ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

TÄTIGKEITSBERICHT
2025

ULD – SCHLESWIG-HOLSTEINS ZENTRUM FÜR DATENSCHUTZ UND INFORMATIONSZUGANG

Tätigkeitsbericht 2025
des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein

BERICHTSZEITRAUM: 2024

REDAKTIONSSCHLUSS: 31.12.2024

LANDTAGSDRUCKSACHE: 20/2985

(43. TÄTIGKEITSBERICHT DER LANDESBEAUFTRAGTEN FÜR DATENSCHUTZ –

UMFASST DEN TÄTIGKEITSBERICHT DER LANDESBEAUFTRAGTEN FÜR INFORMATIONSZUGANG)

Dr. h. c. Marit Hansen

Landesbeauftragte für Datenschutz Schleswig-Holstein
Landesbeauftragte für Informationszugang Schleswig-Holstein

Leiterin des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein

Impressum

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstraße 98

24103 Kiel

Mail: mail@datenschutzzentrum.de

Web: https://www.datenschutzzentrum.de

Satz und Lektorat: Gunna Westphal, Kiel

Umschlaggestaltung: Martin Papp, Eyekey Design, Kiel

Titelfoto: ULD, Kiel

Druck: hansadruck und Verlags-GmbH & Co KG, Kiel

Inhaltsverzeichnis

01

KERNPUNKTE

Zwischenfazit DSGVO

Zahlen und Fakten

Beschwerde-Dauerbrenner Videoüberwachung

Vorsitz der DSK – auch im Jahr 2024

1 Datenschutz und Informationsfreiheit

Das Jahr 2024 war ein besonderes Jahr für den Datenschutz in Deutschland und auf der europäischen Ebene. In Deutschland, weil die Datenschutzkonferenz – der **Zusammenschluss der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder** – nicht wie üblich *einen* Vorsitz hatte, sondern insgesamt drei Landesbeauftragte nacheinander beauftragt wurden, für die Datenschutzkonferenz zu sprechen: Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen, die eigentlich das ganze Jahr lang Vorsitzende der Datenschutzkonferenz sein sollte, stand ab Ende Januar nicht mehr zur Verfügung, sodass wir gebeten wurden, unsere Vorsitzrolle aus dem Jahr 2023 für mehrere Monate fortzuführen, bis der Hessische Datenschutzbeauftragte für Datenschutz und Informationsfreiheit übernehmen konnte. Unsere Amtszeit als **Vorsitz der Datenschutzkonferenz** erstreckte sich damit über **15 ½ Monate** – so lange wie noch nie zuvor.

Auf europäischer Ebene war das Jahr ebenfalls besonders, da Rechtsakte zu künstlicher Intelligenz und Cyberresilienz verabschiedet wurden und in Kraft traten. Bereits in den vergangenen Jahren waren die weiteren **Bausteine der europäischen Gesetzgebung für den digitalen Bereich** auf den Weg gebracht worden. Dazu gehören – neben der Datenschutz-Grundverordnung (DSGVO) – der Daten-Governance-Rechtsakt (DGA), das Gesetz über digitale Märkte (DMA), das Gesetz über digitale Dienste (DSA), die Datenverordnung (DA), die KI-Verordnung (KI-VO) und im Bereich der Informationssicherheit die NIS-2-Richtlinie, die CER-Richtlinie und das Cyberresilienzgesetz (CRA).

Soweit die Verarbeitung personenbezogener Daten betroffen ist, ist das Datenschutzrecht einzuhalten. Hier zeigen sich **zahlreiche Schnittmengen** der DSGVO mit diesen Digitalrechtsakten, die u. a. den fairen Umgang mit Daten und eine Verbesserung der Informationssicherheit zum Ziel haben. Diese Digitalrechtsakte bilden die Grundlage für den Weg in eine Zukunft, in der die Informationsgesellschaft im Sinne der europäischen Grundrechte weiterentwickelt werden soll.

Unser Titelbild für den gedruckten Tätigkeitsbericht visualisiert den Weg in die Zukunft in Form einer Treppe, deren **Stufen die verschiedenen europäischen Digitalrechtsakte** repräsentieren. Die Treppe ist insgesamt stabil, allerdings sind die Stufen nicht gleichartig, sondern in Form und Höhe verschieden gestaltet. In einigen historischen Bauwerken, in denen man ähnlich unterschiedliche Stufen findet, ist damit das Konzept verbunden, dass man auf seinen Weg achten und jeden Schritt bewusst gehen soll.

