 Absatz 1

Buchstabe f) DSGVO verankerten Grundsatz der „Integrität und Vertraulichkeit“ müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter und unrechtmäßiger Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen. Artikel 28 DSGVO bestimmt, dass ein Verantwortlicher mit Auftragsverarbeitern nur zusammenarbeiten darf, wenn diese die hinreichende Garantie dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit der Datenschutzgrundverordnung und dem Schutz der Rechte der betroffenen Person erfolgt, also insbesondere auch dem Grundsatz der Integrität und Vertraulichkeit.

Bei der Anwendung dieser Vorgaben der Datenschutzgrundverordnung ist oft unklar, wie die datenschutzrechtlichen Rollen – also wer Verantwortliche beziehungsweise Verantwortlicher und wer Auftragsverarbeiterin beziehungsweis Auftragsverarbeiter ist – verteilt sind. So tritt Microsoft in bestimmten Bereichen nicht als Auftragsverarbeiter, sondern als (gemeinsamer) Verantwortlicher auf. Das erschwert den Abschluss von Auftragsverarbeitungsverträgen nach Artikel 28 DSGVO und die unklare Rollenverteilung widerspricht dem Prinzip, dass die oder der Verantwortliche in transparenter Art und Weise die Mittel und Zwecke der Verarbeitung bestimmt.

Neben diesen Schwierigkeiten bei der Zuordnung der datenschutzrechtlichen Rolle der Beteiligten und den unterschiedlichen Versionen von Microsoft 365, die jeweils datenschutzrechtlich geprüft werden müssen (siehe hierzu 7. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 4.4), stellen zudem die fortlaufenden Funktions- und Sicherheitsupdates eine besondere Herausforderung für die Prüfung der Software dar. Diese regelmäßigen Änderungen betreffen nicht nur die Benutzeroberflächen, sondern auch zentrale Datenverarbeitungsprozesse, Schnittstellen und Systemkonfigurationen. Vor dem Hintergrund der Vorgaben der Datenschutzgrundverordnung, insbesondere der Rechenschaftspflicht nach Artikel 5 Absatz 2 DSGVO sowie der Überwachung der Einhaltung von Datenschutzanforderungen, erschwert dies eine vollständige und belastbare Prüfung erheblich. Für den Landesbeauftragten für Datenschutz und Informationsfreiheit gestaltet sich die kontinuierliche Nachverfolgung der Softwareanpassungen als nahezu unmöglich, wodurch eine lückenlose Kontrolle der Einhaltung datenschutzrechtlicher Bestimmungen derzeit nicht gewährleistet werden kann.

Der Senat der Freien Hansestadt Bremen hat eine Vielzahl von Maßnahmen ergriffen, die die datenschutzrechtlichen Bedenken, die von Microsoft 365 ausgehen, mindern. Hierunter fällt der Abschluss eines gesonderten Auftragsverarbeitungsvertrages mit Microsoft, mit dem die Einhaltung europäischen Rechtes gewährleistet werden soll. Zudem wird die „EU Boundary“, nach der Daten den europäischen Wirtschaftsraum grundsätzlich nicht verlassen, weitestgehend eingehalten, wie beispielsweise die Beibehaltung der bisherigen Speicherorte vor Ort im

Rechenzentrum des IT-Dienstleisters Dataport. Schließlich soll die Nutzung von Online-Speichern – insbesondere OneDrive oder Sharepoint Online – nicht für einen Schutzbedarf oberhalb von „normal“ erfolgen (Bremische Bürgerschaft, Drucksache 21/1352, Seite 2). Dem Senat kann vor diesem Hintergrund in der Einschätzung gefolgt werden, dass der Einsatz von Microsoft 365 akzeptabel sein kann, wobei dies aus den oben beschriebenen Gründen kontinuierlich zu hinterfragen ist. Zudem ist zu begrüßen, dass der Senat auch auf Erfahrungen aus anderen Ländern zurückgreifen will, um zusätzliche Maßnahmen zur Verbesserung des Datenschutzes zu gewährleisten (siehe hierzu auch Bremische Bürgerschaft, Drucksache 21/1352, Seite 2).

Aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit sprechen dennoch die besseren Gründe – gerade vor dem Hintergrund des Datenschutzes – dafür, weiterhin das Ziel der digitalen Souveränität in der Freien Hansestadt Bremen anzustreben und die Anstrengung in dieser Hinsicht zu verstärken. Digitale Souveränität bezeichnet die Fähigkeit einer Organisation oder Institution, ihre digitalen Systeme, Daten und Prozesse eigenständig, nachvollziehbar und unter eigener Kontrolle zu gestalten. Sie umfasst sowohl die technische Unabhängigkeit von einzelnen Anbietern als auch die Kontrolle über Datenzugriffe und Verarbeitungsprozesse. Ein hoher Grad an digitaler Souveränität erleichtert den datenschutzkonformen Betrieb von IT-Systemen, weil Verantwortliche die Mittel und die Zwecke der Datenverarbeitung klar bestimmen, Änderungen an Software und Infrastruktur selbst steuern und die Einhaltung datenschutzrechtlicher Vorgaben kontinuierlich überprüfen können. Durch transparente, eigenständig kontrollierte Systeme können Datenschutzaufsichtsbehörden leichter prüfen, ob die Anforderungen der Datenschutzgrundverordnung eingehalten werden, wodurch Risiken in Hinblick auf unkontrollierte Datenflüsse oder unzureichende Rechenschaftspflichten deutlich reduziert werden.

Im Fall von Microsoft 365 zeigt sich, dass die fehlende digitale Souveränität die datenschutzrechtliche Prüfung zusätzlich erschwert und das System gegebenenfalls nur unter Einschränkungen genutzt werden kann. Die Software ist stark proprietär geprägt, das heißt, sie basiert auf einem unternehmenseigenen, also nicht frei zugänglichen, Quellcode, und ist eng an die Cloud-Infrastruktur des Anbieters gebunden, wodurch Verantwortliche nur eingeschränkten Einfluss auf Datenflüsse, Funktionsänderungen und Sicherheitskonfigurationen haben. Die Kontrolle über die Verarbeitung personenbezogener Daten liegt damit weitgehend beim Anbieter, was die Umsetzung der Rechenschaftspflicht nach der Datenschutzgrundverordnung erheblich behindert. Durch diese Abhängigkeit von Microsoft ist eine kontinuierliche und belastbare Überwachung durch den Landesbeauftragten für Datenschutz und Informationsfreiheit nur mit einem erheblichen Aufwand möglich beziehungsweise sogar ausgeschlossen, sodass Risiken, wie unkontrollierte Datenübermittlungen, einschließlich der Telemetriedaten, und nicht präzise definierte Verantwortlichkeitsverhältnisse, möglicherweise bestehen bleiben. Vor diesem Hintergrund wird deutlich, dass die Sicherstellung eines datenschutzkonformen

Betriebes bei proprietären Clouddiensten – also Clouddienste, deren Quellcode geschlossen und nicht öffentlich zugänglich sind – ohne die Voraussetzungen digitaler Souveränität erheblich erschwert beziehungsweise eingeschränkt und ein erhöhtes Risiko für Datenschutzverstöße gegeben ist.

4.2 Online-Dolmetscherdienst

Bereits seit Ende des vorletzten Berichtsjahres begleitet der Landesbeauftragte für Datenschutz und Informationsfreiheit die Einführung des Online-Dolmetscherdienstes in der Freien Hansestadt Bremen durch den Senator für Finanzen. Der Online-Dolmetscherdienst soll es sowohl berechtigten privaten Stellen als auch öffentlichen Stellen ermöglichen, Dolmetscherinnen und Dolmetscher online dazuzuschalten und so eine Echtzeit Übersetzung zu erhalten. Ermöglicht werden soll der Dienst durch einen Auftragsvertrag mit einem Anbieter. Der Dienst soll auch eine Maßnahme zur Umsetzung der Istanbul-Konvention zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt sein.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit wies im Rahmen seiner Beratungstätigkeit gegenüber dem Senator für Finanzen darauf hin, dass die Einführung eines solchen Dienstes die Durchführung einer Datenschutzfolgenabschätzung erfordere. Aus seiner Sicht resultiert dieses Erfordernis unter anderem daraus, dass es bei der Inanspruchnahme des Dienstes zur Offenlegung sensibler Daten gegenüber der Auftragsnehmerin beziehungsweise dem Auftragsnehmer kommen kann, etwa wenn Frauenhäuser diesen Dienst nutzen. Des Weiteren ist aus seiner Sicht zu berücksichtigen, dass bei dem Online-Dolmetscherdienst Daten Betroffener aus der gesamten Freien Hansestadt Bremen zusammenlaufen können. Infolgedessen kommt der Landesbeauftragte für Datenschutz und Informationsfreiheit zu dem Ergebnis, dass die Einführung des Online-Dolmetscherdienstes voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen im Sinne des Artikels 35 Datenschutzgrundverordnung zur Folge haben könne.

In diesem Zusammenhang machte der Landesbeauftragte für Datenschutz und Informationsfreiheit auch darauf aufmerksam, dass nach seiner Auffassung alle Stellen, die den Dienst nutzen werden, als verantwortliche Stellen im Sinne der Datenschutzgrundverordnung anzusehen seien, weil sie über die Nutzung des Online-Dolmetscherdienstes und damit über die Verarbeitung personenbezogener Daten im Rahmen der Dienstnutzung entschieden. Jede Stelle habe daher die Pflicht, eine datenschutzkonforme Nutzung durch diese sicherzustellen, abhängig vom Schutzbedarf der Daten die erforderlichen Sicherheitsstandards einzuhalten und eine Datenschutzfolgenabschätzung vorzunehmen. Möglich sei auch, dass gemeinsam eine kumulative Datenschutzfolgenabschätzung erstellt werde, die jedoch auf die Besonderheiten aller nutzenden Stellen eingehen müsse.

Zunächst wurde mit dem Senator für Finanzen auch die Durchführung einer solchen kumulativen Datenschutzfolgenabschätzung vereinbart, dem Landesbeauftragten für Datenschutz und Informationsfreiheit wurde sodann ein Musterformular, das im Wesentlichen nur die Prüfpunkte einer Datenschutzfolgenabschätzung enthält, für die Erstellung einer Datenschutzfolgenabschätzung durch die nutzenden Stellen übermittelt. Dies bedingt, dass nun doch jede Stelle selbst eine Datenschutzfolgenabschätzung durchführen und in der Mehrzahl der Fälle dem Landesbeauftragten für Datenschutz und Informationsfreiheit zur Prüfung übermitteln muss. Entsprechende Eingänge konnte der Landesbeauftragte für Datenschutz und Informationsfreiheit bis zum Stichtag des Jahresberichtes allerdings noch nicht feststellen.

Aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit ist weiterhin, nicht zuletzt aus Effizienzgründen, empfehlenswert, dass der Senator für Finanzen federführend bei einer etwaigen kumulativen Datenschutzfolgenabschätzung für alle nutzenden Stellen ist. Bei Anwendungen, die von einer Vielzahl von Stellen genutzt werden sollen, sollte zudem bereits im Stadium der Beschaffung – auch unabhängig von einer späteren datenschutzrechtlichen Verantwortlichkeit – durch den Landesbeauftragten für Datenschutz und Informationsfreiheit geprüft werden, ob die Angebote den datenschutzrechtlichen Belangen aller Nutzenden Rechnung tragen.

4.3 Faxnutzung in der Verwaltung der Freien Hansestadt Bremen

Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat im Berichtsjahr die in dem 2. Jahresbericht nach der Datenschutzgrundverordnung behandelte Problematik der Übermittlung personenbezogener Daten per Fax erneut aufgegriffen (siehe hierzu 2. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 5.1). In seiner Stellungnahme zu dem 2. Jahresbericht nach der Datenschutzgrundverordnung hatte der Senat der Freien Hansestadt Bremen erklärt, dass die Nutzung von Faxgeräten mit den heutigen Übertragungsstandards als unsicher einzustufen sei und die Faxkommunikation daher vollständig ersetzt werden solle (Bremische Bürgerschaft Drucksache 20/597, Seite 2). Daraufhin wurde auch gegenüber dem Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit erklärt, dass die Faxgeräte in der Verwaltung bis Ende 2022 abgeschafft werden sollten (Bremische Bürgerschaft Drucksache 20/816, Seite 2). Im Rahmen einer anlasslosen Überprüfung ist der Landesbeauftragte für Datenschutz und Informationsfreiheit der Frage nachgegangen, in welchem Umfang heute noch Faxgeräte zum Einsatz kommen und den Zusagen gegenüber der Bremischen Bürgerschaft nachgekommen wurde.

Wie bereits in der Handlungsempfehlung „Telefax ist nicht datenschutzkonform“[5] des Landesbeauftragten für Datenschutz und Informationsfreiheit vom 20. Mai 2021 beschrieben, stehen

[5] Handlungsempfehlung abrufbar unter: https://www.datenschutz.bremen.de/sixcms/media.php/13/Telefax%20ist%20nicht%20Datenschutz%20konform.pdf.

der Nutzung von Kommunikationsmitteln, die sich des Faxens bedienen, datenschutzrechtliche Bedenken entgegen, soweit mit ihnen personenbezogene Daten übermittelt werden. Kern des Problems ist die Empfangsseite; denn Absenderinnen oder Absender können sich nicht sicher sein, welche Technik auf der Empfangsseite eingesetzt wird. An die Stelle der herkömmlichen Faxgeräte sind zunehmend Multifunktionsgeräte mit Faxfunktion oder digitale Fax-Server getreten. Diese Systeme wandeln eingehende Faxe automatisch in E-Mails um und leiten diese an die jeweiligen Postfächer weiter. Darüber hinaus werden vermehrt Cloud-Fax-Dienste eingesetzt, die als virtuelle Fax-Server fungieren. Sie empfangen Faxe über das Internet, konvertieren diese in E-Mail-Nachrichten und stellen sie elektronisch zu. Eine Überprüfung, ob diese Übertragungen verschlüsselt erfolgen oder ob die verwendeten Cloud-Dienste datenschutzkonform betrieben werden, ist für die absendende Stelle jedoch sehr häufig nicht möglich.

Aufgrund dieser fehlenden Transparenz und Kontrollmöglichkeiten wird das Fax inzwischen als Kommunikationsmittel mit einem vergleichbaren Sicherheitsniveau wie eine unverschlüsselte E-Mail eingestuft. Es bietet somit kein angemessenes Schutzniveau für vertrauliche oder personenbezogene Daten. In der Regel verfügen Fax-Dienste über keine technischen Maßnahmen, um die Vertraulichkeit der übermittelten Informationen sicherzustellen. Daher sind sie aus datenschutzrechtlicher Sicht – wie auch unverschlüsselte E-Mails – grundsätzlich nicht für die Übertragung personenbezogener Daten geeignet.

Um einen Überblick zu erhalten, bat der Landesbeauftragte für Datenschutz und Informationsfreiheit alle Ressorts des Senates um Stellungnahme bezüglich der Faxnutzung auch für deren nachgeordneten Dienststellen. Diese Abfrage ergab, dass von vielen Stellen der Verwaltung der Freien Hansestadt Bremen trotz der geplanten Abschaffung auch heute noch Faxgeräte für die Kommunikation genutzt werden. In einigen Fällen war der Einsatz von Faxgeräten bundesgesetzlichen Vorgaben geschuldet, so sieht § 130 Nummer 6 Zivilprozessordnung noch das Faxgerät als technische Empfangsvorrichtung vor. In einer Vielzahl von Fällen bestand jedoch kein Grund für den Einsatz von Faxgeräten.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit regt daher weiterhin an, schnellstmöglich alternative Lösungen zu etablieren, die die Anforderungen an den Schutz personenbezogener Daten unter Berücksichtigung des Standes der Technik gemäß der Datenschutzgrundverordnung erfüllen, soweit nicht gesetzliche Regelungen den Einsatz von Faxgeräten rechtfertigen.

4.4 Meldungen von Datenschutzbeauftragten nach Artikel 37 Absatz 7 Datenschutzgrundverordnung

Im aktuellen Berichtsjahr erhielt der Landesbeauftragte für Datenschutz und Informationsfreiheit von verantwortlichen Stellen und Auftragsverarbeiterinnen und Auftragsverarbeitern 286 Meldungen nach Artikel 37 Absatz 7 Datenschutzgrundverordnung (DSGVO) im Hinblick auf die Benennung von behördlichen und betrieblichen Datenschutzbeauftragten. Hierunter fielen die Erstmeldungen bezüglich der Benennung der oder des Datenschutzbeauftragten sowie Änderungsmeldungen zu einer bestehenden Benennung oder auch die Beendigung dieser Funktion. Wie in den Vorjahren gingen dem Landesbeauftragten für Datenschutz und Informationsfreiheit die Meldungen nach Artikel 37 Absatz 7 DSGVO größtenteils über das online verfügbare Meldeformular auf seiner Website zu.

4.5 Anfragen und Beschwerden zu Datenschutzbeauftragten

Mehrfach erhielt der Landesbeauftragte für Datenschutz und Informationsfreiheit Anfragen bezüglich eventueller Unvereinbarkeiten bei Ausübung der Funktion der oder des Datenschutzbeauftragen mit anderen Aufgaben und Funktionen, welche die beziehungsweise der Datenschutzbeauftragte wahrnimmt. Artikel 38 Absatz 6 Datenschutzgrundverordnung (DSGVO) in Verbindung mit § 7 Absatz 2 Bundesdatenschutzgesetz (BDSG) sieht vor, dass die Übertragung anderer Aufgaben und Pflichten möglich ist, etwa in Fällen, in denen Aufgaben und Pflichten der oder des Datenschutzbeauftragten nicht hauptamtlich wahrgenommen werden. In diesen Fällen hat die oder der Verantwortliche beziehungsweise die Auftragsverarbeiterin oder der Auftragsverarbeiter aber sicherzustellen, dass die anderen übertragenen Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen, der die Amtswahrnehmung der oder des Datenschutzbeauftragten beeinträchtigt. So wurde ein Datenschutzbeauftragter auf mögliche Interessenkonflikte hingewiesen, die bei gleichzeitig wahrgenommenen Aufgaben hinsichtlich der von ihm getroffenen Entscheidungen zu personenbezogenen Datenverarbeitungen innerhalb seines Unternehmens bestehen.

In Bezug auf die Lösung eines Interessenkonfliktes stellt sich die Frage, ob es, um Interessenkonflikte aufzulösen, eine praktikable Lösung sein könnte, die streitigen Aufgaben von einer oder einem stellvertretenden Datenschutzbeauftragten übernehmen zu lassen. Grundsätzlich kann jedoch weder eine präventive noch eine reaktive Aufgabenteilung zwischen Datenschutzbeauftragten und Stellvertreterinnen und Stellvertretern einen systematischen Interessenkonflikt lösen. Wenn Interessenkonflikte vor der Ernennung einer oder eines Datenschutzbeauftragten erkennbar sind, so dürfen von vornherein keine „anderen Aufgaben“ (Artikel 38 Absatz 6 DSGVO) übertragen werden. Andernfalls kann sie oder er nicht zur oder zum Datenschutzbeauftragten ernannt werden.

Weiter erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit Anfragen in Bezug auf die Veröffentlichung von Kontaktdaten der oder des Datenschutzbeauftragten und deren beziehungsweise dessen Erreichbarkeit. Gemäß Artikel 37 Absatz 7 DSGVO und § 5 Absatz 5 BDSG ist die verantwortliche Stelle verpflichtet, die Kontaktdaten der oder des Datenschutzbeauftragten zu veröffentlichen. Dies stellt sicher, dass die Datenschutzaufsichtsbehörde oder auch Beschwerdeführerende direkt mit der oder dem Datenschutzbeauftragten in Kontakt treten können. Der jeweilige Gegenstand der Anfragen wurde durch den Landesbeauftragten für Datenschutz und Informationsfreiheit überprüft und festgestellte Mängel wurden behoben.

Zudem ist die Stellvertreterfunktion der oder des Datenschutzbeauftragten eine nicht eindeutig gesetzlich geregelte Frage. Dies liegt nicht zuletzt an der Formulierung des Artikel 37 Absatz 1 DSGVO, wonach die oder der Verantwortliche bei Vorliegen der entsprechenden Voraussetzungen „auf jeden Fall eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten“ benennt. Eine weitergehende Regelung hinsichtlich der Stellvertretung enthält weder die Datenschutzgrundverordnung noch das Bundesdatenschutzgesetz. Einige Landesdatenschutzgesetze sehen dagegen die Pflicht oder zumindest die Möglichkeit vor, eine stellvertretende Datenschutzbeauftragte oder einen stellvertretenden Datenschutzbeauftragten zu benennen.

Auch wenn das Bremische Ausführungsgesetz zur EU-Datenschutz-Grundverordnung keine explizite Regelung enthält, so erachtet der Landesbeauftragte für Datenschutz und Informationsfreiheit die Möglichkeit, eine stellvertretende Datenschutzbeauftragte oder einen stellvertretenden Datenschutzbeauftragten benennen zu können, dennoch im Hinblick auf die Gewährleistung eines hohen Datenschutzniveaus für empfehlenswert. Nur so kann die oder der Verantwortliche sicherstellen, dass auch bei längeren – geplanten oder ungeplanten – Abwesenheiten der oder des Datenschutzbeauftragten die datenschutzrechtlichen Vorgaben und Pflichten aus der Datenschutzgrundverordnung, wie zum Beispiel die Erfüllung der Betroffenenrechte, weiterhin umgesetzt werden. Dies spiegelt sich auch in den Regelungen zur Stellung der oder des Datenschutzbeauftragten wider, wonach der Verantwortliche gemäß Artikel 38 Absatz 2 DSGVO der oder dem Datenschutzbeauftragten die zur Aufgabenerfüllung erforderlichen Ressourcen zur Verfügung stellen muss. Hierunter sind nicht nur Räumlichkeiten, sondern insbesondere auch finanzielle Mittel und personelle Ressourcen zu verstehen. So soll gewährleistet werden, dass Datenschutzbeauftragte in der Lage sind, ihre Aufgaben nicht nur unabhängig, sondern auch effektiv erfüllen zu können. Je nach Größe des Unternehmens beziehungsweise der öffentlichen Stelle kann es auch sinnvoll sein, ein Team, bestehend aus einer oder einem Datenschutzbeauftragten und deren oder dessen Mitarbeitenden, einzurichten. In diesen Fällen sollte jedoch die Zusammensetzung des Teams sowie die Aufteilung der Aufgaben und Zuständigkeiten eindeutig festgelegt werden.

5. Inneres

5.1 Gemeldete Datenschutzverletzungen

Aus dem Bereich „Inneres“, also den Polizeibehörden und Bürger- und Ordnungsämtern, erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit 18 Meldungen der Verletzung des Schutzes personenbezogener Daten. Wie bereits im vorherigen Berichtsjahr lagen diesen Meldungen überwiegend fehlerhafte Versendungen zugrunde.

5.2 Videoüberwachung zu Bekämpfung illegaler Müllablagerung bei Containerplätzen

Sowohl im letzten als auch im aktuellen Berichtsjahr erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit mehrere Anfragen und Bitten um Stellungnahme zu den Möglichkeiten, Containerplätze mit Videokameras zu überwachen, um illegale Müllablagerungen zu vermeiden. Diese Anfragen kamen sowohl von senatorischen Behörden, wie der Senatorin für Umwelt, Klima und Wissenschaft und der Senatorin für Inneres und Sport, als auch von Beiräten. Die Aufforderungen zur Stellungnahme resultierten aus Petitionen, die von Bürgerinnen und Bürgern eingereicht wurden.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit machte in allen Fällen darauf aufmerksam, dass nach der aktuellen Gesetzeslage eine Videoüberwachung von Containerplätzen nicht möglich ist. Weder § 15 Absatz 1 Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG) noch, sofern eine polizeiliche Überwachung erfolgen soll, § 32 Absatz 3 Satz 1 Nummer 1 Bremisches Polizeigesetz (BremPolG) können eine derartige Überwachung gegenwärtig legitimieren. Soll gleichwohl eine entsprechende Überwachung erfolgen, müsste durch den bremischen Gesetzgeber geprüft werden, ob eine Befugnis unter Wahrung des Verhältnismäßigkeitsgrundsatzes geschaffen werden soll.

Derzeit sind die Voraussetzungen des § 15 Absatz 1 BremDSGVOAG in seiner aktuellen Fassung für die Legitimation einer Videoüberwachung nicht erfüllt, um die illegale Müllablagerung bei Containerplätzen zu bekämpfen. Gemäß § 15 Absatz 1 BremDSGVOAG ist eine Videoüberwachung durch öffentliche Stellen zulässig, soweit sie zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die der oder dem Verantwortlichen übertragen wurde, zum Schutz von Personen, Eigentum oder Besitz oder zur Kontrolle von Zugangsberechtigungen erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen betroffener Personen überwiegen.

In der Gesetzesbegründung zum Bremischen Ausführungsgesetz zur EU-Datenschutz-Grundverordnung hat der Gesetzgeber dabei konkretisiert, wann nach seiner Vorstellung eine

Videoüberwachung zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe zulässig sein soll. Ausweislich der Gesetzesbegründung soll dies nur der Fall sein, wenn die Videoüberwachung der „Gewährleistung der Funktionsfähigkeit öffentlicher Stellen und damit der Aufrechterhaltung des Dienstbetriebes“ dient (Bremische Bürgerschaft, Drucksache 19/1501, Seite 30). Primär soll die Videoüberwachung nach den Vorstellungen des Gesetzgebers dazu dienen, unberechtigte Personen zu erfassen, die sich in Bereichen aufhalten, die nicht für jedermann, sondern nur für bestimmte Gruppen von Personen zugänglich sind und die durch ihren Aufenthalt den Dienstbetrieb stören. Im Fokus steht mithin vor allem die Durchsetzung des Hausrechtes. Die diskutierte Videoüberwachung soll hingegen das Entdeckungsrisiko für Personen erhöhen, die illegal Müll abladen, um sie so von ihrer Tat abzuhalten oder aber zumindest ihr Verhalten zu sanktionieren. Damit dient die Überwachung Müllablagerungsorten nicht dem vom Gesetzgeber festgelegten Zwecken im Sinne von § 15 Absatz 1 BremDSGVOAG.

Des Weiteren verfolgte die Videoüberwachung nicht den Zweck, Personen, Eigentum oder Besitz zu schützen oder die Kontrolle von Zugangsberechtigungen zu ermöglichen. Zumindest wurden dem Landesbeauftragten für Datenschutz und Informationsfreiheit bislang keine Erkenntnisse dahingehend vorgetragen, dass durch illegale Müllablagerungen Sachen in ihrer Substanz beeinträchtigt werden, die im Eigentum oder im Besitz der öffentlichen Hand stehen. Auch eine unmittelbare Gefährdung von Personen findet nach den Erkenntnissen des Landesbeauftragten für Datenschutz und Informationsfreiheit bisher durch eine illegale Müllablagerung nicht statt.

Die polizeirechtliche Legitimation einer Videoüberwachung nach § 32 Absatz 3 Satz 1 Nummer 1 BremPolG scheitert daran, dass eine vermehrte Straftatenbegehung nach den Informationen, die dem Landesbeauftragten für Datenschutz und Informationsfreiheit vorliegen, durch die illegale Müllentsorgung nicht festzustellen ist. Das illegale Abladen von Müll dürfte zwar im Regelfall eine Ordnungswidrigkeit nach § 69 Absatz 1 Nummer 2 Kreislaufwirtschaftsgesetz (KrWG) in Verbindung mit § 28 Absatz 1 Satz 1 KrWG darstellen, bei der es sich jedoch nicht um eine Straftat in Sinne des § 32 Absatz 3 Satz 1 Nummer 1 BremPolG handelt.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit hält dieses Ergebnis ebenfalls für nicht sachgerecht. Sofern eine Videoüberwachung illegaler Müllablagerungsplätze künftig erfolgen soll, obliegt es daher dem bremischen Gesetzgeber, hierfür eine geeignete Rechtsgrundlage zu schaffen. Denkbar wäre insbesondere eine Änderung des § 15 Absatz 1 BremDSGVOAG, um auch die Videoüberwachung von Gebieten zu ermöglichen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass wiederholt illegal Müll in erheblichem Umfang dort abgelagert wird. Die konkrete Ausgestaltung einer entsprechenden Vorschrift müsste sich am Grundsatz der Verhältnismäßigkeit ausrichten und im Einzelnen debattiert werden.

5.3 Videoüberwachung von Gewahrsamszellen

Der Landesbeauftragte für Datenschutz und Informationsfreiheit beriet die Polizei Bremen sowie die Ortspolizeibehörde Bremerhaven im Berichtsjahr zu der Thematik der Videoüberwachung von Gewahrsamszellen. Die Beratung erfolgt insbesondere anlässlich der Errichtung neuer Gebäude der beiden Polizeibehörden in Bremen und in Bremerhaven.

Rechtsgrundlage für die Überwachung von Gewahrsamsräumen ist § 34 Absatz 2 Bremisches Polizeigesetz (BremPolG). Gemäß § 34 Absatz 2 BremPolG darf eine Bildübertragung und -aufzeichnung in Gewahrsamszellen nur erfolgen, wenn die ständige Überwachung der Vitalfunktionen einer betroffenen Person erforderlich ist, die Gefahr der Selbsttötung oder -verletzung besteht oder aus Anlass und für die Dauer des Betretens der Gewahrsamszelle durch Beschäftigte. Daneben hat eine Videoüberwachung auf Verlangen der in Gewahrsam befindliche Person zu erfolgen oder, wenn gegen sie unmittelbarer Zwang angedroht oder angewandt wird.

Nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit stellt die Überwachung von in Gewahrsam befindlichen Personen einen schwerwiegenden Grundrechtseingriff dar, der nur unter engen Voraussetzungen gerechtfertigt ist. Neben den eindeutig normierten gesetzlichen Voraussetzungen und Rahmenbedingungen, wie Rücksicht auf die Intimsphäre und Kenntlichmachen der Videoüberwachung, ist die Vorschrift daher eng an ihrem Zweck orientiert auszulegen, um den Grundsatz der Verhältnismäßigkeit zu wahren. Hierbei ist vor allem zu berücksichtigen, dass die Überwachung von Gewahrsamszellen eine doppelte Schutzrichtung aufweist: Zum einen dient sie dazu, den Dienstbetrieb der Polizeibehörden zu erleichtern, zum anderen dient sie aber dem Schutz der sich in Gewahrsam befindlichen Person und dies nicht ausschließlich durch die Überwachung ihrer Vitalfunktion, sondern auch durch einen Schutz vor möglicherweise unrechtmäßiger Polizeigewalt. Die Videoüberwachung kann insoweit einen disziplinierenden Effekt haben, als auch einer eventuell später erforderlichen Beweissicherung dienen.

Um diese Zwecke zu erreichen und damit den Verhältnismäßigkeitsgrundsatz zu wahren, ist die Rechtsgrundlage nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit derart auszulegen, dass immer dann, wenn eine Bildübertragung nach § 34 Absatz 2 BremPolG erfolgt, auch eine Bildaufzeichnung erfolgen muss, die Speicherfrist von zwei Monaten (§ 34 Absatz 6 BremPolG in Verbindung mit § 33 Absatz 6 BremPolG) nicht unterschritten werden darf und dass bei einer Bildübertragung und -aufzeichnung die kontinuierliche Beobachtung des Bildschirmes durch Bedienstete der Polizei sichergestellt werden muss. Ein nur gelegentliches Blicken auf den entsprechenden Bildschirm ist aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit nicht ausreichend, weil so weder sichergestellt werden kann, dass Störungen der Vitalfunktion rechtzeitig erkannt werden, noch,

dass die Überwachung ihren disziplinarischen Effekt entfaltet und gegebenenfalls ein rechtzeitiges Einschreiten von Polizistinnen und Polizisten gewährleistet ist. Somit erfordert eine Videoüberwachung von Gewahrsamszellen eine entsprechende personelle sowie technische Ausstattung – Speicherkapazitäten – der Polizeibehörden.

5.4 Stellungnahme zum Entwurf des Bremischen Polizeigesetzes

Dem Landesbeauftragten für Datenschutz und Informationsfreiheit wurde im Berichtsjahr der Gesetzesentwurf zur beabsichtigen Novelle des Bremischen Polizeigesetzes vorgelegt. Zu diesem Entwurf, der noch nicht verabschiedet wurde, hat er am 11. Juni 2025 eine Stellungnahme abgegeben.

In dieser Stellungnahme hat er sich zu einer Vielzahl von Punkten kritisch geäußert, von denen er exemplarisch die folgenden, aus seiner Sicht besonders wichtigen, darlegt.

5.4.1 Durchsicht elektronischer Speichermedien

Durch einen neugeschaffenen § 18 Absatz 3 des vorlegten Entwurfes zur Änderung des Bremischen Polizeigesetzes soll klargestellt werden, dass eine Durchsuchung von Sachen auch elektronische Speichermedien betreffen kann. In der vorgelegten Fassung soll dabei eine umfangreiche Durchsuchung von Speichermedien durch die Polizei allein schon deshalb zulässig sein, weil sich eine Person an einem Gefahrenort im Sinne von § 27 Absatz 1 Nummer 2 Bremisches Polizeigesetz (BremPolG) in der geltenden Fassung aufhält und ein nicht näher definiertes auffälliges Verhalten zeigt.

Angesichts der vergleichsweise niedrigen Eingriffsschwelle einerseits und des stetig anwachsenden Volumens an elektronisch gespeicherten persönlichen Daten andererseits ist die Verhältnismäßigkeit einer derartigen Regelung aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit fraglich. So ist zu bedenken, dass bei einer Durchsicht von Speichermedien auch sehr sensible Informationen, etwa Gesundheitsdaten, zur Kenntnis genommen werden können. Eine Durchsicht von Speichermedien unterscheidet sich mithin grundlegend von einer Durchsuchung anderer Sachen. Zudem dürfte die Durchsicht von elektronischen Speichermedien im Rahmen einer Durchsuchung von Personen und/oder Sachen zur Abwehr von Gefahren tatsächlich nur in seltenen Fällen erforderlich sein.

Ferner wird der Fall, dass sich das räumlich getrennte Speichermedium in einer Wohnung befindet, nicht spezielleren Anforderungen unterworfen. Die Vorschrift eröffnet daher nach ihrer jetzigen Entwurfsfassung die Möglichkeit, einen Bereich innerhalb einer Wohnung zu durchsuchen, ohne dass die speziellen Voraussetzungen gemäß Artikel 13 Grundgesetz gewahrt sind. Überdies ist nicht sichergestellt, dass es sich nicht um eine heimliche Durchsuchung aus Anlass einer Durchsuchung einer Sache gemäß § 18 Absätze 1 und 2 BremPolG

handelt, weil diese unter Umständen nur unter den engen Voraussetzungen möglich ist, die das Bundesverfassungsgericht in seinem Urteil vom 27. Februar 2008 (Aktenzeichen 1 BvR 370/07 und 1 BvR 595/07) spezifiziert hat. Das Bundesverfassungsgericht hatte in der Entscheidung den heimlichen Zugriff auf ein informationstechnisches System nur dann für zulässig erachtet, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen.

Zur Wahrung des Verhältnismäßigkeitsgrundsatzes hat der Landesbeauftragte für Datenschutz und Informationsfreiheit daher dazu geraten, für die Durchsicht von Speichermedien eine erhöhte Eingriffsschwelle zu normieren, entweder durch die Einführung eines Gefahrenerfordernisses oder durch die Präzisierung, wann aus Sicht des Gesetzgebers eine Durchsicht von elektronischen Speichermedien tatsächlich erforderlich ist. Für die Durchsuchung von Speichermedien, die sich örtlich innerhalb von Wohnungen befinden, wird empfohlen, § 19 BremPolG und § 20 BremPolG, die zum Schutz der Wohnung polizeiliche Maßnahmen an besondere Voraussetzungen knüpfen, entsprechend für anwendbar zu erklären.

5.4.2 Elektronische Fußfessel

Mit der Novelle des Bremischen Polizeigesetzes soll auch die Möglichkeit der elektronischen Aufenthaltsüberwachung, der sogenannten elektronischen Fußfessel, eingeführt werden. Die grundsätzliche Möglichkeit zum Einsatz elektronischer Fußfesseln ist inzwischen für einen eng beschränken Teilbereich der Führungsaufsicht verfassungsgerichtlich bestätigt worden (Bundesverfassungsgericht, Beschluss vom 1. Dezember 2020, Aktenzeichen 2 BvR 916/11, 2 BvR 636/12). Gleichwohl ist bei der Beurteilung der Verhältnismäßigkeit einer entsprechenden Befugnis stets zu berücksichtigen, dass der Einsatz einer elektronischen Fußfessel einen schwerwiegenden Eingriff in das informationelle Selbstbestimmungsrecht sowie in das Grundrecht auf Datenschutz der betroffenen Person bedingt. Daher hat der Landesbeauftragte für Datenschutz und Informationsfreiheit darauf hingewiesen, dass in anderen Bundesländern, in denen der Einsatz elektronischer Fußfesseln bereits jetzt legitimiert ist, die Einsatzszenarien mit Ausnahme Bayerns deutlich enger gefasst sind als im vorgelegten Entwurf. Nach dem vorgelegten Entwurf soll das Tragen einer Fußfessel bereits angeordnet werden können, wenn dies zur Abwehr einer erheblichen Gefahr erforderlich ist. In Baden-Württemberg, Hessen, Sachsen, Mecklenburg-Vorpommern und Niedersachsen ist eine derartige Anordnung hingegen nur möglich, wenn ein Bezug zu einer terroristischen Straftat oder aber zumindest einer schweren organisierten Gewaltstraftat besteht. Auch die Regelung in Nordrhein-Westfalen nimmt Bezug auf einige bestimmte, schwerwiegende Straftaten.

Zudem ist, um die Verhältnismäßigkeit der Befugnis auch in Anbetracht der Entscheidung des Bundesverfassungsgerichtes zu beurteilen, die Frage zu untersuchen, ob mit der elektronischen Fußfessel überhaupt Erfolge erzielt werden können. Das Bundesverfassungsgericht hat

in seiner Entscheidung zur elektronischen Fußfessel nur für einen eng begrenzten Teilbereich der Führungsaufsicht zwar angenommen, dass die grundsätzliche Geeignetheit der elektronischen Fußfessel nicht in Frage zu stellen ist. Überdies hat es den Gesetzgeber zugleich aufgefordert, die Eignung in tatsächlicher und technischer Hinsicht zu beobachten und entsprechende Normen gegebenenfalls nachzubessern (Bundesverfassungsgericht, Beschluss vom 1. Dezember 2020, Aktenzeichen 2 BvR 916/11, 2 BvR 636/12, Randnummer 265), und somit die Einwände gegen die Geeignetheit nicht vollständig zurückgewiesen.

Im Hinblick auf die Regelungen in anderen Ländern, den schwerwiegenden Eingriff in das informationelle Selbstbestimmungsrecht sowie mit Blick auf die Zweifel hinsichtlich der Geeignetheit der elektronischen Fußfessel hat der Landesbeauftragte für Datenschutz und Informationsfreiheit daher angeregt, zu prüfen, ob die Einsatzszenarien nicht auf erhebliche Gefahren terroristischer Straftaten sowie auf Gefahren für die sexuelle Selbstbestimmung begrenzt werden können.

Auch die zweite vorgesehene Befugnis, nach der das Tragen einer elektronischen Fußfessel angeordnet werden kann, ist nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit kritisch zu bewerten. Danach ist die Anordnung, eine Fußfessel zu tragen, bei tatsächlichen Anhaltspunkten für die Annahme zulässig, dass eine Person, die für eine Gefahr verantwortlich ist, an einem bestimmten Ort mit einer gefährdeten Person zusammentrifft und die für die Gefahr verantwortliche Person innerhalb eines übersehbaren Zeitraumes Leib, Leben oder Freiheit der gefährdeten Person gefährden oder eine mit einer Mindeststrafe von drei Monaten sanktionierbare Straftat gegen die sexuelle Selbstbestimmung einer bestimmten Person begehen wird. Die unbestimmte Weite des Anwendungsbereiches, die nicht nur auf Hochrisikofälle beschränkt ist, führt dazu, dass die vorgelegte Fassung einen weiten Anwendungsspielraum lässt. Nach dem Gesetzeswortlaut ist es sogar möglich, Kinder und Jugendliche mit der Maßnahme zu belegen. Kritisch ist daneben auch zu bewerten, dass diese Befugnis die Möglichkeit schafft, bereits im Gefahrenvorfeld polizeilich aktiv zu werden.

5.4.3 Standortdatenerhebung

Durch die Neufassung des § 43a Absatz 3 des vorgelegten Entwurfes zur Änderung des Bremischen Polizeigesetzes soll die Befugnis zur Ermittlung von Standortdaten weiter gefasst werden. Bislang ist die Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes durch den Einsatz technischer Mittel oder mittels Auskunft beim Diensteanbieter zulässig, um eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person abzuwehren. Diese Befugnis soll erweitert werden, indem der Tatbestand um die Formulierung „oder der Begehung einer Straftat von auch im Einzelfall erheblicher Bedeutung“ ergänzt wird. Nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit können die Befugnisse

zur Standortdatenerhebung grundsätzlich in verfassungskonformer Weise ausgeweitet werden. Nach seiner Bewertung ist aber die gewählte Form der Ergänzung problematisch. Sie dürfte insbesondere dazu führen, dass die Tatbestandsalternativen der Gefährdung der benannten Rechtsgüter Leib, Leben oder Freiheit einer Person einerseits und der Begehung einer Straftat von auch im Einzelfall erheblicher Bedeutung andererseits nicht trennscharf voneinander abzugrenzen sind.

Des Weiteren soll nach dem übermittelten Entwurf die Subsidiaritätsklausel gestrichen und durch eine allgemein gehaltene Verhältnismäßigkeitsklausel ersetzt werden. Entsprechend der Subsidiaritätsklausel ist die Erhebung des Standortes aktuell nur zulässig, wenn die Ermittlung des Aufenthaltsortes auf andere Weise weniger erfolgversprechend oder erschwert ist. Demgegenüber soll sie nach dem Entwurf künftig bereits zulässig sein, soweit sie für die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes der oder des Betroffenen erforderlich ist.

Das vollständige Entfallen der Subsidiaritätsklausel kritisiert der Landesbeauftragte für Datenschutz und Informationsfreiheit. Die Standortdatenerhebung ist eine verdeckte Maßnahme und weist daher schon auf abstrakter Ebene eine erhöhte Eingriffsintensität auf. Bereits die Annahme, die Polizeibehörden könnten über ihr Mobilfunktelefon ihren Standort ermitteln, kann Bürgerinnen und Bürger daran hindern, die ihnen zustehenden Freiheiten wahrzunehmen. Zudem ist zu berücksichtigen, dass etwa bei der Standortermittlung über einen sogenannten IMSI-Catcher nicht nur in das informationelle Selbstbestimmungsrecht der Zielperson eingegriffen wird, sondern in das aller Personen, deren Mobiltelefone sich in die vom IMSI-Catcher erzeugte Funkzelle eingewählt haben und deren Standort – zumindest kurzfristig – gespeichert wird. Die Heimlichkeit der Maßnahme sowie der Umstand, dass Dritte im Regelfall zwangsläufig mitbetroffen werden, spricht aus der Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit insbesondere gegen die dem Gesetzesentwurf augenscheinlich zugrundeliegende Annahme, dass etwa ein Aufbrechen der Wohnungstür zwecks Aufenthaltsermittlung eingriffsintensiver als die Ermittlung des Standortes via Mobiltelefon ist.

5.4.4 Befugnisse des Landesbeauftragten für Datenschutz und Informationsfreiheit

Im Rahmen seiner Stellungnahme hat der Landesbeauftragte für Datenschutz und Informationsfreiheit ferner darauf hingewiesen, dass ihm auch nach dem nunmehr vorgelegten Entwurf keine voraussetzungslose Anordnungsbefugnis zugestanden wird und ihm damit eine wirksame Abhilfebefugnis fehlt. Nach der derzeitigen Regelung steht ihm erst eine Anordnungsbefugnis zu, nachdem er zuvor eine Beanstandung ausgesprochen hat (siehe hierzu § 85 Absatz 2 Bremisches Polizeigesetz). Dieses Stufenverhältnis führt insbesondere in Fällen der Eilbedürftigkeit, in welcher der Landesbeauftragte für Datenschutz und Informationsfreiheit

zum Schutz der Grundrechte der Betroffenen unverzügliche Maßnahmen anordnen können sollte, zu einer Aushöhlung der aufsichtsbehördlichen Abhilfebefugnisse und setzt Artikel 47 JI-Richtlinie damit nicht vollständig um.

5.4.5 Auskunftsanspruch betroffener Personen

Neben diesen kritischen Punkten bewertet der Landesbeauftragten für Datenschutz und Informationsfreiheit positiv, dass der Auskunftsanspruch betroffener Personen auf die Herausgabe von Protokolldaten erstreckt wird. Damit wird einem wichtigen Anliegen des Landesbeauftragten für Datenschutz und Informationsfreiheit Rechnung getragen.

5.5 Überwachungsgesamtrechnung

Am 2. Mai 2025 wurde die vom Max-Planck-Institut durchgeführte „Überwachungsgesamtrechnung für Deutschland“ auf der Website des Bundesministeriums für Inneres veröffentlicht. Diese „Überwachungsgesamtrechnung“ kommt für die Freie Hansestadt Bremen zu wichtigen und aus der Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit für die Gesetzgebung in der Freien Hansestadt Bremen beachtlichen Erkenntnissen.

Auffällig ist insbesondere, dass die Freie Hansestadt Bremen bezogen auf die Polizeibehörden im Vergleich zu allen anderen Bundesländern den höchsten Befugniswert hat (siehe hierzu Überwachungsgesamtrechnung für Deutschland, Band 1, Seite 74). Der Befugniswert setzt sich zusammen aus unterschiedlichen Intensitätskriterien in einer bestimmten Gewichtung einerseits und verschiedenen mitigierenden Faktoren, das heißt eingriffsmildernden Umstände, in differenzierter Gewichtung andererseits (siehe Überwachungsgesamtrechnung für Deutschland, Band 1, Seite 34 folgende). Der im bundesweiten Vergleich höchste Befugniswert der Freien Hansestadt Bremen bedeutet hinsichtlich der vom Max-Planck-Institut begutachteten Befugnisse mithin, dass das Bremische Polizeigesetz (BremPolG) die höchste Eingriffsintensität aufweist.

Dieser Umstand ist bei einer möglichen Erweiterung der Befugnisse der Polizei nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit zwingend zu berücksichtigen, insbesondere, weil sich im vorgelegten Entwurf zur Änderung des Bremischen Polizeigesetzes vor allem derartige Erweiterungen der Befugnisse, aber nur vereinzelt Erweiterungen der Rechte betroffener Personen oder neue Begrenzungen der polizeilichen Befugnisse finden lassen. Dabei kann die Eingriffsintensität von Maßnahmen schon dadurch abgeschwächt werden, dass mitigierende Faktoren, wie Prüfungsvorbehalte, ein besonderer Schutz von Berufsgeheimnisträgerinnen und -trägern und weitere Benachrichtigungs- und Protokollierungspflichten, eingeführt werden (siehe hierzu Überwachungsgesamtrechnung für

Deutschland, Band 1, Seite 34 folgende). Hierbei ist im Einzelfall eine Abwägung zu dem Aufwand erforderlich, der durch die mitigierenden Faktoren veranlasst wird. Auch in Anbetracht des Aufwandes bietet es sich aus der Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit an, etwa bei der Bestandsdatenerhebung (§ 44 BremPolG), bei der die Freie Hansestadt Bremen den höchsten Befugniswert aller Bundesländer aufweist, einen umfassenderen Richtervorbehalt einzuführen und die Befugnis auf den Schutz bedeutsamer Rechtsgüter zu beschränken. Ebenso bietet es sich an, bei der Rasterfahndung (§ 49 BremPolG), bei der die Freie Hansestadt Bremen ebenfalls den höchsten Befugniswert aufweist, einen solchen Richtervorbehalt einzuführen.

Zusammenfassend regt der Landesbeauftragte für Datenschutz und Informationsfreiheit daher an, zu prüfen, ob derartige Maßnahmen, wie soeben exemplarisch aufgezeigt, verstärkt eingeführt werden können, um die Eingriffsintensität des Bremischen Polizeigesetzes abzuschwächen.

5.6 Stichprobenartige Überprüfung der Vergabe des personengebundenen Hinweises „Psychische und Verhaltensstörung“

Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat anlässlich der öffentlichen Diskussionen über die Gefährlichkeit psychisch erkrankter Personen den Datenaustausch über psychisch erkrankte „potenzielle Täterinnen und Täter“ im Rahmen der Erstellung polizeilicher Lagebilder bei der Senatorin für Inneres und Sport überprüft. Dabei stellte die Polizei Bremen selbst fest, dass der datenschutzrechtliche Grundsatz der Erforderlichkeit nicht stringent eingehalten wurde und personenbezogene Daten über potenzielle Täterinnen und Täter gegenüber der Innenbehörde offengelegt wurden. Diese personenbezogenen Daten wären zur Wahrung des Erforderlichkeitsgrundsatzes zu anonymisieren, zumindest aber zu pseudonymisieren, weil Klarnamen nicht erforderlich sind, um ein Lagebild zu erstellen.

Zudem hat der Landesbeauftragte für Datenschutz und Informationsfreiheit mit einer stichprobenartigen Prüfung der Vergabe des personengebundenen Hinweises „Psychische und Verhaltensstörung“ durch die Polizeibehörden im polizeilichen Vorgangsbearbeitungssystem gemäß § 51 Absatz 5 Satz 1 Nummer 1 Bremisches Polizeigesetz begonnen. Personengebundene Hinweise sollen dem Schutz der Betroffenen und der Eigensicherung von Polizeibeamtinnen und -beamten dienen. Sie werden deutschlandweit einheitlich nach den Kriterien des Leitfadens zur Vergabe personengebundener Hinweise vergeben. Im Rahmen der Überprüfung erhebt der Landesbeauftragte für Datenschutz und Informationsfreiheit die Häufigkeit der Vergabe und wird stichprobenartig die Einhaltung der Vergabevoraussetzungen überprüfen. Erkrankte Bürgerinnen und Bürger unterliegen einem besonderen Schutzbedarf. Die Einhaltung gesetzlicher Vorgaben sowie des Leitfadens zur Vergabe personengebundener Hinweise ist daher unerlässlich.

5.7 Datenschutzfolgenabschätzung zur pmOWi-App beim Ordnungsdienst Bremen

Bereits im letzten Berichtsjahr hat der Landesbeauftragte für Datenschutz und Informationsfreiheit die Nutzung der pmOWi-App durch das Ordnungsamt Bremen thematisiert (siehe hierzu 7. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 5.6). Mithilfe dieser Anwendung ahnden die Außendienstmitarbeiterinnen und -mitarbeiter über eine sichere Datenverbindung Ordnungsverstöße, wobei sie dienstliche Mobilfunkgeräte nutzen. Im Bereich der Verkehrsverstöße ermöglicht die Anwendung, auf eine Datenbank der Anbieterinnen und Anbieter für sogenanntes Handyparken zuzugreifen. Mit dieser Plattform sowie mit den einzelnen Anbieterinnen und Anbietern für das Handyparken hat nicht das Ordnungsamt Bremen oder die übergeordnete Dienstelle, die Senatorin für Inneres und Sport, im Jahr 2022 Rahmenverträge unterzeichnet, sondern die Senatorin für Bau, Mobilität und Stadtentwicklung.

Die erbetenen Unterlagen sowie eine Datenschutzfolgenabschätzung im Sinne des Artikels 35 Datenschutzgrundverordnung in Verbindung mit § 67 Absatz 1 Bundesdatenschutzgesetz wurden von dem Ordnungsamt Bremen vorgelegt und durch den Landesbeauftragten für Datenschutz und Informationsfreiheit geprüft. Für die Ahndung der Ordnungswidrigkeiten wurde im Rahmen der Datenschutzfolgenabschätzung in zutreffender Weise auf die JI-Richtlinie abgestellt. Der Landesbeauftragte für Datenschutz und Informationsfreiheit begrüßte die sehr konstruktive Zusammenarbeit mit dem Ordnungsamt Bremen im Rahmen der Prüfung der Datenschutzfolgenabschätzung.

Die Prüfung war zum Redaktionsschluss noch nicht abgeschlossen, weil einige Einzelverträge mit den im Jahr 2022 aktiven Anbieterinnen und Anbietern von Handyparksystemen sowie mit dem Gatewaybetreiber dem Landesbeauftragten für Datenschutz und Informationsfreiheit durch die Senatorin für Bau, Mobilität und Stadtentwicklung, nachdem der Landesbeauftragte für Datenschutz und Informationsfreiheit sie angefordert hatte, im August des Berichtsjahres vorgelegt wurden. Diese Verträge liegen der Möglichkeit des Ordnungsamtes Bremen zu Grunde, auf die Datensammlung des Gatewaybetreibers zum Zwecke der Ahndung von Ordnungswidrigkeiten zuzugreifen. Zurzeit dauert die Prüfung des Rahmenvertrages mit dem Plattformbetreiber sowie die Prüfung der Einzelverträge mit den Handyparkanbieterinnen und -anbietern an. Insbesondere prüft der Landesbeauftragte für Datenschutz und Informationsfreiheit, ob im Vorfeld der Vertragsunterzeichnungen durch die Senatorin für Bau, Mobilität und Stadtentwicklung im Hinblick auf die intendierte Nutzung der Daten für Ordnungswidrigkeitenverfahren durch das Ordnungsamt Bremen vorab eine umfassende datenschutzrechtliche Bewertung erfolgt ist.

Die Verträge wurden im Jahr 2022 ohne Einbindung des Ordnungsamtes oder der Senatorin für Inneres und Sport als dessen Aufsichtsbehörde direkt von der Senatorin für Bau, Mobilität

und Stadtentwicklung abgeschlossen. Daher hat der Landesbeauftragte für Datenschutz und Informationsfreiheit die Verträge erst im Nachgang bei der zuständigen Senatorin für Bau, Mobilität und Stadtentwicklung angefordert.

6. Justiz

6.1 Gemeldete Datenschutzverletzungen

Im Jahr 2024 wurden von Rechtsanwältinnen und Rechtsanwälten sowie Notarinnen und Notaren bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit fünf Verletzungen des Schutzes personenbezogener Daten nach Artikel 33 Datenschutzgrundverordnung gemeldet.

Zwei Fälle hatten fehlerhafte Übermittlung von personenbezogenen Daten an einen unberechtigten Empfänger zum Gegenstand.

Durch die Staatsanwaltschaft Bremen, als verantwortliche Stelle, wurden dem Landesbeauftragten für Datenschutz und Informationsfreiheit im Berichtsjahr 29 Datenschutzverletzungen gemeldet. In allen Fällen waren auf dem behördlichen oder ordentlichen Postweg Ermittlungsakten verloren gegangen.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit nimmt die gestiegene Anzahl der Meldungen bezüglich verlorengegangener Akten wahr (19 Meldungen in 2024, zwei Meldungen in 2023). Der Landesbeauftragte für Datenschutz und Informationsfreiheit begrüßt ausdrücklich das geänderte Meldeverhalten von Datenschutzverletzungen im Bereich der Staatsanwaltschaft Bremen. Unabhängig davon wird der Landesbeauftragte für Datenschutz und Informationsfreiheit mit der Generalstaatsanwaltschaft Bremen über Maßnahmen zur Vermeidung von Datenschutzverletzungen durch verlorengegangene Akten diskutieren, sobald die Zuständigkeit des Landesbeauftragten für Datenschutz und Informationsfreiheit als datenschutzrechtliche Aufsichtsbehörde im Bremischen Ausführungsgesetz zur EU-Datenschutz-Grundverordnung Bremen kodifiziert ist (siehe hierzu Ziffer 6.5 dieses Berichtes).

Im Jahr 2025 wurden durch die Finanzverwaltung Bremen, die Landeshauptkasse Bremen sowie durch die Angehörigen der steuerberatenden Berufe insgesamt 14 Fälle von Datenschutzverletzungen gemeldet. In einigen Fällen war Ursache der Datenschutzverletzungen der Fehlversand von Unterlagen an falsche Empfängerinnen und Empfänger per Briefpost oder E-Mails. In drei Fällen erfolgten vorsorgliche Meldungen im Nachgang zu Hacking-Angriffen.

Durch die Amtsgerichte im Land Bremen wurden vier Vorgänge mit Datenschutzverletzungen gemeldet. In einem Fall wurde einer anderen Behörde versehentlich eine unzutreffende Akte zur elektronischen Einsichtnahme zur Verfügung gestellt. In einem Fall des Amtsgerichtes Bremen haben mehrere Bedienstete des Gerichtes ihre beruflich eingerichteten Zugriffe auf das Melderegister der Stadtgemeinde Bremen sowie der Melderegister weiterer Kommunen im Bundesgebiet genutzt, um Melderegisterabfragen über andere Bedienstete sowie deren Angehörige durchzuführen (siehe hierzu Ziffer 6.6 dieses Berichtes).

6.2 Auskunftsverweigerung durch Rechtsanwälte und Notare

In einem Fall hatte eine Rechtsanwältin und Notarin eine Datenschutzverletzung, nämlich den Fehlversand einer E-Mail samt Vertragsentwurf, beim Landesbeauftragten für Datenschutz und Informationsfreiheit gemeldet. Um die Sachverhaltsdarstellung sowie die Vollständigkeit der Meldung überprüfen zu können, hatte der Landesbeauftragte für Datenschutz und Informationsfreiheit die entsprechende fehlversandte E-Mail samt Vertragsentwurf angefordert. Die Rechtsanwältin und Notarin hat die Herausgabe mit Verweis auf das Berufsgeheimnis verweigert. Zudem legte die Rechtsanwältin und Notarin ein entsprechendes Schreiben des Landgerichtes Bremen vor, das ihre Rechtsauffassung bestätigte.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat nachfolgend die Stellungnahme zu datenschutzrechtlichen Fragestellungen durch das Landgericht Bremen gerügt und trat für zukünftige Fälle einer vergleichbaren Tätigkeit im Bereich der Datenschutzaufsicht entgegen. Denn die Befugnisse des Landgerichtes Bremen im Rahmen der Berufsaufsicht über Notare beschränken sich auf die Prüfung, ob die Amtsgeschäfte durch die Notarin beziehungsweise den Notar ordnungsgemäß erledigt werden. Die regelmäßige Prüfung erstreckt sich also nur auf die Amtsführung der jeweiligen Notarin beziehungsweise des jeweiligen Notars. Zur Amtsführung einer Notarin oder eines Notars sowie einer Rechtsanwältin oder eines Rechtsanwaltes gehört allerdings nicht die Führung eines datenschutzaufsichtsbehördlichen Verfahrens. Deshalb kann sich die Berufsaufsicht nicht zu etwaigen Rechtsfragen äußern, die aufsichtsbehördliche Verfahren des Landesbeauftragten für Datenschutz und Informationsfreiheit betreffen.

In der Sache ist die Rechtsauffassung der Rechtsanwältin und Notarin sowie des Landgerichtes Bremen unzutreffend. Denn nach Artikel 58 Absatz 1 Buchstabe a) Datenschutzgrundverordnung (DSGVO) kann der Landesbeauftragte für Datenschutz und Informationsfreiheit die Verantwortliche, die Auftragsverarbeiterin und gegebenenfalls die Vertreterin der Verantwortlichen oder der Auftragsverarbeiterin anweisen, alle Informationen bereitzustellen, die für die Erfüllung seiner Aufgaben erforderlich sind. Nach der ständigen Rechtsprechung gehören dazu nicht nur reine Auskünfte, sondern für die Erfüllung der Aufgaben der Datenschutzaufsichtsbehörde können auch Beschreibungen, Aufstellungen, Kopien, Screenshots oder Informationen in sonstigen Formaten, also auch die Vorlage von E-Mails oder Verträgen, erforderlich sein. Dieser Rechtsprechung hat sich auch das Verwaltungsgericht Bremen in einem anderen Fall angeschlossen (siehe hierzu Verwaltungsgericht Bremen, Urteil vom 27. November 2023, Aktenzeichen 4 K 1160/22).

Die Datenschutzgrundverordnung genießt im Übrigen Anwendungsvorrang gegenüber den nationalen Vorschriften, also beispielsweise auch denen aus der Bundesrechtsanwaltsord-

nung und der Bundesnotarordnung. Insoweit kann nationales materielles Recht, wie der nationale Berufsgeheimnisschutz, nicht ohne Weiteres herangezogen werden, um die Datenschutzgrundverordnung einzuschränken, sondern es bedarf Regelungen und Öffnungsklauseln in der Datenschutzgrundverordnung selbst. Eine solche Öffnungsklausel, die die Auskunftsbegehren der Datenschutzaufsichtsbehörden nach Artikel 58 Absatz 1 Buchstabe a) DSGVO beschränkt, existiert nicht und kann daher auch nicht für einen Ausschluss herangezogen werden. Insoweit besteht keine Möglichkeit der Rechtsanwältin und Notarin, die Beantwortung seitens des Landesbeauftragten für Datenschutz und Informationsfreiheit gestellten Fragen aufgrund des Berufsgeheimnisschutzes zu verweigern.

6.3 Urteil des Verwaltungsgerichtes Bremen zur Veröffentlichung von Daten in Gläubigerinformationssystemen

Bereits im 5. Jahresbericht nach der Datenschutzgrundverordnung ist über die unbeschränkte Veröffentlichung der personenbezogenen Daten von Insolvenzschuldnerinnen und -schuldnern in den Gläubigerinformationssystemen der meistbestellten deutschlandweit tätigen Insolvenzkanzleien mit Standort in Bremen berichtet worden (siehe hierzu 5. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 7.4). Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat zwischenzeitlich aufgrund der festgestellten Verstöße Verwarnungen erlassen und Geldbußen gegen die betreffenden Kanzleien verhängt. Die Rechtmäßigkeit der Maßnahmen wurde vom Verwaltungsgericht Bremen mit Urteil vom 21. Mai 2025 (Aktenzeichen 4 K 3063/23 [nicht rechtskräftig]) bestätigt. Danach verstößt die unbeschränkte für jedermann zugängliche Veröffentlichung personenbezogener Daten in einem Gläubigerinformationssystem gegen Artikel 6 Absatz 1 Datenschutzgrundverordnung, weil § 5 Absatz 5 Insolvenzordnung den Zugriff auf die Gläubigerinformationssysteme ausschließlich den tatsächlichen Insolvenzgläubigern vorbehalten will.

6.4 Aufsichtsbehördliche Zuständigkeit des Landesbeauftragten für Datenschutz und Informationsfreiheit für die Staatsanwaltschaft Bremen

In Bezug auf den Geschäftsbereich der Senatorin für Justiz und Verfassung behinderte die ungenügende rechtliche Ausgestaltung der aufsichtsbehördlichen Zuständigkeit des Landesbeauftragten für Datenschutz und Informationsfreiheit in Bezug auf die Staatsanwaltschaft Bremen im Berichtsjahr die Arbeit der Datenschutzaufsichtsbehörde. Eine fehlende Zuständigkeit des Landesbeauftragten für Datenschutz und Informationsfreiheit hat zur Folge, dass datenschutzrechtliche Beschwerden gegen die Staatsanwaltschaft nicht sachgerecht bearbeitet werden können. Entscheidendes Hindernis für die Wahrnehmung der Aufsichtsfunktionen

ist weiterhin, dass die JI-Richtlinie nicht umfassend in der Freien Hansestadt Bremen umgesetzt worden ist.

Nach europäischem Recht ist der Landesbeauftragte für Datenschutz und Informationsfreiheit für die datenschutzrechtliche Aufsicht sowohl im Anwendungsbereich der Datenschutzgrundverordnung (DSGVO) als auch im Anwendungsbereich der JI-Richtlinie zuständig. Diese Richtlinie reguliert die Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ordnungswidrigkeiten oder der Strafvollstreckung. Im Unterschied zur Datenschutzgrundverordnung, die als Rechtsverordnung in den Mitgliedsstaaten unmittelbar gilt, bedarf es bei der JI-Richtlinie einer Transformation in nationales Recht. Gemäß Artikel 41 Absatz 1 JI-Richtlinie sind in den Mitgliedsstaaten Aufsichtsbehörden zu bestimmen, die die Anwendung der Richtlinie überwachen. Dies geschieht in den Mitgliedsstaaten durch nationales Recht.

Das Bremische Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG) bestätigt in § 2 Absatz 6 BremDSGVOAG die Zuständigkeit des Landesbeauftragten für Datenschutz und Informationsfreiheit als datenschutzrechtliche Aufsichtsbehörde in der Freien Hansestadt Bremen bisher ausschließlich für den Anwendungsbereich der Datenschutzgrundverordnung. Im Falle der Anwendbarkeit der JI-Richtlinie ist der Landesbeauftragte für Datenschutz und Informationsfreiheit bisher nur zuständige Aufsichtsbehörde, sofern es sich um Datenverarbeitungen nach dem Bremischen Polizeigesetz (BremPolG) oder dem Bremischen Gesetz zum Schutz personenbezogener Daten im Justizvollzug (BremJVollzDSG) handelt. Daraus folgt, dass bei einer Datenverarbeitung der Staatsanwaltschaft Bremen für Zwecke der Strafverfolgung eine aufsichtsbehördliche Zuständigkeit bisher nicht gegeben ist.

Auch eine ersatzweise Heranziehung des § 500 Absatz 1, Absatz 2 Nummer 2 Strafprozessordnung (StPO) begründet keine aufsichtsbehördliche Zuständigkeit des Landesbeauftragten für Datenschutz und Informationsfreiheit für die Staatsanwaltschaft Bremen, weil diese Norm auf den dritten Teil des Bundesdatenschutzgesetzes (BDSG) verweist, der die JI-Richtlinie auf Bundesebene umsetzt, nicht aber auf den ersten Teil des Bundesdatenschutzgesetzes (insbesondere § 16 BDSG), in dem die aufsichtsbehördlichen Zuständigkeiten und Befugnisse geregelt sind.

Dies hat zur Folge, dass mangels einer Transformation einiger Artikel der JI-Richtlinie in nationales Recht, diese direkt anwendbar sind. Somit sieht der Landesbeauftragte für Datenschutz und Informationsfreiheit auch jetzt schon seine aufsichtsbehördliche Zuständigkeit für die Staatsanwaltschaft Bremen gemäß den Artikeln 41 fortfolgende JI-Richtlinie als gegeben.

Der Verpflichtung zur Transformation der JI-Richtlinie in nationales Recht ist dennoch nachzukommen. Daher hat der Landesbeauftragte für Datenschutz und Informationsfreiheit der Senatorin für Justiz und Verfassung eine Änderung des Bremischen Ausführungsgesetzes zur

EU-Datenschutz-Grundverordnung dahingehend vorgeschlagen, dass dort ergänzend eine Zuständigkeitsregelung – vergleichbar mit den Regelungen in anderen Bundesländern – kodifiziert wird. Dies wurde von der Senatorin für Justiz und Verfassung zunächst abgelehnt. Sodann wurde ein Entwurf für eine Änderung des bremischen Gesetzes zur Ausführung der Strafprozessordnung formell als Befassung im Sinne von § 21 Absatz 3 Nummer 2 BremDSGVOAG vorgelegt.

In seiner Stellungnahme wies der Landesbeauftragte für Datenschutz und Informationsfreiheit den Entwurf zurück, weil er unter anderem nicht umfassend die Aufsichtsbefugnis des Landesbeauftragten für Datenschutz und Informationsfreiheit regelt. Zum Beispiel ist die Zuständigkeit des Landesbeauftragten für Datenschutz und Informationsfreiheit für Ordnungswidrigkeiten nicht in der gebotenen Weise kodifiziert und dem Landesbeauftragten für Datenschutz und Informationsfreiheit werden keine Abhilfe- und Beratungsbefugnisse zugestanden.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit sieht für die Ausübung seiner vollumfänglichen aufsichtsbehördlichen Tätigkeit im Anwendungsbereich der JI-Richtlinie eine kurzfristige Ergänzung des Bremischen Ausführungsgesetzes zur EU-Datenschutz-Grundverordnung im Sinne seiner Stellungnahme an die Senatorin für Justiz und Verfassung weiterhin als dringend erforderlich an (siehe hierzu 7. Jahresbericht nach der Datenschutzgrundverordnung; Ziffer 6.4).

6.5 Aufsichtsbefugnis des Landesbeauftragten für Datenschutz und Informationsfreiheit bei der Einführung von E-Akten bei der ordentlichen Gerichtsbarkeit

Ende des Jahres 2024 erlangte der Landesbeauftragte für Datenschutz und Informationsfreiheit über die Berichterstattung in der Presse Kenntnis darüber, dass in der Freien Hansestadt Bremen in der ordentlichen Gerichtsbarkeit die digitale Akte (E-Akte) eingeführt worden ist und dass bis zum 1. Januar 2026 bundesweit und somit auch in der Freien Hansestadt Bremen die gesamte Justiz die dortigen analogen Prozesse auf digitale Aktenführung transformieren muss. Auf schriftliche Nachfrage bei den Gerichten und in der weiteren Kommunikation erhielt der Landesbeauftragte für Datenschutz und Informationsfreiheit eine Antwort durch die Senatorin für Justiz und Verfassung. Diese bestätigte, dass bereits im Januar des Berichtsjahres an allen Amtsgerichten der Freien Hansestadt Bremen, am Landgericht Bremen und am Hanseatischen Oberlandesgericht in Bremen in Zivilsachen alle Akten digital geführt würden. Außerdem war man bei Gerichtsakten für Insolvenzen, Nachlassangelegenheiten, Grundbuchangelegenheiten und Familiensachen im Wesentlichen zu diesem Zeitpunkt ebenfalls schon zur digitalen Aktenführung übergegangen.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit forderte daraufhin weitere Informationen zur datenschutzrechtlichen Ausgestaltung der E-Akte an und bat um Vorlage der Dokumentation der Vorabprüfung (zum Beispiel zu einer Datenschutzfolgenabschätzung im Sinne des Artikels 35 Datenschutzgrundverordnung [DSGVO]). Seitens der Senatorin für Justiz und Verfassung wurde die Vorlage jeglicher Dokumentation mit dem Hinweis auf Artikel 55 Absatz 3 DSGVO verweigert.

Artikel 55 Absatz 3 DSGVO schützt die Unabhängigkeit der Gerichte und nimmt deren Verarbeitungstätigkeiten im Rahmen ihrer justiziellen Tätigkeit von der Aufsichtsbefugnis der Datenschutzaufsichtsbehörden aus, um die Unabhängigkeit der Tätigkeit der Gerichte sicherzustellen. Nach der Rechtsauffassung der Senatorin für Justiz und Verfassung erstreckt sich die richterliche Unabhängigkeit auf sämtliche mithilfe der E-Akten durchgeführte Handlungen. Folglich gehöre das Implementieren und Nutzen elektronischer Gerichtsakten vollumfänglich in den Bereich der justiziellen Tätigkeit im Sinne des Artikels 55 Absatz 3 DSGVO und sei daher von der datenschutzrechtlichen Aufsichtsbefugnis des Landesbeauftragten für Datenschutz und Informationsfreiheit ausdrücklich ausgenommen.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit legte im Folgenden seine Auffassung dar, dass das Anlegen der digitalen Fallakten, die Speicherung von Dokumenten, die Protokollierung von Zugriffsdaten und die Umsetzung eines Löschkonzeptes keine richterlichen Tätigkeiten darstellten, sondern reines Verwaltungshandeln der Gerichte beinhalteten, das der aufsichtsbehördlichen Kontrolle unterliege. Bei der Einführung des digitalen Aktensystems für die ordentliche Gerichtsbarkeit handele es sich um reines Verwaltungshandeln der Gerichte und damit nicht um richterliche Tätigkeit. Schließlich sei für die Implementierung der Software im Gericht nicht die Richterin oder der Richter, sondern eine andere Organisationseinheit aus dem Bereich der Verwaltung der Gerichte zuständig.

Im Herbst übersandte der Landesbeauftragte für Datenschutz und Informationsfreiheit den ordentlichen Gerichten der Freien Hansestadt Bremen Anhörungen nach § 28 Absatz 1 Verwaltungsverfahrensgesetz zur beabsichtigten Anordnung nach Artikel 58 Absatz 1 Buchstabe a) DSGVO. Darin gewährte er als zuständige Aufsichtsbehörde für den Datenschutz nach Artikel 55 DSGVO in Verbindung mit § 21 Absatz 1 Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG) rechtliches Gehör und die Möglichkeit einer Stellungnahme zu der beabsichtigen Anordnung, zunächst eine Schwellenwertanalyse vorzulegen.

Die Leitungen der Gerichte haben als Reaktion auf die Anhörungen ausgeführt, dass sie die Rechtsauffassung der Senatorin für Justiz und Verfassung teilten und mangels Aufsichtsbefugnis des Landesbeauftragten für Datenschutz und Informationsfreiheit der Anordnung nicht nachzukommen beabsichtigten. Die weitere Prüfung des Sachverhaltes dauert an.

6.6 Ermittlungen zu Meldeauskünften beim Amtsgericht Bremen

Einer durch das Amtsgericht Bremen gemeldeten Datenschutzverletzung lag der folgende Sachverhalt zugrunde: Mehrere Bedienstete des Gerichtes haben ihre beruflich eingerichteten Zugriffe auf das Melderegister der Stadtgemeinde Bremen sowie der Melderegister weiterer Kommunen im Bundesgebiet genutzt, um Melderegisterabfragen über andere Bedienstete sowie deren Angehörige durchzuführen. Die Sachverhaltsaufklärung gestaltete sich unter anderem als schwierig, weil dem Landesbeauftragten für Datenschutz und Informationsfreiheit die die Zugriffe dokumentierenden Protokolldaten nicht oder nur unzureichend vorgelegt wurden. Zu Redaktionsschluss stand der Abschluss der Sachverhaltsaufklärung noch aus.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit wird unter anderem prüfen, ob das Gericht hinreichende technische und organisatorische Maßnahmen zur Verhinderung derartiger Abfragen ergriffen hat.

6.7 Hafenkriminalität

Das Thema der Hafenkriminalität kam in diesem Berichtsjahr verstärkt und in unterschiedlicher Ausprägung auf den Landesbeauftragten für Datenschutz und Informationsfreiheit zu.

Zum einen meldeten sich Fuhrparkunternehmerinnen und -unternehmer bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit. Diese berichteten darüber, ein Terminalbetreiber führe unter Berufung auf den International Ship and Port Facility Security Code ein neues Fahreridentifizierungssystem ein, das die ursprüngliche Truckerkarte durch einen digitalen Gatepass ersetze. Aufgrund dieser Information leitete der Landesbeauftragte für Datenschutz und Informationsfreiheit mit den ebenfalls betroffenen Datenschutzaufsichtsbehörden aus Hamburg und Niedersachsen eine gemeinsame Prüfung ein.

Zum anderen wurde dem Landesbeauftragten für Datenschutz und Informationsfreiheit die Verordnung über Vorgaben für ein sicheres und digitales Containerfreistellungsverfahren auf Grundlage des Bremischen Hafensicherheitsgesetzes zur Stellungnahme übermittelt. Im Rahmen dessen musste der Landesbeauftragte für Datenschutz und Informationsfreiheit feststellen, dass er bei den vorherigen Änderungen des Bremischen Hafensicherheitsgesetzes nicht nach § 21 Absatz 3 Satz 2 Nummer 2 Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung beteiligt wurde und entsprechend keine Möglichkeit zur Stellungnahme hatte, obwohl die Änderungen auch die Verarbeitung personenbezogener Daten betrafen. Grundlegende Hinweise konnten seinerseits daher nicht mehr erfolgen. Er regte aber an, explizit zu regeln, welche personenbezogenen Daten erforderlich sind, um die vorgesehene Fahrer-ID zu erstellen. Wünschenswert ist aus der Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit zudem, dass das Zusammenspiel von Fahreridentifizierungssystemen

der Terminalbetreiber mit den Containerfreigabesystemen gesetzlich geregelt wird, auch um eine unnötige doppelte Datenerhebung zu vermeiden.

Aufgrund der Berichterstattung in der Presse befasste sich der Landesbeauftragte für Datenschutz und Informationsfreiheit außerdem mit dem Hinweis-Meldeportal Hafenkriminalität. Er prüfte insbesondere, ob die Nichtabrufbarkeit der eingegangenen Meldungen eine Verletzung des Schutzes personenbezogener Daten im Sinne des Artikels 33 Datenschutzgrundverordnung (DSGVO) beziehungsweise § 65 Bundesdatenschutzgesetz (BDSG) darstellte, weil die lang gespeicherten und nicht abgerufenen Daten möglicherweise dem Zugriff Dritter hätten ausgesetzt sein können. Der Stellungnahme der Staatsanwaltschaft Bremen konnte der Landesbeauftragte für Datenschutz und Informationsfreiheit jedoch entnehmen, dass dies nicht der Fall war, sodass er keine Meldepflicht nach Artikel 33 DSGVO beziehungsweise § 65 BDSG annahm.

Ebenfalls prüfte er im Rahmen dessen, ob die Einführung des Portals eine Datenschutzfolgenabschätzung nach Artikel 35 DSGVO beziehungsweise § 67 BDSG bedingt hätte, kam aber auch hier zu dem Ergebnis, dass auf eine solche verzichtet werden konnte. Er wies jedoch darauf hin, dass die falsche Rechtsgrundlage für die Datenverarbeitung im Meldeportal angegeben wurde.

6.8 Befassung nach dem Bremischen Ausführungsgesetz zur EU-Datenschutz-Grundverordnung mit einem Gesetzesentwurf

Im vorigen Berichtsjahr wurde dem Landesbeauftragen für Datenschutz und Informationsfreiheit durch die Senatorin für Justiz und Verfassung ein Entwurf eines Bremischen Gesetzes über den Erlass eines Gesetzes über die Sicherheit in Justizgebäuden (BremJustizGG-E) und die Änderung des Bremischen Polizeigesetzes mit der Bitte übersandt, den Entwurf in datenschutzrechtlicher Hinsicht zu prüfen (siehe hierzu 7. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 6.7). Insbesondere wurde auf § 6 BremJustizGG-E – generelle Einlasskontrollen – hingewiesen. Die Übersendung erfolgte per E-Mail an das Office-Postfach des Landesbeauftragten für Datenschutz und Informationsfreiheit. Somit war der Landesbeauftragte für Datenschutz und Informationsfreiheit mit dem Entwurf offiziell befasst im Sinne des § 21 Absatz 3 Nummer 2 Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG).

Zu den Aufgaben und Befugnissen des Landesbeauftragten für Datenschutz und Informationsfreiheit gehört es, Stellung zu Rechts- und Verwaltungsvorschriften zu nehmen, die die Verarbeitung personenbezogener Daten betreffen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit ist rechtzeitig über die entsprechenden Entwürfe zu unterrichten.

Er nahm Stellung zum Gesetzesentwurf und erläuterte, insbesondere in Bezug auf § 6 BremJustizGG-E seine datenschutzrechtlichen Bedenken.

In der Stellungnahme zum 7. Jahresbericht des Landesbeauftragten für Datenschutz nach der Datenschutzgrundverordnung teilte die Senatorin für Justiz und Verfassung zu Ziffer 6.7 des Vorjahresberichtes mit, dass man dort Trennlinien zwischen einem informatorischen Vorfeldaustausch auf Referentenebene und der gesetzlich vorgesehenen Befassung des Landesbeauftragten für Datenschutz und Informationsfreiheit mit Entwürfen von Rechts- und Verwaltungsvorschriften erörtern wolle (Bremische Bürgerschaft, Drucksache 21/1352, Seite 14).

Der Landesbeauftragte für Datenschutz und Informationsfreiheit weist in diesem Zusammenhang darauf hin, dass er hinsichtlich des Entwurfes des Bremischen Gesetzes über den Erlass eines Gesetzes über die Sicherheit in Justizgebäuden offiziell im Sinne von § 21 Absatz 3 Nummer 2 BremDSGVOAG befasst worden und seiner gesetzlichen Aufgabe nachgekommen ist, zu Rechts- und Verwaltungsvorschriften, welche die Verarbeitung personenbezogener Daten betreffen, Stellung zu nehmen. Hierüber hat er ebenfalls entsprechend der gesetzlichen Vorgaben der Bremischen Bürgerschaft berichtet.

7. Gesundheit

7.1 Gemeldete Datenschutzverletzungen

Verantwortliche aus dem Gesundheitsbereich haben bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit im Berichtszeitraum 37 Meldungen zu Datenschutzverletzungen abgegeben. Neben dem Zugriff auf personenbezogene Daten im Zusammenhang mit Cyberangriffen (siehe hierzu Ziffer 7.1.1 dieses Berichtes) betrafen die Meldungen insbesondere Fehlübermittlungen von Gesundheitsdaten oder die unsachgemäße Entsorgung sensibler Daten.

7.1.1 Hackerangriff auf Krankenhauskonzern

Es zeigte sich auch im aktuellen Berichtsjahr erneut, dass Gesundheitseinrichtungen zu Angriffszielen von Cyberkriminellen gehören. Dieses Mal traf es einen Krankenhauskonzern, der mehrere Einrichtungen verschiedener Fachrichtungen in der Freien Hansestadt Bremen neben Einrichtungen in anderen Bundesländern betreibt. Hacker verschafften sich durch das Ausnutzen von Schwachstellen zunächst Zugang zu der zentralen Dateiablage des Krankenhauskonzerns. Glücklicherweise konnten die Hauptsysteme für die Verarbeitung von Patientinnen- und Patientendaten, wie etwa das Krankenhausinformationssystem sowie zentrale Personaldatenverarbeitungssysteme, nicht erreicht werden. Dennoch wurden im Zuge des Angriffes sowohl Daten von Patientinnen und Patienten als auch Beschäftigtendaten verschlüsselt und teilweise kopiert und entwendet. Da der Krankenhauskonzern in der Stadt Bremen unter anderem ein Fachkrankenhaus für Psychiatrie, Psychotherapie und Psychosomatik betreibt, führt jegliche Kompromittierung zu sehr hohen Risiken bei den betroffenen Patientinnen und Patienten sowie zu der Gefahr eines Vertrauensverlustes.

Das Herunterfahren der IT-Systeme sowie die Nutzung von Backup-Dateien verhinderte, dass die Einrichtungen durch den Angriff handlungsunfähig wurden. Zwar war die Verfügbarkeit der verarbeiteten Daten zum Teil eingeschränkt, einen großflächigen Ausfall der medizinischen Versorgung konnte der Krankenhauskonzern jedoch verhindern.

Betroffene Personen stellen sich im Nachgang eines solchen Vorfalles zu Recht die Frage, was mit ihren Daten passiert, in wessen Händen sie gelangt sind und zu welchen Zwecken sie verwendet werden. Diese Fragen lassen sich – wie auch in diesem Fall – häufig nicht beantworten. Um sich dennoch auf mögliche negative Folgen einstellen zu können, bedarf es seitens der oder des Verantwortlichen einer transparenten Kommunikation über die Geschehnisse. In enger Abstimmung mit den Datenschutzaufsichtsbehörden der anderen betroffenen Länder nahm der Landesbeauftragte für Datenschutz und Informationsfreiheit frühzeitig nach

Erhalt der Meldung des Vorfalles Kontakt zu dem Krankenhauskonzern auf. Neben der Ermittlung und dem Abstellen der Schwachstellen, die den Zugang zu den Daten ermöglichten, stand hierbei die Beratung zu den öffentlichen Bekanntmachungen auf der Website des Krankenhauskonzerns sowie zu der Umsetzung einer individuellen Benachrichtigung der betroffenen Personen im Fokus. Ziel des Verfahrens ist es, dass die Systeme durch das Nachschärfen von technischen Datensicherungsmaßnahmen zukünftig soweit gehärtet werden, dass bei möglichen erneuten Angriffen ein Zugang zu personenbezogenen Daten verhindert wird.

Zugleich sind, wie in solchen Fällen üblich, auch die Polizeibehörden der betroffenen Länder sowie das Bundesamt für Sicherheit in der Informationstechnik mit dem Vorfall in eigener Zuständigkeit befasst.

7.1.2 Diebstahl von Laptop und Backup-Datenträger

Eine Meldung im Berichtsjahr betraf den Verlust von Datenträgern einer Logopädie-Praxis. Die Inhaberin der Praxis war mit einem Rucksack unterwegs, in dem sich ein Laptop mit Patientinnen- und Patientendaten sowie eine Festplatte mit einer Sicherungskopie dieser Daten befanden. Versehentlich ließ die Inhaberin den Rucksack an einer Straßenbahnhaltestelle liegen, was sie erst einige Zeit später bemerkte. Als sie den Rucksack holen wollte, war dieser nicht mehr aufzufinden. Erst am Abend wurde der Rucksack ohne die Datenträger wiedergefunden. Zwar waren sowohl der Laptop als auch die Festplatte sicher verschlüsselt, wodurch nicht von einer unbefugten Offenlegung der darauf befindlichen Patientinnen- und Patientendaten auszugehen ist. Allerdings führte der Vorfall zu einem vollständigen Verlust der gespeicherten Patientinnen- und Patientendaten. Dieser wäre vermeidbar gewesen, wenn das primäre Speichermedium und der Backup-Datenträger nicht zusammen transportiert worden wären. Denn eine Datensicherung ist nur dann wirksam, wenn sie nicht den gleichen Risiken wie die Hauptdatenspeicherung unterworfen wird. Durch den gemeinsamen Transport und den zeitgleichen Verlust konnte der Zweck der Datensicherung, die Verfügbarkeit der Daten im Falle eines physischen oder technischen Zwischenfalles sicherzustellen, nicht mehr erfüllt werden und das Risiko des Datenverlustes hat sich verwirklicht.