Die Europäische Union verfolgt mit den Digitalrechtsakten sicherlich kein derartiges spirituelles Konzept. Als Sinnbild erschien es uns jedoch geeignet, um deutlich zu machen, dass die Beteiligten auf dieser insgesamt tragfähigen Treppe in die Zukunft noch nicht trittsicher sind und es **noch nötig** ist, sich in den einzelnen Schritten **auszubalancieren**. Denn bisher sind viele Fragen in Bezug auf die europäischen Rechtsakte offen, beispielsweise welche Best-Practice-Lösungen und Standards leitend sein und wie die Prüfungen und Beratungen der verschiedenen zuständigen Aufsichtsbehörden zu einer Rechtssicherheit für Unternehmen und Behörden insgesamt führen können.

Unser Bericht für das Jahr 2024 beschreibt die **Tätigkeiten** der Behörde der Landesbeauftragten für Datenschutz und, in Personalunion, der Landesbeauftragten für Informationszugang. Die ausgewählten Einzelfälle und im Bericht behandelten Themen geben einen Einblick in wichtige Entwicklungen aus Recht und Technik. Sie zeigen beispielhaft, wie man Fehler vermeidet oder Verbesserungsbedarfe umsetzen kann, um die **Anforderungen aus dem Datenschutz- und Informationszugangsrecht** zu erfüllen.

Ich wünsche Ihnen viel Spaß beim Lesen!

Dr. h. c. Marit Hansen

Landesbeauftragte für Datenschutz Schleswig-Holstein
Landesbeauftragte für Informationszugang Schleswig-Holstein

1.1 Zwischenfazit Datenschutz-Grundverordnung – vieles verstanden, vieles auf dem Weg

2012 hatte die Europäische Kommission den ersten Entwurf für eine Datenschutz-Grundverordnung (DSGVO) veröffentlicht. Nach intensiven Verhandlungen trat im Jahr 2016 die DSGVO in Kraft, und wirksam wurden die Regeln ab dem 25. Mai 2018. Zeit für ein **Zwischenfazit**.

Die meisten Verantwortlichen sind nach unserer Beobachtung recht gut über ihre Pflichten im Bilde. Websites sind mit Datenschutzerklärungen versehen, viele Verantwortliche haben ihre Prozesse passabel dokumentiert, auf Auskunftsersuchen von betroffenen Personen wird zumindest reagiert (Tz. 11.2). Bei der **Einführung neuer Technik (Stichwort künstliche Intelligenz (KI))** bestehen allerdings Unsicherheiten – dazu gibt es auch seit Kurzem Hinweise, Orientierungshilfen oder Leitlinien vonseiten der Aufsichtsbehörden (Tz. 2.1, Tz. 6.2.5 und Tz. 6.2.6), und weitere sind in Arbeit. Aufgefallen ist uns, dass einige Organisationen es bei der Benennung von Datenschutzbeauftragten nicht immer so genau mit Interessenkonflikten nehmen (Tz. 5.1). Das geht so natürlich nicht. Das Bewusstsein für meldepflichtige Datenpannen ist gewachsen, doch in der Handhabung besteht noch viel Verbesserungspotenzial (Tz. 6.3.1).

Ein **gesteigertes Beschwerdeaufkommen** (Tz. 1.2) zeigt, dass vielen Menschen bewusst ist, dass es Datenschutzaufsichtsbehörden gibt. Jedoch vermuten einige Beschwerdeführenden Verstöße, wo es keine gibt. Andere scheinen die Erwartung zu haben, dass die Aufsichtsbehörden als schnelle Eingreiftruppe agieren, direkt vor Ort unzulässige Datenverarbeitungssysteme abbauen und standardmäßig Bußgelder in Millionenhöhe verhängen. So ist es gerade nicht. Ein **rechtsstaatliches Vorgehen auf Basis unserer gesetzlichen Befugnisse** mit Anhörungen und Aufklärung des Sachverhalts dauert diesen Personen zu lange. Sie sind dann nicht nur unzufrieden mit dem Verantwortlichen, sondern auch mit den Datenschutzaufsichtsbehörden. Einige machen dann von ihrem Recht Gebrauch, die Aufsichtsbehörde vor dem Verwaltungsgericht zu verklagen – auch das gehört zum Rechtsstaat.