7.2 Neuorganisation des Bremer Krebsregisters

Die Senatorin für Gesundheit, Frauen und Verbraucherschutz informierte den Landesbeauftragten für Datenschutz und Informationsfreiheit im Berichtsjahr über eine Änderung in der Organisation des Bremer Krebsregisters. Dieses besteht organisatorisch aus einer sogenannten Vertrauensstelle, einer Auswertungsstelle sowie einer gemeinsamen ärztlichen Leitung. Die Vertrauensstelle übernimmt in diesem Gefüge eine Art Gatekeeper-Funktion. Sie verwaltet die identifizierenden Daten von Krebspatientinnen und -patienten und gibt diese in pseudonymisierter Form für Auswertungs- und Forschungszwecke an die Auswertungsstelle weiter.

Bisher wurde die Aufgabe der Vertrauensstelle von der Kassenärztlichen Vereinigung Bremen übernommen. Die Auswertungsstelle sowie die gemeinsame ärztliche Leitung übertrug die Senatorin für Gesundheit, Frauen und Verbraucherschutz dem Leibniz-Institut für Präventionsforschung und Epidemiologie. Nun kündigte die Kassenärztliche Vereinigung Bremen an, die Aufgabe der Vertrauensstelle zum Jahreswechsel aufzugeben, woraufhin seitens der Senatorin für Gesundheit, Frauen und Verbraucherschutz ein neuer Träger gefunden werden musste. Die senatorische Dienststelle entschied sich, auch diese Aufgabe dem Leibniz-Institut für Präventionsforschung und Epidemiologie zu übertragen, sodass zukünftig alle drei Organisationseinheiten des Bremer Krebsregisters vom Leibniz-Institut für Präventionsforschung und Epidemiologie übernommen werden sollen.

Im Rahmen seiner Beteiligung äußerte der Landesbeauftragte für Datenschutz und Informationsfreiheit tiefgreifende datenschutzrechtliche Bedenken gegen die geplante Neuorganisation. Die Bündelung aller Organisationseinheiten an einer Stelle führt aus seiner Sicht zu einer Aufhebung der Unabhängigkeit der Vertrauensstelle. Sämtliche Entscheidungen hinsichtlich der Verarbeitung der Registerdaten werden dann – mit Ausnahme der teilweise gesetzlich geforderten Einbindung der Fachaufsichtsbehörde und des wissenschaftlichen Beirates – lediglich in einer Stelle getroffen. Die Kontroll- und Schutzfunktion, die der Vertrauensstelle hinsichtlich der Identitätsdaten von Patientinnen und Patienten zukommt, wird somit geschwächt. Erschwerend kommt hinzu, dass es sich bei dem Leibniz-Institut für Präventionsforschung und Epidemiologie um eine Forschungseinrichtung handelt, die selbst mit Krebsregisterdaten forscht. Dies führt nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit zu einer Interessenkollision in Bezug auf die Aufgabe der Vertrauensstelle, die unabhängig und allein im Interesse der betroffenen Person sowie der Senatorin für Gesundheit, Frauen und Verbraucherschutz agieren soll. Bestehen daneben auch eigene Interessen, erhöht dies Missbrauchsgefahren.

Die kritische Positionierung des Landesbeauftragten für Datenschutz und Informationsfreiheit hatte zur Folge, dass die Beteiligten im Rahmen von mehreren Gesprächsrunden technische und organisatorische Maßnahmen erörterten, um den erhöhten Risiken zu begegnen. Hierbei stellte sich heraus, dass eine umfassende Separierung der Vertrauensstelle im institutionellen Gefüge des Leibniz-Institutes für Präventionsforschung und Epidemiologie bereits geplant war. In diesem Zusammenhang drang der Landesbeauftragte für Datenschutz und Informationsfreiheit insbesondere darauf, durch geeignete technische Protokollierungen sicherzustellen, dass ein unbefugter Umgang mit den Registerdaten jederzeit nachvollzogen und aufgeklärt werden kann. Um Missbrauchsrisiken zu begegnen, bedarf es zudem regelmäßiger Kontrollen durch die Senatorin für Gesundheit, Frauen und Verbraucherschutz als zuständige Fachaufsichtsbehörde sowie einer eindeutigen Definition und verlässlichen Kommunikation der bestehenden Weisungsrechte. Die Beteiligten setzten die geforderten Nachbesserungen zum Teil bereits um und kündigten im Übrigen weitere Maßnahmen an.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit wird den Prozess weiter begleiten und die getroffenen Kompensationsmaßnahmen prüfen. Mit der Datenverarbeitung im Bremer Krebsregister geht unweigerlich ein hohes Risiko für die betroffenen Personen einher. Letztere, die sich aufgrund der Krebserkrankung ohnehin in einer Notsituation befinden, können sich der Verarbeitung kaum entziehen, weil es sich bei dem Bremer Krebsregister um ein Pflichtregister handelt. Das Bremer Krebsregister enthält daher hochsensible Gesundheitsdaten einer Vielzahl von Bürgerinnen und Bürgern. Eine Verringerung des Schutzniveaus kann vor diesem Hintergrund nur hingenommen werden, wenn von Seiten des Verantwortlichen allen dadurch entstehenden bekannten und vorhersehbaren Risken durch technische und organisatorische Maßnahmen angemessen begegnet wird.

7.3 Beratung bei umfassender Softwareumstellung im Gesundheitsamt Bremen

Im Dezember 2024 informierte das Gesundheitsamt Bremen den Landesbeauftragten für Datenschutz und Informationsfreiheit darüber, dass für das Jahr 2025 die Einführung einer neuen Software geplant sei. Diese werde als Vorgangsbearbeitungssystem unter anderem im Fachbereich Psychiatrie und Sucht, beim zahnärztlichen Dienst, beim Kinder- und Jugendgesundheitsdienst sowie in der Kinder- und Jugendpsychiatrischen Beratungsstelle eingesetzt. Die datenschutzrechtliche Dokumentation, inklusive einer Datenschutzfolgenabschätzung, sollte dem Landesbeauftragten für Datenschutz und Informationsfreiheit zugeleitet werden. Auf Nachfrage wurde einige Wochen später mitgeteilt, die Durchführung einer Datenschutzfolgenabschätzung werde nicht mehr für erforderlich gehalten.

Sinn und Zweck einer Datenschutzfolgenabschätzung ist es, vor der Einführung einer Datenverarbeitung mögliche Risiken für die betroffenen Personen zu identifizieren und zu evaluieren, ob die getroffenen Maßnahmen diese hinreichend eindämmen können. Sie dient ferner dazu, einen vollständigen Überblick über die Datenverarbeitung zu erlangen. Die Datenschutzgrundverordnung schreibt eine Datenschutzfolgenabschätzung für diejenigen Datenverarbeitungen vor, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge haben. Als Hilfestellung für Verantwortliche hat der Europäische Datenschutzausschuss im Rahmen einer Leitlinie aufgeschlüsselt, welche Faktoren für ein hohes Risiko sprechen. Werden in großem Umfang besondere Kategorien personenbezogener Daten, wie etwa Gesundheitsdaten oder Daten zur ethnischen Herkunft, verarbeitet oder betrifft die Verarbeitung besonders schützenswerte Personen, wie zum Beispiel Minderjährige, ist von einem hohen Risiko auszugehen.

Da das Gesundheitsamt Bremen seine neue Software als zentrales Vorgangsbearbeitungssystem sowohl für sensible Bereiche, wie die Gemeindepsychiatrie, als auch für die Verarbeitung von Daten Minderjähriger im Bereich des Kinder- und Jungendgesundheitsdienstes sowie

weiterer Bereich einsetzen wird, sind die Kriterien, die für ein hohes Risiko sprechen, ohne Weiteres erfüllt. Der Landesbeauftragte für Datenschutz und Informationsfreiheit sprach sich aus diesem Grund wiederholt für das Erfordernis einer Datenschutzfolgenabschätzung aus. Die Unsicherheiten führten im Gesundheitsamt Bremen dazu, dass sich die Erstellung der datenschutzrechtlichen Dokumentation verzögerte. Aufgrund terminlicher Zwänge wurde sodann begonnen, die Software einzuführen, ohne dass die datenschutzrechtlichen Folgen abschließend bewertet wurden. Auch aus diesem Grund gestaltet es sich für den Landesbeauftragten für Datenschutz und Informationsfreiheit schwierig, das Vorhaben zu begleiten.

Bei einem aufgabenübergreifenden Vorgangsbearbeitungssystem ist darauf zu achten, dass die personenbezogenen Daten der einzelnen Bereiche getrennt voneinander verarbeitet werden, um sicherzustellen, dass die Datenverarbeitung auf den gesetzlich erlaubten Umfang beschränkt bleibt. Zudem müssen Missbrauchsrisiken von innen wie von außen durch angemessene Maßnahmen eingedämmt werden. Der Landesbeauftragte für Datenschutz und Informationsfreiheit wirkte in mehreren Stellungnahmen und Gesprächen daraufhin, dass eine datenschutzkonforme systemseitige Protokollierung implementiert wird und die Löschfristen den einzelnen Aufgabengebieten entsprechend eingerichtet werden. Er beabsichtigt, das Ausrollen der Software im Gesundheitsamt Bremen weiter zu begleiten.

Der Vorgang zeigt allerdings: Eine umfassende Softwareumstellung sollte gut geplant sein. Dabei ist die Erstellung einer datenschutzrechtlichen Dokumentation mehr als die bloße Erfüllung einer Nachweispflicht. Sie trägt dazu bei, die Verarbeitung im Vorfeld umfassend zu prüfen, um ungewollte und folgenreiche Verletzungen des Schutzes personenbezogener Daten zu verhindern.

7.4 Angebot zur Durchführung einer HPV-Impfung

Bereits in den beiden vorigen Jahresberichten nach der Datenschutzgrundverordnung wurde über die datenschutzrechtlichen Probleme bei der Umsetzung des Impfangebotes des Gesundheitsamtes Bremen zur Durchführung einer HPV-Impfung in Kooperation mit den Schulen im Stadtgebiet Bremen berichtet (siehe hierzu 7. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 7.2; 6. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 8.5).

In diesem Berichtsjahr stand abermals die datenschutzkonforme Bereitstellung von Schülerinnen- und Schülerdaten an das Gesundheitsamt Bremen im Zentrum der Beratung. Zunächst konnte diesbezüglich keine abschließende Klärung erfolgen, woraufhin das Impfangebot nach den Informationen des Landesbeauftragten für Datenschutz und Informationsfreiheit zunächst ausgesetzt wurde.

Derweil schuf auch das Gesundheitsamt Bremerhaven ein Impfangebot zur Durchführung einer HPV-Impfung für Schülerinnen und Schüler. Es wurde ein Verfahren implementiert, das

ohne eine personenbezogene Übermittlung von Schülerinnen- und Schülerdaten an das Gesundheitsamt Bremerhaven auskommt. Lediglich die Anzahl der Schülerinnen und Schüler aus den jeweiligen Klassen, in denen das Impfangebot stattfindet, werden vom Schulamt Bremerhaven an das Gesundheitsamt Bremerhaven übermittelt. Mangels Personenbezuges bestehen gegen eine solche Übermittlung aus datenschutzrechtlicher Sicht keine Bedenken. Hinsichtlich des Verfahrens sowie der verwendeten Informationsschreiben zog das Gesundheitsamt Bremerhaven den Landesbeauftragten für Datenschutz und Informationsfreiheit beratend hinzu. In diesem Rahmen wurden Empfehlungen für kleinere Anpassungen, insbesondere hinsichtlich der Freiwilligkeit des Angebotes, ausgesprochen.

Das Gesundheitsamt Bremen ist schließlich dem Vorbild Bremerhavens gefolgt und teilte im November des Berichtsjahres mit, dass nunmehr nur noch die Anzahl der Schülerinnen und Schüler der Klassen, in denen das Impfangebot unterbereitet werde, von dem Senator für Kinder und Bildung an das Gesundheitsamt Bremen übermittelt werden solle.

Dem Landesbeauftragten für Datenschutz und Informationsfreiheit zeigt dieses Beispiel, dass es manchmal nur wenige Anpassungen im Verfahren braucht, um datenschutzrechtlichen Anforderungen zu entsprechen und somit Gesundheits- und Datenschutz in Einklang zu bringen. Er begrüßt, dass dem Vorbild Bremerhavens insofern gefolgt worden ist.

7.5 Einsatz von Dienstleistern in Heilberufspraxen

Damit der Praxisalltag reibungslos ablaufen kann, werden am Markt zahlreiche Dienstleistungen zur Unterstützung angeboten. Praxen können hierdurch zum Beispiel den Prozess der Terminbuchung vereinfachen, etwa indem Online-Terminbuchungen ermöglicht oder Telefonassistenten eingesetzt werden. Auf mögliche datenschutzrechtliche Fallstricke im Bereich der Terminverwaltung hat der Landesbeauftragte für Datenschutz und Informationsfreiheit bereits im 6. Jahresbericht hingewiesen (siehe hierzu 6. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 8.3). Im vorliegenden Berichtsjahr veröffentlichte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu dem Thema „Datenschutz bei der Terminverwaltung durch Heilberufspraxen“ ein Positionspapier, das die rechtliche Situation beleuchtet und die Pflichten der Praxen in diesem Zusammenhang erläutert.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit stellt fest, dass Dienstleister zunehmend auch Produkte unter Verwendung Künstlicher Intelligenz anbieten. Gerade bei der Verarbeitung von Gesundheitsdaten ist der Einsatz einer Anwendung von Künstlicher Intelligenz gründlich zu prüfen. Neben den grundlegenden datenschutzrechtlichen Fragen ist hierbei in besonderem Maße zu untersuchen, ob durch die Anwendung von Künstlicher Intelligenz bei der Verarbeitung von Gesundheitsdaten die Patientinnen- und Patientendaten auch für eigene Zwecke des Dienstleisters verarbeitet werden, etwa für das Training einer Anwendung, die

Künstliche Intelligenz verwendet. Ist dies der Fall, muss geklärt werden, ob hierfür eine rechtliche Grundlage existiert. Auch stellen sich Fragen der datenschutzrechtlichen Verantwortlichkeit, weil eine Auftragsverarbeitung gemäß Artikel 28 Datenschutzgrundverordnung ausscheidet, wenn der Dienstleister die Daten zu eigenen Zwecken verwendet. Praxen sollten sich zudem vergewissern, dass die Daten im eigenen Herrschaftsbereich verbleiben und das Berufsgeheimnis gewahrt bleibt.

7.6 Videoüberwachung in Heilberufspraxen

Es mehren sich Berichte von Praxisinhaberinnen und -inhabern über eine Veränderung des sozialen Klimas in ihren Praxen. Aggressives Verhalten sowie verbale und in Extremsituationen auch tätliche Angriffe auf das Praxispersonal nähmen zu. Um sich gegen diese Entwicklung zu schützen, wird zunehmend in Betracht gezogen, die Praxisräumlichkeiten mit Videokameras auszustatten. Potenzielle Täterinnen und Täter sollen dadurch abgeschreckt oder im Nachgang ermittelt und zur Rechenschaft gezogen werden können.

Allerdings sind die Voraussetzungen für eine zulässige Videoüberwachung eng: Mangels einer spezifischen Rechtsgrundlage für den Einsatz von Videoüberwachung in Heilberufspraxen kann diese regelmäßig nur auf Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f) Datenschutzgrundverordnung (DSGVO) als Erlaubnistatbestand gestützt werden. Eine Videoüberwachung ist daher nur zulässig, wenn eine durchgeführte Interessenabwägung zu Gunsten der Sicherheitsinteressen der Praxis(-beschäftigten) ausfällt. Hierbei ist zunächst eindeutig festzulegen, welcher Zweck mit der Videoüberwachung erreicht werden soll. Ist der Zweck klar definiert – also die Frage, welches Ziel erreicht werden soll, eindeutig beantwortet –, gilt es zu überprüfen, ob die geplante Videoüberwachung den Zweck erfüllen kann und welche alternativen Möglichkeiten existieren.

Geht es beispielsweise darum, potenzielle Einbrecherinnen und Einbrecher abzuhalten, rechtfertigt dies nicht eine Videoüberwachung während des regulären Praxisbetriebes. Besteht der Zweck in dem Schutz des Praxispersonals vor übergriffigen Personen, ist zu prüfen, ob mildere Alternativen in Betracht kommen. Im Fall von Übergriffen auf Praxisbeschäftigte wäre es vorstellbar, dass eine räumliche Trennung die Übergriffe verhindert; so stellt ein entsprechender Anmeldetresen eine nur schwer überwindbare und nicht ohne Weiteres zu umgehende Barriere dar. Auch kann gegebenenfalls genügen, um das Ziel, dem die Videoüberwachung dienen soll, zu erreichen, dass Personen die Praxis nur nach Betätigung einer Türklingel betreten könnten. Ebenfalls wäre ein Notfallknopf denkbar, der im Falle einer Aktivierung sowohl die Polizei informiert als auch eine Videoaufzeichnung starten könnte, die erst dann beginnt und keine permanente Überwachung darstellt. Im Bereich Deeskalation besonders geschulte Personen vor Ort könnten zudem die Situation entschärfen, bevor es zu Übergriffen kommt.

Sind die Zwecke der Videoüberwachung ermittelt, müssen diese den schutzwürdigen Interessen aller von der Videoüberwachung betroffenen Personen gegenübergestellt werden und im Ergebnis überwiegen. Die Rechtsprechung (Bundesverwaltungsgericht, Urteil vom 27. März 2019 – 6 C 2/18) verlangt diesbezüglich, dass „in Bezug auf die beobachteten Räume eine erhebliche über das allgemeine Lebensrisiko hinausgehende Gefährdungslage besteht". Lassen die von der Videokamera erfassten Bilder konkrete Rückschlüsse auf den Gesundheitszustand der betroffenen Personen zu, sind die Anforderungen noch höher.

Bei einem Unsicherheitsgefühl überwiegen regelmäßig die schutzwürdigen Interessen der von der Videoüberwachung erfassten Personen. Dies betrifft sowohl die Patientinnen und Patienten als auch die Beschäftigten oder auch Mitarbeitende von Lieferanten oder anderen Dienstleistern. Entscheidend ist aber, auf welche tatsächlichen Anhaltspunkte das Unsicherheitsgefühl sich gründet und welche Rechtsgüter durch die Gefahr betroffen sein können.

Die rechtliche Bewertung hängt auch davon ab, welche Bereiche von der Videoüberwachung erfasst werden sollen. So ist etwa eine dauerhafte Überwachung des Wartezimmers mit einem stärkeren Eingriff in die Persönlichkeitsrechte verbunden als eine Überwachung des Eingangsbereiches außerhalb der Öffnungszeiten, weil Patientinnen und Patienten über einen viel längeren Zeitraum der Videoüberwachung ausgesetzt sind als in einem reinen Durchgangsbereich.

Die Eingriffsintensität wird zudem davon bestimmt, wie die Videoüberwachung technisch ausgestaltet ist. Diesbezüglich ist zum Beispiel zu klären, ob die Aufnahmen gespeichert werden, für welchen Zeitraum und an welchem Ort die Speicherung erfolgt und wie die Zugriffsrechte ausgestaltet sind.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit sieht den Einsatz von Videoüberwachung in dem sensiblen Bereich von Heilberufspraxen sehr kritisch und rät Verantwortlichen dringend dazu, zuvor relevante Vorfälle zu dokumentieren und alternative Maßnahmen auszuschöpfen, mit denen die Sicherheit der Beschäftigten sowie der Patientinnen und Patienten sichergestellt werden kann. Sofern die Voraussetzungen für eine zulässige Videoüberwachung ausnahmsweise erfüllt sind, gelten hierfür sämtliche Pflichten der Datenschutzgrundverordnung. Insbesondere ist auf eine hinreichende Information gemäß Artikel 13 DSGVO in Form eines Hinweisschildes, das bei Betreten des überwachten Bereiches gut sichtbar ist, zu achten.

8. Soziales

8.1 Gemeldete Datenschutzverletzungen

Verantwortliche aus dem Sozialbereich haben bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit im Berichtszeitraum 23 Meldungen zu Datenschutzverletzungen abgegeben. Schwerpunktmäßig handelte es sich bei diesen um Vorfälle, bei denen es zu Fehlversendungen von Dokumenten und zum Abhandenkommen von elektronischen Geräten kam, auf denen personenbezogene Daten gespeichert waren.

8.2 Einführung der elektronischen Patientenakte

Nachdem die gesetzlichen Krankenkassen bereits seit dem 15. Januar 2025 verpflichtet waren, allen Versicherten, die nicht widersprochen haben, eine elektronische Patientenakte bereitzustellen, ist die Nutzung der elektronischen Patientenakte seit dem 1. Oktober 2025 nun auch für alle Leistungserbringer verpflichtend.

Verantwortliche Stellen für den Einsatz der elektronischen Patientenakte sind die gesetzlichen Krankenkassen. Mit Ausnahme der AOK Bremen/Bremerhaven handelt es sich bei den übrigen in Bremen ansässigen Krankenkassen um bundesunmittelbare Krankenkassen, die der datenschutzrechtlichen Aufsicht der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterliegen. Die Aufsichtsbefugnis des Landesbeauftragte für Datenschutz und Informationsfreiheit ist im Kontext der elektronischen Patientenakte demgegenüber beschränkt. Insbesondere erfolgt auch die Prüfung von datenschutzrechtlichen Problemen in der IT-Architektur der elektronischen Patientenakte wegen ihrer Zuständigkeit für die gematik durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Die gematik trägt als Nationale Digitalagentur für Gesundheit die Gesamtverantwortung für die Telematikinfrastruktur, über die neben der elektronischen Patientenakte auch andere zentrale Anwendungen, wie das E-Rezept, laufen.

Aus datenschutzrechtlicher Sicht bringt die Einführung der elektronischen Patientenakte zwei wesentliche Vorteile mit sich. Zum einen stärkt sie die Patientensouveränität in Bezug auf die Verarbeitung der Gesundheitsdaten. Durch das Zugriffsrecht auf die elektronische Patientenakte über die jeweilige App der elektronischen Patientenakte der gesetzlichen Krankenkasse haben Versicherte die Möglichkeit, jederzeit Einblick in wesentliche sie betreffende Dokumente, wie Arztbriefe, Medikationspläne oder Ähnliches, zu nehmen. Zusätzlich können sie steuern, ob andere Gesundheitseinrichtungen Einsicht in die Dokumente nehmen können.

Zum anderen entfällt durch die elektronische Patientenakte in vielen Fällen die Übermittlung von Arztbriefen und anderen Dokumenten an Mit- oder Weiterbehandler auf herkömmlichem

Weg. Eine Übermittlung der Daten ist in diesen Fällen nicht mehr erforderlich, was zugleich das Risiko von der Nutzung unsicherer Kommunikationskanäle senkt.

Allerdings müssen die Versicherten sich ihrer Kontroll- und Einstellmöglichkeiten auch bewusst sein. Die elektronische Patientenakte erfordert somit entsprechende digitale Fähigkeiten. Ohne aktives Handeln der Versicherten haben durch die elektronische Patientenakte mehr Stellen als zuvor Zugriff auf die sensiblen medizinischen Daten.

Auch stehen den Versicherten der gesetzlichen Krankenkassen im Zusammenhang mit der elektronischen Patientenakte die datenschutzrechtlichen Betroffenenrechte zu. Insbesondere ist hierbei zu betonen, dass die Nutzung der elektronischen Patientenakte weiterhin freiwillig bleibt. So steht es allen Versicherten zu, der Einrichtung der elektronischen Patientenakte vollständig zu widersprechen oder, sofern eine elektronische Patientenakte bereits angelegt wurde, der Aktenanlage vollständig zu widersprechen, was die Löschung der elektronischen Patientenakte und der in ihr gespeicherten Daten zur Folge hat.

Im Rahmen der Einführung der elektronischen Patientenakte kam es zu einigen Meldungen von IT-Sicherheitsschwachstellen innerhalb der IT-Infrastruktur. Nach den Informationen des Landesbeauftragten für Datenschutz und Informationsfreiheit wurden diese mittlerweile geschlossen.

8.3 Digitale Akteneinsicht durch Sozialbehörden

Im Berichtsjahr erreichte den Landesbeauftragen für Datenschutz und Informationsfreiheit der Hinweis einer Bürgerin auf eine Datenschutzverletzung im Zusammenhang mit einer digitalen Akteneinsicht. Diese hatte bei dem Amt für Versorgung und Integration Bremen (AVIB) einen Antrag auf Akteneinsicht gestellt. Um diesem Gesuch nachzukommen, wurde ihr von der Sozialbehörde per E-Mail ein Link zu einem Datenraum zur Verfügung gestellt. Innerhalb dieses Datenraumes befanden sich circa fünfzig digitale Akten anderer Personen. Diese Akten konnte die Antragsstellerin vollständig einsehen und herunterladen.

Grundsätzlich bietet eine digitale Akteneinsicht einige Vorteile gegenüber der analogen Akteneinsicht. So müssen Bürgerinnen und Bürger nicht mehr vor Ort bei den entsprechenden Behörden vorstellig werden. Auch wird die Gefahr einer falschen postalischen Versendung, sei es durch falsche Adressierung oder veraltete Adressdatenbanken, ausgeschlossen.

Wie sich in diesem Fall jedoch zeigt, birgt die digitale Akteneinsicht selber aber einige Gefahren, deren sich die Akteneinsicht gewährenden Stellen bewusst sein müssen. Eine Akteneinsicht per Versand eines Dokumentes per E-Mail, deren Inhalt beispielsweise nicht durch einen Passwortschutz gesichert ist, ist dabei in jedem Fall keine taugliche Variante. Bei der Akteneinsicht in Akten aus dem Sozialbereich werden darüber hinaus regelmäßig Sozialdaten und besondere Kategorien personenbezogener Daten Teil der Akten sein. Solche Daten sollten,

unabhängig davon, ob es sich um eine Akteneinsicht handelt, nicht per unverschlüsselter E-Mail versendet werden. Die versendende Stelle kann, wenn die Akte mit einer unverschlüsselten E-Mail verschickt wird, nicht sicherstellen, dass Unbefugte keine Kenntnis von den Inhalten der E-Mail erhalten. Die Integrität sowie Vertraulichkeit der Daten können in so einem Fall nicht sichergestellt werden. Verantwortliche sollten sich dabei an der Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail orientieren.[6] Die Nutzung von E-Mails zur Akteneinsicht wird sich zudem schon aus praktischen Gründen häufig nicht anbieten, weil die digitalen Akten oftmals eine beträchtliche Dateigröße haben werden.

Vorzugswürdig ist dagegen die Nutzung sogenannter Datenräume, wie sie auch von der Sozialbehörde im zugrundeliegenden Fall genutzt wurden. Diese ermöglichen das Hoch- und Herunterladen großer Dateimengen. Gleichzeitig sollte ein Datenraum aber stets ebenfalls durch ein für den Einzelfall generiertes Passwort geschützt werden.

Aber selbst, wenn, wie vorliegend, alle oben genannten technischen Voraussetzungen erfüllt sind, bedarf es weiterhin auch organisatorischer Maßnahmen, um zu verhindern, dass personenbezogene Daten offengelegt werden.

Die Sozialbehörde hat im Anschluss an das Tätigwerden des Landesbeauftragen für Datenschutz und Informationsfreiheit ein Vier-Augen-Prinzip zur Kontrolle der Freigabe der digitalen Akteneinsicht eingeführt. Durch diese und ähnliche organisatorische Maßnahmen muss sichergestellt werden, dass nicht durch Fehler einer Bearbeiterin oder eines Bearbeiters die falschen Akten Teil einer Akteneinsicht auf dem digitalen Weg werden.

[6] Orientierungshilfe abrufbar unter „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf.

9. Bildung

9.1 Gemeldete Datenschutzverletzungen

Im aktuellen Berichtsjahr gab es im Bereich Bildung und Schule zehn Meldungen nach Artikel 33 Datenschutzgrundverordnung seitens der oder des Verantwortlichen an den Landesbeauftragten für Datenschutz und Informationsfreiheit. Hierbei betrafen sechs Meldungen Schulen und vier Meldungen die Hochschulen in der Freien Hansestadt Bremen.

Die Gründe für die gemeldeten Datenschutzverletzungen waren überwiegend Sicherheitsvorfälle durch versandte Phishing- und Spam-E-Mails oder auch die Offenlegung von personenbezogenen Daten durch den Fehlversand von E-Mails. Darüber hinaus erreichten den Landesbeauftragen für Datenschutz und Informationsfreiheit in diesem Berichtsjahr mehrere Beschwerden im Bildungsbereich. Auch hier war die unbefugte Offenlegung von personenbezogenen Daten der Hauptbeschwerdegegenstand, so wurde sich in zwei Fällen über den Aushang von Klassenfotos in der Schule beschwert, weil hierfür die entsprechende Einwilligung der Eltern nicht vorlag. Ferner betrafen mehrere Beschwerden den Versand von E-Mails mit offenem E-Mail-Verteiler.

9.2 Umgang mit personenbezogenen Daten bei der Schulaufsicht

Für Schülerinnen und Schüler haben datenschutzrechtliche Fragestellungen eine hohe Relevanz. Nur wenn sich eine Schülerin oder ein Schüler sicher sein kann, dass auf personenbezogene Informationen auch nur die Personen Zugriff haben, die diese angehen, kann sie oder er auf Missstände ohne Angst vor Konsequenzen hinweisen. Wer immer damit rechnen muss, dass Informationen über die eigene Person verbreitet werden, die er oder sie geheim oder vertraulich behandelt wissen will, kann nicht so stark und mutig auftreten, wie sie oder er es für sachgerecht und angemessen hält. Auch aus diesem Grund schützt das Grundgesetz das Grundrecht auf informationelle Selbstbestimmung in Artikel 2 Absatz 1 Grundgesetz (GG) in Verbindung mit Artikel 1 Absatz 1 GG die personenbezogenen Daten, also auch personenbezogene Schülerinnen- und Schülerdaten, in besonderem Maße.

In diesem Berichtsjahr erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit mehrere Beschwerden in Bezug auf den Umgang mit personenbezogenen Daten von Schülerinnen und Schülern beziehungsweise deren Erziehungsberechtigten durch das für die Schulaufsicht zuständige Referat bei dem Senator für Kinder und Bildung.

So wurde in einem Fall die E-Mail eines Beschwerdeführers ohne dessen Einwilligung durch die Schulaufsicht an die betreffende Schulleitung weitergeleitet. Gemäß § 11 Absatz 1 Bremisches Schuldatenschutzgesetz (BremSchulDSG) darf der Senator für Kinder und Bildung personenbezogene Daten von Schülerinnen und Schülern, von Schulbewerberinnen und

-bewerbern sowie deren Erziehungsberechtigten verarbeiten, wenn dies erforderlich ist, um seine Aufgaben zu erfüllen. Immer wenn Daten übermittelt werden, sind insbesondere der Erziehungs- und Bildungsauftrag der Schule sowie das Vertrauensverhältnis zwischen den Schülerinnen beziehungsweise den Schülern und der Schule zu berücksichtigen. Sofern es sich lediglich um eine allgemeine Anfrage handelt, die auch ohne Weiterleitung an die Schule beantwortet werden kann, so ist die Erforderlichkeit einer Weiterleitung regelmäßig nicht gegeben.

Im Rahmen des Prüfverfahrens teilte der Senator für Kinder und Bildung mit, dass der konkrete Vorfall zum Anlass genommen worden sei, noch einmal auf die zu beachtende Verfahrensweise hinzuweisen. Dementsprechend ist in derartigen Fällen stets die Einwilligung für die Weiterleitung von E-Mails von der senatorischen Dienststelle an die Schulen einzuholen. Lediglich, wenn die Absenderinnen und Absender ausdrücklich darauf hinweisen, dass die E-Mail weitergeleitet werden dürfe, kann von einer erneuten Nachfrage bei den Absenderinnen und Absendern abgesehen werden.

Die eingegangenen Beschwerden wurden darüber hinaus zum Anlass für einen intensiven Austausch mit der Schulaufsicht und zur Prüfung der dortigen Verarbeitungsvorgänge genommen. Auch die Schulaufsicht hat in sehr konstruktiver Art und Weise aufgrund der datenschutzrechtlichen Aufsichtsverfahren die Erarbeitung beziehungsweise Anpassung von Prozessen geprüft. So wurde ein Leitfaden zum Umgang mit Beschwerden durch die Schulaufsicht entwickelt, der dem Landesbeauftragten für Datenschutz und Informationsfreiheit zur Abstimmung in Bezug auf die datenschutzrechtlichen Fragestellungen übersandt wurde. Das Verfahren und der Austausch sind aktuell noch nicht abgeschlossen.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit geht davon aus, dass die Schulaufsicht bei dem Senator für Kinder und Bildung auch zukünftig bei geplanten Änderungen auf den Landesbeauftragten für Datenschutz und Informationsfreiheit zukommt, um die datenschutzrechtlichen Voraussetzungen abzuklären.

9.3 Einführung der auf Künstlicher Intelligenz beruhenden Software telli in den Schulen

Die Digitalisierung der Schulen ist weiterhin ein aktuelles Thema. Aufgrund der in diesem Zusammenhang bestehenden datenschutzrechtlichen Fragestellungen hat sich der Landesbeauftragte für Datenschutz und Informationsfreiheit schon in den vergangenen Jahren mit dem Senator für Kinder und Bildung auf einen regelmäßigen Austausch verständigt. Der fachliche Austausch erfolgt mehrmals jährlich mit der zuständigen Abteilung bei dem Senator für Kinder und Bildung. Ziel ist es, bei den geplanten Projekten der Schuldigitalisierung frühzeitig even-

tuelle Datenschutzfragen beziehungsweise Datenschutzrisiken festzustellen und Lösungsvorschläge zu erarbeiten. Eine frühzeitige Einbeziehung des Landesbeauftragten für Datenschutz und Informationsfreiheit, die sich als sehr konstruktiv erweist, ist nicht nur sinnvoll, sondern auch notwendig, um die datenschutzrechtlichen Möglichkeiten, aber auch die rechtlichen und technischen Grenzen aufzeigen zu können.

So beriet der Landesbeauftragte für Datenschutz und Informationsfreiheit den Senator für Kinder und Bildung unter anderem im Nachgang zu der Einführung der auf Künstlicher Intelligenz beruhenden Software telli, die von den Schulen seit Beginn des Schuljahres 2025/2026 genutzt werden kann. Im Frühjahr 2025 wurde der Landesbeauftragte für Datenschutz und Informationsfreiheit zunächst in allgemeiner Form über eine mögliche Einführung von telli informiert. In diesem Zusammenhang wies er bereits darauf hin, dass es notwendig sei, eine Datenschutzfolgenabschätzung zu erstellen.

Bei telli handelt es sich um eine vom Institut für Film und Bild in Wissenschaft und Unterricht gemeinnützige GmbH angebotene Anwendung, welche die Nutzung verschiedener Large Language Models ermöglicht. Die Schülerinnen und Schüler erhalten über die Lehrkräfte mittels eines zeitlich befristeten QR-Codes Zugang zu der Anwendung. Neben Chat-Funktionen wird telli nach den vorgelegten Unterlagen Funktionalitäten, wie zum Beispiel die Erstellung von Dialogpartnerinnen und -partnern, Klassendialogen oder die zeitlich begrenzte Speicherung der Chatverläufe, enthalten.

Die Datenschutzfolgenabschätzung sowie die weiteren datenschutzrechtlich relevanten Dokumente konnten durch den Senator für Kinder und Bildung erst nach der bereits erfolgten Einführung von telli übermittelt werden. Da die Einführung von telli auch in weiteren Bundesländern geplant ist, ist zeitnah eine Abstimmung mit den betreffenden Datenschutzaufsichtsbehörden im Rahmen des Arbeitskreises Schulen und Bildungseinrichtungen geplant. Im Arbeitskreis Schulen und Bildungseinrichtungen stimmen sich alle Landesdatenschutzaufsichtsbehörden ab, um ein möglichst einheitliches Vorgehen bei länderübergreifenden Fragestellungen zu erreichen. Die datenschutzrechtliche Bewertung ist daher noch nicht abgeschlossen und erfolgt, abgestimmt mit den anderen Datenschutzaufsichtsbehörden, um ein möglichst hohes und einheitliches Datenschutzniveau in ganz Deutschland zu gewährleisten.

9.4 Stichprobenartige Überprüfung der Videoüberwachung an Schulen

Aufgrund von zwei Beschwerden, die sich gegen eine Videoüberwachung an einer Bremer Grundschule richteten, hat der Landesbeauftragte für Datenschutz und Informationsfreiheit im Berichtsjahr mit einer stichprobenartigen Überprüfung der Videoüberwachung an Schulen im Stadtgebiet Bremen begonnen. Zwecks dieser Prüfung hat er zehn weitere Schulen angeschrieben, die nach seinen Informationen über eine Videoüberwachung verfügen sollen. Von

diesen zehn Schulen betrieben derzeit tatsächlich sieben eine Videoüberwachung, die der Landesbeauftragte für Datenschutz und Informationsfreiheit derzeit noch prüft.

Die Zulässigkeit einer Videoüberwachung von Schulgebäuden hängt von einer Vielzahl von Faktoren ab. Rechtsgrundlage für die Videoüberwachung ist § 15 Absatz 1 Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG). Gemäß § 15 Absatz 1 BremDSGVOAG ist eine Videoüberwachung durch öffentliche Stellen zulässig, soweit sie zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die der oder dem Verantwortlichen übertragen wurde, zum Schutz von Personen, Eigentum oder Besitz oder zur Kontrolle von Zugangsberechtigungen erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen betroffener Personen überwiegen.

Die Videoüberwachung muss daher zunächst zu einem der genannten Zwecke erforderlich sein. Diese Erforderlichkeit muss von den Schulen nachgewiesen werden (sogenannte Rechenschaftspflicht, siehe auch Artikel 5 Absatz 2 Datenschutzgrundverordnung [DSGVO]). Wenn die Erforderlichkeit bejaht werden kann, ist aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit in einem nächsten Schritt zwischen einer Videoüberwachung außerhalb und innerhalb der Schulzeiten zu differenzieren. Letztere ist nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit im Regelfall aus Gründen der Verhältnismäßigkeit unzulässig. Allerdings ist zum Beispiel die Überwachung von Fahrradständern, bei denen den gesamten Tag über eine erhöhte Diebstahlsgefahr angenommen werden kann und bei denen sich Schülerinnen und Schülern während des Schulalltages nicht über einen längeren Zeitraum hinweg aufhalten, nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit im Regelfall auch während der Schulzeit zulässig. Bei einem Fahrraddiebstahl handelt es sich in der Regel um einen Diebstahl in einem besonders schweren Fall, der einen Strafrahmen mit bis zu zehn Jahren Freiheitsstrafe aufweist. Gerade für Familien mit geringen Einkommen stellen Fahrräder für ihre Kinder zudem Gegenstände von erheblichem Wert dar, sodass diese auch in ihrer Lebensführung durch einen Fahrraddiebstahl stark betroffen sind. Die Überwachung des Schulgeländes und eine partielle Überwachung des Schulgebäudes im Inneren während der Schulzeiten muss hingegen ein Ausnahmefall sein. Hier sind nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit besonders hohe Rechtfertigungsanforderungen zu erfüllen. Denkbar sind insbesondere Fälle, in denen die Zugangsberechtigung nicht anders sichergestellt werden können und damit nur durch eine Videoüberwachung der Schutz der Schülerinnen und Schüler vor Dritten sichergestellt werden kann, etwa bei Schulen in der Nähe von Kriminalitätsschwerpunkten.

Entscheidend ist zudem, dass die Videoüberwachung in transparenter Weise erfolgt. Hierzu ist eine regelmäßige Information an die Lehrerinnen und Lehrer sowie Schüler- und Elternschaft sowie das Aufstellen von Hinweisschildern erforderlich. Des Weiteren müssen die Rahmenbedingungen eindeutig geregelt werden, etwa die Frage, wer darf, zu welchen Zwecken Einsicht nehmen. Darüber hinaus muss eine hinreichende technische Sicherheit der Anlage gewährleistet werden (siehe hierzu Artikel 32 DSGVO).

10. Bau, Wohnen, Umwelt, Energie und Verkehr

10.1 Gemeldete Datenschutzverletzungen

In den Bereichen Bau, Wohnen, Umwelt, Energie und Verkehr erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit insgesamt 14 Meldungen über Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung.

Bereits im vorangegangenen Berichtsjahr war ein deutlicher Rückgang der gemeldeten Vorfälle festzustellen (siehe hierzu 7. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 10.1). Diese Entwicklung setzt sich fort. Die Ursache für die abnehmende Anzahl der Meldungen lässt sich gegenwärtig noch nicht abschließend beurteilen.

10.2 SCHUFA-Eintrag bei Schwarzfahrenden

Anlässlich verschiedener Presseberichte sowie einer Bürgerschaftsanfrage erhielt der Landesbeauftragte für Datenschutz und Informationsfreiheit Kenntnis von einem seitens eines Verkehrsunternehmens geplanten Pilotprojektes, wonach bei Fahren ohne ein gültiges Fahrticket nicht mehr eine Strafanzeige wegen Erschleichens von Leistungen gestellt werden soll, sondern dieses Verhalten über Meldungen an eine private Wirtschaftsauskunftei durch ein Inkassounternehmen verfolgt und geahndet werden sollte. Ziel des Projektes sei gewesen, die Bremer Justiz zu entlasten. Daraufhin leitete der Landesbeauftragte für Datenschutz und Informationsfreiheit ein aufsichtsbehördliches Verfahren ein und forderte das Verkehrsunternehmen auf, eine datenschutzrechtliche Stellungnahme zu dem beabsichtigten Vorhaben einzureichen.

In seiner Stellungnahme teilte das Unternehmen mit, dass die Realisierbarkeit des Vorhabens bislang noch nicht geprüft worden sei, sich das Projekt noch in der Konzeptionsphase befinde und daher eine abschließende Beantwortung der Fragen des Landesbeauftragten für Datenschutz und Informationsfreiheit derzeit nicht möglich sei.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit wies in diesem Zusammenhang darauf hin, dass im Falle einer konkreten Umsetzung eine rechtzeitige Stellungnahme zu den aufgeworfenen Fragestellungen zu erfolgen habe. Bei der Weiterleitung von Forderungen an eine private Wirtschaftsauskunftei durch ein Inkassobüro ist zudem zu berücksichtigen, dass diese erhebliche negative Auswirkungen auf die Bewertung der Kreditwürdigkeit der betroffenen Personen haben kann. Zweck der privaten Wirtschaftsauskunfteien ist zudem nicht, Verhalten ohne Gerichtsverfahren zu sanktionieren, um die Strafjustiz zu entlasten.

10.3 Rauchwarnmelder mit Klimamonitoring

Im Berichtsjahr befasste sich der Landesbeauftragte für Datenschutz und Informationsfreiheit erneut mit dem geplanten Einbau smarter Rauchmelder eines deutschlandweit tätigen großen Wohnungsunternehmens, die neben der klassischen Warnfunktion über eine zusätzliche Raum- und Klimamonitoringfunktion verfügen. Bereits im vergangenen Berichtsjahr hatte der Landesbeauftragte für Datenschutz und Informationsfreiheit seine Bedenken hinsichtlich des Einbaus derartiger Geräte geäußert, insbesondere im Hinblick auf einen ausreichenden Schutz des Grundrechtes auf informationelle Selbstbestimmung. Durch die zusätzliche Erhebung von Raum- und Klimadaten können Bewegungs- und Nutzungsprofile erstellt werden, die tiefgehende Rückschlüsse auf das Wohnverhalten und die individuellen Lebensgewohnheiten der Betroffenen ermöglichen (siehe hierzu 7. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 10.5).