Einige Instrumente der Datenschutz-Grundverordnung entwickeln sich nur langsam. So existieren erst wenige Verhaltensregeln (Codes of Conduct) nach Artikel 40 DSGVO. **Zertifizierungen** nach Artikel 42 DSGVO stecken noch im Anfangsstadium, sind jetzt aber möglich (Tz. 9.2). Die **Umsetzung des Prinzips „Datenschutz by Design und by Default"** nach Artikel 25 DSGVO steckt ebenfalls noch in den Kinderschuhen. Da gibt es jedenfalls Luft nach oben.

Die Notwendigkeit der Risikobeherrschung nach der DSGVO ist vielen Verantwortlichen bewusst, selbst wenn immer noch eine Interpretation vorherrscht, die sich an den Risiken der Informationssicherheit orientiert, sodass noch zu wenig Übung darin besteht, darüber hinausgehende **Datenschutzrisiken – z. B. Diskriminierung oder Rufschädigungen von betroffenen Personen** – zu identifizieren. Gerade in Bezug auf neue Technologien (wieder das Stichwort KI) besteht Verbesserungsbedarf bei der Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO. Die Anforderungen für Hochrisiko-KI-Systeme nach der KI-VO werden übergreifende Risikobewertungen erforderlich machen (siehe Tz. 8.2 für Grundrechte-Folgenabschätzungen).

Von Vorteil ist es, dass **Compliance und Risikobeherrschung in vergleichbarer Art und Weise** auch von den neuen **europäischen Digitalrechtsakten** verlangt werden. Hier besteht die Herausforderung sowohl für die Verantwortlichen als auch für die Aufsichtsbehörden, zu rechtssicheren Lösungen zu kommen, die *alle* rechtlichen Anforderungen erfüllen. Das wird nur klappen, wenn die verschiedenen Bereiche und Zuständigkeiten in den Organisationen ebenso wie die verschiedenen zuständigen Aufsichtsbehörden **miteinander kommunizieren** und sich abstimmen. Dies ist eigentlich keine neue Anforderung, denn zumindest für die Schnittmengen zwischen Informationssicherheit und Datenschutz war dies in der Vergangenheit schon wichtig. Doch in der Praxis besteht aus unserer Sicht in vielen Fällen Verbesserungsbedarf – faktisch bedeutet dies auch, Klarheit über die **ver-**

schiedenen Begriffswelten zu erlangen und **Brücken zwischen den unterschiedlichen Disziplinen und organisationsüblichen Methoden zu bauen**, damit sich das nötige Verständnis im Sinne der umfassenden Risikobeherrschung entwickelt.

1.2 Zahlen und Fakten zum Jahr 2024

Nachdem in den Jahren 2022 und 2023 die Zahl der von uns bearbeiteten Beschwerden gegenüber dem Wert aus 2021 leicht zurückgegangen war (2021: 1.464, 2022: 1.334, 2023: 1.344), war im Jahr 2024 **mit 1.628 Beschwerden ein neuer Spitzenwer**t zu verzeichnen. Dies stellt eine Steigerung von 21 Prozent gegenüber dem Vorjahreswert dar.

Die Höchstzahl von 649 Meldungen im Jahr 2021 wurde allerdings noch nicht erreicht; jenes Jahr war durch eine Häufung von Massenmeldungen bei mehreren Angriffswellen und Schwachstellen in weithin eingesetzter Technik gekennzeichnet gewesen (40. TB, Tz. 6.3.3).

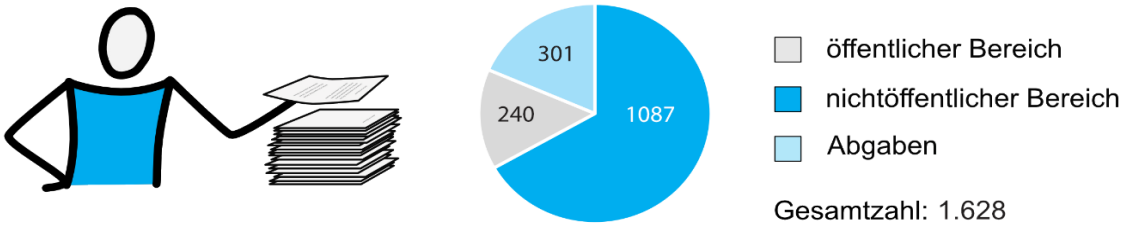

Abb. 1: Zahl der bearbeiteten Beschwerden 2024

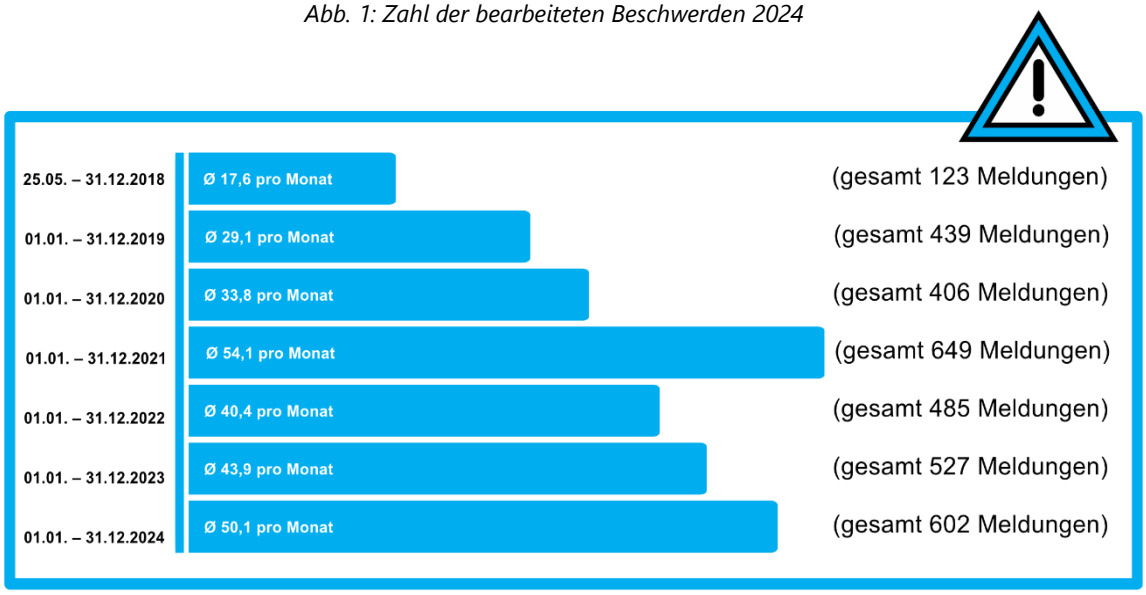

Abb. 2: Zahl der bearbeiteten Meldungen nach Artikel 33 DSGVO

Auch die Zahl der gemeldeten Verletzungen des Schutzes personenbezogener Daten (sogenannte Datenpannen) ist gestiegen: Im Jahr 2024 sind **602 Meldungen** bei uns eingegangen. Im Vergleich zum Vorjahr mit 527 Meldungen handelt es sich um eine Steigerung von 14 Prozent.

Im Folgenden sind die genauen Zahlen dargestellt:

Im Jahr 2024 erreichten uns 1.628 schriftliche **Beschwerden** (Vorjahr: 1.344), von denen 301 (Vorjahr: 284) nicht in unserer Zuständigkeit

(öffentliche und nichtöffentliche Stellen in Schleswig-Holstein mit Ausnahme bestimmter Bereiche in Bundeszuständigkeit, z. B. Telekommunikation) lagen und an die zuständigen Behörden abgegeben werden mussten.

Insgesamt wurden in eigener Zuständigkeit 1.327 (Vorjahr: 1.060) Beschwerden bearbeitet, davon richteten sich **mehr als 80 Prozent der Beschwerden gegen Unternehmen** und andere nichtöffentliche Stellen (1.087; Vorjahr: 799), der Rest gegen Behörden (240; Vorjahr: 261). Dazu kamen 443 (Vorjahr: 570) Beratungen für den öffentlichen und den nichtöffentlichen Bereich.

Ohne vorherige Beschwerde wurden zehn (Vorjahr: eine) **Prüfungen** im öffentlichen und zwölf **Prüfungen** (Vorjahr: zwei) im nichtöffentlichen Bereich begonnen und neue Verfahren eingeleitet; zahlreiche Prüfungen aus dem Vorjahr wurden **fortgeführt**.

Die Zahl von 602 (Vorjahr: 527) **gemeldeten Verletzungen des Schutzes personenbezogener Daten** nach Artikel 33 DSGVO, § 41 LDSG oder § 65 BDSG i. V. m. § 500 StPO (Datenpannen) ist im Vergleich zum Vorjahr wieder signifikant gestiegen. Vielen Verantwortlichen ist die Pflicht zur Meldung von Datenpannen bekannt, dennoch sehen wir auch immer wieder Fälle in unseren Prüfungen, bei denen nicht ordnungsgemäß gemeldet wurde. Wir gehen von einer hohen Dunkelziffer von Fällen aus, in denen die Verantwortlichen der Meldepflicht nicht nachgekommen sind. Die Gründe dafür sind vielfältig: Unkenntnis, Fehleinschätzungen, eine entgegenstehende Fehlerkultur in der Organisation oder auch nur der Glaube daran, dass bestimmt keiner das Malheur bemerken würde.