Im Berichtsjahr begann nun auch in der Freien Hansestadt Bremen der Einbau der smarten Geräte. Dies führte zu einer hohen Anzahl von Beschwerden und Beratungsanfragen bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit. Zahlreiche Mieterinnen und Mieter hatten ihre Skepsis gegenüber der vorgesehenen Datenverarbeitung geäußert und diese auch unmittelbar gegenüber dem Konzerndatenschutzbeauftragten des Unternehmens vorgetragen.

Zunächst erhielten sie ein Ankündigungsschreiben hinsichtlich des beabsichtigten Einbaus der Geräte im Rahmen einer Modernisierungsmaßnahme nach § 555b Bürgerliches Gesetzbuch in nahezu allen Räumen inklusive der Küche, ausgenommen waren lediglich Badezimmer und Abstellräume. In dem Schreiben wurde eine „Komfortfunktion“ beschrieben, mit deren Hilfe das Wohnklima durch intelligente Lüftungshinweise per Applikation des Wohnungsunternehmens optimiert werde. Die Raumklimadaten, wie Temperatur und Luftfeuchtigkeit, sollten hierbei in einem Intervall von zwei Minuten auf Raumebene erfasst werden. Dies lässt aber Rückschlüsse auf das jeweilige Nutzungsverhalten der Mieterinnen und Mieter hinsichtlich einzelner Räume zu. Nach lokaler Speicherung sollen aus diesen Werten stündlich Durchschnittswerte gebildet und bis zu 48 Stunden gespeichert werden, bevor eine tägliche Übermittlung an einen Smart Reader (Gateway) erfolgen soll. Darüber hinaus ist eine Speicherung der Durchschnittswerte in einem Profil über einen Zeitraum von drei Jahren vorgesehen. Neben Hinweisen zum Raumklima sollen anhand von Vergleichen mit Referenzzeiträumen auch Empfehlungen zur Optimierung der Energieeffizienz erfolgen. Zusätzlich sind aggregierte und anonymisierte Auswertungen durch das Wohnungsunternehmen vorgesehen, wobei nach Angaben des Unternehmens Rückschlüsse auf einzelne Wohnungen oder Bewohnende ausgeschlossen sein sollen.

Die Aktivierung der sogenannten „Komfortfunktion“ mit den oben aufgeführten zusätzlichen Funktionalitäten soll auf einer Einwilligung nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a) Datenschutzgrundverordnung (DSGVO) beruhen. Wird diese nicht spätestens 14 Tage vor dem Einbau erteilt, soll die Installation der Geräte mit deaktivierter Komfortfunktion erfolgen. Nach Angaben des Unternehmens ist eine spätere manuelle Aktivierung an dem Gerät jederzeit möglich, die als konkludente Einwilligung in die Klimadatenverarbeitung gewertet werden soll.

Die für eine informierte Einwilligung notwendigen Informationen in Form einer zum jeweiligen Gerät passende Bedienungsanleitung waren ausschließlich online verfügbar; eine gedruckte Version konnte ebenfalls nur digital angefordert werden. Gerade für Mieterinnen und Mieter ohne Internetzugang stellt dies eine erhebliche Hürde dar. An den Geräten selbst ist zudem eine Lüftungsempfehlung über ein LED-Signal vorgesehen, wofür ausschließlich die im Rauchwarnmelder gespeicherten Luftfeuchtigkeitswerte genutzt werden sollen.

Besondere hervorzuheben ist aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit auch die im Ankündigungsschreiben dargestellte Gestaltung der Datenverarbeitung, die mehrere Datenempfängerinnen und -empfänger einschließt, welche die personenbezogenen Daten teils im Rahmen von Auftragsverarbeitungsverträgen und teils im Rahmen von gemeinsamen Verantwortlichkeiten nach der Datenschutzgrundverordnung verarbeiten. Darunter befinden sich auch große internationale Cloud-Dienstleister. Die genauen Rollenverteilungen, die Speicherorte sowie die genauen Zugriffsmöglichkeiten waren aus den Unterlagen nicht eindeutig erkennbar.

Nach Rücksprache mit der für das besagte Wohnungsunternehmen federführenden Datenschutzaufsichtsbehörde übermittelte der Landesbeauftragte für Datenschutz und Informationsfreiheit dieser das Ankündigungsschreiben sowie einen daraus erwachsenen Fragenkatalog, um die offenen Fragen in dem dort bereits laufenden Verfahren weiter abzuklären.

Im Rahmen der Sichtung der Unterlagen stellte sich für den Landesbeauftragten für Datenschutz und Informationsfreiheit insbesondere auch die Frage, inwieweit die engmaschige Erhebung der Raumklimadaten im Zwei-Minuten-Intervall, die stündliche Bildung von Durchschnittswerten sowie die dreijährige Profilspeicherung mit dem Grundsatz der Datenminimierung vereinbar ist. Von Bedeutung im Zusammenhang mit der Fernwartung ist ferner, ob die Datenübermittlung, wie angegeben, ausschließlich unidirektional erfolgt oder ob Rückkanäle bestehen, die Fernzugriffe ermöglichen könnten. Auch die konkreten Rollenzuweisungen innerhalb des mehrstufigen Empfängerinnen- und Empfängermodelles bedürfen weiterer Klärung.

Kritisch sah der Landesbeauftragte für Datenschutz und Informationsfreiheit zudem die Möglichkeit einer unbeabsichtigten Aktivierung der Sendefunktion durch manuelle Betätigung des

Gerätes an, die gleichwohl als konkludente Einwilligung interpretiert werden soll. Aus dem Ankündigungsschreiben des Wohnungsunternehmens ging außerdem hervor, dass bei smarten Geräten, die vor November 2024 installiert worden waren, die aktive Sendefunktion offenbar unabhängig von einer erteilten Einwilligung nicht deaktiviert war und erst nachträglich abgeschaltet werden sollte.

Zum Zeitpunkt des Redaktionsschlusses lagen die Antworten auf die von dem Landesbeauftragten für Datenschutz und Informationsfreiheit gestellten Fragen noch nicht vor.

10.4 Identifikation bei Auskunftsersuchen

Der Landesbeauftragte für Datenschutz und Informationsfreiheit befasst sich derzeit mit einem Vorgang, in dem ein Verkehrsunternehmen die Auskunftserteilung nach Artikel 15 Datenschutzgrundverordnung (DSGVO) verweigerte, weil die oder der Betroffene keine „ladungsfähige Anschrift“ angegeben hatte. Die oder der Betroffene hatte eine Postfachadresse sowie ihren beziehungsweise seinen vollständigen Namen und ihr beziehungsweise sein Geburtsdatum mitgeteilt. Hintergrund des Auskunftsersuchens war, dass die oder der Betroffene Mobilitätsdienste des Unternehmens genutzt hatte und erfahren wollte, welche Daten im Zuge dieses Vertragsverhältnisses über sie beziehungsweise ihn verarbeitet wurden.

Die verantwortliche Stelle begründete die Ablehnung mit angeblichen Identitätszweifeln und verwies dabei auf sachfremde Rechtsgrundlagen außerhalb des Datenschutzrechtes. Nach der vorläufigen Bewertung des Landesbeauftragten für Datenschutz und Informationsfreiheit ist diese Vorgehensweise nicht mit Artikel 12 Absatz 6 DSGVO vereinbar. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat in ihrem „Kurzpapier Nr. 6 Auskunftsrecht der betroffenen Person, Artikel 15 DS-GVO“ ausdrücklich hervorgehoben, dass zusätzliche Informationen zur Identitätsfeststellung nur verlangt werden dürften, wenn begründete Zweifel an der Identität der betroffenen Person bestünden. Eine generelle Pflicht, eine ladungsfähige Anschrift anzugeben, besteht daher nicht.

Im vorliegenden Fall war eine Identifizierung der Person bereits anhand der vorliegenden Angaben möglich. Da im Datenbestand des Verantwortlichen keine Anschrift der antragstellenden Person gespeichert war, konnte diese auch nicht als Identitätsmerkmal zum Abgleich herangezogen werden. Die Nachforderung der Wohnadresse war in dem Vorgang daher nicht erforderlich und widerspricht dem Grundsatz der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c) DSGVO.

10.5 Verhaltensregeln für die Messgeräteindustrie

Der Landesbeauftragte für Datenschutz und Informationsfreiheit war am Abstimmungsverfahren zu einem Code of Conduct der Messgeräteindustrie beteiligt, der am 25. Juni 2025 nach vorheriger Abstimmung in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder durch die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen genehmigt wurde. Der Code of Conduct des Verbandes der Deutschen Wasser- und Wärmezählerindustrie e.V. (VDDW) legt datenschutzrechtliche Verhaltensregeln für den Umgang mit personenbezogenen Daten bei der Entwicklung und beim Einsatz fernauslesbarer Messgeräte für Kalt- und Warmwasser sowie thermische Energie fest. Besonders im Wohnungsbereich kommt dem Thema eine hohe datenschutzrechtliche Relevanz zu, weil funkbasierte Messgeräte im Gegensatz zu herkömmlichen mechanischen Zählern in der Lage sind, personenbezogenen Daten in weit größerem und detaillierterem Umfang zu erfassen und Verhaltensprofile anzulegen. Dem Code of Conduct kommt dabei lediglich ein empfehlender Charakter zu, es handelt sich nicht um rechtlich verbindliche Vorgaben.

Das Thema funkbasierte Messgeräte im Kaltwasserbereich wird seit mehreren Jahren durch den Landesbeauftragten für Datenschutz und Informationsfreiheit begleitet. Bereits im 4. Jahresbericht nach der Datenschutzgrundverordnung wurde erstmals auf die datenschutzrechtliche Problematik funkbasierter Wasserzähler hingewiesen (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 15.3). Dort wurde festgehalten, dass die neuen, smarten Geräte im Gegensatz zu den herkömmlichen Wasserzählern in der Lage seien, personenbezogene Daten in weit größerem und detaillierterem Umfang zu erfassen, und es wurde eine bereichsspezifische Rechtsgrundlage gefordert. Im 5. Jahresbericht wurde diese Position fortgeführt (siehe hierzu 5. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 11.4).

Der Landesbeauftragte für Datenschutz und Informationsfreiheit arbeitete ferner mit sechs weiteren Landesdatenschutzaufsichtsbehörden zusammen, um dem Bundesgesetzgeber Vorschläge für eine solche bundeseinheitliche spezialgesetzliche Regelung in diesem Bereich zu übermitteln. Diese Forderungen flossen seinerzeit in die von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 11. Mai 2023 beschlossene Stellungnahme „Daten der Verbraucherinnen und Verbraucher beim Einsatz von Smart Meter zur Erfassung des Kaltwasserverbrauchs durch einheitliche Regelungen schützen“ ein, an dessen Erarbeitung der Landesbeauftragte für Datenschutz und Informationsfreiheit maßgeblich beteiligt war. Das Papier fordert bundesweit einheitliche und spezialgesetzliche Regelungen, bevor funkbasierte Messgeräte im Kaltwasserbereich in Privathaushalten eingesetzt werden dürfen.

Vor diesem Hintergrund hat der Landesbeauftragte für Datenschutz und Informationsfreiheit im Rahmen des Abstimmungsverfahrens zum Code of Conduct darauf hingewiesen, dass dieser für den Einsatz von funkbasierten Messgeräten im Kaltwasserbereich lediglich auf den industriellen Bereich beschränkt ist, weil hier regelmäßig keine personenbezogenen Daten betroffen sind. Für den Einsatz in Privathaushalten hält der Landesbeauftragte für Datenschutz und Informationsfreiheit weiterhin eine bereichsspezifische spezialgesetzliche Regelung für erforderlich, weil eine bloße Berufung auf Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e) Datenschutzgrundverordnung in Verbindung mit § 4 Absatz 1 Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung in diesem Bereich nicht ausreicht. Der Code of Conduct kann in diesem Zusammenhang daher nur als ergänzender branchenspezifischer Orientierungsrahmen dienen und ersetzt keine gesetzliche Grundlage.

10.6 Rückübermittlung von Daten an eine öffentliche Stelle

Den Landesbeauftragten für Datenschutz und Informationsfreiheit erreichte im Berichtsjahr ein Beratungsersuchen des Landesamtes für GeoInformation Bremen zur datenschutzrechtlichen Bewertung einer von einem Versorgungsunternehmen beabsichtigten Rückübermittlung personenbezogener Daten.

Hintergrund des Ersuchens war, dass das Landesamt für GeoInformation Bremen gemäß § 7 Absatz 1 Gesetz über die Landesvermessung und das Liegenschaftskataster (Vermessungs- und Katastergesetz) verpflichtet ist**,** das Liegenschaftskataster fortlaufend auf dem neuesten Stand zu halten. Die Wohnanschriften von Grundstückseigentümerinnen beziehungsweise -eigentümern und Erbbauberechtigten sowie Namen und Anschrift bevollmächtigter Vertreterinnen oder Vertreter der Grundstückseigentümerinnen oder -eigentümern, Erbbauberechtigten sowie Gebäudeeigentümerinnen oder -eigentümern sind nach Angaben des Landesamtes für GeoInformation Bremen in der Stadtgemeinde Bremen derzeit jedoch nur teilweise aktualisiert. Die entsprechenden personenbezogenen Daten sind aber nach § 9 Absatz 2 Vermessungs- und Katastergesetz im Liegenschaftskataster zu speichern.

Im Rahmen der Neufestlegung der Gebühren für die Stadtgemeinde Bremen und der damit verbundenen Beleihung werden dem Versorgungsunternehmen zur postalischen Kontaktaufnahme mit allen Grundstückseigentümerinnen beziehungsweise -eigentümern und Erbbauberechtigten personenbezogene Daten aus dem Liegenschaftskataster bereitgestellt. Die noch fehlenden Anschriften wird das Versorgungsunternehmen im Rahmen ihrer Aufgabenerfüllung eigenständig recherchieren und vervollständigen. Das Landesamt für GeoInformation Bremen beabsichtigt nun eine Rückübermittlung der im Rahmen des Abrechnungsverfahrens aktualisierten Daten von dem Versorgungsunternehmen, um das Liegenschaftskataster zu vervollständigen und zu berichtigen. Eine derartige Rückübermittlung beinhaltet neue Datenverarbeitungen personenbezogener Daten.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat dem Landesamt für GeoInformation Bremen, um die maßgeblichen datenschutzrechtlichen Anforderungen zu klären, einen strukturierten Fragenkatalog übermittelt. Dieser betrifft insbesondere die Datenerhebung durch die Versorgungsunternehmen, die konkreten Datenkategorien, deren jeweilige Übermittlungen und die erforderlichen Angaben zu einer etwaigen Zweckänderung und den jeweiligen Rollenverteilungen sowie die Erforderlichkeit einer Datenschutzfolgenabschätzung nach Artikel 35 Datenschutzgrundverordnung. Zum Zeitpunkt des Redaktionsschlusses lag zu einem Teil der Fragen eine Stellungnahme des Landesamtes für GeoInformation Bremen vor.

Der Vorgang verdeutlicht die datenschutzrechtlichen Herausforderungen im Rahmen derartiger Übermittlungen von personenbezogenen Daten, insbesondere in Bezug auf die Erforderlichkeit einer präzisen Zweckbestimmung, einer eindeutigen Rechtsgrundlage für jeden Verarbeitungsschritt sowie einer klaren Abgrenzung der datenschutzrechtlichen Verantwortlichkeiten.

10.7 Meldung von Mieterinnen- und Mieterdaten an den Grundversorger

Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat im Rahmen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder an dem am 28. Mai 2025 verabschiedeten Beschluss „Meldung von Mieter:innendaten an Grundversorger“ mitgewirkt.[7]

Hintergrund des Beschlusses ist, dass Mieterinnen und Mieter im Rahmen von Umzügen häufig Strom beziehen, ohne zuvor einen Energielieferungsvertrag mit einem Stromversorger abgeschlossen zu haben. In diesen Fällen kommt nach § 2 Absatz 2 der Stromgrundversorgungsverordnung (StromGVV) aufgrund der Realofferte des Grundversorgers automatisch ein Stromlieferungsvertrag mit diesem zustande. Die daraus resultierende Pflicht, dem Grundversorger die Stromentnahme anzuzeigen, war vielen Mieterinnen und Mietern nicht bekannt oder wurde häufig vergessen. Dies führte dazu, dass Grundversorger die Namen ihrer Vertragspartnerinnen und Vertragspartner regelmäßig nicht kannten und deren Vermieterinnen beziehungsweise Vermieter oder Verwalterinnen beziehungsweise Verwalter fragen mussten.

Bisher konnten Mieterinnen und Mieter innerhalb der ersten sechs Wochen nach Wohnungsübergabe unter den verschiedenen Stromversorgern auswählen. Dieser rechnete dann den Leistungszeitraum des Grundversorgers ebenfalls ab.

Diese Möglichkeit besteht seit dem 6. Juni 2025 nicht mehr. Hintergrund ist, dass mit dem 6. Juni 2025 die technischen Voraussetzungen geschaffen wurden, den Stromlieferanten an

[7] abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/Beschluss_Meldung_von_Mieter-innendaten_an_Grundversorger.pdf.

jedem Werktag binnen 24 Stunden zu wechseln. Aufgrund dieser Verkürzung der technischen Umstellungsfristen entfällt die Rechtfertigung, für eine Frist von sechs Wochen die Leistungen des Grundversorgers mitabrechnen zu können.

Da nunmehr der Grundversorger selbst den Stromverbrauch abrechnet, bedarf es, wenn die Mieterin oder der Mieter nicht eingewilligt hat, die für die Abrechnung erforderlichen personenbezogenen Daten zu verarbeiten, einer anderen Rechtsgrundlage für die Datenverarbeitung. Die Übermittlung der vertragsrelevanten Daten an den Grundversorger seitens Vermieterinnen oder Vermieter beziehungsweise Verwalterinnen oder Verwalter ab dem Zeitpunkt der Wohnungsübergabe kann in diesen Fällen auf ein berechtigtes Interesse des Grundversorgers, die Identität der Vertragspartnerin oder des Vertragspartners zu kennen, und ein Interesse der Vermieterin oder des Vermieters, nicht für die seitens der Mietenden bezogenen elektrischen Energie in Anspruch genommen zu werden, gestützt werden (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f) Datenschutzgrundverordnung [DSGVO]).

Zwingend notwendig ist jedoch, dass die Betroffenen rechtzeitig, vorab und transparent, nämlich am besten bereits bei Abschluss des Mietvertrages, gemäß Artikel 13 Absatz 3 DSGVO über die beabsichtigte Datenübermittlung informiert werden. Zudem sollten Vermieterinnen oder Vermieter sowie Verwalterinnen oder Verwalter frühzeitig erfragen, ob rechtzeitig vor der Übergabe des Mietobjektes ein Stromlieferungsvertrag abgeschlossen wurde, oder beabsichtigt wird, sich eigenständig beim Grundversorger anzumelden. Auf diese Weise kann eine Datenübermittlung an den Grundversorger häufig vermieden werden.

11. Beschäftigtendatenschutz

11.1 Gemeldete Datenschutzverletzungen

Im Berichtsjahr wurden dem Landesbeauftragten für Datenschutz und Informationsfreiheit insgesamt 37 Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung seitens einer oder eines Verantwortlichen gemeldet, die den Beschäftigtendatenschutz betrafen. 28 Meldungen stammten aus dem nicht öffentlichen Bereich und neun Meldungen aus dem öffentlichen Bereich. Viele Meldungen betrafen in diesem Bereich den Versand von E-Mails mit offenem E-Mail-Verteiler, auch die Veröffentlichung von Beschäftigtendaten auf sozialen Medien war Gegenstand der Meldungen. Nicht zuletzt hatte zudem eine größer werdende Anzahl an Meldungen Datenschutzverletzungen durch Hackerangriffe zum Inhalt.

Ferner erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit erneut eine hohe Anzahl an Beschwerden über den Umgang mit Beschäftigtendaten, wobei die Beschwerden sich überwiegend auf den nicht öffentlichen Bereich bezogen. Bei den betroffenen Personen besteht weiterhin ein erheblicher Beratungsbedarf, insbesondere zu den Fragen der Übermittlung von Beschäftigtendaten durch die Arbeitgeberin beziehungsweise den Arbeitgeber sowie der Überwachung von Beschäftigten durch die Arbeitgeberin oder den Arbeitgeber, sodass hierzu eine Vielzahl an telefonischen und auch schriftlichen Beratungen erfolgte.

11.2 Datenschutz im Bewerbungsverfahren

Auch in diesem Berichtsjahr bezogen sich mehrere Beschwerden auf den Umgang der Unternehmen mit personenbezogenen Daten im Bewerbungsverfahren. Ein häufiges Problem war hierbei die nicht erfolgte Löschung der Bewerbungsunterlagen.

Personenbezogene Daten von Beschäftigten, zu denen auch Bewerberinnen und Bewerber zählen, dürfen nur für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies unter anderem für die Begründung des Beschäftigungsverhältnisses erforderlich ist. Entsprechend dem Grundsatz der Datenminimierung sind Bewerbungsunterlagen daher zu löschen, soweit sie für die Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sind. Möchten Arbeitgeberinnen oder Arbeitgeber Daten der Bewerberinnen und Bewerber für zukünftige Bewerbungsverfahren behalten, so ist hierfür eine Einwilligung der Bewerberinnen oder der Bewerber erforderlich. Dies gilt auch im Rahmen von Initiativbewerbungen.

Die Daten aus einem Bewerbungsverfahren unverzüglich zu löschen, kann jedoch häufig nicht verlangt werden, weil diese noch für einen gewissen Zeitraum mit einer zulässigen Rechtfertigung aufbewahrt werden dürfen, etwa wenn die Verarbeitung für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Hierzu zählt auch der Nach-

weis, dass nicht gegen die Bestimmungen des Allgemeinen Gleichbehandlungsgesetzes verstoßen wurde. Dieser Zeitraum beträgt höchstens sechs Monate nach Beendigung des Bewerbungsverfahrens, und zwar auch in Fällen, in denen die Bewerbungen von den Betroffenen selbst zurückgezogen wurden. Im Anschluss an diesen Zeitraum müssen nicht zurückgesandte Unterlagen von der Arbeitgeberin beziehungsweise vom Arbeitgeber vernichtet beziehungsweise gelöscht werden.

Hintergrund ist, dass gemäß Artikel 17 Absatz 1 Datenschutzgrundverordnung eine Löschpflicht besteht, wenn die Daten für die Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sind. Die Speicherung von Daten über das für das Bewerbungsverfahren erforderliche Maß hinaus ist daher datenschutzrechtlich unzulässig. Die betroffenen Unternehmen wurden seitens des Landesbeauftragten für Datenschutz und Informationsfreiheit auf diese Vorgaben hingewiesen und zur Anpassung ihres Umgangs mit Bewerbungsunterlagen aufgefordert.

11.3 Nutzung von WhatsApp im Beschäftigungsverhältnis

Bereits mehrfach hat der Landesbeauftragte für Datenschutz und Informationsfreiheit in den letzten Jahren darauf hingewiesen, dass die Nutzung von WhatsApp im betrieblichen Kontext, insbesondere im Hinblick auf die Übermittlung von Beschäftigtendaten, unzulässig ist (siehe hierzu 7. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 11.4; 5. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 12.7 und 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 10.4).

Eine wirksame, das heißt informierte und freiwillige, Einwilligung durch Beschäftigte in die Nutzung des Messengerdienstes im betrieblichen Kontext ist kaum vorstellbar. Dies liegt unter anderem daran, dass die Verarbeitung von personenbezogenen Daten durch WhatsApp beziehungsweise Meta nicht transparent ist. Sofern der Beitritt zu WhatsApp-Gruppen im betrieblichen Kontext erfolgt, darf bei der Beurteilung der Freiwilligkeit darüber hinaus der soziale und wirtschaftliche Druck im Rahmen eines Beschäftigungsverhältnisses nicht außer Acht gelassen werden.

Weitere datenschutzrechtliche Bedenken in Bezug auf die Datenverarbeitung durch WhatsApp beziehungsweise Meta kommen hinzu. So behält sich WhatsApp zum Beispiel die Erhebung von Telefonnummern mittels Adressbuch-Upload vom Handy der Mobiltelefonnutzerin oder des Mobiltelefonnutzers vor und kann so sämtliche Kontaktdaten eines Nutzers verarbeiten, die auf dessen Mobiltelefon gespeichert sind. Dies betrifft auch Kontakte, die selbst kein WhatsApp nutzen. Hinzu kommt, dass WhatsApp beziehungsweise Meta diese Daten auch für eigene Zwecke nutzt. Dies ist datenschutzrechtlich unzulässig, weil die im Adressbuch gespeicherten Personen zu einer solchen Verarbeitung in der Regel keine Einwilligung erteilt

haben. Auch werden bei Versendung von Nachrichten regelmäßig Daten an Meta beziehungsweise WhatsApp übermittelt, ohne dass die Verwendung dieser Daten geklärt ist.

Auch im Berichtsjahr gingen Beschwerden zu diesem Thema ein. So wurde in einem Fall durch eine Einrichtungsleitung eine WhatsApp-Gruppe genutzt, um bei Dienstausfällen einen Ersatz für die ausgefallenen Kolleginnen und Kollegen zu finden. Dabei wurden hierfür die privaten Mobilfunknummern verwendet, die sich aus den Personalfragebögen der Beschäftigten ergaben. Da in der WhatsApp-Gruppe auch Krankmeldungen erfolgten, wurden Gesundheitsdaten, die zu den besonderen Kategorien personenbezogener Daten gehören, unter Nutzung eines datenschutzrechtlich problematischen Übermittlungsmediums verarbeitet.

Parallel zu der eingegangenen Beschwerde meldete auch der Arbeitgeber selbst den Verstoß beim Landesbeauftragten für Datenschutz und Informationsfreiheit. Der Verantwortliche zeigte sich im Rahmen des Prüfverfahrens äußerst kooperativ und setzte zeitnah die geforderten Anpassungen um. Es erfolgte unter anderem eine Sensibilisierung der Beschäftigten, eine Unterweisung zur Nutzung von Messengerdiensten und Social Media im betrieblichen Kontext sowie die Überarbeitung einer bereits existierenden IT-Richtlinie in Bezug auf diese Punkte.

11.4 Umgang mit Krankmeldungen im Beschäftigtenverhältnis

Immer wieder erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit auch Beschwerden oder Beratungsanfragen in Bezug auf Krankmeldungen durch Beschäftigte. Hintergrund der Beschwerden ist häufig, dass unberechtigte Personen Zugriff auf die Krankmeldungen hatten, dass Krankmeldungen im betriebsinternen Kalender – zum Teil sogar mit einer Diagnose – eingetragen oder dass Krankmeldungen nicht ordnungsgemäß aufbewahrt wurden.

Gesundheitsdaten zählen zu den sensiblen personenbezogenen Daten und sind dementsprechend in Artikel 9 Absatz 1 Datenschutzgrundverordnung (DSGVO) besonders geschützt. Nach Artikel 9 Absatz 2 Buchstabe b) DSGVO dürfen Arbeitgeberinnen oder Arbeitgeber Gesundheitsdaten verarbeiten, wenn dies zur Erfüllung arbeitsrechtlicher Pflichten erforderlich ist. Die Erforderlichkeit zur Verarbeitung von Gesundheitsdaten im Fall von Krankmeldungen ergibt sich aus dem Entgeltfortzahlungsgesetz (EFZG). In § 3 EFZG ist geregelt, dass im Krankheitsfall eine gesetzliche Verpflichtung der Arbeitgeberinnen und Arbeitgeber zur Lohnfortzahlung in der Regel bis zur Dauer von sechs Wochen besteht. Der Arbeitnehmer oder die Arbeitnehmerin muss dementsprechend nach § 5 Absatz 1 Satz 1 und Satz 2 EFZG eine Arbeitsunfähigkeit und deren voraussichtliche Dauer unverzüglich der Arbeitgeberin beziehungsweise dem Arbeitgeber mitteilen und, wenn die Arbeitsunfähigkeit länger als drei Kalendertage dauert, eine ärztliche Bescheinigung vorlegen.

Die Verarbeitung der Gesundheitsdaten, welche die Arbeitnehmerin oder der Arbeitnehmer im Falle einer Arbeitsunfähigkeit bei Krankheit mitteilt, ist dabei auf das notwendige Maß zu beschränken. So unterfallen etwa Informationen zu Diagnosen der Privatsphäre der Arbeitnehmerin beziehungsweise des Arbeitnehmers und müssen in der Regel nicht mitgeteilt werden. Die Informationspflicht umfasst grundsätzlich nur den Umstand der Arbeitsunfähigkeit sowie die voraussichtliche Dauer der Abwesenheit, weil dies die für das Arbeitsverhältnis relevanten Informationen sind.

Auch die betriebsinterne Kommunikation ist im Falle von Krankmeldungen auf die erforderlichen Informationen zu beschränken. So ist zwar die Information über Abwesenheitszeiten für die Durchführung des Beschäftigungsverhältnisses grundsätzlich erforderlich, nicht erforderlich und damit unzulässig ist hingegen die Angabe von konkreten Abwesenheitsgründen, zum Beispiel Urlaub, Krankheit oder andere Fehlzeiten.

Darüber hinaus ist durch technische und organisatorische Maßnahmen sicherzustellen, dass nur diejenigen Personen Zugriff auf die Krankmeldungen der Beschäftigten haben, die diese benötigen, um ihre Aufgaben zu erfüllen.

11.5 Datenschutz im BEM-Verfahren

Sind Beschäftigte innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig, ist die Arbeitgeberin beziehungsweise der Arbeitgeber verpflichtet, ein Betriebliches Eingliederungsmanagement (BEM) durchzuführen. Die Teilnahme ist für die Beschäftigten freiwillig, denn das Verfahren kann nur mit Zustimmung und Beteiligung der betroffenen Person erfolgen. Ziel des BEM-Verfahrens ist es, die Arbeitsunfähigkeit zu überwinden, erneuter Arbeitsunfähigkeit vorzubeugen und den Arbeitsplatz zu erhalten. Dem Landesbeauftragten für Datenschutz und Informationsfreiheit wurde aufgrund einer Beschwerde bekannt, dass in einer Dienststelle, Informationen aus dem BEM-Gespräch an einen Fachkoordinator weitergeleitet wurden, ohne dass die betroffene Person in diese Weiterleitung eingewilligt hatte.

Im Rahmen der datenschutzrechtlichen Prüfung stellte sich heraus, dass die betreffende Dienststelle eine eigene Dienstvereinbarung zum Betrieblichen Eingliederungsmanagement abgeschlossen hatte, die in diversen Punkten von der „Handlungshilfe Betriebliches Eingliederungsmanagement (BEM) nach § 167 (2) SGB IX für den bremischen öffentlichen Dienst“ abwich. Insbesondere enthielt die Dienstvereinbarung keine ausreichenden Regelungen zum Schutz der personenbezogenen Daten der Beschäftigten. Regelungen zum Datenschutz sind jedoch das wesentliche Instrument der Vertrauensbildung im BEM-Verfahren. Sie gewährleisten, dass den Beschäftigten ein Verfahren angeboten wird, in dem die Verarbeitung von allen erhobenen Daten ausschließlich auf die Ziele des Betrieblichen Eingliederungsmanagementes

abgestellt ist und in dem die Daten nicht für andere Zwecke genutzt werden. Auf diese Weise ist ausgeschlossen, dass die Teilnahme an einem BEM-Verfahren zum Nachteil der oder des Betroffenen führt.

Dass es erforderlich war, die Unterlagen aus dem BEM-Gespräch an den Fachkoordinator im Fall der Beschwerde weiterzuleiten, konnte nicht dargelegt werden, es bestanden diesbezüglich infolgedessen erhebliche datenschutzrechtliche Bedenken. Der Landesbeauftragte für Datenschutz und Informationsfreiheit wies daher darauf hin, dass auch im BEM-Verfahren zwingend das Prinzip der Datenminimierung zu beachten sei und dass nur die Personen Zugriff auf die Daten haben dürften, die diese für die Erfüllung ihrer Aufgaben benötigten. Auch kann die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im BEM-Verfahren nur mit schriftlicher Einwilligung der Beschäftigten erfolgen (Artikel 7 Datenschutzgrundverordnung [DSGVO] in Verbindung mit Artikel 9 Absatz 2 DSGVO). Aus dem dazu verwendeten Vordruck müssen Zweck, Art und Umfang der Datenerhebung und -verarbeitung eindeutig hervorgehen. Die Dienststelle wurde daher aufgefordert, die örtliche Dienstvereinbarung entsprechend anzupassen.

Die „Handlungshilfe Betriebliches Eingliederungsmanagement (BEM) nach § 167 (2) SGB IX für den bremischen öffentlichen Dienst“ ist im Transparenzportal zu finden und enthält umfangreiche Hinweise zum Verfahren sowie zum Datenschutz im Rahmen des Verfahrens. Die Handlungshilfe enthält auch ein mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit abgestimmtes Datenschutzkonzept.

11.6 Datenschutz bei Beendigung des Beschäftigtenverhältnisses

Bei jedem Ende einer Beschäftigung stellt sich die Frage, wie mit den personenbezogenen Daten ausgeschiedener Beschäftigten umzugehen ist. Auch in diesem Berichtsjahr erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit mehrere Beschwerden und Beratungsanfragen zu diesem Thema.

Nach den Vorgaben der Datenschutzgrundverordnung (DSGVO) dürfen personenbezogene Beschäftigtendaten nur verarbeitet werden, soweit dies zur Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Mit dem Ende des Arbeitsverhältnisses entfällt dieser Zweck in der Regel. Eine weitere Verarbeitung ist nur zulässig, wenn eine entsprechende gesetzliche Pflicht oder ein berechtigtes Interesse besteht. Darüber hinaus sind personenbezogene Daten nach Artikel 17 DSGVO zu löschen, sobald sie für den ursprünglichen Zweck nicht mehr erforderlich sind oder eine erteilte Einwilligung widerrufen wurde. Dies betrifft insbesondere Daten, die auf Websites von Unternehmen oder in sozialen Netzwerken veröffentlicht wurden.

In diesem Berichtsjahr stellte der Landesbeauftragte für Datenschutz und Informationsfreiheit in mehreren Verfahren fest, dass personenbezogene Daten von ausgeschiedenen Beschäftigten teilweise weiterhin online veröffentlicht wurden. In zwei Verfahren beschwerten sich ehemalige Beschäftigte darüber, dass Bilder und Videos von ihnen in sozialen Medien verblieben, obwohl sie ihren ehemaligen Arbeitgeber um die Löschung baten. In diesen Fällen hat der Landesbeauftragte für Datenschutz und Informationsfreiheit erfolgreich darauf hingewirkt, dass die Daten unverzüglich entfernt wurden. Die betroffenen Arbeitgeber zeigten sich dabei einsichtig und kamen der Aufforderung des Landesbeauftragten für Datenschutz und Informationsfreiheit umgehend nach.

Die Dauer der Aufbewahrung personenbezogener Daten von Beschäftigten bei Beendigung des Beschäftigtenverhältnisses richtet sich nach gesetzlichen Vorschriften, etwa den steuer- und handelsrechtlichen Aufbewahrungspflichten oder den zivilrechtlichen Verjährungsfristen. Nach Ablauf dieser Fristen sind die Daten zu löschen. Arbeitgeberinnen und Arbeitgeber sind daher verpflichtet, sorgfältig zu prüfen, welche Daten weiterhin gespeichert werden dürfen und welche unverzüglich zu löschen sind. Um eine datenschutzkonforme Verarbeitung sicherzustellen, empfiehlt es sich daher, ein strukturiertes Löschkonzept einzuführen, das klare Verantwortlichkeiten und technische Maßnahmen zur fristgerechten Löschung vorsieht.

12. Digitale Dienste, Medien, Digitalisierung und Künstliche Intelligenz

12.1 Gemeldete Datenschutzverletzungen

Im Berichtsjahr wurden im Bereich Digitale Dienste, Medien, Digitalisierung und Künstliche Intelligenz insgesamt drei Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung an den Landesbeauftragen für Datenschutz und Informationsfreiheit gemeldet. Die Meldungen bezogen sich darauf, dass Fotos von Personen aus einer sozialen Einrichtung über den privaten Account einer Mitarbeiterin auf den sozialen Medien veröffentlicht worden waren, sowie darauf, dass personenbezogenen Daten durch fehlerhafte oder gehackte IT-Systeme offengelegt worden waren.

12.2 Veröffentlichung von Kinderfotos im Internet

Im Berichtsjahr erhielt der Landesbeauftragte für Datenschutz und Informationsfreiheit mehrere Beschwerden von Eltern, welche die Löschung von Fotos oder Videos ihrer Kinder in sozialen Medien, insbesondere Instagram, Facebook und Snapchat, verlangten. Meist handelte es sich um geschiedene oder getrennt lebende Eltern mit gemeinsamem Sorgerecht, die Inhalte durch den anderen Elternteil entfernen lassen wollten.

Die Veröffentlichung von Fotos und Videos, auf denen Personen erkennbar sind, stellt eine Verarbeitung personenbezogener Daten nach der Datenschutzgrundverordnung (DSGVO) dar. Kinder und Minderjährige benötigen einen besonderen Schutz. Inhalte, die in sozialen Netzwerken für einen unbestimmten Personenkreis zugänglich sind, können weltweit eingesehen, kopiert, weitergeleitet oder für andere Zwecke genutzt werden. Selbst die Beschränkung auf eine Sichtbarkeit nur für „Freunde“ birgt Risiken, weil dieser Kreis oft zu groß oder unter Umständen nicht vertrauenswürdig ist. Das Haushaltsprivileg des Artikel 2 Absatz 2 Buchstabe c) DSGVO, das dazu führen würde, dass die Datenschutzgrundverordnung keine Anwendung findet, greift nur im privaten familiären Umfeld. Veröffentlichungen in sozialen Medien überschreiten diese Grenzen in der Regel.

Für die Veröffentlichung von Kinderfotos im Internet ist dann, wie für alle anderen Verarbeitungen von personenbezogenen Daten auch, eine Rechtsgrundlage nach Artikel 6 Absatz 1 DSGVO erforderlich. Nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit kann hier nur die Einwilligung nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a) DSGVO eingreifen; ein berechtigtes Interesse nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f) DSGVO ist wegen der besonderen Schutzbedürftigkeit von Kindern regelmäßig nicht einschlägig. Die Datenschutzgrundverordnung betont in Erwägungsgrund 38, dass Kinder einen besonderen Schutz verdienen, weil sie sich der Risiken, Folgen und Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger als Erwachsene bewusst sind.

Eine Interessenabwägung sollte daher zugunsten der Kinder erfolgen. Für den Rechtfertigungsgrund der Einwilligung gilt zudem: Bei einem gemeinsamen Sorgerecht nach §§ 1626, 1629 Bürgerliches Gesetzbuch müssen beide Elternteile in die Veröffentlichung einwilligen. Fehlt die Zustimmung eines Sorgeberechtigten, ist die Veröffentlichung unrechtmäßig.

Das Recht am eigenen Bild ist im digitalen Raum besonders herausgefordert. Einmal veröffentlichte Inhalte sind weltweit zugänglich und lassen sich in der Praxis kaum vollständig löschen oder in ihrer Weiterverbreitung kontrollieren, wie auch die Rechtsprechung wiederholt festgestellt hat (Oberlandesgericht Oldenburg, Beschluss vom 24. Mai 2018, Aktenzeichen 13 W 10/18; Oberlandesgericht Düsseldorf, Beschluss vom 20. Juli 2021, Aktenzeichen 1 UF 74/21). Gerade bei Kindern kann die dauerhafte Verfügbarkeit von Fotos erhebliche Auswirkungen auf die Persönlichkeitsentwicklung haben und stellt eine nicht hinnehmbare Beeinträchtigung ihrer Rechte dar. Auch das Recht auf Löschung („Recht auf Vergessenwerden“, Artikel 17 DSGVO) kann häufig nicht effektiv durchgesetzt werden. Der Landesbeauftragte für Datenschutz und Informationsfreiheit unterstützte betroffene Eltern bei der Durchsetzung des Rechtes auf Löschung und wies die Verantwortlichen darauf hin, dass künftige Veröffentlichungen ohne Einwilligung des anderen Elternteiles zu unterlassen seien.

Auch das Thema „Influencer-Kinder“ beschäftigte den Landesbeauftragten für Datenschutz und Informationsfreiheit. Eltern, die Kinderfotos unter wirtschaftlichen Interessen veröffentlichen, schaffen einen Interessenkonflikt zwischen dem Publikationsinteresse der Eltern und dem Wohl des Kindes. Besonders kritisch ist dies, wenn das Kind noch nicht einsichtsfähig ist. Das Kindeswohl muss stets Vorrang haben. Die Persönlichkeitsrechte der Kinder sind unabhängig davon zu wahren, ob die Eltern Influencer sind oder nicht. Da regulatorische Eingriffsmöglichkeiten bisher fehlen, sind Selbstverpflichtungen erforderlich.

Der Medienrat der Bremischen Landesmedienanstalt (brema) empfiehlt unter anderem, das Gesicht von Kindern unter drei Jahren im Influencer-Marketing nicht zu zeigen, keine echten Namen zu verwenden, keine Aufnahmen aus dem Kinderzimmer zu veröffentlichen und keine Fotos von Kleinkindern in kompromittierenden Situationen zu teilen. Diese Empfehlungen unterstützt der Landesbeauftragte für Datenschutz und Informationsfreiheit ebenfalls und betont auch in Bezug auf den Schutz von personenbezogenen Daten die besondere Schutzbedürftigkeit von Kindern im digitalen Raum.

12.3 Political Targeting und neue Zuständigkeit

Mit dem Inkrafttreten der Verordnung über die Transparenz und das Targeting politischer Werbung (TTPW-VO) am 10. Oktober 2025 ergeben sich für den Landesbeauftragten für Datenschutz und Informationsfreiheit zusätzliche Aufgaben und Zuständigkeiten.

Die Verordnung enthält umfangreiche Transparenz- und Sorgfaltspflichten im Zusammenhang mit der Erbringung politischer Werbung sowie detaillierte Regelungen zum Einsatz von Targeting- und Anzeigenschaltungsverfahren, die eine Verarbeitung personenbezogener Daten bei politischer Online-Werbung beinhalten (Artikel 1 Absatz 1 TTPW-VO). Darüber hinaus legt sie Bestimmungen zur Überwachung und Durchsetzung der Vorgaben der Verordnung fest, einschließlich der erforderlichen Zusammenarbeit und Koordinierung zwischen den zuständigen Aufsichtsbehörden.

Nach Artikel 22 Absatz 1 TTPW-VO ist der Landesbeauftragte für Datenschutz und Informationsfreiheit zuständig, die Anwendung der Artikel 18 und 19 TTPW-VO zu überwachen. Diese Artikel enthalten spezifische Anforderungen an Targeting und Anzeigenschaltung im Zusammenhang mit politischer Werbung im Internet, sofern dabei personenbezogene Daten verarbeitet werden.