Von den **Abhilfemaßnahmen** als Reaktion auf festgestellte Verstöße gegen das Datenschutzrecht wurde im Berichtsjahr insgesamt wie folgt Gebrauch gemacht:

- 29 Warnungen (Vorjahr: 28),
- 7 Verwarnungen (Vorjahr: 7),
- 2 Anordnungen zur Änderung oder Einschränkung der Verarbeitung (Vorjahr: 1),
- 3 Geldbußen (Vorjahr: 0).

Nach unserem Eindruck wird die Dienststelle der Landesbeauftragten für Datenschutz in **Gesetzgebungsvorhaben** auf Landesebene weitgehend eingebunden, wenn Aspekte des Datenschutzes oder des Informationszugangs betroffen sein könnten. Dies geschah im Berichtsjahr über die Ministerien parallel zur Anhörung von Verbänden oder über die Ausschüsse im Landtag in 18 (Vorjahr: 12) neuen Gesetzgebungsvorhaben; einige Themen aus Gesetzgebungsvorhaben des Vorjahres wurden auch im Berichtsjahr weiterverfolgt.

1.3 Beschwerde-Dauerbrenner Videoüberwachung

Welcher Anteil an Beschwerden war im Jahr 2024 am größten? Seit mehreren Jahren ist der **ständige Dauerbrenner die Videoüberwachung**: Mehr als 20 Prozent aller Beschwerden betrifft diese Art der Verarbeitung personenbezogener Daten. Im Vergleich zum Jahr 2022 haben sich die absoluten Zahlen der von uns bearbeiteten Beschwerden über Videoüberwachung fast verdoppelt (2022: 191; 2023: 255; 2024: 352).

Ein großer Teil der Beschwerden zu Videoüberwachung bezieht sich auf den **Einsatz von Kameras durch Privatpersonen**, typischerweise in der Nachbarschaft. Über die letzten Jahre beträgt dieser Anteil um die 40 Prozent aller Videoüberwachungsbeschwerden (2022: 40 Prozent, 2023: 49 Prozent, 2024: 39 Prozent, siehe auch 42. TB, Tz. 5.12). Wir vermuten, dass für den Einsatz von Videoüberwachungskameras entscheidend ist, dass sie so **leicht verfügbar** sind: Nicht nur in Fachgeschäften, sondern auch in Discountern vor Ort oder auf Einkaufsplattformen im Internet werden Videoüberwachungskameras für den Außeneinsatz zu recht geringen Kosten angeboten.

Nicht allen, die solche Kameras einsetzen, ist bewusst, dass sie Datenschutzanforderungen erfüllen müssen – jedenfalls soweit nicht nur das eigene Grundstück, sondern der öffentliche

Raum betroffen ist. Wenn sich die Videoüberwachung **ausschließlich auf das eigene, private Grundstück richtet, ohne dass öffentliche Flächen oder benachbarte Grundstücke** erfasst werden, handelt es sich um eine Datenverarbeitung, die einer persönlichen oder familiären Tätigkeit gleichkommt. Auf diese Videoüberwachungsanlagen findet die Datenschutz-Grundverordnung daher gemäß Art. 2 Abs. 2 Buchst. c DSGVO (sogenannte Haushaltsausnahme) keine Anwendung. Erfasst die Videoüberwachung jedoch Bereiche außerhalb des privaten Grundstücks, ist die Datenschutz-Grundverordnung vollständig anzuwenden.

Die meisten Beschwerden in Bezug auf Videoüberwachung durch Privatpersonen stammen von Nachbarn, die sich beobachtet fühlen. Vielfach sind den Beschwerden **Nachbarschaftsstreitigkeiten aus ganz anderen Gründen** vorausgegangen, manchmal hat man einander bereits mit Anzeigen bei der Polizei überzogen. Es wird dann gar nicht erst versucht, ein klärendes Gespräch mit dem Nachbarn zu suchen, der vermeintlich auch Teile des eigenen Grundstücks überwacht, sondern die Betroffenen wenden sich direkt an das ULD.