Darüber hinaus ist davon auszugehen, dass der Landesbeauftragte für Datenschutz und Informationsfreiheit künftig auch für die Überwachung von Artikel 20 TTPW-VO zuständig sein wird. Dieser Artikel regelt eine ausdrückliche Übermittlungspflicht, die in engem sachlichen Zusammenhang mit den bereits durch die Datenschutzaufsichtsbehörden zu überwachenden Bestimmungen des Artikels 19 TTPW-VO steht. Aus Gründen der Kohärenz und Effektivität der Aufsicht erscheint es sachgerecht, auch die Kontrolle der Anwendung von Artikel 20 TTPW-VO dem Landesbeauftragten für Datenschutz und Informationsfreiheit zuzuordnen. Er geht derzeit davon aus, dass der Bundesgesetzgeber keine gesonderte Zuständigkeitsregelung für die Landesdatenschutzbehörden schaffen wird. Für die Freie Hansestadt Bremen hat er daher die Aufnahme einer entsprechenden Zuständigkeitsbestimmung im Bremischen Ausführungsgesetz zur EU-Datenschutz-Grundverordnung angeregt.

12.4 Einführung des Künstliche Intelligenz nutzenden Textassistenten LLMoin

Im Berichtsjahr erfolgte der Beginn der Einführung des Künstliche Intelligenz nutzenden Textassistenten LLMoin für einen Teil der Verwaltung der Freien Hansestadt Bremen. LLMoin soll zukünftig fast allen an „Basis-Bremen“ angeschlossenen Beschäftigten der Freien Hansestadt Bremen zur Verfügung stehen. Außerdem wird LLMoin auch in anderen Ländern, wie unter anderem in Hamburg, bereits genutzt oder eingeführt. Betrieben und entwickelt wird LLMoin von Dataport AöR, diese wird hierbei als Auftragsverarbeiterin für die jeweiligen öffentlichen Stellen, die LLMoin nutzen, tätig.

Bei LLMoin handelt es sich um ein Künstliche Intelligenz nutzendes System auf Basis eines Large Language Modell. Aktuell kommt dabei das Large Language Modell GPT-4.1 des US-amerikanischen Softwareunternehmens OpenAI Inc. zum Einsatz, das innerhalb der Azure

Cloud des US-amerikanischen Softwareunternehmens Microsoft bereitgestellt wird. Die entsprechenden Server sollen sich ausschließlich innerhalb der Europäischen Union befinden. Selbst wenn für LLMoin ausschließlich europäische Server genutzt werden, sind dennoch aufgrund des Clarifying Lawful Overseas Use of Data Act (U.S.-CLOUD Act), dem Microsoft als US-amerikanisches Unternehmen unterliegt, weitergehende Vorkehrungen zu treffen. Der U.S.-CLOUD Act ermöglicht es Behörden der Vereinigten Staaten von Amerika, amerikanische Firmen dazu zu verpflichten, ihnen Zugriff auf gespeicherte Daten zu gewährleisten, unabhängig davon, ob diese Daten innerhalb oder außerhalb der Vereinigten Staaten von Amerika gespeichert sind. In einem solchen Fall sind durch die Auftragsverarbeiterin beziehungsweise den Auftragsverarbeiter hinreichende Garantien zu leisten, welche die Risiken einer europarechtswidrigen Datenverarbeitung durch technische und/oder organisatorische Maßnahmen ausgleichen (siehe hierzu den Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 31. Januar 2023). Ob entsprechende Maßnahmen getroffen wurden, muss die verantwortliche Stelle nachweisen können.

Von zentraler Bedeutung, einen rechtskonformen Betrieb von LLMoin sicherzustellen, ist auch die Schaffung ausreichender gesetzlicher Grundlagen. Eine entsprechende Erlaubnisnorm zum Einsatz von Systemen der Künstlichen Intelligenz durch die öffentliche Verwaltung, wie es diese in § 13 Hamburgisches Verwaltungsdigitalisierungsgesetz gibt, hat die Freie Hansestadt Bremen bislang nicht.

Der Austausch mit dem Senator für Finanzen, wie LLMoin die datenschutzrechtlichen Vorgaben erfüllt, um entsprechend der Planung eingesetzt zu werden, dauert an.

12.5 Facebook-Fanpages – Urteil des Verwaltungsgerichtes Köln und die Übergangslösung

Im Berichtsjahr 2025 rückte der Betrieb sogenannter Facebook-Fanpages abermals verstärkt in den Fokus datenschutzrechtlicher Betrachtungen. Öffentliche Stellen nutzen Fanpages weiterhin, um Bürgerinnen und Bürger zu informieren und mit ihnen in den Austausch zu treten. Gleichzeitig ergeben sich daraus erhebliche datenschutzrechtliche Herausforderungen, insbesondere hinsichtlich der gemeinsamen Verantwortlichkeit nach Artikel 26 Datenschutzgrundverordnung (DSGVO) sowie der Transparenz- und Einwilligungspflichten bei der Verwendung von Cookies.

Seit dem Urteil des Europäischen Gerichtshofes vom 5. Juni 2018 („Wirtschaftsakademie Schleswig-Holstein“, Aktenzeichen C-210/16) ist anerkannt, dass Betreibende von Facebook-Fanpages grundsätzlich gemeinsam mit Meta für die Verarbeitung personenbezogener Daten verantwortlich sein können. Die Datenschutzaufsichtsbehörden haben wiederholt betont, dass

der Betrieb solcher Seiten nur zulässig sei, wenn Transparenz, Rechtsgrundlage und Betroffenenrechte gewahrt blieben (siehe hierzu 5. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 13.3, 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 17.4 und 1. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 17.1).

Im Berichtsjahr sorgte insbesondere das Urteil des Verwaltungsgerichtes Köln vom 17. Juli 2025 (Aktenzeichen 13 K 1419/23) für Aufmerksamkeit. Gegenstand war die Facebook-Fanpage des Presse- und Informationsamtes der Bundesregierung, deren Betrieb die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit untersagt hatte. Sie bemängelte fehlende Rechtsgrundlagen für die durch Meta erfolgende Datenverarbeitung, insbesondere im Zusammenhang mit Cookies und statistischen Nutzungsdaten (Insights). Das Verwaltungsgericht Köln hob den Bescheid jedoch auf. Nach dessen Auffassung liegt die Verantwortung für die datenschutzrechtlich relevanten Verarbeitungen bei Meta. Eine gemeinsame Verantwortlichkeit nach Artikel 26 DSGVO verneinte das Gericht, weil das Presse- und Informationsamt der Bundesregierung keine Mitbestimmung über Zwecke und Mittel der Verarbeitung habe. Das Urteil ist nicht rechtskräftig und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat Berufung gegen das Urteil eingelegt. Der Landesbeauftragte für Datenschutz und Informationsfreiheit begrüßt, dass die Rechtsfragen nunmehr einer obergerichtlichen Klärung zugeführt werden. Diese gilt es abzuwarten.

12.6 Auf Künstliche Intelligenz gestützte Fahrzeugüberwachung

Ein Verkehrsunternehmen hat dem Landesbeauftragten für Datenschutz und Informationsfreiheit mitgeteilt, dass es die Einführung einer Videoanalyse mithilfe Künstlicher Intelligenz (KI) in Echtzeit auf den Bildern der Überwachungskamera plane. Zweck dieser Verarbeitung sei es, die Sicherheit in den vom Unternehmen betriebenen Schienenfahrzeugen zu erhöhen. Das Unternehmen hat kooperativ mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit zusammengearbeitet und dessen Hinweise aufgenommen, um die Verarbeitung der personenbezogenen Daten so eingriffsarm wie möglich zu gestalten.

Problematisch kann eine solche Verarbeitung personenbezogener Daten per live Analyse sein, weil sie jede oder jeden, die oder der das Schienenfahrzeug nutzt, erfasst und ihr oder sein Verhalten in Echtzeit analysiert und bewertet. Die Künstliche Intelligenz entscheidet dann selbstständig, ob das beobachtete Verhalten als gefährlich gilt und ob es gemeldet wird oder nicht. Solche Systeme, die Künstliche Intelligenz verwenden, und ihre getroffenen Entscheidungen sind bis heute selbst für ihre Entwicklerinnen beziehungsweise Entwickler schwer zu verstehen und nachzuvollziehen. Deswegen können falsche Ergebnisse und Diskriminierung weder ausgeschlossen noch nachvollzogen werden.

Zudem ist es schwierig, die Betroffenen vollumfänglich über die Verarbeitung ihrer Daten zu informieren, weil die Systeme sehr komplex sind. Die Informationspflichten nach Artikel 13 Datenschutzgrundverordnung (DSGVO) müssen dennoch erfüllt werden. Die Komplexität solcher Systeme führt auch zu einem weiteren Problem, es wird zum Teil sehr viel Rechenleistung benötigt. Deswegen werden KI-Systeme häufig auf leistungsstarken Servern ausgelagert und in einer Cloud betrieben. Eine solche Lösung kann jedoch weitere Probleme mit sich bringen, weil hierbei oft eine Datenübermittlung stattfindet, die einer eigenen Rechtsgrundlage bedarf. Auch die Datenübertragung an sich muss hinreichend abgesichert werden, um einen unbefugten Zugriff zu vermeiden. Zudem muss es ein eigenes Konzept für die Datenverarbeitung auf den Servern geben, das zum Beispiel ein Rechte- und Rollenkonzept sowie ein Löschkonzept umfasst.

Das in diesem Fall betrachtete System arbeitet jedoch komplett lokal, dabei werden die verarbeiteten Daten weder gespeichert noch an einen anderen Ort übertragen oder in eine Cloud hochgeladen. Es muss darüber hinaus ausgeschlossen werden, dass es durch das System, das Künstliche Intelligenz verwendet, zu einer automatisierten Entscheidung nach Artikel 22 DSGVO kommt. So kann die Einschätzung der Situation durch das System fehlerbehaftet sein, wenn beispielsweise ein Kind auf seine Mutter zustürmt, könnte das durchaus nach einem tätlichen Angriff aussehen. Strukturelle Diskriminierung kann ebenso wenig ausgeschlossen werden. Um diesen Problemen entgegenzusteuern und keine automatisierte Entscheidung nach Artikel 22 DSGVO zu treffen, wurde unter anderem eine menschliche Aufsicht der Entscheidung der Künstlichen Intelligenz von dem Unternehmen implementiert. Auch werden die durch das System verarbeiteten Daten nicht zu einem weiteren Training der Künstlichen Intelligenz genutzt.

Die Prüfung durch den Landesbeauftragten für Datenschutz und Informationsfreiheit ergab zwar, dass das Unternehmen viele Maßnahmen getroffen hatte, um den genannten Risiken zu begegnen, dennoch lässt sich für den Landesbeauftragte für Datenschutz und Informationsfreiheit bislang nicht abschließend bewerten, ob das Systems tatsächlich hinreichend geeignet und erforderlich ist, um den benannten Zweck zu erfüllen, die Sicherheit in den Schienenfahrzeugen zu erhöhen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit begrüßt die Einbindung in der Pilotphase des Systems und die damit einhergehenden Vorteile für beide Seiten. Er wird auch das noch andauernde Verfahren weiter begleiten.

12.7 DeepSeek

Das Berichtsjahr war geprägt vom rasanten Aufstieg von Systemen, die Künstliche Intelligenz auf der Basis von Large Language Modells (LLM) verwenden. Insbesondere Chat-Bots US-amerikanischer Unternehmen, wie ChatGPT, CoPilot oder Gemini, standen dabei im Mit-

telpunkt. Einer dieser Chat-Bots auf Basis eines LLMs ist DeepSeek zweier chinesischer Softwareunternehmen. Problematisch an DeepSeek ist, dass es für die Volksrepublik China, anders als für die Vereinigten Staaten von Amerika, keinen entsprechenden Angemessenheitsbeschluss der EU-Kommission gibt.

Darüber hinaus hatte DeepSeek keine Vertreterin beziehungsweise keinen Vertreter nach Artikel 27 Datenschutzgrundverordnung (DSGVO) benannt. Nach Artikel 27 Absatz 1 DSGVO hat jede verantwortliche Stelle, die nicht innerhalb der Europäischen Union niedergelassen ist, ihre Dienstleistung aber Personen innerhalb der Europäischen Union anbietet, eine Vertreterin oder einen Vertreter innerhalb der Europäischen Union zu benennen.

Dies nahm der Landesbeauftrage für Datenschutz und Informationsfreiheit zusammen mit anderen deutschen Landesdatenschutzbeauftragten zum Anlass, zu Beginn des Berichtsjahres ein Informationsersuchen nach Artikel 58 Absatz 1 Buchstabe a) DSGVO an die hinter DeepSeek stehenden Unternehmen zu stellen. Hintergrund dieses Ersuchens war, dass der Landesbeauftragte für Datenschutz und Informationsfreiheit davon ausging, dass DeepSeek seine Dienste auch innerhalb der Europäischen Union beziehungsweise auf dem deutschen Markt anbietet und sich damit auch an die hier ansässigen Personen richtet. Daher ist damit der sachliche und räumliche Anwendungsbereich der Datenschutzgrundverordnung gemäß Artikel 2 Absatz 1 und Artikel 3 Absatz 2 Buchstabe a) DSGVO eröffnet.

In einem zweiten Schreiben wurde DeepSeek abermals aufgefordert, Stellung zu nehmen, weil der Landesbeauftragte für Datenschutz und Informationsfreiheit überprüfen will, ob DeepSeek die personenbezogenen Daten seiner europäischen Nutzerinnen und Nutzer an die Volksrepublik China übermittelt. DeepSeek hat nunmehr auf diese Schreiben reagiert und neben einem umfangreichen Vortrag in der Sache, der derzeit ausgewertet wird, einen Vertreter gemäß Artikel 27 DSGVO innerhalb der Europäischen Union benannt. Der Landesbeauftragte für Datenschutz und Informationsfreiheit und die weiteren beteiligten Landesdatenschutzbeauftragten befinden sich weiterhin im Austausch mit DeepSeek.

12.8 Standortdatenverarbeitung durch Apps

Zu Beginn des Berichtsjahres berichteten mehrere Medien, dass eine Vielzahl von Apps die Standortdaten der Nutzerinnen und Nutzer sammelten und an sogenannte Datenbroker weitergäben, obwohl dies vielfach für die Funktion der App nicht notwendig sei. Dabei wurde deutlich, dass es für die Nutzerinnen und Nutzer dieser Apps vielfach nicht möglich ist, nachzuvollziehen, mit welchen Dritten ihre Standortdaten geteilt werden.

Obwohl es sich bei den durch die Berichterstattung bekanntgewordenen Apps nicht um Apps von verantwortlichen Stellen aus der Freien Hansestadt Bremen handelte, nahm der Landesbeauftragte für Datenschutz und Informationsfreiheit die Medienberichterstattung zum

Anlass, um Apps in seinem Zuständigkeitsbereich, die angeben, Standortdaten zu verarbeiten, einer Prüfung zu unterziehen.

Bei dieser Prüfung von Apps öffentlicher sowie nicht öffentlicher Stellen konnte der Landesbeauftragte für Datenschutz und Informationsfreiheit keine Verstöße gegen die datenschutzrechtlichen Vorgaben feststellen. Insbesondere kam es auch bei keiner dieser Apps zum Prüfzeitpunkt zu einer Weitergabe von Standortdaten an etwaige Datenbroker.

12.9 Fehlende Datenschutzerklärungen auf Websites

Auch in diesem Berichtsjahr erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit wieder eine Vielzahl von Beschwerden aufgrund von fehlenden oder fehlerhaften Informationen nach Artikel 13 Datenschutzgrundverordnung auf Websites. Wie auch schon in den letzten Jahren ist es aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit unverständlich, wie fehlerhafte oder fehlende Datenschutzerklärungen weiterhin in einer solchen Vielzahl im nunmehr achten Jahr nach Inkrafttreten der Datenschutzgrundverordnung auftreten können (siehe hierzu 7. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 12.5 und 6. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 13.3).

12.10 Authentifizierungsschwachstelle bei einem Anbieter von Webshops

Der Landesbeauftragte für Datenschutz und Informationsfreiheit ist aufgrund eines Hinweises auf eine Authentifizierungsschwachstelle bei einem Anbieter von Webshops tätig geworden. Aufgrund dieser Schwachstelle war es möglich, die personenbezogenen Daten registrierter Kundinnen und Kunden einzusehen und zu verändern, ohne das Passwort zu kennen. Dies konnte passieren, weil jede Kundin beziehungsweise jeder Kunde nach erfolgreicher Registrierung eine fortlaufende Identifikationsnummer zugewiesen bekam. Bei erratener oder bekannter Nummer und einer leichten Modifikation anderer Aspekte der Authentifizierung konnte sich direkt in den Kundenbereich eingeloggt werden, ohne dass eine erneute Passwortabfrage oder eine andere Sicherheitsmaßnahme dies verhinderte.

Gemäß Artikel 32 Absatz 1 Datenschutzgrundverordnung (DSGVO) ist der Verantwortliche verpflichtet, durch geeignete technische und organisatorische Maßnahmen ein dem Risiko angemessenes Schutzniveau zu schaffen, das unter anderem die Integrität und Vertraulichkeit der Daten wahrt. Dies ist bei Webshops besonders relevant, weil zum einen die Adresse und Bestellhistorie der Kundinnen und Kunden, zum Beispiel für Spam oder zum Stalking, missbraucht werden kann und zum anderen Artikel in deren oder dessen Namen und auf deren oder dessen Kosten zu einer anderen Adresse bestellt werden könnten.

Artikel 25 DSGVO regelt, dass die Verarbeitung personenbezogener Daten durch technische und organisatorische Maßnahmen begleitet werden soll, die dem Stand der Technik entsprechen müssen. Bei der Entwicklung von Software sollte immer das Prinzip Security-by-Design verfolgt werden. Das bedeutet, dass Datenschutz und damit auch die Sicherheit der Daten schon in der Designphase der Software mitbedacht werden. Vertraulichkeit und Integrität können in Fällen, bei denen sich in einen bestimmten Bereich eingeloggt wird, durch eine erneute Passwortabfrage gestärkt werden. Dies wäre dann unabhängig von dem Link, über den die Website erreicht wurde. Auch ein Deep-Link, ein langer Link, der nicht ohne Weiteres erraten oder iterativ überprüft werden kann, wäre eine Möglichkeit, Daten ohne eine erneute Authentifizierung zur Verfügung zu stellen. Allerdings fällt diese Maßnahme in den Bereich der Security-by-Obscurity, also Sicherheit durch Verschleierung, und sollte daher nur nach einer sorgsamen Abwägung der Frage eingesetzt werden, ob diese technische Maßnahme zum Schutz der verarbeiteten Daten ausreichend ist.

Im vorliegenden Fall konnte die verantwortliche Stelle durch das Tätigwerden des Landesbeauftragten für Datenschutz und Informationsfreiheit sowie des Hinweisgebers auf die Sicherheitslücke aufmerksam gemacht werden, woraufhin dieser diese beseitigen konnte.

12.11 Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von Künstliche Intelligenz einsetzenden Systemen

Im Berichtsjahr wurde die „Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen“ von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder veröffentlicht, die umfassend die technischen und organisatorischen Maßnahmen für die datenschutzkonforme Entwicklung und den Betrieb von Systemen, die Künstliche Intelligenz einsetzen, darstellt. Die Orientierungshilfe richtet sich insbesondere an Herstellerinnen und Hersteller sowie Entwicklerinnen und Entwickler von Künstliche Intelligenz verwendete Systeme, um die Einhaltung der datenschutzrechtlichen Anforderungen gemäß der Datenschutzgrundverordnung (DSGVO) sicherzustellen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat aktiv an der Erarbeitung dieser Orientierungshilfe mitgewirkt.

Die Orientierungshilfe gliedert den Lebenszyklus eines Systems, das Künstliche Intelligenz verwendet, in vier Phasen: Design, Entwicklung, Einführung sowie Betrieb und Monitoring. Jede dieser Phasen umfasst spezifische datenschutzrechtliche Anforderungen, die es zu beachten gilt. Dabei sind die grundlegenden Datenschutzprinzipien aus Artikel 5 DSGVO, wie Rechtmäßigkeit, Zweckbindung, Datenminimierung, Transparenz, Integrität, Vertraulichkeit

und Intervenierbarkeit, durchgängig zu berücksichtigen. Die Orientierungshilfe soll dabei unterstützen, diese Grundsätze einzuhalten. Als methodischer Rahmen wird das Standard-Datenschutzmodell verwendet, das zum Ziel hat, die rechtlichen Vorgaben der Datenschutzgrundverordnung in technische und organisatorische Maßnahmen zu übersetzen. Stetig weiterentwickelt wird das Standard-Datenschutzmodell von einer Unterarbeitsgruppe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, an der auch der Landesbeauftragte für Datenschutz und Informationsfreiheit beteiligt ist. Die Gewährleistungsziele aus dem Standard-Datenschutzmodell entsprechen hierbei den Grundsätzen für die Verarbeitung personenbezogener Daten aus Artikel 5 DSGVO.

Herstellerinnen und Hersteller sowie Entwicklerinnen und Entwickler sollten die Gewährleistungsziele in allen Phasen systematisch beachten und umsetzen, um ein angemessenes Datenschutzniveau sicherzustellen und die Rechte und Freiheiten der betroffenen Personen zu schützen. Die Orientierungshilfe stellt, indem sie auf die Bedeutung der datenschutzrechtlichen Vorgaben für die jeweilige Lebensphase eines Systems, das Künstliche Intelligenz verwendet, eingeht, einen wichtigen Beitrag zu einem systematischeren Vorgehen und damit zur rechtskonformen Gestaltung von solchen Systemen dar und unterstützt die verantwortlichen Akteure, die komplexen datenschutzrechtlichen Vorgaben einzuhalten.

13. Werbung

13.1 Gemeldete Datenschutzverletzungen

Von Unternehmen aus dem Bereich Werbung erhielt der Landesbeauftragte für Datenschutz und Informationsfreiheit im Berichtsjahr eine Meldung über Verletzungen des Schutzes personenbezogener Daten nach Artikel 33 Datenschutzgrundverordnung (DSGVO). Hierbei handelte es sich um einen Zugriff auf Daten von Kundinnen und Kunden durch einen unberechtigten Dritten.

Dagegen erreichten ihn 61 Beschwerden über Unternehmen, die aus Sicht der Beschwerdeführenden im Zusammenhang mit Werbemaßnahmen gegen die Datenschutzgrundverordnung verstoßen hatten. Eine Vielzahl der Beschwerden richteten sich gegen die unberechtigte Verarbeitung von personenbezogenen Daten zur Werbezwecken ohne Rechtsgrundlage und die Nichtumsetzung von Werbewidersprüchen nach Artikel 21 DSGVO. Dies ist ein deutlicher Anstieg im Vergleich zum Vorjahr.

13.2 Bundesverwaltungsgerichtsurteil zur rechtlichen Zulässigkeit von Werbung mit E-Mails

Der wesentliche Teil der Beschwerden über Unternehmen im Werbebereich betraf erneut die Kontaktierung zu Werbezwecken per E-Mail, obwohl die Betroffenen hierfür keine Einwilligung erteilt hatten.

Bereits im 4., 5. und 6. Jahresbericht nach der Datenschutzgrundverordnung hatte der Landesbeauftragte für Datenschutz und Informationsfreiheit darauf hingewiesen, dass Werbung, insbesondere E-Mail-Werbung, nur unter Berücksichtigung der Anforderungen des § 7 Unlauterer Wettbewerb-Gesetz (UWG) erfolgen darf (siehe hierzu 6. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 14.2 sowie 5. und 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 14.3). Danach ist Werbung mit einem Telefonanruf bei Verbraucherinnen und Verbrauchern ohne deren vorherige ausdrückliche Einwilligungen oder bei sonstigen Marktteilnehmerinnen und -teilnehmern ohne deren zumindest mutmaßliche Einwilligung stets unzulässig. Werbung per E-Mail ohne die vorherige Einwilligung der Betroffenen ist nur noch unter den strengen Voraussetzungen des § 7 Absatz 3 UWG möglich. Das heißt: Die oder der Verantwortliche muss die E-Mail-Adresse der oder des Betroffenen im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung erhalten haben. Sie oder er darf die E-Mail-Adresse nur zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwenden, wobei der Begriff der „Ähnlichkeit“ eng auszulegen ist. Die oder der Betroffene darf der Verwendung der E-Mail-Adresse nicht widersprochen haben und sie oder er muss bei Erhebung der E-Mail-Adresse und bei jeder weiteren Verwendung eindeutig darauf hingewiesen werden,

dass sie oder er der Verwendung jederzeit widersprechen kann. Diese Rechtsansicht hat nunmehr auch das Bundesverwaltungsgericht mit Urteil vom 29. Januar 2025 (Aktenzeichen 6 C 3.23) bestätigt.

Vor dem Hintergrund dieser Rechtsprechung ist Werbenden zu raten, die vorherige Einwilligung der jeweiligen Betroffenen einzuholen.

13.3 Datenschutzrechtliche Informationspflichten bei Erhebung von Daten an der Haustür

Im Berichtszeitraum erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit einige Beschwerden über die Erhebung von personenbezogenen Daten an der Haustür. Dabei erfolgte die Datenerhebung entweder durch eine persönliche Ansprache an der Haustür, aber auch durch Erfassen oder Fotografieren der Klingelschilder. In der Folge erhielten die Betroffenen dann Werbeschreiben, beispielsweise für Glasfaserverträge oder den Kauf von Solaranlagen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit weist darauf hin, dass auch bei der Datenerhebung an der Haustür, selbst wenn nur die Daten auf dem Klingelschild notiert oder in ein elektronisches Gerät eingegeben werden, gemäß den Anforderungen der Artikel 13 und 14 Datenschutzgrundverordnung über die Datenerhebung zu informieren ist. Die Information muss dabei zum Zeitpunkt der Datenerhebung, also bereits beim Erfassen der Klingelschilder oder der Datenmitteilung durch die Hausbewohnerinnen und -bewohner, erfolgen.

Daneben stellt sich für die werbliche Ansprache der Hausbewohnerinnen oder -bewohner per Briefpost ohnehin die Frage, ob die Erhebung der Namensdaten erforderlich ist, denn aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit können Schreiben anonym an die Bewohnerinnen und Bewohner des Hauses gerichtet werden.

13.4 Unverzügliche Umsetzung Werbewiderspruch

Im Berichtsjahr erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit erneut zahlreiche Beschwerden über die Nichtumsetzung von Werbewidersprüchen.

Gemäß den Vorgaben der Datenschutzgrundverordnung sind Werbewidersprüche von den jeweiligen Verantwortlichen unverzüglich umzusetzen und die Umsetzung gegenüber den Betroffenen zu bestätigen. Dabei haben die jeweiligen Verantwortlichen durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass beispielsweise eine Abmeldung von Newsletter-E-Mails nicht ausschließlich über einen „Abmeldelink“ möglich ist, sondern auch entsprechende Werbewidersprüche, die per E-Mail eingehen, unverzüglich bearbeitet und umgesetzt werden.

13.5 Durchsetzung eines Auskunftsverlangens

In einem Fall wandte sich ein Marketingunternehmen, dessen Unternehmensgegenstand der Versand von E-Mail-Werbung war, gegen eine auf die Beantwortung von Fragen gerichtete datenschutzrechtliche Auskunftsanordnung sowie eine im Hinblick auf diese erfolgte Zwangsgeldfestsetzung des Landesbeauftragten für Datenschutz und Informationsfreiheit. Der Landesbeauftragte für Datenschutz und Informationsfreiheit hatte die Auskunftsanordnung bereits im Jahr 2023 erlassen.

Das Marketingunternehmen versuchte nachfolgend, indem es zahlreiche Klageverfahren einleitete, eine Sitzverlegung und die Liquidation vollzog, sich der Auskunftsanordnung zu entziehen. Die Beantwortung seiner Fragen ist für den Landesbeauftragten für Datenschutz und Informationsfreiheit von erheblicher Bedeutung, um aufzuklären, in welchem Umfang personenbezogene Daten verarbeitet wurden und ob diese Verarbeitung rechtmäßig erfolgte, und letztendlich die Betroffenenrechte entsprechend den gesetzlichen Vorgaben durchsetzen zu können. Das Verwaltungsgericht Bremen wies die Anfechtungsklage gegen die Auskunftsanordnung ab. Im Berichtszeitraum hat das Oberverwaltungsgericht Bremen mit Beschluss vom 14. April 2025 (Aktenzeichen 1 LA 11/25) den Antrag auf Zulassung der Berufung gegen das Urteil des Verwaltungsgerichtes Bremen vom 17. Dezember 2024 (Aktenzeichen 4 K 2298/23) abgelehnt. Die Auskunftsanordnung ist nunmehr bestandskräftig und wird vom Landesbeauftragten für Datenschutz und Informationsfreiheit vollstreckt.

Durch die vorliegenden verwaltungsgerichtlichen und oberverwaltungsgerichtlichen Entscheidungen ist nunmehr sichergestellt, dass das pauschale Berufen darauf, dass Daten gelöscht seien, nicht dazu führt, dass Auskunftsanordnungen des Landesbeauftragten für Datenschutz und Informationsfreiheit unterlaufen werden können. Dies stärkt die Position der Aufsichtsbehörde in vergleichbaren Fällen und eröffnet den Weg zu einer effektiveren Aufsicht.

14. Videoüberwachung im nicht öffentlichen Bereich

14.1 Gemeldete Datenschutzverletzungen

Im Bereich der Videoüberwachung durch nicht öffentliche Stellen gab es in diesem Berichtsjahr, wie im Vorjahr, keine gemeldeten Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung seitens einer oder eines Verantwortlichen.

Die Anzahl der Beschwerden stieg jedoch mit nunmehr 148 Beschwerden in diesem Bereich im Vergleich zum Vorjahr erneut an. Darüber hinaus beriet der Landesbeauftragte für Datenschutz und Informationsfreiheit auch in diesem Berichtsjahr eine hohe Anzahl von Bürgerinnen und Bürgern, die sich telefonisch und schriftlich mit Fragen zur Videoüberwachung an ihn gewandt haben. Die meisten Beschwerden sowie Beratungsanfragen betrafen die Videoüberwachung in der Nachbarschaft. Daneben gab es auch eine hohe Anzahl an Beschwerden und Beratungsanfragen über in Cafés und Restaurants angebrachte Überwachungskameras. Positiv hervorzuheben ist der Anstieg an Beratungsanfragen durch Personen, die sich, bevor sie eine Überwachungsanlage installieren, bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit über die Zulässigkeitsvoraussetzungen erkundigten. Diese Entwicklung deutet auf eine Sensibilisierung im Umgang mit der Videoüberwachung hin.

14.2 Videoüberwachung im Beschäftigtenverhältnis

Auch in diesem Berichtsjahr gingen beim Landesbeauftragten für Datenschutz und Informationsfreiheit Beschwerden und Beratungsanfragen ein, die sich auf die Videoüberwachung von Beschäftigten bezogen. Die Betroffenen äußerten dabei häufig die Sorge, dass die installierten Überwachungskameras von ihren Vorgesetzten zur Verhaltens- und Leistungskontrolle eingesetzt werden könnten. Hierbei ist zu berücksichtigen, dass Arbeitnehmerinnen und Arbeitnehmer grundsätzlich keinem dauerhaften Kontrolldruck durch die Arbeitgeberin beziehungsweise den Arbeitgeber ausgesetzt sein dürfen.

Die aufgrund der Beschwerden angeschriebenen Unternehmen führten im Rahmen der aufsichtsbehördlichen Verfahren oftmals Gründe für den Einsatz von Videoüberwachung an, die auf den ersten Blick keinen unmittelbaren Bezug zu den Beschäftigten hatten. Hierzu zählt zum Beispiel, Diebstähle zu verhindern. Gleichwohl sind jedoch auch die schutzwürdigen Interessen der Beschäftigten zu beachten. Bei der Abwägung, ob eine Videoüberwachung angesichts des Eingriffes in das Recht der Beschäftigten auf informationelle Selbstbestimmung verhältnismäßig ist, ist insbesondere zu prüfen, in welchem Umfang den Beschäftigten noch Rückzugsmöglichkeiten verbleiben. So ist eine dauerhafte Videoüberwachung des Produktionsbereiches, in dem die Beschäftigten überwiegend tätig sind, grundsätzlich unzulässig. Ebenso ist der Einsatz von Kameras in Umkleideräumen, Pausenbereichen oder sanitären

Einrichtungen nicht gestattet. Darüber hinaus ist stets zu prüfen, ob weniger eingriffsintensive Maßnahmen zur Verfügung stehen, die den Sicherheitsinteressen des Unternehmens in gleicher Weise gerecht werden können. So kann beispielsweise der Einsatz einer Alarmanlage bereits ausreichen, um Einbruchsversuchen wirksam entgegenzuwirken.

In einem, aufgrund einer Beschwerde eingeleiteten, Verfahren waren in einem Unternehmen der Pausen- sowie Büroraum, in dem die Arbeitsplätze der Beschäftigten eingerichtet waren, von durch den Arbeitgeber angebrachten Überwachungskameras erfasst. Der Arbeitgeber gab an, dass die Kameras nicht zur Überwachung, sondern zum Schutz der Beschäftigten installiert worden seien. Dies sei ein berechtigtes Interesse des Arbeitgebers, das gemäß Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f) Datenschutzgrundverordnung als zulässig eingestuft werden könne.

Dies war jedoch nicht der Fall, weil den Beschäftigten unter anderem keine Rückzugsmöglichkeit eingeräumt wurde. Im Rahmen des Verfahrens zeigte sich der Arbeitgeber kooperativ und teilte mit, dass die Videoüberwachungsanlage nunmehr abgebaut worden sei. Seitens des Landesbeauftragten für Datenschutz und Informationsfreiheit wurde eine Verwarnung ausgesprochen, weil die Videoüberwachung bis zu dem Zeitpunkt des Abbaus unrechtmäßig durchgeführt worden war.

14.3 Videoüberwachung in Gastronomien

Zahlreiche der beim Landesbeauftragten für Datenschutz und Informationsfreiheit eingereichten Beschwerden im Bereich Videoüberwachung durch nicht öffentliche Stellen bezogen sich auf Videoüberwachungsanlagen, die durch Café- und Restaurantbetreiber installiert worden waren. Da sich die Beschwerden zumeist auf die oftmals unzureichende Hinweisbeschilderung bezogen, wirkte der Landesbeauftragte für Datenschutz und Informationsfreiheit in den zu prüfenden Fällen darauf hin, dass durch eine Hinweisbeschilderung, die alle nach Artikel 13 Datenschutzgrundverordnung (DSGVO) erforderlichen Angaben beinhaltet, eine ausreichende Transparenz über die Datenverarbeitung hergestellt wurde.

In einer Vielzahl der Fälle genügte es jedoch nicht, die Transparenz in Bezug auf die Datenverarbeitung durch eine verbesserte Hinweisbeschilderung zu erhöhen. Auch wenn in den meisten Fällen als Zwecke der Videoüberwachung angegeben wurden, das Hausrecht zu wahren und den Schutz gegen Warendiebstahl zu gewährleisten sowie Beweise bei Vandalismus und Einbruchsversuchen zu sichern, konnten die Verantwortlichen nämlich häufig darüber hinaus die Erforderlichkeit der Videoüberwachung, insbesondere für jede einzelne angebrachte Überwachungskamera, nicht nachvollziehbar darstellen. Vor allem konnte der Einsatz der in Ess- und Aufenthaltsbereichen angebrachten Kameras nicht begründet werden.

Die Rechtmäßigkeit einer Videoüberwachung in einer gastronomischen Einrichtung liegt lediglich dann vor, wenn sie zur Wahrung berechtigter Interessen der Betreiberin beziehungsweise des Betreibers erforderlich ist und schutzwürdige Interessen der betroffenen Personen nicht überwiegen (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f) DSGVO). Der Besuch in einer Gaststätte und insbesondere der Aufenthalt in Essbereichen sind dem Freizeitgestaltungsbereich zuzuordnen, sodass die Persönlichkeitsrechte betroffener Personen in diesen Bereichen besonders schützenswert sind und die Überwachung dieser Bereiche während der Öffnungszeiten regelmäßig unzulässig ist. In den geprüften Fällen sorgte der Landesbeauftragte für Datenschutz und Informationsfreiheit daher dafür, dass die Verantwortlichen eine räumliche und/oder zeitliche Beschränkung der Videoüberwachung vornahmen und ihre Videoüberwachungsanlagen den gesetzlichen Anforderungen entsprechend anpassten.

14.4 Videoüberwachung des öffentlichen Bereiches durch Privatpersonen

Im Bereich der Videoüberwachung durch Privatpersonen ist die Anzahl der Beschwerden sowie der Beratungsanfragen in diesem Berichtsjahr erneut gestiegen und richtete sich überwiegend gegen auf Privatgrundstücken angebrachte Überwachungskameras.

In diesem Bereich zeigt sich oft ein eindeutiges Spannungsfeld: Während sich insbesondere Nachbarinnen und Nachbarn durch die angebrachten Überwachungskameras in ihren Persönlichkeitsrechten beeinträchtigt fühlen, möchten die Verantwortlichen in den meisten Fällen durch die Überwachungskameras den Schutz ihres Eigentumes sicherstellen. Dabei nehmen die Verantwortlichen oft an, dass die Datenschutzgrundverordnung (DSGVO) bei Überwachungskameras, die zum Schutz des eigenen Grundstückes installiert worden sind, aufgrund der Haushaltsausnahme in Artikel 2 Absatz 2 Buchstabe c) DSGVO nicht anwendbar sei.

Dies gilt jedoch lediglich dann, wenn sich die Videoüberwachung ausschließlich auf das eigene, private Grundstück richtet. Erfasst die Videoüberwachung Bereiche außerhalb des privaten Grundstückes, zum Beispiel Teile der öffentlichen Gehwege sowie Straßen oder Nachbargrundstücke, kommt die Datenschutzgrundverordnung zur Anwendung und die Videoüberwachung bedarf einer Rechtsgrundlage. Diese kann sich aus Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f) DSGVO ergeben.

Da die Videoüberwachung regelmäßig einen Eingriff in die Persönlichkeitsrechte der von derartigen Maßnahmen betroffenen Personen darstellt, sind die Zulässigkeitsvoraussetzungen, die von einer Betreiberin beziehungsweise einem Betreiber einer Videokamera erfüllt werden müssen, sehr hoch. Nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f) DSGVO ist die Erhebung personenbezogener Daten mit Videotechnik nur zulässig, soweit sie unter anderem zur Wahrung berechtigter Interessen erforderlich ist und sofern nicht schutzwürdige Interessen der betroffenen Personen überwiegen.

Gemessen an diesem Maßstab, stellte der Landesbeauftragte für Datenschutz und Informationsfreiheit häufig Verbesserungsbedarfe in Bezug auf die Datenschutzkonformität fest. Dementsprechend wurden Verantwortliche vom Landesbeauftragten für Datenschutz und Informationsfreiheit schriftlich auf die Zulässigkeitsvoraussetzungen der Videoüberwachung hingewiesen und zur Anpassung der aktuellen Videoüberwachung aufgefordert, insbesondere wenn bei einer Grundstücküberwachung auch Teile des öffentlichen Raumes oder der Nachbargrundstücke betroffen waren. Zudem wurden die Verantwortlichen darauf hingewiesen, dass es sich bei der Missachtung der gesetzlichen Voraussetzungen um einen datenschutzrechtlichen Verstoß handelt, der mit einer Geldbuße nach Artikel 83 DSGVO geahndet werden kann.

15. Kredit-, Versicherungs- und allgemeine Wirtschaft

15.1 Gemeldete Datenschutzverletzungen

Erfolgreiche Angriffe auf die IT-Infrastruktur von Unternehmen in der Kredit- sowie Versicherungswirtschaft und in den weiteren Wirtschaftsbereichen, die einen unbefugten Zugriff auch auf personenbezogene Daten zur Folge hatten, beispielsweise durch Phishing-Mail- oder Ransomware-Attacken, waren auch in diesem Berichtsjahr wieder der hauptsächliche Anlass für die Meldung von Datenschutzvorfällen.

Legt man die Analysen des Bundesamtes für Sicherheit in der Informationstechnik zur IT-Bedrohungslage zugrunde, dürfte jedoch davon auszugehen sein, dass die Meldungen an den Landesbeauftragten für Datenschutz und Informationsfreiheit trotz einer deutlich erhöhten Anzahl gegenüber dem Vorjahr gleichwohl nur einen Bruchteil der tatsächlichen meldepflichtigen Vorfälle abbilden. Im öffentlichen Fokus scheint bei diesen „Cyberattacken“ nach wie vor oftmals der wirtschaftliche Schaden für das Unternehmen zu stehen, weniger der Schaden für das Persönlichkeitsrecht der Betroffenen, namentlich zumeist Kundinnen und Kunden sowie Mitarbeiterinnen und Mitarbeiter des Unternehmens, die einen regelmäßig irreversiblen Kontrollverlust bezüglich ihrer persönlichen Daten mit ungewissen Folgen hinzunehmen haben.

Wie bereits im Vorjahr berichtet (siehe hierzu 7. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 15.2), hatte der Europäische Gerichtshof in einem wegweisenden Urteil entschieden, dass die begründete Befürchtung einer betroffenen Person, ihre Daten würden durch Dritte missbräuchlich verwendet, einen immateriellen Schaden darstellen und nach weiterer Maßgabe des Artikel 82 Datenschutzgrundverordnung auch einen Schadensersatzanspruch gegen das Unternehmen begründen könne (Europäischer Gerichtshof, Urteil vom 14. Dezember 2023, Aktenzeichen C-340/21).

Weitere Vorfallsmeldungen betrafen die üblichen Vorkommnisse, etwa das Abhandenkommen von Daten im Zuge eines Diebstahles mobiler IT-Geräte, den Fehlzugang von Nachrichten beziehungsweise Unterlagen bei einer oder einem Dritten aufgrund Fehladressierung von elektronischer oder brieflicher Post, die zigfache Offenlegung von E-Mail-Adressen von Kundinnen und Kunden aufgrund Nutzung des „offenen“ E-Mail-Adressfeldes.

15.2 Versicherungswirtschaft

Im Bereich der Versicherungswirtschaft erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit im Berichtsjahr zwei Meldungen nach Artikel 33 Datenschutzgrundverordnung zu einer möglichen Datenschutzverletzung einer Verantwortlichen.

Bei der Meldung handelte es sich um einen Sachverhalt, der lediglich vorsorglich bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit gemeldet wurde und bei dem sich letztendlich nach Abschluss der forensischen Untersuchungen aber herausgestellt hat, dass keine Verletzung des Schutzes personenbezogener Daten im Sinne der Datenschutzgrundverordnung vorlag, sodass dieser Vorfall tatsächlich nicht meldepflichtig war. Daneben erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit insgesamt vier Beschwerden von Bürgerinnen und Bürgern, beispielsweise zur Löschung von personenbezogenen Daten durch Versicherungsunternehmen.