Wir sind verpflichtet, jeder berechtigten Beschwerde nachzugehen. Sofern ein hinreichend konkreter Verdacht auf einen datenschutzrechtlichen Verstoß besteht, wird ein Verwaltungsverfahren gegen den kamerabetreibenden Nachbarn eröffnet. Hierbei wird er unter Zuhilfenahme eines Fragebogens angehört. Nach Vorlage der erbetenen Stellungnahme wird eine datenschutzrechtliche Bewertung der Videoüberwachung vorgenommen, gegebenenfalls werden vorhandene Anpassungsbedarfe aufgezeigt und die Umsetzung eingefordert. In den meisten Fällen **überwachen die Kamerabetreiber jedoch nur das eigene Grundstück** – auch wenn der Kamerawinkel anderes vermuten lässt.

Entgegen dem oft kommunizierten Wunsch vieler Beschwerdeführenden findet bei Videoüberwachung unter Nachbarn **grundsätzlich keine Prüfung vor Ort** statt. Das ginge in diesen Fällen zumeist auch gar nicht: Uns steht für Privatgrundstücke kein Betretungsrecht zu.

Liefert die Beschwerde keinen konkreten Verdacht auf einen datenschutzrechtlichen Verstoß oder ist von vornherein ersichtlich, dass es sich um eine Datenverarbeitung im rein persönlichen oder familiären Bereich handelt, wird auf die Einleitung eines Verwaltungsverfahrens verzichtet. In diesem Fall erhält die kamerabetreibende Person einen **rechtlichen Hinweis** nach Art. 58 Abs. 1 Buchst. d DSGVO. Die Person, die sich bei uns beschwert hat, erhält ebenso ein informatorisches Schreiben mit rechtlicher Einordnung und dem Verweis auf den Zivilrechtsweg.

Was viele Beschwerdeführende überrascht, ist die Tatsache, dass allein das Vorhandensein einer Kamera noch keinen datenschutzrechtlichen Verstoß begründet. Trotz einer vermeintlichen Ausrichtung der Kamera des Nachbarn auf das eigene Grundstück kann eine **Kamera datenschutzrechtlich zulässig** sein, z. B. wenn Bereiche durch technische Maßnahmen wie Schwärzung oder Verpixelung ausgenommen werden.

Vielfach heißt es, dass die Videoüberwachung aus Gründen der Sicherheit betrieben wird. Für ein **Mehr an Sicherheit** kann es aber besser sein, wenn es ein gutes Miteinander mit den Nachbarn gibt und man im positiven Sinne aufmerksam ist (z. B. wenn man einen Einbruch oder eine Bedrohungslage erkennt) und Bereitschaft zur Hilfe und an einem konstruktiven Miteinander zeigt. Technisch helfen beispielsweise Sicherungen an Fenstern und Türen oder Alarmanlagen. Und wenn Videoüberwachung zum Einsatz kommt, hilft ein direktes klärendes Gespräch oft mehr als das Einschalten von Polizei oder Datenschutzbehörde.

Die Broschüre in unserer **Praxisreihe** „Datenschutzbestimmungen praktisch umsetzen“ zur Videoüberwachung ist hier verfügbar:

https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-5-Videoueberwachung.pdf

Kurzlink: *https://uldsh.de/tb43-1-3a*

1.4 Evaluation und Anpassung der Gesetze zu Datenschutz und Informationsfreiheit

Wir hatten in den vorherigen Tätigkeitsberichten auf die **Evaluierungsklauseln in einigen Gesetzen zu Datenschutz und Informationsfreiheit** hingewiesen (40. TB, Tz. 1.4; 41. TB, Tz. 1.3; 42. TB, Tz. 1.3) und von der Evaluierung des Bundesdatenschutzgesetzes im Jahr 2021 berichtet, die auf die Evaluierung der DSGVO im Jahr 2020 (39. TB, Tz. 1.4) folgte. In Schleswig-Holstein betrifft dies das Landesdatenschutz (LDSG) sowie das Informationszugangsgesetz (IZG-SH).

Nach unseren Informationen wird das **IZG-SH** nunmehr **wissenschaftlich evaluiert**, sodass im Laufe des Jahres 2025 mit Ergebnissen und vielleicht schon Vorschlägen für eine Novellierung zu rechnen ist.

Für das **LDSG** hatte die Regierung bereits vor einiger Zeit Änderungsbedarfe abgefragt. Im letzten Bericht (42. TB, Tz. 1.3) hatten wir optimistisch formuliert, dass die Reform auf Bundesebene – nämlich in Bezug auf das Bundesdatenschutzgesetz (BDSG) – beobachtet und abgewartet werden solle. Dies erschien uns vernünftig. Leider ist die **Novellierung des BDSG** nicht mehr vor der Wahl im Februar 2025 gelungen, sodass der neue Zeitplan auf Bundesebene völlig unklar ist. Die Anpassungsbedarfe, die wir aus unserer Sicht der Praxis einer Aufsichtsbehörde identifiziert haben, haben wir bereits kommuniziert.

Was ist zu tun?

Wir bieten unsere Unterstützung beim Herausarbeiten der Anpassungsbedarfe sowohl beim LDSG als auch beim IZG-SH an.

1.5 Vorsitz der DSK – auch im Jahr 2024

Im Jahr 2023 hatten wir den Vorsitz der Datenschutzkonferenz (DSK) inne. Die Datenschutzkonferenz ist der Zusammenschluss der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Ein zeitlich und natürlich auch inhaltlich erfüllender Job, ein Jahr lang **für die Datenschutzkonferenz sprechen zu dürfen** und sprechen zu müssen. Organisatorisch galt es, die neun Tagungen und 40 Wochenbesprechungen der DSK auszurichten und zu leiten. Es gab viele Diskussionen und vor allem viele Ergebnisse – so wie wir es uns vorgestellt hatten. Damit die Lasten fair verteilt sind, wird der Staffelstab des Vorsitzes nach zwölf Monaten weitergegeben. Im Prinzip gilt: Jedes Land sowie der Bund kommen einmal dran, und zwar im Durchschnitt alle 17 Jahre.

Doch **im Jahr 2024 kam es anders**: Der Vorsitz war zum Jahresbeginn auf die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen übergegangen, Frau Dr. Imke Sommer. Doch bereits im Januar 2024 wurde sie zur Präsidentin des Rechnungshofs der Freien Hansestadt Bremen gewählt. Was tun? Ein Vorziehen des bereits ausgewählten Vorsitzes für das Jahr 2025 kam aus organisatorischen Gründen nicht infrage, da in der dortigen Behörde bereits alle Planungen auf das Folgejahr ausgerichtet waren.

Die DSK reagierte schnell und beschloss einstimmig, den **Vorsitz erneut nach Schleswig-Holstein zu geben**. Schließlich waren wir eingearbeitet und konnten ohne große Anlaufzeiten die Rolle inhaltlich und organisatorisch erneut übernehmen. Wir haben uns der Verantwortung gestellt – ja, sogar sehr gern. Jedoch hatten wir im Jahr 2023 gemerkt, wie viel Zusatzbelastung mit der Vorsitzrolle einhergeht, die zwar mit den

vorhandenen Ressourcen zu stemmen gewesen war. Eine Verlängerung, dazu noch ungeplant, sollte sich aber nach Möglichkeit nicht bis zum Jahresende erstrecken. In dieser Situation bot der Hessische Beauftragte für Datenschutz und Informationsfreiheit an, nach der ersten großen Tagung Mitte Mai den Vorsitz zu übernehmen.

Datenschutzkonferenz

Die Datenschutzkonferenz (DSK) hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Dies geschieht namentlich durch Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen.

Und so wurden wir **ab Ende Januar 2024 wieder Vorsitz der DSK**, nahmen erneut die besonderen Aufgaben wahr und coachten parallel das eilig zusammengestellte Team aus Hessen, um einen geschmeidigen Übergang nach der ersten großen Tagung der DSK im Mai 2024 zu erreichen. Auf diese Weise haben wir den nahtlosen Wechsel vom Bremer Vorsitz über Schleswig-Holstein nach Hessen erreicht. Natürlich standen wir auch in der Folgezeit dem neuen Vorsitz der DSK mit Rat und Tat zur Seite. Laut Geschäftsordnung der DSK waren wir nach Abgabe des Vorsitzes zum ersten stellvertretenden Vorsitz geworden und wurden in dieser Rolle auch dann eingebunden, wenn der Vorsitz verhindert war.

Für das Jahr 2024 hatten wir erwartet, dass das Versprechen aus dem Koalitionsvertrag der früheren Bundesregierung erfüllt werden würde, die Datenschutzkonferenz zu institutionalisieren. Durch den Bruch der Ampelkoalition im November 2024 wurde dieses Unterfangen, für das erste Regeln in einem nicht mehr verabschiedeten Gesetzentwurf zum Bundesdatenschutzgesetz (BDSG) aufgenommen worden waren, erst einmal auf Eis gelegt. Diese Gesetzesänderung hätte dazu geführt, dass die Datenschutzkonferenz – anders als bisher – zu einem Gremium mit **„Pflichtmitgliedschaft" der unabhängigen Datenschutzaufsichtsbehörden** geworden wäre. Wichtiger wäre uns aber eine **ständige Geschäftsstelle** der DSK, die den jeweiligen Vorsitz unterstützt. Wir könnten uns außerdem gut eine technische Plattform bei einer solchen Geschäftsstelle vorstellen, die Verantwortlichen die Möglichkeit bieten soll, Datenpannenmeldungen und Mitteilungen von Datenschutzbeauftragten in einem einheitlichen Format und über eine einheitliche Schnittstelle an die zuständigen Datenschutzaufsichtsbehörden in der DSK weiterzuleiten.