15.3 Schadensersatz bei Meldung einer streitigen Forderung zur Einspeicherung bei einer Wirtschaftsauskunftei

Im Berichtsjahr kam es zu einem höchstrichterlichen Urteil zu der Schadensersatzpflicht, wenn streitige Forderungen an eine Wirtschaftsauskunftei übermittelt wurden. Der Entscheidung lag folgender Sachverhalt zu Grunde: Obgleich Entgeltforderungen zwischen einem Mobilfunkunternehmen und einer Kundin zwischen beiden streitig waren und die Existenz der Forderungen nicht gerichtlich geklärt war, meldete das Unternehmen die Forderung als unbezahlt bei einer Wirtschaftsauskunftei, damit diese die Daten zu den bereits vorhandenen Bonitätsdaten zur Person der Kundin speichert. Da dieser zu Unrecht erfolgte Eintrag über einen längeren Zeitraum gespeichert blieb und die Kreditwürdigkeitseinschätzung der betroffenen Kundin durch Bezieherinnen und Bezieher von Bonitätsauskünften negativ beeinflusste, bestätigte der Bundesgerichtshof mit Urteil vom 28. Januar 2025 wegen des hierin liegenden immateriellen Schadens einen Schadensersatzanspruch der Kundin gegen das Mobilfunkunternehmen nach Artikel 82 Datenschutzgrundverordnung (Bundesgerichtshof, Urteil vom 28. Januar 2025, Aktenzeichen VI ZR 183/22).

So erfreulich das Urteil aus Sicht betroffener Personen dem Grunde nach ist, scheint die zugesprochene Schadensausgleichssumme von 500 € jedoch ob ihrer geringen Höhe wenig überzeugend. Eine so geringe Summe bildet nicht die Beeinträchtigung ab, die von einer Bloßstellung durch eine negative Bonitätsauskunft ausgeht.

15.4 Mutmaßlich unberechtigte Zahlungsaufforderungen zur datenschutzrechtlichen Prüfung

Immer wieder wird der Landesbeauftragte für Datenschutz und Informationsfreiheit um eine datenschutzrechtliche Überprüfung gebeten, weil sich die hilfesuchende Person einer aus ihrer Sicht unberechtigten Zahlungsaufforderung eines Unternehmens, gegebenenfalls unter Einschaltung eines Inkassodienstleisters, ausgesetzt sieht.

In den weitaus meisten Fällen kann der Landesbeauftragte für Datenschutz und Informationsfreiheit insoweit jedoch zunächst datenschutzaufsichtsrechtlich nicht weiterhelfen. Zumeist dreht sich die Streitigkeit im Kern nämlich um das Zustandekommen beziehungsweise Nicht-Zustandekommen eines Vertrages und hieraus folgend um das Bestehen oder Nicht-Bestehen eines vertraglichen Zahlungsanspruches. Ob ein Vertrag und damit gegebenenfalls auch ein vertraglicher Zahlungsanspruch existiert, ist allein eine zivilrechtliche Frage. Diese zivilrechtliche Frage kann und darf im Streitfall letztlich nur ein Zivilgericht klären. Der Landesbeauftragte für Datenschutz und Informationsfreiheit ist hingegen als Datenschutzaufsichtsbehörde nicht befugt, über das Zustandekommen und Bestehen von Verträgen beziehungsweise über vertragliche Ansprüche zu entscheiden.

Für die datenschutzrechtliche Bewertung der Verarbeitung von personenbezogenen Daten gilt in diesem Zusammenhang: Sofern ein Vertrag besteht, darf nach geltendem Datenschutzrecht die Vertragspartnerin (Gläubigerin) oder der Vertragspartner (Gläubiger) im vertragserforderlichen Umfang personenbezogene Daten ihrer oder seiner Schuldnerin beziehungsweise ihres oder seines Schuldners verarbeiten (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe b) Datenschutzgrundverordnung [DSGVO]). Ebenso darf sie oder er die personenbezogenen Daten der Schuldnerin beziehungsweise des Schuldners zur Geltendmachung einer aus ihrer oder seiner Sicht bestehenden Vertragsforderung grundsätzlich auch an eine Rechtsanwältin oder einen Rechtsanwalt oder ein Inkassounternehmen übermitteln (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f) DSGVO). Solange um den Vertrag beziehungsweise Ansprüche gestritten wird, kann auch keine Datenlöschung verlangt werden.

15.5 Mystery-Pakete

Wie andere Landesdatenschutzaufsichtsbehörden erhielt auch der Landesbeauftragte für Datenschutz und Informationsfreiheit im Berichtszeitraum Hinweise auf datenschutzrechtliche Mängel beim Handel mit sogenannten Mystery-Paketen. Kurz gesagt, handelt es sich bei den Mystery-Pakten um Warenrücksendungen der ehemaligen Bestellerinnen und Besteller beziehungsweise Paketadressatinnen und -adressaten, die nicht mehr von dem ursprünglich ver-

sendenden Handelsunternehmen zurückgenommen werden, sondern über Zwischenhandelswege ungeöffnet in Warenautomaten oder im Geschäftslokal landen und dort von Endabnehmerinnen und -abnehmern aufgekauft werden, weil sie auf einen wertvollen Paketinhalt hoffen.

Als datenschutzrechtlich problematisch können sich namentlich die aufgebrachten Rücksendeetiketten erweisen; diese geben nämlich regelmäßig Namen und Kontaktdaten der ursprünglichen Empfängerin oder des ursprünglichen Empfängers der Versandware und der nunmehrigen Absenderin beziehungsweise des Absenders preis. Wenn diese Etiketten vor dem Verkauf der Retourensendung nicht beziehungsweise nur unvollständig entfernt beziehungsweise nicht hinreichend und irreversibel unkenntlich gemacht wurden und daher einem x-beliebigen Käufer an unbekanntem Ort zur Kenntnis gelangen, kann jener je nach Inhalt des Paketes neben den Kontaktdaten Erkenntnisse zu der Person der Warenrücksenderin beziehungsweise des Warenrücksenders gewinnen, die schützenswerte personenbezogene Daten darstellen.

Der betroffene lokale Händler war ohne Weiteres problemeinsichtig und sagte dem Landesbeauftragten für Datenschutz und Informationsfreiheit eine Lösung zu. Gleichwohl sollte bereits beim Erstaufkauf der Retourensendungen für eine endgültige Unkenntlichmachung der Kontaktdaten der Warenrücksenderin oder des Warenrückensenders gesorgt werden, auch wenn dies angesichts der Paketmassen vorhersehbar einiges an Aufwand bereiten dürfte.

Die Unkenntlichmachung der Information der Absenderinnen und Absender ändert aber nichts daran, dass unter Umständen mit dem Paketinhalt, etwa im Falle eines beiliegenden ausgefüllten Rückgabe-Formulars, unbefugt personenbezogene Daten offengelegt werden können. Auch dies gilt es zu vermeiden.

15.6 Orientierungshilfe Asset-Deal

Im Jahr 2024 wurde von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder ein Beschluss in Bezug auf die Übermittlungen personenbezogener Daten an die Erwerberin oder den Erwerber eines Unternehmens im Rahmen eines sogenannten Asset-Deals gefasst.[8] Ein Asset Deal liegt zum Beispiel vor, wenn eine Einzelunternehmerin oder ein Einzelunternehmer, die Veräußerin oder der Veräußerer, ihren beziehungsweise seinen Betrieb an eine Nachfolgerin oder einen Nachfolger, die Erwerberin oder den Erwerber, übergibt und diese beziehungsweise dieser dabei beispielsweise die Maschinen, den Kundenstamm und die Firmierung übernimmt und den Betrieb fortführt.

[8] abrufbar unter https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_Beschluss%20DSK_%20Asset_Deals.pdf.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gibt im vorgenannten Beschluss nunmehr datenschutzrechtliche Hinweise, in welchem Umfang und unter welchen Maßgaben Kunden-, Lieferanten- und Beschäftigtendaten dabei verarbeitet (übermittelt) werden dürfen. Dabei ist insbesondere zu beachten, dass der Erwerber, innerhalb einer angemessenen Frist, spätestens innerhalb eines Monats nach Erhalt der Datensätze vom Veräußerer, die Kundinnen und Kunden im Sinne des Artikel 14 Datenschutzgrundverordnung über die Erhebung ihrer personenbezogenen Daten informieren muss. Diese Information dient dazu, dass die Betroffenen nach den Grundsätzen einer fairen und transparenten Verarbeitung unter anderem über die Existenz des Verarbeitungsvorganges und seine Zwecke unterrichtet sind. Sofern die Erwerberin beziehungsweise der Erwerber ausschließlich die Kundendatenbank als einziges losgelöstes „Asset“ von der Veräußerin beziehungsweise vom Veräußerer erwerben möchte, ist dies regelmäßig nur mit vorheriger Einwilligung der betroffenen Kundinnen und Kunden möglich.

16. Internationales und Europa

16.1 Digital Omnibus

Am 19. November 2025 veröffentlichte die Europäische Kommission einen Vorschlag zur Änderung der Datenschutzgrundverordnung und weiterer Digitalrechtsakte, den sogenannten Digital Omnibus. Der Regelungsvorschlag enthält unter anderem eine Änderung der Definition der personenbezogenen Daten gemäß Artikel 4 Nummer 1 Datenschutzgrundverordnung, wobei Kriterien dafür aufgestellt werden, wann Daten, die pseudonymisiert werden, noch einen Personenbezug aufweisen. Zudem sollen Regelungen in Bezug auf die Verarbeitung von personenbezogenen Daten bei dem Training und der Entwicklung Künstlicher Intelligenz aufgenommen werden. Beachtung verdient vor allem auch, dass die Europäische Kommission im Rahmen des Digital Omnibus eine Begriffsdefinition der wissenschaftlichen Forschung in die Datenschutzgrundverordnung aufnehmen möchte.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat sich auf ihrer Sitzung am 12. Dezember 2025 mit diesen Vorschlägen befasst. Aus ihrer Sicht ist der Zeitdruck eines Omnibusverfahrens nicht angemessen, weil es sich bei den Vorschlägen der Europäischen Kommission teilweise um fundamentale Anpassungsvorschläge handelt, wie beispielsweise bei der Definition der personenbezogenen Daten. Zu Beginn des neuen Jahres soll eine Stellungnahme, in die die Vorstellungen aller europäischen Datenschutzaufsichtsbehörden einfließen, fertiggestellt sein.

16.2 Erarbeitung konkreter Vorschläge für eine gezielte Anpassung der Datenschutzgrundverordnung

Die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder hat im Berichtsjahr Vorschläge für eine Reform der Datenschutzgrundverordnung erarbeitet. Zunächst hat sie hierzu am 20. November 2025 eine Entschließung zur „Verbesserung des Datenschutzes von Kindern“ verabschiedet (siehe hierzu Ziffer 18.5 dieses Berichtes), die eine Vielzahl von konkreten Regelungsvorschlägen enthält, mit denen der Datenschutz von Kindern verbessert werden könnte. Mit der Entschließung „DSGVO-Reform: IT-Hersteller in die Verantwortung nehmen!“ vom 12. Dezember 2025 fordert die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder, dass auch die Hersteller und Anbieter von IT-Diensten datenschutzrechtlich verantwortlich sein sollten (siehe hierzu Ziffer 18.7 dieses Berichtes). Hiermit soll dem Missstand abgeholfen werden, dass kleine und mittelständische Unternehmen häufig datenschutzrechtlich verantwortlich sind, obwohl sie nicht über die Möglichkeit verfügen, datenschutzkonforme Prozesse in den von ihnen eingesetzten IT-Diensten umzusetzen.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat sich vor allem in die Erarbeitung der Entschließung „DSGVO-Reform: Rechtssicherheit und Innovation gehen Hand in Hand – Anpassungen für KI erforderlich“ eingebracht, die ebenfalls am 12. Dezember 2025 verabschiedet worden ist, und er hat an der entsprechenden Unterarbeitsgruppe, die diese Entschließung vorbereitet hat, mitgearbeitet (siehe hierzu Ziffer 18.6 dieses Berichtes). Zentrales Anliegen der Entschließung ist es, dass die Schwierigkeiten, die bei der Durchsetzung von Betroffenenrechten im Kontext von Künstlicher Intelligenz auftreten, gleichwertige in der Datenschutzgrundverordnung verankerte Äquivalente erforderlich machen. Diese äquivalenten Schutzmaßnahmen können dabei nach der Auffassung der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder auch kompensatorisch sein.

Die aktuellen Vorschläge zur Reform der Datenschutzgrundverordnung ergänzen nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit frühere Reformvorschläge, wie sie im „Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO“ dargestellt wurden, der im November 2019 vorgelegt wurde und ebenfalls zahlreiche, weiterhin aktuelle Vorschläge zur Entbürokratisierung enthält.

16.3 Das Latombe-Urteil und was es für das Abkommen mit den Vereinigten Staaten von Amerika aktuell bedeutet

Am 10. Juli 2023 verabschiedete die Europäische Kommission den Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework. Dies hat zur Folge, dass personenbezogene Daten aus der Europäischen Union an die Vereinigten Staaten von Amerika auf der Grundlage des Angemessenheitsbeschlusses wieder an Unternehmen übermittelt werden dürfen, die in der vom Handelsministerium der Vereinigten Staaten von Amerika geführten und öffentlich zugänglichen Liste „Data Privacy Framework EU-USA“ genannt sind, ohne dass weitere Übermittlungsinstrumente oder zusätzliche Maßnahmen erforderlich sind.

Im vorletzten Jahr hatte der Landesbeauftragte für Datenschutz und Informationsfreiheit bereits über den Angemessenheitsbeschluss für die Vereinigten Staaten von Amerika informiert (siehe hierzu 6. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 17.1). Hauptmerkmal im EU-U.S. Data Privacy Framework ist unter anderem der dafür geschaffene Data Protection Review Court. Dies ist eine Instanz, die Beschwerden von Bürgerinnen und Bürgern der Vereinigten Staaten von Amerika sowie Bürgerinnen und Bürgern der Europäischen Union über unrechtmäßige Überwachungsmaßnahmen prüfen soll. Außerdem wurde eine weitreichende Aufsicht über die Geheimdienste die Vereinigten Staaten von Amerika eingeführt.

Am 6. September 2023 beantragte der französische Abgeordnete Herr Philippe Latombe bei dem Gericht der Europäischen Union, den Durchführungsbeschluss der Europäischen Kommission über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen der Europäischen Union und der Vereinigten Staaten von Amerika für nichtig zu erklären. Herr Philippe Latombe kritisierte insbesondere, dass der Data Protection Review Court kein unabhängiges Gericht sei, keine gesetzliche Grundlage habe und somit in seiner Struktur nicht unabhängig von der Regierung sei. Außerdem dürften Geheimdienste der Vereinigten Staaten von Amerika weiterhin in großem Umfang Daten verarbeiten, ohne dass eine vorherige richterliche Genehmigung erforderlich sei.

Nun hat das Gericht der Europäischen Union in einem Urteil vom 3. September 2025 (Aktenzeichen T 553/23) die Nichtigkeitsklage gegen den Angemessenheitsbeschluss abgewiesen. Das Gericht begründet dies vor allem damit, dass der Data Protection Review Court aus seiner Sicht unabhängig sei. Die Richterinnen und Richter des Data Protection Review Court könnten nämlich nur aus triftigen Gründen von der amerikanischen Generalstaatsanwältin abberufen werden. Weder die Generalstaatsanwältin noch die US-Nachrichtendienste dürften die Arbeit des Data Protection Review Court behindern oder beeinflussen. Zudem führe im konkreten Fall auch nicht zu einer Nichtigkeit des Angemessenheitsbeschlusses, dass der Data Protection Review Court nicht aufgrund eines Gesetzes, sondern nur durch einen Erlass der Justizministerin der Vereinigten Staaten von Amerika geschaffen worden sei.

Das Gericht der Europäischen Union entnimmt nämlich insofern aus der Rechtsprechung des Obersten Gerichtshofes der Vereinigten Staaten von Amerika, dass die Exekutive unabhängige Gremien mit Entscheidungsbefugnis einrichten könne und an Entscheidungen von diesem Gremium – solange wie der Erlass in Kraft sei – auch gebunden sei. Das Gericht der Europäischen Union stellte außerdem fest, dass auch nicht jede Form von großer Datenerhebung einer vorherigen Genehmigung durch eine unabhängige Behörde benötige. Ausreichend sei vielmehr, dass eine solche Maßnahme nachträglich gerichtlich überwacht werde. Dies geschieht im Falle der Datenerhebung durch die Nachrichtendienste der Vereinigten Staaten von Amerika in Form einer nachträglichen gerichtlichen Kontrolle durch den Data Protection Review Court.

Ob die Argumentation des Gerichtes der Europäischen Union tragfähig ist, ist weiterhin zweifelhaft. Gerade der Umstand, dass der Data Protection Review Court lediglich auf einem Erlass der Justizministerin der Vereinigten Staaten von Amerika beruht, führt dazu, dass dem entsprechenden Gericht jederzeit die Grundlage entzogen werden kann. Dies beeinträchtigt die Unabhängigkeit der Entscheidungen strukturell, denn die Richterinnen und Richter müssen befürchten, dass ihr Gericht abgeschafft werden wird, wenn sie Entscheidungen gegen die Regierung fällen. Die Garantien für die Unabhängigkeit des Gerichtes setzen nämlich hier ei-

nen entsprechenden Erlass voraus, der zur Disposition desjenigen steht, der kontrolliert werden soll. Zudem können auch nach einer potentiellen Aufhebung des Erlasses, die jederzeit möglich erscheint, personenbezogene Daten gefährdet sein. Ob überdies die Garantien der Unabhängigkeit des Data Protection Review Court selbst bei einer Fortgeltung des Erlasses im Übrigen belastbar sind, hängt davon ab, wie sich die Rechtsprechung des Obersten Gerichtshofes der Vereinigten Staaten in Amerika zu unabhängigen Verwaltungseinheiten und zur Rechtsstellung ihrer leitenden Mitarbeiterinnen und Mitarbeiter fortentwickelt.

Angesichts dieser Umstände muss ernst genommen werden, dass das Gericht der Europäischen Union die Europäische Kommission aufgefordert hat, den relevanten Rechtsrahmen der Vereinigten Staaten von Amerika fortlaufend zu überwachen. Die Europäische Kommission kann nämlich den Angemessenheitsbeschluss jederzeit aussetzen, ändern oder aufheben, falls sich die Situation in den Vereinigten Staaten von Amerika ändern würde. Der Kläger hat überdies gegen das Urteil des Gerichts der Europäischen Union Rechtsmittel eingelegt. Für Unternehmen bedeutet das Urteil daher keine Rechtssicherheit bei der Übertragung von Daten in die Vereinigten Staaten von Amerika. Der Landesbeauftragte für Datenschutz und Informationsfreiheit empfiehlt daher, bereits vorhandene geeignete Garantien und zusätzliche Maßnahmen beizubehalten und fortzuführen.

16.4 Angemessenheitsbeschlüsse für das Vereinigte Königreich

Die Europäische Kommission hat am 22. Juli 2025 den Entwurf für neue Angemessenheitsbeschlüsse mit dem Vereinigten Königreich veröffentlicht und am 19. Dezember 2025 beschlossen. Grundlage sind sowohl die Datenschutzgrundverordnung (DSGVO) als auch die JI-Richtlinie. Die Europäische Kommission kommt darin zum Schluss, dass das britische Datenschutzrecht weiterhin ein größtenteils gleichwertiges Schutzniveau im Vergleich zu dem europäischen Datenschutzrecht besitze.

Die Übermittlung personenbezogener Daten in Drittstaaten ist laut der Datenschutzgrundverordnung nur zulässig, wenn die Europäische Kommission einen Angemessenheitsbeschluss erlassen hat, alternative Schutzmechanismen bestehen oder die Bestimmungen von Artikel 49 DSGVO eintreffen. Ein Angemessenheitsbeschluss ist allerdings für viele Unternehmen der bessere Weg, weil dieser am meisten Rechtssicherheit bietet.

Bisher wurde für das Vereinigte Königreich, als Drittland, am 28. Juni 2021 ein Angemessenheitsbeschluss erlassen, der bis Ende Juni 2025 lief. Die Europäische Kommission hat ihn zunächst bis zum 27. Dezember 2025 befristet verlängert. Da das Vereinigte Königreich verschiedene Anpassungen im Datenschutzrecht plante, wollte die Europäische Kommission genau überprüfen, ob weiterhin ein angemessenes Schutzniveau besteht.

Der nun beschlossene Entwurf für die zwei neuen Angemessenheitsbeschlüsse mit dem Vereinigten Königreich sichert eine längerfristige Bestätigung der Angemessenheit. Die Europäische Kommission bestätigt, dass grundlegende Datenschutzprinzipien unverändert gewährleistet seien und dass der Schutz sensibler Daten auf einem mit der Europäischen Union vergleichbaren Schutzniveau liege. Die Angemessenheitsbeschlüsse gelten bis zum 27. Dezember 2031.

Die Entwürfe wurden vor der endgültigen Beschlussfassung dem Europäischen Datenschutzausschuss zur Stellungnahme vorgelegt. Die Zustimmung des Europäischen Datenschutzausschusses ist nämlich erforderlich, bevor die Beschlüsse endgültig erlassen werden können. Dieser hat dazu zwei Stellungnahmen veröffentlicht, welche die Angemessenheitsbeschlüsse für das Vereinigte Königreich befürworten. Es wird grundsätzlich begrüßt, dass sich das britische Datenschutzrecht trotz der jüngeren Gesetzesänderungen weiterhin eng an der Datenschutzgrundverordnung orientiert. Zugleich fordert er die EU-Kommission auf, bestimmte Entwicklungen genau zu überwachen und eine fortlaufende Bewertung des britischen Datenschutzrechtes durchzuführen. Dies betrifft insbesondere die Änderungen durch den Retained EU Law Act 2023, welche die neuen Befugnisse des britischen Staatssekretärs zur Änderung datenschutzrechtlicher Bestimmungen sowie mögliche Risiken bei internationalen Datenübermittlungen und der Unabhängigkeit der britischen Datenschutzaufsichtsbehörde beinhalten. Auch die Nutzung sogenannter Technical Capability Notices, welche die Unternehmen zur Entschlüsselung von Kommunikation zwingen könnten, sieht der Europäische Datenschutzausschuss kritisch.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit begrüßt die neuen Angemessenheitsbeschlüsse, weil diese zu Erleichterungen im Handel mit dem Vereinigten Königreich führen. Die Betroffenenrechte der EU-Bürgerinnen und EU-Bürger bleiben zudem gewahrt.

17. Die Beschlüsse des Europäischen Datenschutzausschusses

17.1 Leitlinien 03/2025 zum Zusammenspiel zwischen dem Digital Services Act und der Datenschutzgrundverordnung

Mit dem Digital Services Act[9] (DSA) gilt seit dem 17. Februar 2024 in der Europäische Union neben der Datenschutzgrundverordnung ein weiterer Digitalrechtsakt von grundlegender Bedeutung. Bei dem Digital Services Act handelt es sich um eine Verordnung, die eine Regulierung für Vermittlungsdienste, wie soziale Netzwerke, Online-Suchmaschinen oder Online-Plattformen, im Internet beinhaltet (vergleiche Artikel 2 Absatz 1 DSA). Er hat zum Ziel, insbesondere durch die Einführung von Sorgfaltspflichten für diese Vermittlungsdienste im digitalen Raum zu einem Schutz vor rechtswidrigen Inhalten, Desinformationen oder anderen gesellschaftlichen Risiken beizutragen. Gleichzeitig dient die Datenschutzgrundverordnung (DSGVO) dem Schutz der personenbezogenen Daten (vergleiche Artikel 1 Absatz 1 DSGVO). Seit Inkrafttreten des Digital Services Act zeigte sich zudem, wie wichtig es ist, genauer zu bestimmen, wie das Verhältnis der beiden Verordnungen zu einander ist, weil bei der Anwendung des Digital Services Act an vielen Stellen die Beurteilung von Verarbeitungen personenbezogener Daten eine Rolle spielt. Ausgangspunkt der genaueren Bestimmung dieses Verhältnisses ist dabei, dass der Digital Services Act die Datenschutzgrundverordnung unberührt lässt (Artikel 1 Absatz 4 Buchstabe f) DSA).

Der Europäische Datenschutzausschuss hat hierzu nun am 11. September 2025 eine Leitlinie zum Zusammenspiel des Digital Services Act mit der Datenschutzgrundverordnung unter dem Titel „Guidelines 3/2025 on the interplay between the DSA and the GDPR Version 1.1“ verabschiedet, die Grundlage einer öffentlichen Konsultation ist. Der Europäische Datenschutzausschuss ist die Organisationsform, in der die datenschutzrechtlichen Aufsichtsbehörden in der Europäischen Union gemeinsam handeln. Hierzu beschließt der Europäische Datenschutzausschuss unter anderem Leitlinien, Empfehlungen und bewährte Verfahren zur Datenschutzgrundverordnung und trifft verbindliche Beschlüsse in Einzelfällen.

Die Leitlinie betont zunächst, dass der Digital Services Act die Datenschutzgrundverordnung nicht als spezialgesetzliche Regelung verdränge. Die beiden Verordnungen seien so auszulegen, dass sie in einer aufeinander abgestimmten, kohärenten Art und Weise zur Anwendung kommen. Zum einen stellt der Europäische Datenschutzausschuss bei der Verarbeitung personenbezogener Daten klar, dass auf die Definition in Artikel 4 Nummer 2 DSGVO abzustellen sei. Gleichzeitig hebt er mehrere Bereiche hervor, in denen der Digital Services Act in engem Zusammenhang mit der Datenschutzgrundverordnung stehe.

[9] Verordnung (EU) 2022/2065 des Europäischen Parlamentes und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (ABl. L 277 vom 27. Oktober 2022, Seite 1; L 310 vom 1. Dezember 2022, Seite 17).

Ein zentraler Regelungsgegenstand des Digital Services Act, in dem es zur Verarbeitung personenbezogener Daten kommt und bei dem daher die Anforderungen der Datenschutzgrundverordnung zu beachten sind, sind die Meldemechanismen für illegale Inhalte: Plattformanbieter müssen dafür geeignete Verfahren einrichten, über die Nutzerinnen und Nutzer Verstöße einfach melden können. Da im Rahmen dieser Systeme regelmäßig personenbezogene Daten verarbeitet werden, müssen die Vorgaben der Datenschutzgrundverordnung, insbesondere zur Rechtmäßigkeit, Transparenz und Datensicherheit, beachtet werden. Ferner geht die Leitlinie – neben anderen Bereichen – auch darauf ein, wie im Bereich der Online-Werbung auf diversen Plattformen die Bestimmungen der Datenschutzgrundverordnung neben dem Digital Services Act zur Anwendung kommen. So ist die Verarbeitung besonders sensibler personenbezogener Daten, wie zum Beispiel Gesundheitsdaten, für Profiling-basierte Werbung nicht nur nach der Datenschutzgrundverordnung, sondern auch nach Artikel 26 Absatz 3 Digital Services Act untersagt.

Die Leitlinie macht deutlich, dass Datenschutz und digitale Regulierung untrennbar miteinander verflochten sind und nur im Zusammenspiel einen hohen Schutz für die Rechte der Bürgerinnen und Bürger gewährleisten können, wobei auch in dem Regelungsgebiet des Digital Services Actes der Datenschutzgrundverordnung ein weiter Anwendungsbereich verbleibt und bei einer aufeinander abgestimmten Auslegung beider Rechtsakte auch ein hohes Datenschutzniveau gewährleistet werden kann. Das Zusammenspiel der verschiedenen Digitalrechtsakte zueinander zu klären, stellt eine zentrale Aufgabe der Aufsichtsbehörden in den kommenden Jahren dar.

17.2 Leitlinien 02/2024 zu Artikel 48 Datenschutzgrundverordnung

Der Europäische Datenschutzausschuss hat am 5. Juni 2025 die Leitlinien zum Datentransfer an Drittstaatenbehörden nach Artikel 48 Datenschutzgrundverordnung (DSGVO) veröffentlicht. Nach Artikel 48 DSGVO dürfen Gerichtsurteile oder Behördenentscheidungen eines Drittlandes, durch die eine Datenübermittlung an den Drittstaat verlangt wird, anerkannt werden, wenn ein internationales Übereinkommen, wie beispielsweise ein Rechtshilfeabkommen, mit dem Drittstaat besteht. Dabei bleiben nach Artikel 48 DSGVO die Gründe für die Übermittlung der Daten, wie sie im 5. Kapitel der Datenschutzgrundverordnung geregelt sind, unberührt.

Nach der Leitlinie ist Artikel 48 DSGVO nicht so zu verstehen, dass Urteile und behördliche Entscheidungen eines Drittstaates grundsätzlich keine Grundlage für eine Datenübermittlung an Gerichte oder Behörden in Drittstaaten darstellen. Ein internationales Abkommen könnte demgegenüber auch als Rechtsgrundlage gemäß Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe c) DSGVO in Verbindung mit Absatz 3 DSGVO für den Datentransfer in Frage kommen. Denn auf der Grundlage eines Rechtshilfeabkommens kann das Ersuchen, ein Urteil

oder eine Verwaltungsentscheidung anzuerkennen oder zu vollstrecken, eine rechtliche Verpflichtung darstellen. Auch kommt als Rechtsgrundlage für die Datenübermittlung Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e) DSGVO in Betracht, wenn das nationale Recht in Verbindung mit Artikel 6 Absatz 3 DSGVO entsprechende öffentliche Zwecke enthält.

Nach dem sogenannten two-step-test müssen bei Datenübermittlung in einem Drittstaat nicht nur eine Rechtsgrundlage nach Artikel 6 DSGVO gegeben, sondern auch die Bedingungen nach Kapitel 5 Datenschutzgrundverordnung eingehalten sein. Das internationale Abkommen kann zudem in beiden Fällen gegebenenfalls auch ein geeignetes rechtlich bindendes und durchsetzbares Dokument im Sinne des Artikel 46 Absatz 2 Buchstabe a DSGVO darstellen, wenn in dem Abkommen hinreichende datenschutzrechtliche Garantien enthalten sind. In Betracht kommt neben den eben angesprochenen geeigneten Garantien gemäß Artikel 46 DSGVO oder einem Angemessenheitsbeschluss, der dem Drittland ein hinreichendes Datenschutzniveau attestiert, auch die ausnahmsweise rechtliche Zulässigkeit der Übermittlung von personenbezogenen Daten nach Artikel 49 DSGVO.

Der Europäische Datenschutzausschuss weist insofern darauf hin, dass es unter strengen Voraussetzungen auch ohne internationale Abkommen Möglichkeiten geben könne, personenbezogene Daten zu übermitteln. Hier würden alternative Rechtsgrundlagen oder Transfermechanismen wie Artikel 49 DSGVO in Betracht kommen. Artikel 49 DSGVO sei aber eng auszulegen und die Anwendung müsse eine Einzelfallentscheidung bleiben.

17.3 Pseudonymisierung im Urteil des Europäischen Gerichtshofes

Ein praxisrelevantes Urteil des Europäischen Gerichtshofes vom 4. September 2025 (Aktenzeichen C-413/23 P) bringt Klarstellungen unter anderem zu dem Begriff der personenbezogenen Daten und pseudonymisierten Daten. Es hebt ein Urteil des Gerichtes der Europäischen Union vom 26. April 2023 (Aktenzeichen T-557/20) auf, in dem eine Entscheidung des Europäischen Datenschutzbeauftragten für nichtig erklärt wurde. Das Urteil des Europäischen Gerichtshofes verdeutlicht, dass der Begriff der personenbezogenen Daten weit auszulegen ist, vor allem wenn persönliche Ansichten betroffen sind. Auf der anderen Seite hält der Europäische Gerichtshof fest, dass pseudonymisierte Daten nicht in jedem Fall und für jede Person personenbezogene Daten darstellen. Dies kann zum Beispiel nicht der Fall sein, wenn nach den Umständen des Einzelfalles eine andere Person als der oder die Verantwortliche tatsächlich an einer Identifizierung der betroffenen Person durch die Pseudonymisierung gehindert ist.

In dem Sachverhalt, der der Entscheidung des Europäischen Gerichtshofes zu Grunde lag, ging es um die Verarbeitung von Daten im Rahmen der Abwicklung eines Kreditinstitutes durch

den Einheitlichen Abwicklungsausschuss, die für die Abwicklung von Banken zuständige Behörde der Europäischen Bankenunion. Die Daten stammten von Anteilseignern und Gläubigern, die eine Entschädigung begehrten und im Rahmen des Abwicklungsprozesses von dem Einheitlichen Abwicklungsausschuss angehört wurden. Dieser veröffentlichte vor der Anhörung eine Datenschutzerklärung, in der er über die Verarbeitung personenbezogener Daten im Rahmen des Anhörungsverfahrens informierte. In der Datenschutzerklärung fanden sich aber keine Angaben dazu, dass personenbezogene Daten an einen Sachverständigen weitergegeben würden.

Im Einzelnen vollzog sich die Verarbeitung der personenbezogenen Daten wie folgt: Die Anteilseigner und Gläubiger wurden bei der Teilnahme an dem Anhörungsverfahren vom Einheitlichen Abwicklungsausschuss unter anderem dazu eingeladen, Stellungnahmen einzureichen. Ferner sollten sie sich registrieren. Bei dieser Registrierung musste man Identitäts- und Eigentumsnachweise vorlegen. Die Stellungnahmen wurden dann unter einem Code, der zufällig generiert wurde und aus 33 Ziffern bestand, an einen externen Gutachter für eine Bewertung, die aus abwicklungsrechtlichen Gründen erforderlich war, übermittelt. Dabei konnte aber lediglich der Einheitliche Abwicklungsausschuss die Stellungnahmen mit den personenbezogenen Daten, die während der Registrierung erhoben worden waren, zusammenführen.

Fünf Betroffene reichten daraufhin beim Europäischen Datenschutzbeauftragten Beschwerde ein. Sie kritisierten, dass in der Datenschutzerklärung des Einheitlichen Abwicklungsausschusses keine Hinweise zu finden gewesen seien, dass ihre Kommentare samt pseudonymisiertem Code, an Dritte, hier den externen Gutachter, weitergeleitet würden. Darin liege ein Verstoß gegen Artikel 15 Absatz 1 Buchstabe d) Datenschutzverordnung für Organe der Europäischen Union[10] , weil Betroffene bereits bei einer Datenerhebung über die Empfänger oder Empfängerinnen ihrer Daten informiert werden müssen. Nach Artikel 15 Absatz 1 Buchstabe d) Datenschutzverordnung für Organe der Europäischen Union müssen Verantwortliche, die bei einer betroffenen Person personenbezogene Daten erheben, dieser unter anderem die Empfängerinnen beziehungsweise Empfänger oder Kategorien von Empfängerinnen oder Empfängern der personenbezogenen Daten mitteilen. Die Vorschrift entspricht Artikel 13 Absatz 1 Buchstabe e) Datenschutzgrundverordnung (DSGVO). Der Europäische Datenschutzbeauftragte entschied, dass der Einheitliche Abwicklungsausschuss gegen Artikel 15 Absatz 1 Buchstabe d) Datenschutzverordnung für Organe der Europäischen Union und somit gegen das Auskunftsrecht der betroffenen Personen verstoßen habe, weil er die Betroffenen nicht über die Datenübertragung an den externen Gutachter informiert habe.

[10] Verordnung (EU) 2018/1725 des Europäischen Parlamentes und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstiger Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG.

Das Gericht der Europäischen Union ging jedoch nicht von personenbezogenen Daten im Sinne des Artikel 3 Nummer 1 Datenschutzverordnung für Organe der Europäischen Union, der Artikel 4 Nummer 1 DSGVO entspricht, aus und hob die Entscheidung des Europäischen Datenschutzbeauftragten auf, weil der Europäische Datenschutzbeauftragte allein daraus, dass es sich bei den eingereichten Stellungnahmen um Meinungen oder Sichtweisen gehandelt habe, gefolgert habe, dass die Informationen sich auf eine Person beziehe. Zudem bezögen sich, so das Gericht der Europäischen Union, die an den externen Gutachter übermittelten Informationen nicht auf eine identifizierbare Person. Es komme nämlich nicht darauf an, ob der Einheitliche Abwicklungsausschuss die Stellungnahmen einer Person wieder zuordnen könne, weil er über die Zuordnung der Codes weiterhin verfüge, sondern ob der externe Gutachter dies praktisch durchführen könne und das Recht für eine solche Zuordnung habe.

Der Europäische Datenschutzbeauftragte beantragte daraufhin, das Urteil aufzuheben.

Hinsichtlich der ersten Frage, ob sich Meinungen oder Stellungnahmen stets auf Personen bezögen und daher dieses Tatbestandsmerkmal personenbezogener Daten zu bejahen sei, hob der Europäische Gerichtshof hervor, dass persönliche Ansichten immer einen engen Bezug zu betroffenen Personen hätten. Das Gericht der Europäischen Union hatte demgegenüber gefordert, zusätzlich Inhalt, Zweck und Auswirkungen der übermittelten Stellungnahmen prüfen zu müssen, um erst den Personenbezug feststellen zu können. Dies wies der Europäische Gerichtshof zurück. Laut des Gerichthofes sind persönliche Ansichten immer ein Ausdruck individueller Gedanken. Diese Gedanken sind somit untrennbar mit der Person verknüpft, die sie äußert, und müssen als personenbezogene Daten gewertet werden.

In Bezug auf das Problem, ob es darauf ankomme, ob der externe Gutachter die personenbezogenen Informationen auch einer identifizierbaren Person zuordnen könne oder ob eine Zuordnung durch den Einheitlichen Abwicklungsausschuss genüge, betonte der Europäische Gerichtshof, dass die pseudonymisierten Daten nicht automatisch in jeder Konstellation einen Personenbezug aufwiesen. Ob eine Einordnung als personenbezogenes Datum möglich sei, hänge hauptsächlich davon ab, welche zusätzlichen Informationen einer oder einem Verantwortlichen beziehungsweise eine oder einem Dritten zur Verfügung stünden.

Darüber hinaus stellte das Gericht fest, dass Artikel 3 Nummer 1 Datenschutzverordnung für Organe der Europäischen Union, der Artikel 4 Absatz 1 Nummer 1 DSGVO entspricht, nicht regele, aus wessen Perspektive die Identifizierbarkeit beurteilt werden müsse. Dies bestimme sich nach den Umständen der Datenverarbeitung im Einzelfall. Für die Informationspflichten gemäß Artikel 15 Absatz 1 Buchstabe d) Datenschutzverordnung für Organe der Europäischen Union sei dabei auf die Perspektive des Verantwortlichen abzustellen, sodass den Einheitlichen Abwicklungsausschuss hier eine Informationspflicht getroffen habe, der er nicht nachgekommen sei.

Das Urteil macht zwei Dinge deutlich. Zum einen ist zukünftig die weite Auslegung des Begriffes personenbezogener Daten zu berücksichtigen, insbesondere wenn es um persönliche Äußerungen geht. Positiv ist ferner zu würdigen, dass den Verantwortlichen auch in der pseudonymisierten Weitergabe von Daten, die bei ihm einen Personenbezug aufweisen, weiterhin die Informationspflichten treffen. Hier müssen Verantwortliche gegebenenfalls ihre Datenschutzhinweise anpassen. Allerdings erkennt der Europäische Gerichtshof an, dass die Daten bei dem Empfänger oder der Empfängerin, sofern diesem oder dieser es nicht möglich ist, die Daten zuzuordnen, und dies auch nicht rechtlich zulässig wäre, die hierfür erforderlichen Informationen zu erlangen, keinen Personenbezug mehr aufweisen.

18. Die Entschließungen der Datenschutzkonferenzen im Jahr 2025

18.1 Eckpunkte für eine freiheitliche und grundrechtsorientierte digitale Zukunft

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 26. März 2025)

Eine Demokratie beweist ihre Stärke dann, wenn sie die Grundrechte der Bürgerinnen und Bürger auch angesichts großer Herausforderungen gewährleistet. Zu diesen Grundrechten zählt auch das Recht auf Datenschutz, das sich angesichts der fortschreitenden Digitalisierung zu einem zentralen Grundrecht entwickelt. Datenschutz wirkt nicht nur als informationelle Selbstbestimmung, sondern ist auch Basis für freie Meinungsäußerung und politische Partizipation. Deutschland kommt zudem innerhalb Europas daten- und digitalpolitisch eine Schlüsselrolle zu. Umso entscheidender ist es, dass die künftige Bundesregierung ein stimmiges daten- und digitalpolitisches Maßnahmenpaket vorlegt, welches die nachhaltige Digitalisierung in Europa voranbringt und menschenzentrierte Datennutzung sicherstellt. In diesem Sinne fordert die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK):

1. Die Gesetzgebungsprojekte zur Novellierung des Bundesdatenschutzgesetzes und zum Beschäftigtendatenschutz zu finalisieren.

Die bereits begonnenen Gesetzgebungsvorhaben müssen wieder aufgegriffen werden. Das schafft Rechtssicherheit für diejenigen, die in Wirtschaft und Verwaltung Verantwortung tragen, und sichert eine einheitliche Anwendung des Datenschutzrechtes in Deutschland. Die Novellierung des Bundesdatenschutzgesetzes drängt. Vor allem gilt dies für:

- Regelungen zum Scoringverfahren in Folge der Rechtsprechung des Europäischen Gerichtshofes
- eine zentrale Zuständigkeitsregelung bei innerstaatlichen, länderübergreifenden Sachverhalten (One-Stop-Shop)
- die Institutionalisierung der DSK mit einer Geschäftsstelle. Die DSK als gemeinsame Instanz der Datenschutzaufsichtsbehörden sichert eine effektive Datenschutzaufsicht. Sie bietet eine einheitliche Ansprechpartnerin für Wirtschaft und Verbände, fördert Synergieeffekte bei der Zusammenarbeit und baut Bürokratie ab. Auch das Zusammenwirken von Datenschutzaufsicht und anderen Aufsichtsbehörden, die Aspekte der Digitalisierung überwachen, wird unter Einbeziehung der DSK besser strukturiert. So wird der Aufbau klarer und nachhaltiger Kooperationsbedingungen der beteiligten Behörden erreicht.

Ein Beschäftigtendatenschutzgesetz sollte insbesondere das Unionsrecht konkretisieren durch Regelungen:

- zum Einsatz von algorithmischen Systemen
- zu den Grenzen der Verhaltens- und Leistungskontrolle
- zu Rahmenbedingungen der Einwilligung im Beschäftigtenverhältnis
- zu Datenverarbeitungen auf der Grundlage von Kollektivvereinbarungen
- zu Beweisverwertungsverboten
- zu Datenverarbeitungen im Bewerbungs- und Auswahlverfahren

2. Einen systematischen Grundrechtecheck bei der Fortentwicklung der modernen Sicherheitsarchitektur durchzuführen.

Angesichts eingriffsintensiver Techniken, wie Gesichtserkennung, biometrischer Fernerkennung, automatisierter Datenanalysen und Künstlicher Intelligenz, ist die Bundesregierung gefordert, zusätzliche Befugnisse der Sicherheitsbehörden grundrechtssensibel und verfassungskonform zu realisieren. Aufbauend auf der bereits begonnenen und fortzuführenden unabhängigen wissenschaftlichen Untersuchung der Sicherheitsgesetze von Bund und Ländern muss die Bundesregierung:

- den rechtsstaatlichen Rahmen für moderne, digitale Befugnisse setzen
- die Streubreite eingriffsintensiver Maßnahmen eindämmen
- den Grundrechtsschutz durch Verfahren und die Transparenz sicherstellen
- für Integrität und Qualität polizeilicher Daten Sorge tragen
- die Datenschutzaufsicht als integralen Bestandteil der Sicherheitsarchitektur garantieren

Die Bundesregierung muss angesichts der enormen technischen Möglichkeiten die Grundrechteverträglichkeit ihrer Gesetzesentwürfe systematisch überprüfen und dabei die Rechtsprechung des Bundesverfassungsgerichts beachten.

3. Sich in Europa dafür einzusetzen, dass EU-Digitalrechtsakte und Datenschutzgrundverordnung (DSGVO) besser aufeinander abgestimmt werden

Die Digitalrechtsakte der Europäischen Union[11] verfehlen bisher das Ziel einer effektiven Gesamtregelung der Datennutzung. Die Datenschutzgrundverordnung als grundlegende und technologieoffene allgemeine Regelung des Datenschutzrechtes gilt umfassend, ist aber an einigen Punkten mit den Digitalrechtsakten schwer vereinbar. Im Interesse von Rechtssicherheit und effektivem Grundrechtsschutz besteht Handlungsbedarf. Beispielsweise können die in der Datenschutzgrundverordnung garantierten Betroffenenrechte aufgrund der technischen Architektur in KI-Anwendungen nicht uneingeschränkt verwirklicht werden. Hier könnte und sollte ein gleichwertiger Schutz von Betroffenenrechten für die KI-Technologie als bereichsspezifisches Datenschutzrecht geregelt werden. Auch Synergien können zum Beispiel erreicht werden:

- bei der Regelung der Rechtsfolgen von Konformitätsbewertungen
- oder durch die Zusammenfassung von Meldepflichten (zum Beispiel NIS-2-Richtlinie und Datenschutzgrundverordnung)

Die Digitalrechtsakte verfolgen das legitime Ziel, den digitalen Binnenmarkt zu stärken und eine angemessene Datennutzung zu ermöglichen. Datennutzung und Datenschutz müssen dabei Hand in Hand gehen, deswegen bedarf es dringend insgesamt einer rechtlichen Fortentwicklung des europäischen Rechtsrahmens bei gleichwertigem Schutz aber besserer Harmonisierung der Rechtsakte untereinander.

4. Produktive Rahmenbedingungen für KI, Forschung und Innovation im Einklang mit dem Datenschutz gesetzgeberisch zu gestalten.

Forschung, Gesundheitsmanagement, Verkehrskonzepte, nutzerfreundliche Produktentwicklung, Effektivität der Verwaltung und viele nützliche, sinnvolle und für die Menschen gewinnbringende Vorhaben können entscheidend vorangebracht werden, wenn Forschende, Entwicklerinnen und Entwickler sowie Verantwortliche in Wirtschaft, Politik und Verwaltung auf eine gute Datengrundlage und den Einsatz künstlicher Intelligenz zurückgreifen können. Dabei müssen die Rechte derjenigen gewahrt bleiben, um deren Daten es geht. Die Förderung von Innovation muss daher mit den im Unionsrecht verankerten Werten menschenzentriert und vertrauenswürdig Hand in Hand gehen.

[11] Etwa Data Governance Act, Data Act, Artificial Intelligence Act, Digital Services Act, Digital Markets Act, European Health Data Space und andere.

Hierfür braucht es:

- Rechtsgrundlagen, die Rechtssicherheit schaffen, ob und unter welchen Bedingungen Daten für Forschung und das Training von KI-Modellen beziehungsweise KI-Systemen verwendet werden dürfen. Der zu schaffende Ausgleich zwischen öffentlichen oder wirtschaftlichen Interessen und den Grundrechten und Schutzansprüchen Einzelner im Hinblick auf personenbezogene Daten muss in den wesentlichen Grundzügen durch den Gesetzgeber festgelegt werden, indem die Öffnungsklauseln der Datenschutzgrundverordnung konstruktiv genutzt werden.

- Eine Aufsichtsstruktur, die unabhängig agiert und sich mit der Abwägung von Grundrechten auskennt.

- Experimentierräume in Form von behördlich kontrollierten Reallaboren, die die Erprobung innovativer Datennutzungen ausloten, ohne den Grundrechtsschutz Betroffener zu vernachlässigen. Ein solches Reallaborgesetz sollte den Rahmen zur Zusammenarbeit zwischen den an der Beaufsichtigung der Reallabore beteiligten Behörden und die Vernetzung zwischen Europa, Bund, Ländern und Aufsichtsbehörden beschreiben – vor allem, aber nicht nur im KI-Umfeld.

5. Die von der DSK erstellten Kriterien für Souveräne Clouds zu berücksichtigen und das Datenschutzcockpit zügig weiter auszubauen.

Eine bürgerfreundliche und datenschutzkonform digitalisierte Verwaltung ist Grundbedingung für einen modernen Staat und eine moderne Wirtschaft. Eine weitere Grundvoraussetzung ist digitale Souveränität. Dazu müssen IT-Lösungen auch die Einhaltung der datenschutzrechtlichen Pflichten effektiv, nachprüfbar und dauerhaft sicherstellen. In Bezug auf den Einsatz von Souveränen Clouds hat die DSK Kriterien formuliert, die erfüllt sein sollten oder müssen, um von einer „Souveränen Cloud“ sprechen zu können.[12]

Dazu zählen:

- Nachvollziehbarkeit durch Transparenz

- Datenhoheit und Kontrollierbarkeit

- Offenheit

- Vorhersehbarkeit und Verlässlichkeit

[12] Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023: Kriterien für Souveräne Clouds, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf.

- regelmäßige Prüfung der aufgestellten Kriterien

Die Fortentwicklung der Registermodernisierung setzt voraus, dass auch das Datenschutzcockpit zügig ausgebaut wird. Das Datenschutzcockpit ist ein notwendiges Transparenz- und Steuerungsinstrument für die einzelnen Bürgerinnen und Bürger, um die Kontrolle über Datenflüsse und -verarbeitungen in einer digitalisierten Verwaltung zu behalten.

18.2 Confidential Cloud Computing

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 16. Juni 2025)

Der Begriff „Confidential Computing“ bezeichnet nicht eine einzelne Technologie, sondern wird von verschiedenen Anbietern unterschiedlich belegt. So wird beispielsweise eine Verschlüsselung von Daten im Arbeitsspeicher oder aber auch eine reine Zugriffsbeschränkung auf reservierte Speicherbereiche als Confidential Computing bezeichnet. Unter dem Begriff „Confidential Cloud Computing” werden teilweise Technologien damit beworben, dass Daten sogar vor dem Cloud-Betreiber geheim gehalten werden können. Eine solche allgemeine Aussage trägt jedoch nicht der tatsächlichen Komplexität der eingesetzten Technologie Rechnung. Um solche Werbeversprechen kritisch einzuordnen, werden im Nachfolgenden wichtige zu berücksichtigende Punkte angesprochen.

Angreifermodell

Zuerst sollte festgehalten werden, dass die zugrundeliegenden Technologien ursprünglich insbesondere dem Szenario entstammen, in welchem sich mehrere Nutzende die gleiche Hardware bei einem Cloud-Betreiber teilen. In einer solchen Situation soll sichergestellt werden, dass die eigenen Daten vor den Daten anderer Nutzender geheim gehalten werden können, möglicherweise sogar dann, wenn sich ein anderer Nutzender Administrationsrechte verschafft und auf Teile der Cloud-Betriebsinfrastruktur zugreift.

Wenn jedoch die Daten nicht mehr nur vor anderen Nutzenden, sondern vor dem Cloud-Betreiber geheim gehalten werden sollen, erfordert dies ein komplett anderes und viel stärkeres Angreifermodell. Denn der Betreiber hat physikalischen Zugang zu den Systemen und umfangreiche Möglichkeiten, die Hardware und Software zu manipulieren. Für eine valide Bewertung der Wirksamkeit von Maßnahmen ist ein differenziertes Angreifermodell erforderlich, das auch unterschiedliche Gruppen von Mitarbeitenden des Betreibers und seiner Auftragnehmer berücksichtigt.

Eine Verbesserung der Sicherheit kann sich dadurch ergeben, dass (zum Beispiel mittels Verschlüsselung) Zugriffsmöglichkeiten innerhalb der Organisation des Betreibers (und gegebenenfalls seiner Auftragsverarbeiter) eingeschränkt werden. Auch vor einer missbräuchlichen Nutzung (zum Beispiel Start geklonter virtueller Maschinen oder Container) oder Manipulation gibt es einen gewissen Schutz.

Solche Maßnahmen gehören aber nicht im engeren Sinne zum „Confidential Computing“: Sie ändern nichts an der Tatsache, dass der Betreiber grundsätzlich Zugriff auf die Daten hat beziehungsweise sich verschaffen kann. Die teilweise anzutreffende Behauptung, dass die Kontrolle über die Datenverarbeitung vollständig auf den Nutzenden übergehe, ist nicht haltbar. So ist es beispielsweise offensichtlich, dass die Kontrolle über die Verfügbarkeit der Datenverarbeitung auch beim Cloud-Betreiber liegt. Auch ist es offensichtlich nicht möglich, jede unrechtmäßige Datenverarbeitung im Cloud-Kontext zu verhindern, beispielsweise eine unrechtmäßige Löschung.

Schlüsselmanagement

Eine besondere Bedeutung kommt dem eingesetzten Schlüsselmanagement zu. Tatsächliche Geheimhaltung vor dem Cloud-Betreiber (als Organisation) ist nur gewährleistet, wenn die Daten zu jedem Zeitpunkt so verschlüsselt sind, dass der Cloud-Betreiber den zur Entschlüsselung notwendigen Schlüssel nicht in Erfahrung bringen oder nutzen kann. Vor dem Hintergrund des oben angesprochenen sehr starken Angreifermodelles eines „bösartigen Cloud-Betreibers“ müssen hierbei auch Analysen und Manipulationen von Hardware und Software berücksichtigt werden. Das bedeutet auch, dass der Cloud-Betreiber nachweisen muss, dass er zu keinem Zeitpunkt die Möglichkeit hat, die Verschlüsselung zu manipulieren (zum Beispiel durch Machine-in-the-Middle-Angriffe oder den Austausch eines Nutzenden-Schlüssels durch einen selbst gewählten Schlüssel).

Nicht in allen Fällen ist für die Nutzenden klar überprüfbar, ob Confidential Computing überhaupt eingesetzt wird. Zwar ist es je nach Technologie möglich, dass über auf der Hardware hinterlegte Zertifikate attestiert wird, dass eine Operation in einer vertraulichen Umgebung ausgeführt wird. Um diese Attestierung aber an die Nutzenden durchreichen zu können und somit überprüfbar zu machen, muss die jeweilige Anwendung in der Regel speziell dafür implementiert werden.

Ein besonderes Augenmerk sollte hier auf die Übergänge zwischen den verschiedenen „Verschlüsselungsdomänen“ gelegt werden, etwa der Übergang von „data-at-rest“ zu „data-in-use“. Wenn bei solchen Übergängen ein Wechsel der eingesetzten Schlüssel vorgenommen wird und zu diesem Zweck eine kurzzeitige Entschlüsselung der Daten stattfindet, liegen die Daten möglicherweise kurzzeitig in unverschlüsselter Form vor.

Um die Aussagen der Cloud-Betreiber sowie der Hersteller der eingesetzten Hard- und Software (zum Beispiel Hersteller von Chips, Firmware, Virtualisierungssoftware etc.) einordnen zu können, müssen Einsatzszenarien transparent sein. Ebenso müssen die der Sicherheitsanalyse zugrundeliegenden Annahmen offen kommuniziert werden. Eine typische Annahme ist, dass es keine physikalischen Angriffe (zum Beispiel Seitenkanalattacken) gibt. Unter dieser Annahme kann diese Technik einen hohen Mehrwehrt an Sicherheit und Datenschutz bieten. Ist hingegen die Annahme nicht zutreffend (etwa, weil der Cloud-Betreiber einem Dritten physikalischen Zugang zur Hardware ermöglichen oder Schlüssel beziehungsweise Zertifikate auf Hardware herausgeben oder austauschen muss) oder vertraut man Zusagen von Herstellern oder Betreibern nicht, so hat diese Technik nicht den versprochenen Effekt.

Als Fazit kann „Confidential Cloud Computing“ das allgemeine Sicherheitsniveau erhöhen und typischerweise einen wertvollen Schutz gegen andere Nutzende auf der gleichen Hardware und gegen einzelne Innentäter bieten – letztlich eine weitere Schicht eines „defense-in-depth“-Ansatzes. Der Einsatz sollte daher empfohlen werden, auch wenn nicht alle Datenschutzprobleme so einfach gelöst werden, wie es teilweise beworben wird: Absolute Vertraulichkeit ist nicht möglich und grundsätzlich ist davon auszugehen, dass ein Cloud-Betreiber Zugriffsmöglichkeiten auf die zu schützenden Daten besitzt. Für eindeutig formulierte Angreifermodelle können jedoch konkretere Aussagen getroffen werden. Die Aussagen, mit denen diese Technologie beworben wird, sind daher im Hinblick auf das differenzierte Angreifermodell kritisch zu hinterfragen und die Schlussfolgerungen und die sich aus dem Angebot ergebenden beziehungsweise zusätzlich zu ergreifenden Maßnahmen aus Gründen der Nachweis- und Rechenschaftspflicht nachvollziehbar zu dokumentieren.

18.3 Ohne Sicherheit keine Freiheit – Ohne Freiheit keine Sicherheit

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 16. Juni 2025)

In der aktuellen Diskussion um die Novellierung verschiedener Sicherheitsgesetze betont die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), dass ein starker Datenschutz kein Selbstzweck, sondern ein wesentliches Element des Rechtsstaats und die Voraussetzung für Sicherheit und Freiheit ist.

Grundrechte sind Errungenschaften moderner Demokratien und sichern Wert und Würde der Person und die Teilhabe der Bürgerinnen und Bürger am Gemeinwesen, zum Beispiel bei der Teilnahme an Versammlungen, bei öffentlichen Meinungsäußerungen oder bei Wahlen. Dazu gehört auch die freie Entfaltung der Persönlichkeit in der verfassungsrechtlich anerkannten Ausprägung des Rechts auf informationelle Selbstbestimmung.

Freiheit ist eine wichtige Voraussetzung für eine Demokratie. Ein Leben in Freiheit setzt zugleich voraus, dass die Sicherheit der Bürgerinnen und Bürger gewährleistet ist. Zur Sicherheit gehört wiederum auch, dass sich die Menschen im Land darauf verlassen können, dass der Staat und seine Institutionen ihre Rechte und Freiheiten achten, sich an verfassungskonforme Gesetze und gegebene Garantien halten.

Auf der Welt lässt sich an vielen Stellen beobachten, wie freiheitliche Demokratien in Bedrängnis geraten. In nichtdemokratischen Systemen werden Eingriffsbefugnisse der Sicherheitsbehörden zur Einschüchterung von Bürgerinnen und Bürgern genutzt, sodass letztlich auch die bürgerliche Teilhabe am staatlichen Gemeinwesen ausgehöhlt wird. Das Datenschutzrecht spielt insofern eine wichtige Rolle, da es staatliche Datenverarbeitungen rechtsstaatlich einhegt. Datenschutz ist daher keine bloße Formalie und kein schmückendes Beiwerk.

Daher appelliert die DSK, in der politischen Diskussion Datenschutz und Sicherheit nicht gegeneinander auszuspielen. Zwar stehen sicherheitspolitische Erfordernisse und das Recht auf informationelle Selbstbestimmung in einem gewissen Spannungsverhältnis, allerdings ist dieses nicht unlösbar und kann in verhältnismäßiger Art und Weise aufgelöst werden. Das Datenschutzrecht zielt nicht darauf ab, Täterinnen und Täter oder Gefährderinnen und Gefährder vor Strafverfolgung oder Gefahrenabwehrmaßnahmen zu bewahren. Vielmehr schützt das Datenschutzrecht die Bürgerinnen und Bürger davor, dass ungerechtfertigt in ihre Freiheitsrechte eingegriffen wird.

Datenschutz und Datenqualität in der polizeilichen Praxis

Die Gewährleistung von Datenqualität, klaren Verantwortlichkeiten, effizienten Verfahrensstrukturen sowie digitaler Souveränität sind Belange, die für die Gewährleistung von Sicherheit ebenso wichtig sind wie für den Datenschutz. Die Sicherheitsbehörden wollen Straftaten verfolgen und nicht Personen, die dafür keinen Anlass gegeben haben. Die Sicherheitsbehörden möchten qualitativ hochwertige und sorgfältig austarierte Datenbestände, weil sie rechtsstaatlich arbeiten und nur mit qualitativ hochwertigen Systemen gute Ergebnisse erzielen können. Nichts Anderes wollen die Datenschutzaufsichtsbehörden. Deren Arbeit ist insofern in weiten Teilen eine wesentliche Instanz der Qualitätssicherung. In der Praxis der Sicherheitsbehörden sehen die Datenschutzaufsichtsbehörden eine breite Akzeptanz datenschutzrechtlicher Vorgaben.

Datenschutz steht notwendigem Fortschritt polizeilicher Datenverarbeitung nicht entgegen

Es ist selbstverständlich, dass Sicherheitsbehörden stetig prüfen, an welcher Stelle sie ihre Arbeit weiter verbessern und modernisieren können. Ein Beispiel ist das polizeiliche Projekt

P20 zur Harmonisierung der polizeilichen IT-Struktur und -Architektur, das die Datenschutzaufsichtsbehörden lösungsorientiert und konstruktiv beraten. Hierbei ist es aber wichtig, zunächst den genauen fachlichen Bedarf zu analysieren und abzustecken, welche verhältnismäßigen Lösungen möglich sind. Die DSK hält es hingegen für das falsche Signal, auf Herausforderungen für die innere Sicherheit mit dem Ruf nach weiteren Einschnitten in Grundrechte zu reagieren.

Anstelle voreiliger Gesetzgebungsaktivitäten hält es die DSK für dringend notwendig, die vorhandenen – in den vergangenen Jahren stetig erweiterten – Eingriffsbefugnisse der Sicherheitsbehörden, ihre Anwendung in der Praxis und ihre Wirksamkeit weiter umfassend zu evaluieren. Vorliegende wissenschaftliche Arbeiten zu einer Überwachungsgesamtrechnung, insbesondere die vom Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht im Auftrag des Bundes durchgeführte Studie, bieten hierfür eine geeignete Grundlage.

Die unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder werden künftige Novellierungen der Sicherheitsgesetze eng begleiten und sich weiter dafür einsetzen, dass neue Befugnisse für Sicherheitsbehörden den grundrechtlichen, vom Bundesverfassungsgericht ausgeformten, Maßstäben entsprechen.

18.4 Automatisierte Datenanalyse durch Polizeibehörden verfassungskonform gestalten!

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 17. September 2025)

Die aktuelle politische Diskussion über den Einsatz von Verfahren zur automatisierten Datenanalyse durch die Polizei betrifft rechtliche und technische Anforderungen an polizeiliches Handeln, die auch unter dem Gesichtspunkt der digitalen Souveränität betrachtet werden sollten. Die bisher bekannten Analyseverfahren, die die Polizei in einzelnen Ländern für die Gefahrenabwehr einsetzt, können jede und jeden betreffen. Nicht nur Straftäterinnen und -täter, sondern etwa auch Geschädigte, Zeuginnen und Zeugen, Sachverständige oder Personen, die den Polizeinotruf genutzt haben, können in eine solche Analyse einbezogen sein: Allein in Bayern bezieht sich das dortige Analyseverfahren auf circa 39 Millionen Personendatensätze. Es ist verfassungsrechtlich selbstverständlich, dass die Polizei nur bei sehr schwerwiegenden Rechtsgutverletzungen und unter ganz engen Verfahrensbestimmungen solche einschneidenden Analysemittel einsetzen darf. Vor diesem Hintergrund fordert die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) die Einhaltung grundlegender, teils auf der Rechtsprechung des Bundesverfassungsgerichts beruhender, Anforderungen.

1. Kein Einsatz von komplexen Datenanalyseverfahren ohne spezifische Rechtsgrundlage

Die DSK betont, dass die allgemeinen Vorschriften im Polizeirecht und in der Strafprozessordnung den Besonderheiten komplexer Analysemethoden nicht ausreichend Rechnung tragen, die mit intensiven Eingriffen in die Grundrechte der betroffenen Personen verbunden sein können. Dies gilt insbesondere für Analysen von umfassenden Datenbeständen, die – wie eingangs beschrieben – Daten über Personen enthalten, die durch ihr Verhalten keinen Anlass für polizeiliche Ermittlungen gegeben haben. Durch Datenanalysen kann neues Wissen erzeugt werden, zum Beispiel können Zusammenhänge zwischen Personen, Institutionen, Organisationen oder Objekten hergestellt werden. Daraus entsteht für die betroffenen Personen das Risiko, zum Gegenstand polizeilicher Ermittlungen oder Maßnahmen zu werden. Dies greift in die Grundrechte aller hiervon betroffenen Personen ein; für die Personen, die selbst keinen Anlass hierfür gegeben haben, wiegt dieser Eingriff besonders schwer. Für solche komplexen Analysen bedarf es eigener Rechtsgrundlagen, die nach dem Gewicht der unterschiedlichen Grundrechtseingriffe bei der Erhebung und Weiterverarbeitung der Daten differenzieren müssen. Wird ihr Einsatz fachlich als erforderlich angesehen, ist der Gesetzgeber in der Pflicht, die wesentlichen Grundlagen selbst durch spezifische gesetzliche Vorschriften vorzugeben, um insbesondere Art und Umfang der Daten und die Verarbeitungsmethoden zu begrenzen. Dies umfasst grundlegende Anforderungen an die notwendigen technischen Anwendungen und Infrastrukturen.

2. Die gesetzliche Grundlage muss verfassungsrechtlichen Maßstäben genügen

Das Bundesverfassungsgericht hat sich im Urteil vom 16. Februar 2023 (Aktenzeichen 1 BvR 1547/19 und 1 BvR 2634/20) umfassend mit dem behördlichen Einsatz von automatisierten Datenanalysen befasst und hierfür die verfassungsrechtlichen Weichen gestellt. Das Bundesverfassungsgericht hat entschieden, dass das Gewicht des mit der Datenanalyse verbundenen Grundrechtseingriffes insbesondere durch Art und Umfang der zu verarbeitenden Daten und die zugelassene Methode der Datenanalyse bestimmt wird.

Ein besonderes Eingriffsgewicht aufgrund von Art und Umfang der Daten ist regelmäßig gegeben, wenn viele Daten zu Personen in die Datenanalyse eingehen, die selbst keinen Anlass für polizeiliche Maßnahmen gegeben haben oder wenn die Daten verschiedenster Systeme trotz ursprünglich unterschiedlicher Erhebungs- und Verarbeitungszwecke in eine Gesamtauswertung einbezogen werden (Zweckbindung und Zweckänderung). Das trifft beispielsweise auf Datenbestände aus der Vorgangsbearbeitung und aus Maßnahmen mit großer Streubreite, wie Funkzellenabfragen, zu. Funkzellenabfragen betreffen alle Personen, die in der Funkzelle mit ihrem Mobilgerät eingebucht sind. Datenbestände insbesondere aus Vorgängen der Strafverfolgung enthalten regelmäßig auch Daten von Geschädigten sowie Zeuginnen und Zeugen.

Die herangezogenen Datenbestände müssen für den Zweck der konkreten Datenanalyse geeignet sein. Den Verhältnismäßigkeitsanforderungen genügt eine Maßnahme der Datenverarbeitung grundsätzlich nur, wenn die einzubeziehenden Daten auf solche beschränkt werden, die für den jeweiligen Zweck der Maßnahme Bedeutung haben können.

Besonderes Eingriffsgewicht aufgrund der Methode der Datenanalyse können insbesondere die Verwendung lernfähiger Systeme – Künstliche Intelligenz („KI“) –, aber auch komplexe Formen des Datenabgleiches mit nicht lernfähigen Systemen haben. Die DSK sieht ihre Forderungen aus ihrer Entschließung vom 3. April 2019 „Hambacher Erklärung zur Künstlichen Intelligenz“ in dem Urteil bestätigt.

Ermöglicht das Verfahren nach den vom Bundesverfassungsgericht benannten Kriterien schwerwiegende Grundrechtseingriffe, ist ein Einsatz nur zum Schutz gewichtiger Rechtsgüter – wie etwa Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes – und unter strenger Begrenzung des Anlasses für die Maßnahme zulässig. Außerdem sind Transparenz und individueller Rechtsschutz für die betroffenen Personen und eine aufsichtliche Kontrolle gesetzlich vorzusehen.

3. Die digitale Souveränität muss bei der Auswahl von Verfahren gewährleistet werden

Sollen für die Analysen Systeme von Fremdanbietern eingesetzt werden, kommen nicht nur die gesetzlichen Anforderungen an die Datensicherheit gegenüber dem Anbieter zum Tragen, sondern es ist auch sicherzustellen, dass die digitale Souveränität des Staates gewahrt wird. Ganz besonders bei polizeilichen Datenbeständen hat der Staat gegenüber seinen Bürgerinnen und Bürgern eine Schutzpflicht, dass deren Daten nicht ohne vorherige Prüfung in Drittstaaten weiterverwendet werden können, die hinter dem europäischen Rechtsstaatsniveau zurückbleiben. Die DSK hat zur Gewährleistung der digitalen Souveränität bei Cloud-Lösungen Kriterien erarbeitet, die sinngemäß auch auf Datenanalyseverfahren für die Polizei übertragbar sind (Kriterien für Souveräne Clouds – Positionspapier der DSK vom 11. Mai 2023). Zu diesen Anforderungen gehört der Ausschluss von Zugriffen aus oder Datentransfers in Drittstaaten, deren Rechtsordnung nicht mit dem europäischen Recht vereinbar ist. Darüber hinaus verlangt die digitale Souveränität die Nachvollziehbarkeit und die Beherrschbarkeit der Datenverarbeitung, auch im Wege außergerichtlicher oder gerichtlicher Rechtsdurchsetzung, und die langfristige Vorhersehbarkeit und Verlässlichkeit des Angebotes. Diese Ziele können in aller Regel zuverlässig nur durch den Einsatz von Systemen erreicht werden, deren Anbieter ihren Sitz im Europäischen Wirtschaftsraum (EWR) haben.

Zur Wahrung der digitalen Souveränität durch Unterbindung von Abhängigkeiten ist zudem sicherzustellen, dass die eingesetzten Systeme hinreichend offen sind, um nötigenfalls einen Wechsel auf ein geeigneteres System zu ermöglichen.

4. Projekt P20 als Chance für den Datenschutz nutzen

Mit dem IT-Großprojekt „Polizei 20/20“ (P 20) wird bereits seit längerem eine gemeinsame IT-Infrastruktur der Polizeibehörden von Bund und Ländern vorbereitet. In diesem Projekt besteht die Möglichkeit, datenschutzkonforme Auswerte- und Analysetools zu entwickeln, gegebenenfalls auf Basis von transparenten und kontrollierbaren Open Source-Produkten. Auf dem Markt angebotene umfassende Analysetools können nach hiesiger Einschätzung nicht ohne erheblichen Aufwand die im Projekt zu realisierenden Anforderungen an einen verfassungsgemäßen Austausch von Daten zwischen Bund und Ländern erfüllen.

Die Datenschutzkonferenz bietet weiterhin ihre konstruktive Beratung an, um im Rahmen des Projektes P 20 verfassungskonforme und praxistaugliche Lösungen der Datennutzung für die Polizeien zügig auf den Weg zu bringen. Dies gilt auch in Bezug auf etwaige Analysetools.

18.5 Verbesserung des Datenschutzes von Kindern in der Datenschutzgrundverordnung

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 20. November 2025)

1. Besondere Schutzbedürftigkeit von Kindern

Kinder unterliegen einer besonderen strukturell bedingten Gefährdungslage: Sie verstehen je nach Reifegrad die meist langfristigen Nachteile der Verarbeitung ihrer personenbezogenen Daten noch unzureichend, sind aber für die meist kurzfristigen positiven Effekte der Nutzung von datenverarbeitenden Systemen und Diensten sehr offen und für Verführungen zu ihrer Nutzung leicht zugänglich. Wissen über Handlungsfolgen und -möglichkeiten müssen sich bei Kindern erst nach und nach herausbilden und festigen. Ihnen ist oft nicht klar, dass aus den Daten, die sie preisgeben und die durch die Beobachtung ihres Verhaltens entstehen, neue Daten über sie generiert werden, die ihr Weltverständnis bestimmen, ihre sozialen Beziehungen beeinflussen, ihr Selbstbild prägen und Vorhersagen über ihr Verhalten ermöglichen. Kinder können abhängig von ihrem Reifegrad die Risiken der Verarbeitung ihrer Daten weniger gut vermeiden und sich gegen Eingriffe in ihre Grundrechte weniger gut wehren als Erwachsene dies können. Schließlich ist zu berücksichtigen, dass Kinder in der Regel ihre eigenen Rechte als betroffene Person nicht kennen. Selbst wenn sie ihnen bekannt wären, sind sie meist nicht in der Lage, sie wahrzunehmen. Aus diesen Gründen haben Kinder einen besonderen Bedarf an Schutz und Fürsorge im digitalen Raum und insgesamt bezüglich der Verarbeitung ihrer Daten. Dies ist aufgrund von Artikel 24 der EU-Grundrechte-Charta und der UN-Kinderrechtskonvention geboten.

2. Datenschutz von Kindern in der Datenschutzgrundverordnung

Diese besondere Schutz- und Fürsorgepflicht des Gesetzgebers berücksichtigt auch die Datenschutzgrundverordnung in vielen Zusammenhängen – allerdings nicht in allen notwendigen Aspekten. Nach Erwägungsgrund 38 Satz 1 Datenschutzgrundverordnung (DSGVO) verdienen Kinder „bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind“. Unter „Kind“ versteht das Unionsrecht entsprechend Artikel 1 der UN-Kinderrechtskonvention jede Person, die das 18. Lebensjahr noch nicht erreicht hat.

Die besondere Schutzbedürftigkeit von Kindern berücksichtigt die Datenschutzgrundverordnung in sechs Regelungen für unterschiedliche datenschutzrechtliche Zusammenhänge:

- Nach Artikel 8 Absatz 1 Satz 1 DSGVO gilt die Einwilligung eines Kindes bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, als rechtmäßig, wenn das Kind das 16. Lebensjahr vollendet hat. Nach Artikel 8 Absatz 1 Unterabsatz 2 DSGVO dürfen Mitgliedstaaten diese Grenze auf das 13. vollendete Lebensjahr senken. Von der Öffnungsklausel des Artikel 8 Absatz 1 Unterabsatz 2 DSGVO hat die Mehrzahl der Mitgliedstaaten Gebrauch gemacht und diese Grenze durch gesetzliche Regelung gesenkt. Neun haben die Altersgrenze auf 13 Jahre festgesetzt, sechs auf 14 Jahre, vier auf 15 Jahre und neun Staaten haben die Altersgrenze der DSGVO beibehalten.

- Nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f) DSGVO muss eine Interessenabwägung die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person in besonderer Weise berücksichtigen, „wenn es sich bei der betroffenen Person um ein Kind handelt“.

- Nach Artikel 12 Absatz 1 Satz 1 DSGVO sind Informationen nach Artikel 13 und 14 DSGVO sowie Mitteilungen nach Artikel 15 DSGVO „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten“.

- Eine Löschung personenbezogener Daten hat nach Artikel 17 Absatz 1 Buchstabe f) DSGVO zu erfolgen, wenn die Daten von Kindern aufgrund einer Einwilligung nach Artikel 8 Absatz 1 DSGVO erhoben worden sind.

- Nach Artikel 40 Absatz 2 Buchstabe g) DSGVO können Verbände in Verhaltensregeln auch „Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist,“ regeln.

- Nach Artikel 57 Absatz 1 Buchstabe b) DSGVO ist es eine von vielen Aufgaben der Aufsichtsbehörden, „die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung (zu) sensibilisieren und sie darüber auf(zu)klären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder."

3. Ergänzungsbedürftigkeit der Datenschutzgrundverordnung

Das sind allerdings nicht alle Situationen, in den der besondere Schutz von Kindern erforderlich ist oder ihre besonderen Interessen zu berücksichtigen sind. In den anderen Regelungen differenziert die Datenschutzgrundverordnung nicht explizit zwischen Kindern und Erwachsenen. Für sie gelten grundsätzlich die gleichen Erlaubnistatbestände und die gleichen Verarbeitungsgrundsätze. Sie haben die gleichen Rechte wie Erwachsene. Die Verantwortlichen haben ihnen gegenüber grundsätzlich die gleichen Verpflichtungen und können ihre Daten unter den gleichen Voraussetzungen in Staaten außerhalb des Geltungsbereiches der Datenschutzgrundverordnung übermitteln. Jedoch gebieten Artikel 1 Absatz 2 DSGVO in Verbindung mit Artikel 24 der EU-Grundrechte-Charta und der UN-Kinderrechtskonvention sowie Erwägungsgrund 38 die besondere Schutzbedürftigkeit von Kindern bei ihrer Anwendung besonders zu berücksichtigen. In diesen Fällen bestimmt die Datenschutzgrundverordnung jedoch nicht, unter welchen Bedingungen welche Rechtsfolgen gelten sollen. Unter anderem wird daher diese Pflicht zur Berücksichtigung von den für die Datenverarbeitung Verantwortlichen in der Praxis oft nicht erkannt oder erfüllt.

Die Datenschutzgrundverordnung schützt Kinder in einer ihrer Schutzbedürftigkeit entsprechenden Weise ausdrücklich bisher nur punktuell. Hinter den wenigen Regelungen ist kein Gesamtkonzept erkennbar, das den Verantwortlichen klare Regelungen an die Hand gibt, in welchen Situationen Kinderrechte mit welchen Rechtsfolgen berücksichtigt werden müssen. Ein Konzept zum effektiven Schutz von Kindern sollte alle wesentlichen Situationen legislativ hervorheben, in denen Kinder besonderen Risiken ausgesetzt sind und in denen ihre Möglichkeiten, Risiken zu erkennen, zu bewerten und sich gegen sie zu schützen, eingeschränkt sind. Dabei sind auch die in der Praxis beschränkten Möglichkeiten ihrer Erziehungsberechtigten, sie zu schützen, zu berücksichtigen. Für diese Situationen sind spezifische datenschutzrechtliche Regelungen erforderlich.

4. Vorschläge zur Ergänzung der Datenschutzgrundverordnung

Daher sollte die Datenschutzgrundverordnung um weitere spezifische Regelungen zum Schutz von Kindern dort ergänzt werden, wo besondere Gefahren bestehen, dass die für die Verarbeitung im Einzelfall Verantwortlichen diese besondere Schutzbedürftigkeit mit den gebotenen Folgen außer Acht lassen könnten. Der Wortlaut der Verordnung sollte zumindest in folgenden Vorschriften den besonderen Aspekt des Kindeschutzes zusätzlich und ausdrücklich berücksichtigen:

4.1 Vereinbarkeit eines neuen Verarbeitungszwecks (Artikel 6 Absatz 4 DSGVO)

Bei der Prüfung der Vereinbarkeit eines neuen Verarbeitungszwecks mit dem bisherigen Verarbeitungszweck nach Artikel 6 Absatz 4 DSGVO muss der Schutz von Kinderrechten ebenso ein hervorgehobenes Gewicht haben, wie bei der Ersterhebung. Wenn die Daten eines Kindes für einen anderen Zweck verwendet werden sollen, sollte die Feststellung der Vereinbarkeit einer Zweckänderung mit dem ursprünglichen Zweck restriktiver erfolgen als bei Daten von Erwachsenen. Der Wortlaut des Artikel 6 Absatz 4 Unterabsatz 1 Buchstabe d) DSGVO ist wie folgt zu ergänzen (kursiv):

> „d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen, *insbesondere wenn es sich um die personenbezogenen Daten eines Kindes handelt*;“

4.2 Keine Einwilligung in Profiling und Werbezwecke (Artikel 8 DSGVO)

In den Normtext des Artikel 8 DSGVO sollte die Wertung des Erwägungsgrundes 38 Satz 2 DSGVO ausdrücklich übernommen werden: „Ein solch besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen.“ Dadurch würde die Regelung des Artikel 28 Absatz 2 Digital Services Act sinnvoll ergänzt, der das Ausspielen personalisierter Werbung an Kinder untersagt. Der Unionsgesetzgeber sollte in Artikel 8 DSGVO festlegen, dass die Einwilligung von Kindern in die Verwendung personenbezogener Daten für Werbezwecke oder Persönlichkeits- oder Nutzerprofile unzulässig ist. Ein solches Verbot würde die Werbung für Spiele und Spielsachen nicht ausschließen, sondern nur die Nutzung von Persönlichkeits- oder Nutzerprofilen und andere Sammlungen von Kinderdaten für Werbezwecke. In Artikel 8 Absatz 1 DSGVO sollte nach Satz 1 folgender Satz (kursiv) eingefügt werden. Die bisherigen Sätze 2 und 3 werden 3 und 4:

> *„Die Verarbeitung personenbezogener Daten eines Kindes für Werbezwecke und für die Erstellung von Persönlichkeits- und Nutzerprofilen ist nicht zulässig.“*

4.3 Keine Einwilligung nach Artikel 9 Absatz 2 Buchstabe a) DSGVO

Von der Ausnahme des Verbots der Verarbeitung besonderer Kategorien von personenbezogenen Daten bei einer Einwilligung nach Artikel 9 Absatz 2 Buchstabe a) DSGVO sollte die Einwilligung eines Kindes grundsätzlich ausgenommen werden. Etwas anderes soll nur dann gelten, wenn das Kind die Reife besitzt, die Auswirkungen seiner Einwilligung zu überschauen, und die Verarbeitung dem Wohl des Kindes nicht widerspricht. Im Übrigen bliebe trotz des

grundsätzlichen Verbotes eine Einwilligung oder Zustimmung durch einen Träger der elterlichen Verantwortung weiterhin möglich. Hierzu wird folgende Ergänzung (kursiv) vorgeschlagen:

> „a) Die *erwachsene* ~~betroffene~~ Person hat *für sich oder als Träger der elterlichen Gewalt für ein Kind* in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt oder *ein Kind hat im Rahmen der für die Entscheidung erforderlichen Reife in eine dem Kindeswohl eindeutig nicht widersprechende Verarbeitung eingewilligt,* es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,“

4.4 Datenverarbeitung für Präventions- und Beratungsdienste sowie ärztliche Untersuchungen und Heileingriffe

Die Zielsetzung des Erwägungsgrundes 38 Satz 3 DSGVO, dass „die Einwilligung des Trägers der elterlichen Verantwortung (…) im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein“ sollte, hat im Text der Verordnung keinen Ansatzpunkt gefunden. Ein Kind sollte in psychischen Zwangslagen zum Beispiel eine Sucht- oder Schwangerschaftsberatung in Anspruch nehmen können, ohne befürchten zu müssen, dass die Eltern davon erfahren. Die gleiche Möglichkeit sollte bestehen, wenn das Kind eine ärztliche Untersuchung oder einen Heileingriff durchführen lassen möchte. Dies könnte in Artikel 9 Absatz 2 Buchstabe a) DSGVO als Satz 2 wie folgt geregelt werden:

> *„Die ausdrückliche Einwilligung eines Kindes nach Vollendung des [zwölften] Lebensjahres in die Verarbeitung von personenbezogenen Daten im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, und im Zusammenhang mit ärztlichen Untersuchungen oder Heileingriffen ist bei vorliegender Reife und Einsichtsfähigkeit auch ohne die Einwilligung des Trägers der elterlichen Verantwortung zulässig.“*

Zu Erwägungsgrund 38 DSGVO ist in den Erwägungsgründen der Reform-Verordnung der bisherige Satz 3 durch folgenden Satz zu ersetzen:

> *„Um einen Missbrauch von Präventions- oder Beratungsdiensten zur Verarbeitung personenbezogener Daten besonderer Kategorien von Kindern auszuschließen, sollte diese Verarbeitung nur für anerkannte Präventions- oder Beratungsdienste im öffentlichen Interesse, nur für die Zwecke dieser Dienste und nur im für diese Dienste erforderlichen Umfang zulässig sein.“*

4.5 Widerspruch zur Verarbeitung von Kindesdaten

Nicht nur bei der Forderung nach Löschung, sondern auch beim Widerspruch nach Artikel 21 Absatz 1 DSGVO sollte es in besonderer Weise erwähnt werden, wenn die personenbezogenen Daten im Kindesalter erhoben worden sind. Kinder sind sich gemäß Erwägungsgrund 38 Satz 1 DSGVO „der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst“. Um hier Missverständnisse auszuschließen und Rechtsklarheit zu schaffen, sollte der Wortlaut des Artikel 21 Absatz 1 DSGVO klarstellen, dass der Verantwortliche bei der Prüfung der Berechtigung des Widerspruchs den Umstand, dass er Daten von Kindern verarbeitet, besonders berücksichtigen muss. Dies würde auch mit der Pflicht des Verantwortlichen nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f) DSGVO korrespondieren, bei seiner Interessenabwägung die entgegenstehenden Interessen oder Grundrechte und Grundfreiheiten in besonderer Weise zu berücksichtigen, „wenn es sich bei der betroffenen Person um ein Kind handelt“. Für Datenverarbeitungen, die auf Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e) DSGVO und spezifischen Regelungen des Unions- oder des nationalen Rechtes beruhen, dürfte die „spezifische Situation“ gemäß Artikel 21 Absatz 1 Satz 1 DSGVO nicht vorliegen, wenn die Regelung – wie zum Beispiel im Schulrecht – alle Kinder betrifft. Alternativ könnte diese Regelung zum „Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses“ gemäß Artikel 23 Absatz 1 Buchstabe e) DSGVO Ausnahmen vorsehen, die die Verarbeitung von Kinderdaten ermöglicht. Der Wortlaut des Artikel 21 Absatz 1 Satz 1 DSGVO ist um folgenden Einschub (kursiv) zu ergänzen:

> „(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben*, insbesondere wenn es sich um die personenbezogenen Daten eines Kindes handelt,* jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e) oder f) erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling.“

4.6 Keine Einwilligung in automatisierte Entscheidungen

Von der Ausnahme des Verbots der Verarbeitung personenbezogener Daten bei einer automatisierten Entscheidung aufgrund einer Einwilligung nach Artikel 22 Absatz 2 Buchstabe c) DSGVO sollte die Einwilligung eines Kindes ausdrücklich ausgenommen werden. Die Wertung von Erwägungsgrund 71 Satz 5 DSGVO („Diese Maßnahme sollte kein Kind betreffen.“) findet bisher im Normtext keinen Niederschlag. Der Wortlaut ist um ein Adjektiv (kursiv) zu ergänzen:

> „c) mit ausdrücklicher Einwilligung der *erwachsenen* betroffenen Person erfolgt.“

4.7 Datenschutzgerechte Systemgestaltung

Bei der datenschutzgerechten Systemgestaltung nach Artikel 25 Absatz 1 DSGVO sollte der Schutz der Grundrechte und Interessen von Kindern in besonderer Weise hervorgehoben werden. Gerade bei der Systemgestaltung wäre ein grundlegender Schutz von Kindern – vor allem in Social Networks und anderen Angeboten mit datengetriebenen Geschäftsmodellen – besonders wichtig – und meist auch leicht zu realisieren. Der Wortlaut des Absatzes 1 ist ein weiterer Satz (kursiv) anzufügen:

> „(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfanges, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen, trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie zum Beispiel Pseudonymisierung –, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. *Dabei ist dem Schutz der Rechte von Kindern besonders Rechnung zu tragen.*“

4.8 Datenschutzfreundliche Voreinstellung

Auch bei der datenschutzfreundlichen Voreinstellung nach Artikel 25 Absatz 2 DSGVO sollte der Schutz von Kindern in besonderer Weise gefordert werden. Sie übernehmen – mehr noch als Erwachsene – die voreingestellten Werte und konzentrieren sich allein auf die Nutzung des Gerätes oder des Dienstes. Diese spezifische Voreinstellung für Kinder ist vor allem für Social Networks wichtig. Gerade von Kindern kann nicht angenommen werden, dass sie Voreinstellungen erkennen und deren Bedeutung für ihre informationelle Selbstbestimmung verstehen. Sie sind in besonderer Weise darauf angewiesen, dass die Grundeinstellung jedes Risiko für ihren Datenschutz vermeidet. Der Wortlaut ist um einen neuen Satz 4 (kursiv) zu ergänzen:

> *„Die Voreinstellungen berücksichtigen insbesondere die Schutzbedürftigkeit von Kindern.“*

4.9 Meldung von Datenschutzverletzungen

Bei Verletzungen des Schutzes personenbezogener Daten ist eine Meldung an die zuständige Aufsichtsbehörde nicht erforderlich, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen

führt. Als Risiken, die zu berücksichtigen sind, gelten vor allem ökonomische Nachteile, Verletzungen des Persönlichkeitsrechts, Veröffentlichung geheimhaltungsbedürftiger Daten und möglicher Missbrauch der Daten für weitere Angriffe. Die besonderen Risiken von Kindern stehen bei der Risikobewertung nicht im Vordergrund, obwohl bereits die Kenntnisnahme ihres Namens und ihres Wohn- oder Aufenthaltsortes bedeutsame Risiken für sie verursachen können. Daher sollte auf diese Risiken besonders hingewiesen und Artikel 33 Absatz 1 Satz 1 DSGVO um folgenden Passus (kursiv) ergänzt werden.

> „(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, *wobei das Risiko für Kinder besonders zu berücksichtigen ist*."

4.10 Datenschutzfolgenabschätzung

In der Datenschutzfolgenabschätzung nach Artikel 35 DSGVO sollte das besondere Risiko und der besondere Schutzbedarf von Kindern in adäquater Weise berücksichtigt werden. Daher sollte sowohl für die Bestimmung der Notwendigkeit einer Datenschutzfolgenabschätzung nach Absätze 2 bis 4 als auch bei der Risikoanalyse und bei der Festlegung der Schutzmaßnahmen nach Absatz 7 dem Schutz der Grundrechte und Interessen von Kindern eine besondere Aufmerksamkeit entgegengebracht werden. Artikel 35 Absatz 1 DSGVO ist um einen neuen Satz 2 (kursiv) zu ergänzen. Der bisherige Satz 2 wird Satz 3:

> „(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. *Soweit Kinder von der Verarbeitung betroffen sind, ist auf die Risiken und Folgen, die die Verarbeitung für ihre spezifischen Rechte haben kann, ausdrücklich einzugehen*. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden."

Außerdem ist Artikel 35 Absatz 7 Buchstaben c) und d) DSGVO um jeweils einen Einschub (kursiv) zu ergänzen:

> „(7) Die Folgenabschätzung enthält zumindest Folgendes:
>
> (…)

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1, *die in besonderer Weise berücksichtigt, wenn es sich um die personenbezogenen Daten eines Kindes handelt*, und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener, *insbesondere von Kindern, Rechnung getragen wird*."

Diese Schutzregelungen können mit geringem Aufwand, aber hoher Wirkung in den Text der jeweiligen Vorschrift aufgenommen werden. Sie würden den Datenschutz von Kindern deutlich verbessern und die bisherigen Regelungen zum Schutz von Kindern in der Datenschutzgrundverordnung systemgerecht ergänzen.

18.6 DSGVO-Reform: Rechtssicherheit und Innovation gehen Hand in Hand – Anpassungen für KI erforderlich

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12. Dezember 2025)

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) begrüßt im Ansatz die Initiative der Kommission, durch Rechtsanpassungen mehr Rechtssicherheit für die Entwicklung und den Betrieb von KI-Systemen und KI-Modellen mit personenbezogenen Daten anzustreben. Die Datenschutzkonferenz stellt einen datenschutzrechtlichen Regelungsbedarf für Verarbeitungen personenbezogener Daten bei Entwicklung, Training und Betrieb von KI-Modellen und -Systemen fest. Sie hält es darüber hinaus für erforderlich, nicht nur das Thema der Rechtmäßigkeit von Verarbeitungen in den Blick zu nehmen, sondern auch in weiteren Abschnitten der Datenschutzgrundverordnung (DSGVO) einen KI-spezifischen Regelungsbedarf zu prüfen. Die Anpassung der Datenschutzgrundverordnung hinsichtlich KI muss die Technologie ganzheitlich adressieren. Die Datenschutzkonferenz sieht bei den Rechtsgrundlagen einen dringenden Anpassungsbedarf. Sie betont, dass angesichts der Schwierigkeiten bei der effektiven Verwirklichung von Betroffenenrechten gleichwertige Äquivalente dringend erforderlich sind. Durch mehr Rechtssicherheit wird aus Sicht der Datenschutzkonferenz ein wirksamer Vollzug der Datenschutzgrundverordnung erleichtert, der Schutz der Grundrechte der betroffenen Personen gewahrt und gleichzeitig die Möglichkeiten zur Innovation im eindeutigen Rechtsrahmen gestärkt.

Rechtsgrundlagen für Entwicklung und Betrieb von KI-Modellen und -Systemen

Die Datenschutzkonferenz hält es für erforderlich, für die Verarbeitungen von personenbezogenen Daten bei der Entwicklung und dem Betrieb von KI-Modellen und KI-Systemen neue, spezifische Regelungen, insbesondere Rechtsgrundlagen, zu erlassen. Sie sollten sowohl für nicht öffentliche als auch nach Maßgabe vorhandener Kompetenzen für öffentliche Stellen gelten und Schutzmaßnahmen für Betroffene gewährleisten. Die Anforderungen der Rechtsgrundlagen müssen die technischen Besonderheiten von KI-Modellen und KI-Systemen, die sehr vielfältigen Einsatzmöglichkeiten sowie die unterschiedlichen Rollen der Beteiligten berücksichtigen. Dies ist der beste Weg, die betroffenen Grundrechtspositionen im Sinne der praktischen Konkordanz in einen angemessenen Ausgleich zu bringen. Relevante Regelungsbereiche können sein:

- Verarbeitung von durch Web Scraping erlangten personenbezogenen Daten einschließlich besonderen Kategorien für die Entwicklung von KI-Modellen,
- Weiterverarbeitung von für andere Zwecke erhobenen personenbezogenen Daten einschließlich besonderer Kategorien, um interne domänenspezifische KI-Modelle zu entwickeln,
- Verarbeitungen beim Betrieb von in KI-Modellen memorisierten personenbezogenen Daten.

Diese Regelungen müssen einerseits klare Voraussetzungen rechtmäßiger Verarbeitungen für die besonders relevanten Konstellationen abbilden und zugleich rote Linien in Form von Verboten aufzeigen.

Betroffenenrechte mitdenken

Zur Einhaltung des Datenschutzes bei der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen und -Systemen gehört auch, Transparenzvorgaben und Betroffenenrechte der Datenschutzgrundverordnung nach der Rechtsprechung des Europäischen Gerichtshofes zu gewährleisten.[13] Bei der Entscheidung zur Einführung eines KI-Systems, also möglichst frühzeitig, sollte die Sicherung der Rechte der betroffenen Person eine Rolle spielen, quasi als “Betroffenenrechte by Design“. Gleichwohl zeigt sich, dass die Gewährleistung der Betroffenenrechte beim Einsatz vieler KI-Systeme in der Praxis schwierige Fragen aufwerfen kann, wenn die Umsetzung aufgrund der zugrundeliegenden Modelle kaum möglich erscheint.

[13] Orientierungshilfe der Datenschutzkonferenz zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen, Version 1.0 (Stand Juni 2025) abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/DSK-OH_KI-Systeme.pdf. Vergleiche EuGH, Urteil vom 4. Oktober 2024, Koninklijke Nederlandse Lawn Tennisbond, C-621/22, EU:C:2024:857, Rn. 40, 41 und 49.

Um die Rechte der Betroffenen zu wahren und einen eindeutigen rechtssicheren Rahmen für KI zu schaffen, sollten daher im Rahmen des europäischen Reformprozesses zum Datenschutzrecht und zu den Digitalrechtsakten auch Anpassungen in Form von funktionsäquivalenten oder kompensatorischen Schutzmaßnahmen in den Blick genommen werden.

Bislang sind Verantwortliche im Rahmen der datenschutzrechtlichen Transparenzpflichten nicht explizit verpflichtet, Betroffene ausdrücklich darüber zu informieren, dass ihre personenbezogenen Daten in einem KI-System verarbeitet werden. Daher wird die Aufnahme einer entsprechenden Informationspflicht in die Artikel 13 Absatz 2 DSGVO und Artikel 14 Absatz 2 DSGVO vorgeschlagen. Entsprechendes ist für das Recht der Betroffenen auf Auskunft festzustellen. Um diese Regelungslücke zu schließen, wird die Einführung einer entsprechenden Ergänzung in Artikel 15 Absatz 1 DSGVO vorgeschlagen.

Aus technischen Gründen könnte es in manchen Fällen für den Verantwortlichen nur mit unverhältnismäßigem Aufwand möglich sein, beispielsweise dem kompletten Neutraining eines LLMs, die Erfüllung der Betroffenenrechte aus Artikel 16 Seite 1 DSGVO, Artikel 17 Absatz 1 DSGVO, Artikel 18 Absatz 1 DSGVO und Artikel 21 DSGVO zu gewährleisten. Hier sollte der europäische Gesetzgeber prüfen, wie die spezifischen Risiken für nicht umgesetzte Transparenz-, Löschungs-, Berichtigungsrechte und Widerspruchsrechte im KI-Modell mitigiert oder Betroffenenrechte funktionsäquivalent gewährleistet werden können, sodass praxistaugliche Lösungen geschaffen und gleichzeitig der Schutzstandard gehalten werden kann.

Aus technischen Gründen könnte es in manchen Fällen für den Verantwortlichen nur mit unverhältnismäßigem Aufwand möglich sein, beispielsweise dem kompletten Neutraining eines LLMs, die Erfüllung der Betroffenenrechte aus Artikel 16 Absatz 1, Artikel 17 Absatz 1, Artikel 18 Absatz 1 und Artikel 21 DSGVO zu gewährleisten. Hier sollte der europäische Gesetzgeber prüfen, wie die spezifischen Risiken für nicht umgesetzte Transparenz-, Löschungs-, Berichtigungsrechte und Widerspruchsrechte im KI-Modell mitigiert oder Betroffenenrechte funktionsäquivalent gewährleistet werden können, sodass praxistaugliche Lösungen geschaffen und gleichzeitig der Schutzstandard gehalten werden kann.

Die Datenschutzkonferenz wird den laufenden Prozess der Datenschutzgrundverordnung-Reform weiter konstruktiv begleiten und erneut Stellung nehmen.

18.7 DSGVO-Reform: IT-Hersteller in die Verantwortung nehmen!

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12. Dezember 2025)

Die Konferenz der obersten Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) unterstützt das gemeinsame Ziel des Bundeskanzlers und der Regierungschefinnen und Regierungschefs der Länder, die Hersteller und Anbieter von Standardlösungen künftig in die Verantwortung zu nehmen, damit die Anwender unkompliziert und rechtssicher Standardlösungen nutzen können.[14] Sie hält es für erforderlich, die Reform der Datenschutzgrundverordnung (DSGVO) dafür zu nutzen, das System der datenschutzrechtlichen Verantwortlichkeiten durch das Prinzip der Herstellerverantwortung fortzuentwickeln und diesbezüglich an das anderer Digitalrechtsakte, wie des Cyber Resilience Actes oder der KI-Verordnung, anzugleichen. Dies würde zu einer erheblichen Entlastung der Anwender, insbesondere kleinerer und mittlerer Unternehmen (KMU), und einer substanziellen Vereinfachung für sie führen, wenn sie personenbezogene Daten verarbeiten.

Die Datenschutzgrundverordnung stellt bereits heute mit Data Protection by Design and by Default (Artikel 25 DSGVO) Grundsätze auf, die sich in der Sache an Hersteller, Importeure und Anbieter richten, nimmt aber nicht diese, sondern ausschließlich die Anwender von Hard- und Software datenschutzrechtlich in die Pflicht. Die Einbeziehung der Anbieter beziehungsweise Hersteller von Standard-Hard- und Software in das etablierte System datenschutzrechtlicher Pflichten würde daher die Verantwortung dorthin verlagern, wo die Entscheidungen über grundsätzliche Weichenstellungen in Systemen getroffen werden. Gleichzeitig würden die Anwender von IT-Produkten, die keinen Einfluss auf das Produktdesign haben, die Haftungsrisiken nicht alleine tragen.

Die Datenschutzkonferenz hat bereits in ihrer ersten Evaluation der Datenschutzgrundverordnung im Jahr 2019[15] Vorschläge für eine solche Erstreckung des Grundsatzes von Data Protection by Design auf Hersteller und Anbieter von IT-Produkten unterbreitet, die im Wesentlichen unverändert vorgeschlagen werden.

Die Ergänzungen entsprechen der grundsätzlichen Ausrichtung der Kommissionsvorschläge, die Anwendung der Datenschutzgrundverordnung insbesondere für kleine und mittlere Unter-

[14] Beschluss des Bundeskanzlers und der Regierungschefinnen und Regierungschefs der Länder vom 4. Dezember 2025: Die Förderale Modernisierungsagenda, https://www.bundesregierung.de/resource/blob/975228/2397654/c57248be7fa2d61ab6d8b12c0f29f05b/2025-12-04-mpk-staatsmodernisierung-data.pdf.

[15] Datenschutzkonferenz: Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DSGVO, November 2019, https://www.datenschutzkonferenz-online.de/media/dskb/20191213_erfahrungsbericht_zur_anwendung_der_ds-gvo.pdf.

nehmen (KMU) zu vereinfachen und mit den nach ihr erlassenen Digitalrechtsakten zu harmonisieren. Sie erhöhen die Rechtssicherheit für Anwender, denen durch die künftig von Herstellern und Anbietern bereitzustellenden Konformitätserklärungen die Erfüllung ihrer Rechenschaftspflicht erleichtert wird. Demgegenüber entstehen für Hersteller und Anbieter keine erheblichen Zusatzpflichten, da sich diese bereits weitgehend aus dem Cyber Resilience Act ergeben.

In einer weiteren Stufe kann zudem ein an datenschutzrechtliche Zertifizierungen angelehntes Modell auch für Produktzertifizierungen entwickelt werden.

Ergänzend sollten die bisher alleine an den Verantwortlichen gerichteten Verpflichtungen zu den datenschutzfreundlichen Voreinstellungen (Artikel 25 DSGVO) auch auf Auftragsverarbeiter erstreckt werden, um neben Herstellern auch deren Rolle bei der Gewährleistung des Datenschutzes durch Technikgestaltung hervorzuheben und Verantwortliche möglichst umfassend von Aufgaben zu entlasten, die an anderer Stelle effektiver geklärt werden können.

19. Zahlen und Fakten

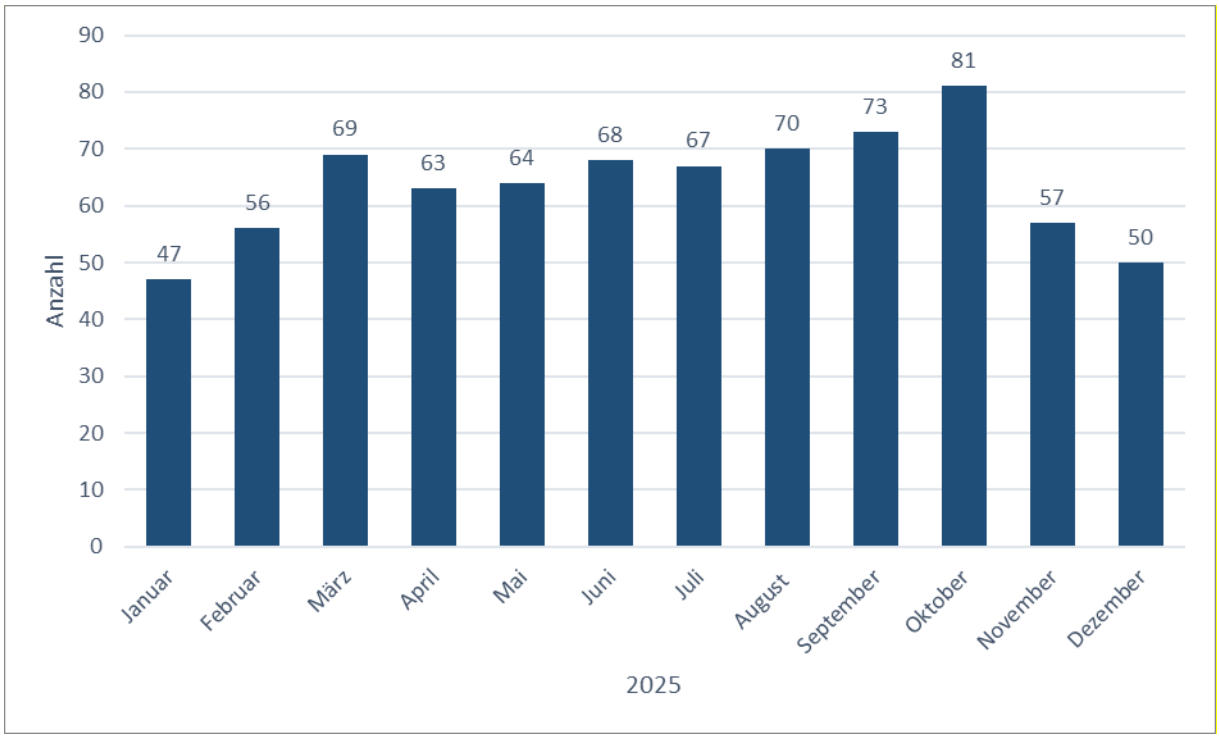
19.1 Auswahl datenschutzrelevanter Sachverhalte, die 2025 an den Landesbeauftragten für Datenschutz und Informationsfreiheit herangetragen wurden

Monat	Beschwerden	Beratungs-anfragen	Meldungen Datenschutz-verletzungen	Meldungen Datenschutz-beauftragte
Januar	47	50	29	30
Februar	56	38	23	30
März	69	51	36	18
April	63	42	5	18
Mai	64	42	21	34
Juni	68	36	27	38
Juli	67	45	20	29
August	70	24	22	16
September	73	31	12	23
Oktober	81	24	27	20
November	57	16	21	8
Dezember	50	19	16	22
Gesamt	**765**	**418**	**259**	**286**

Tabelle 1

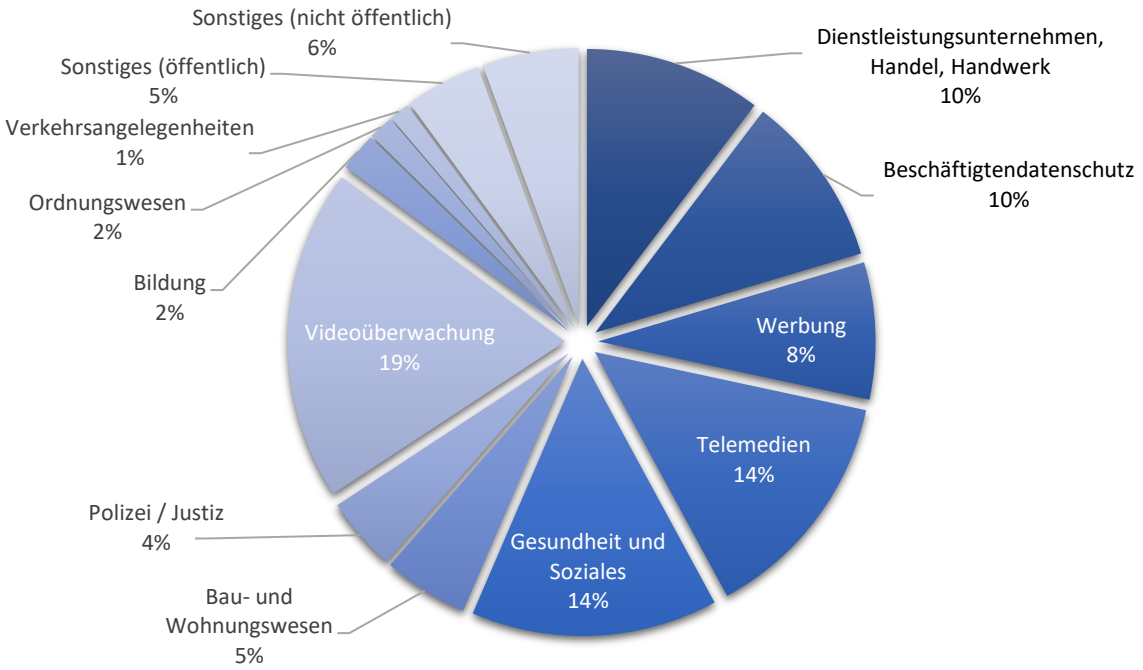
Nähere Angaben hierzu finden sich in den nachfolgenden Ziffern.

19.2 Beschwerden



Säulendiagramm 1

In diesem Diagramm sind die monatlichen Beschwerdezahlen des Jahres 2025 dargestellt.



Tortendiagramm 1

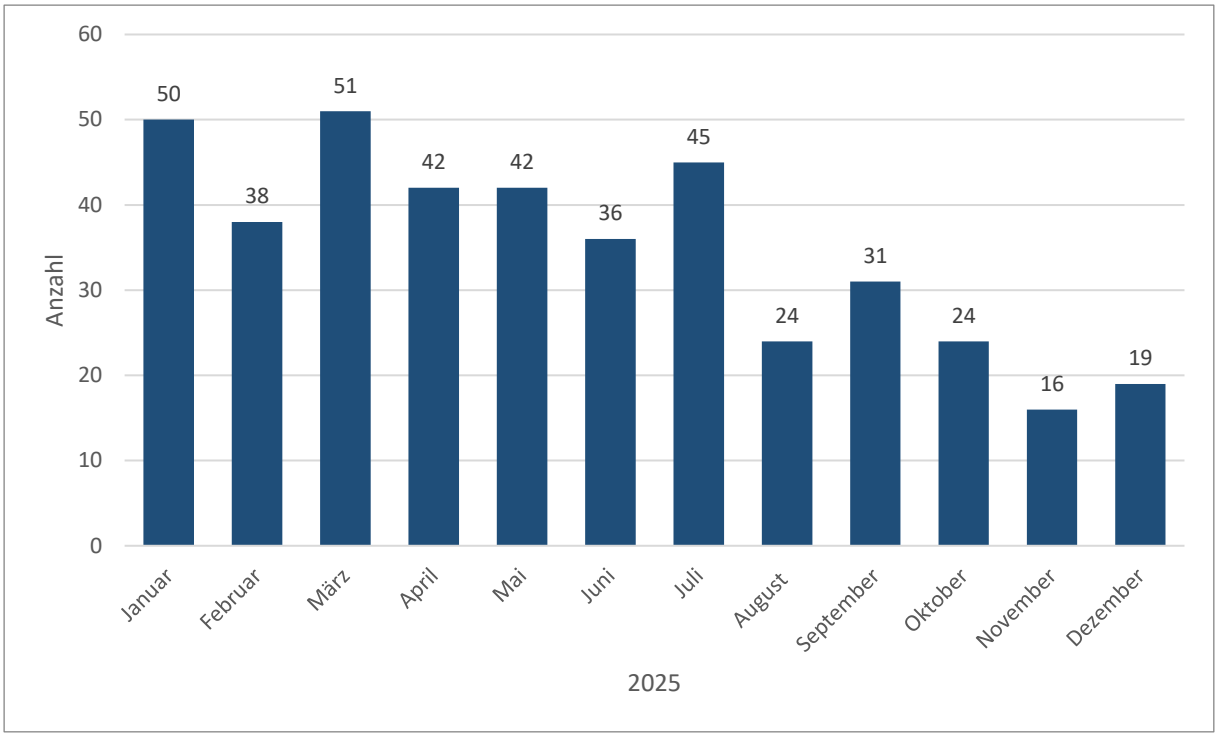
Das Diagramm zeigt die bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit eingegangenen Beschwerden im gesamten Jahr 2025 nach Themengebieten aufgeschlüsselt.

Themengebiet	Absoluter Wert	Relativer Wert
Dienstleistungsunternehmen, Handel, Handwerk	79	10 %
Beschäftigtendatenschutz	77	10 %
Werbung	61	8 %
Telemedien	105	14 %
Gesundheit und Soziales	110	14 %
Bau- und Wohnungsunternehmen	38	5 %
Polizei / Justiz	33	4 %
Videoüberwachung	148	19 %
Bildung	17	2 %
Ordnungswesen	11	2 %
Verkehrsangelegenheiten	9	1 %
Sonstiges (nicht öffentlich)	34	6 %
Sonstiges (öffentlich)	43	5 %

Tabelle 2

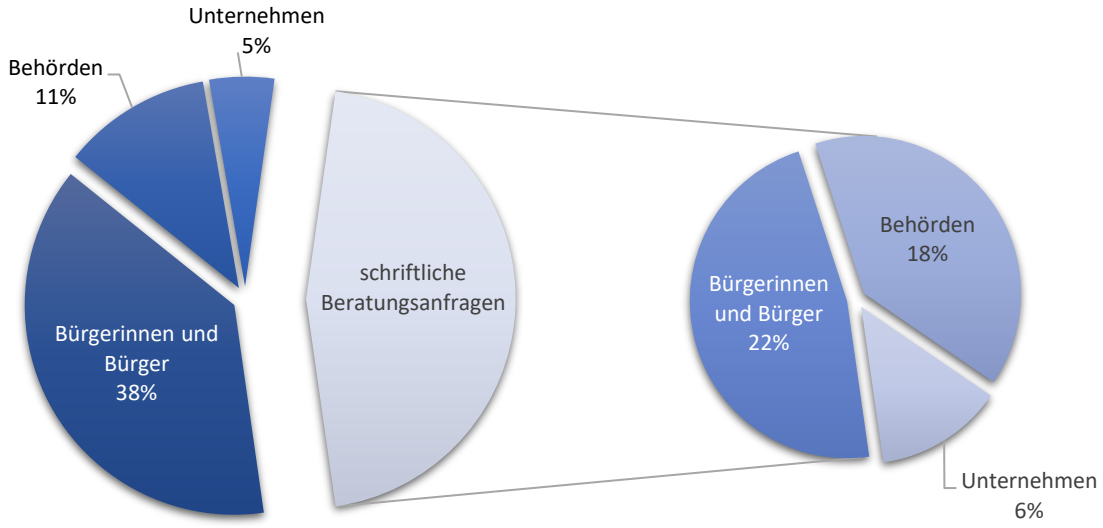
Die Tabelle stellt die absoluten und relativen Werte der unterschiedlichen Themengebiete der Beschwerden dar.

19.3 Beratungen



Säulendiagramm 2

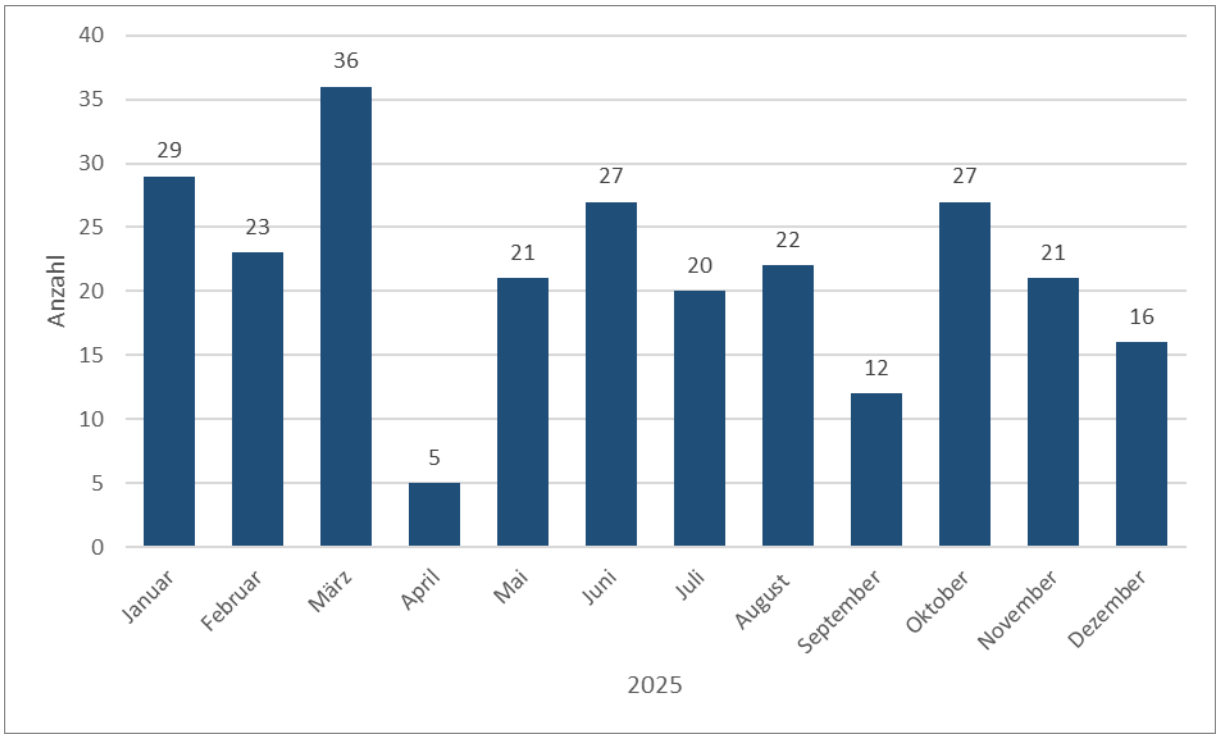
Diese Grafik gibt eine Übersicht über die Anzahl schriftlicher und telefonischer Beratungen von Verantwortlichen und betroffenen Personen.



Tortendiagramm 2

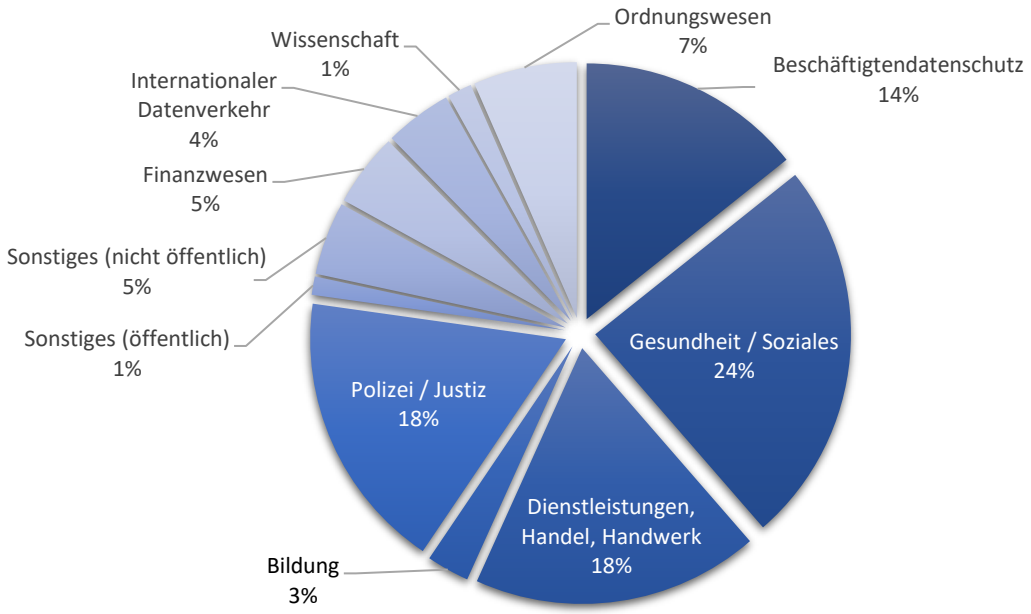
Dieses Tortendiagramm stellt die telefonischen und schriftlichen Beratungen im Jahr 2025 dar. Differenziert wird dabei zwischen telefonischen und schriftlichen Beratungsanfragen.

19.4 Meldungen von Datenschutzverletzungen



Säulendiagramm 3

In dieser Grafik sind die monatlichen Meldungen von Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung im Jahr 2025 dargestellt.



Tortendiagramm 3

Diese Darstellung schlüsselt die gemeldeten Datenschutzverletzungen für das Jahr 2025 nach Themengebieten auf.

19.5 Abhilfemaßnahmen

Warnungen

Nach Artikel 58 Absatz 2 Buchstabe a) Datenschutzgrundverordnung (DSGVO): Keine

Verwarnungen

Nach Artikel 58 Absatz 2 Buchstabe b) DSGVO: Zehn

Anweisungen und Anordnungen

Nach Artikel 58 Absatz 2 Buchstabe c) bis g) DSGVO und § 85 BremPolG: Acht

Widerruf von Zertifizierungen

Nach Artikel 58 Absatz 2 Buchstabe h) DSGVO: Keine

Geldbußen

Nach Artikel 58 Absatz 2 Buchstabe i) DSGVO: 101

19.6 Europäisches Binnenmarkt-Informationssystem

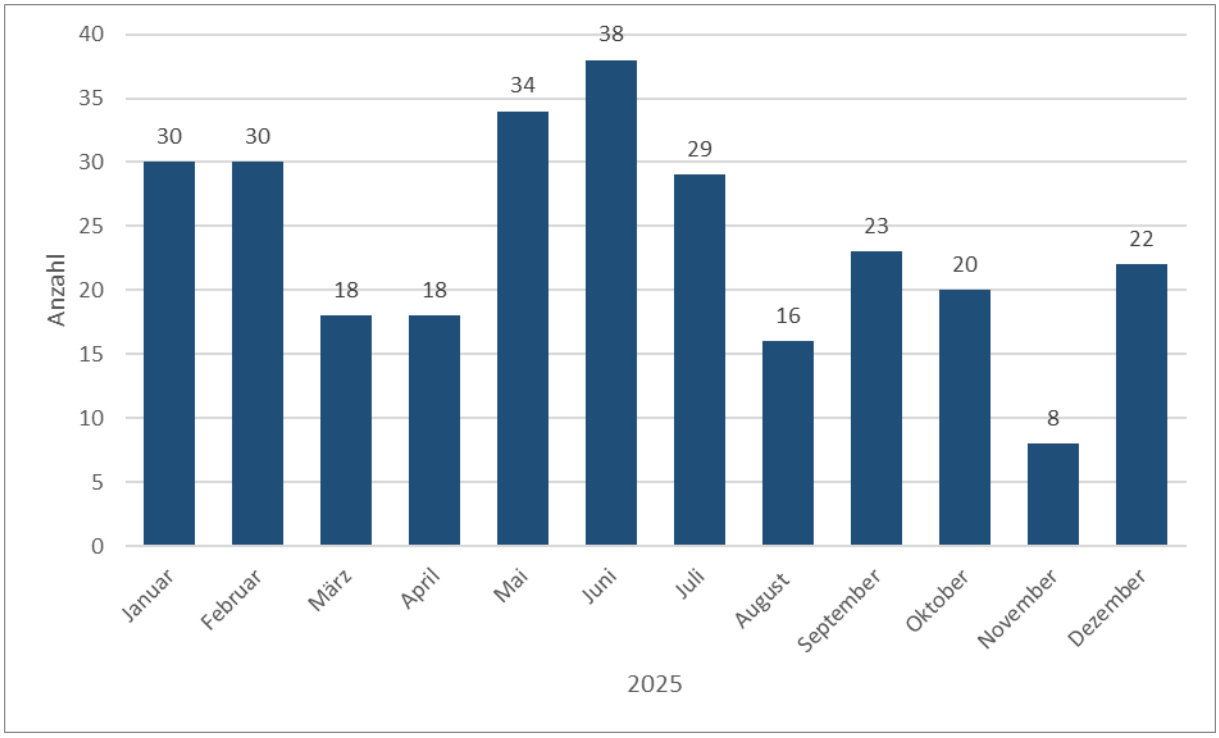
Verfahren mit Betroffenheit nach Artikel 56 DSGVO:	Dreißig Fälle
Verfahren mit Federführung nach Artikel 56 DSGVO:	Kein Fall
Verfahren gemäß Kapitel VII nach den Artikeln 60 ff. DSGVO:	Fünf Fälle (Artikel 60)
	Zwölf Fälle (Artikel 61)
	Kein Fall (Artikel 64)

19.7 Förmliche Begleitung bei Rechtsetzungsvorhaben

- Bremische Verordnung über die Durchführung von Modellvorhaben zu Substanzanalysen (Bremische Drug-Checking-Verordnung – BremDrugCheckingV)
- Verordnung zur Aufhebung der Verordnung zur Übertragung von Aufgaben der Vertrauensstelle des Bremer Krebsregisters
- Entfristung des § 32 Absatz 3 Satz 1 Nummer 4 Bremisches Polizeigesetz
- Bremisches Polizeigesetz (BremPolG)

- Bremisches Verfassungsschutzgesetz (BremVerfSchG)
- Verordnungsentwurf nach dem Bremischen Hafensicherheitsgesetz (BremHaSiG)
- Gesetz zur Änderung des Gesetzes über das Friedhofs- und Bestattungswesen in der Freien Hansestadt Bremen (Land)
- Justizgebäudesicherheitsgesetz oder Bremisches Gesetz über die Sicherheit in Justizgebäuden (BremJSG)
- Dreiunddreißigste Verordnung zur Änderung der eAkten-Verordnung sowie Zweite Verwaltungsvorschrift zur Änderung der Verwaltungsvorschrift zu § 1 a der Verordnung zur elektronischen Aktenführung bei den Gerichten und den Staatsanwaltschaften im Land Bremen
- Gesetz zur Änderung disziplinar- und beamtenrechtlicher Vorschriften sowie zur Änderung der Landeshaushaltsordnung
- Verordnung zur vorübergehenden Ausnahme von der Verpflichtung zur elektronischen Aktenführung für den Landesbeauftragten für Datenschutz und Informationsfreiheit
- Änderung des Bremischen Ausführungsgesetzes zur EU-Datenschutz-Grundverordnung (BremDSGVOAG)
- Landwirtschaftskammergesetz (LwKG)
- Entwurf für Zuständigkeitsregelungen im BremDSGVOAG hinsichtlich der Artikel 18 bis 20 TTPW-VO
- Verlängerung der Verordnung über die zulässige Miethöhe gemäß § 556d Absatz 2 des Bürgerlichen Gesetzbuchs (Mietenbegrenzungsverordnung)
- Ortsgesetz zur Änderung Gebührenordnung für die Abfallentsorgung in der Stadtgemeinde Bremen

19.8 Meldungen über die Bestellung behördlicher und betrieblicher Datenschutzbeauftragter



Säulendiagramm 4

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

19.9 Datenschutzrechtliche Zertifizierung

Die Datenschutzgrundverordnung (DSGVO) verlangt von Verantwortlichen, dass diese die Einhaltung der Datenschutzgrundsätze aus Artikel 5 DSGVO nachweisen können; sie müssen demnach belegen können, dass die Datenschutzgrundsätze tatsächlich umgesetzt werden. Eine datenschutzrechtliche Zertifizierung nach Artikel 42 DSGVO ermöglicht es Verantwortlichen und Auftragsverarbeitern, die Umsetzung der Datenschutzgrundsätze sowie die Einhaltung der Anforderungen der Datenschutzgrundverordnung nachzuweisen. Sie stellt einen formalisierten und objektiv überprüfbaren Nachweis dar, dass bestimmte Verarbeitungsvorgänge datenschutzkonform ausgestaltet sind.

Eine Zertifizierungsstelle darf Datenschutzzertifizierungen nur dann vergeben, wenn sie zuvor von der nationalen Akkreditierungsstelle, in Deutschland handelt es sich dabei um die Deutsche Akkreditierungsstelle GmbH (DAkkS), und der zuständigen Datenschutzaufsichtsbe-

hörde gemäß § 39 Bundesdatenschutzgesetz (BDSG) akkreditiert wurde. Diese Akkreditierung bestätigt, dass die Zertifizierungsstelle unabhängig, fachkundig und nach objektiven, von der Aufsichtsbehörde genehmigten Kriterien arbeitet.

Im Jahr 2018 stellte ein bremisches Unternehmen bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit als eines der ersten deutschen Unternehmen einen Antrag auf Akkreditierung (siehe hierzu 7. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 19.9). An diesem aufwändigen Verfahren müssen neben dem Landesbeauftragten für Datenschutz und Informationsfreiheit und der DAkkS noch weitere deutsche und europäische Datenschutzaufsichtsbehörden mitwirkten. In diesem Fall handelte es sich dabei um die italienische Datenschutzaufsichtsbehörde Garante per la Protezione dei Dati Personali und die Berliner Beauftragte für Datenschutz und Informationsfreiheit, bevor im Anschluss alle europäischen Datenschutzaufsichtsbehörden einbezogen wurden. Im März des Berichtsjahres konnte das Zertifizierungsverfahren abgeschlossen werden, nachdem der Landesbeauftragte für Datenschutz und Informationsfreiheit die deutschlandweit ersten generischen Zertifizierungskriterien – also Kriterien, die nicht auf einen bestimmten Anwendungsfall zugeschnitten sind, sondern allgemein gelten – genehmigt hatte.

Verantwortliche und Auftragsverarbeiter haben nun die Möglichkeit, eine offiziell anerkannte Datenschutzzertifizierung zu erwerben, diese als Nachweis für die Konformität mit der Datenschutzgrundverordnung zu nutzen und möglichst auch Wettbewerbs- beziehungsweise Vertrauensvorteile zu erzielen. Für die Einhaltung der Datenschutzgrundverordnung bleiben die Verantwortlichen und Auftragsverarbeiter jedoch uneingeschränkt selbst verantwortlich.