Was ist zu tun?

Unser Wunsch für die Zukunft auf Basis unserer Erfahrungen als DSK-Vorsitz in den Jahren 2023 und 2024: Die Datenschutzkonferenz möge bitte mit einer Geschäftsstelle ausgestattet werden. Damit soll dem Ziel der einheitlichen Rechtsanwendung durch weitere Professionalität Rechnung getragen und eine Steigerung der Kontinuität im Handeln erreicht werden.

02

KERNPUNKTE

Ergebnisse der DSK im Jahr 2024

Die DSK im Dialog

Digitalzwang

Cyberresilienz: Sicherheit by Design

2 Datenschutz und Informationsfreiheit – global und national

Datenschutz und Informationsfreiheit sind nicht nur Themen für Schleswig-Holstein, sondern werden selbstverständlich stark von **Entwicklungen auf nationaler, europäischer und internationaler Ebene** beeinflusst. Diese Entwicklungen gilt es im Blick zu haben. Einige wichtige Themen im Jahr 2024 werden im Folgenden dargestellt.

2.1 Die Ergebnisse der DSK im Jahr 2024 im Überblick

Da wir unsere Rolle als Vorsitz der DSK aus dem Jahr 2023 mehrere Monate lang im Jahr 2024 fortgesetzt haben, waren wir auch in besonderem Maße an der Abstimmung und Veröffentlichung zahlreicher Positionierungen der Datenschutzkonferenz zuständig. Aus der folgenden Liste ist die Vielfalt der Themen ersichtlich, mit denen sich die DSK im Berichtsjahr beschäftigt hat:

- 24.01.2024: Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressent:innen, Version 1.0

  https://www.datenschutzkonferenz-online.de/media/oh/2024-01-24_DSK-OH_Mietinteresse_V1.0.pdf

  Kurzlink: *https://uldsh.de/tb43-2-1a*

- 03.05.2024: Positionspapier zu nationalen Zuständigkeiten für die Verordnung zur künstlichen Intelligenz

  https://www.datenschutzkonferenz-online.de/media/dskb/20240503_DSK_Positionspapier_Zustaendigkeiten_KI_VO.pdf

  Kurzlink: *https://uldsh.de/tb43-2-1b*

- 06.05.2024: Orientierungshilfe zu künstlicher Intelligenz und Datenschutz, Version 1.0

  https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf

  Kurzlink: *https://uldsh.de/tb43-2-1c*

- 14.05.2024: Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 3.1 (Tz. 6.2.2)

  https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V31.pdf

  Kurzlink: *https://uldsh.de/tb43-2-1d*

- 15.05.2024: Entschließung „Besserer Schutz von Patientendaten bei Schließung von Krankenhäusern"

  https://www.datenschutzkonferenz-online.de/media/en/2024-05-15_DSK-Entschliessung_Krankenhausschliessung.pdf

  Kurzlink: *https://uldsh.de/tb43-2-1e*

- 15.05.2024: Positionspapier „Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken"

  https://www.datenschutzkonferenz-online.de/media/dskb/2024-05-15_DSK-Beschluss_Genetische-Daten.pdf

  Kurzlink: *https://uldsh.de/tb43-2-1f*

- 16.08.2024: Orientierungshilfe zur Datenverarbeitung im Zusammenhang mit funkbasierten Zählern, Version 1.0

https://www.datenschutzkonferenz-online.de/media/oh/240816_DSK_OH_Datenverarbeitung_funkbasierte_Zaehler.pdf

Kurzlink: *https://uldsh.de/tb43-2-1g*

- 19.08.2024: Positionspapier „Datenschutzrechtliche Grenzen des Einsatzes von Bezahlkarten zur Leistungsgewährung nach dem Asylbewerberleistungsgesetz (AsylbLG)"

  https://www.datenschutzkonferenz-online.de/media/dskb/2024_08_19_DSK_Beschluss_Bezahlkarte.pdf

  Kurzlink: *https://uldsh.de/tb43-2-1h*

- 11.09.2024: Entschließung „Recht auf kostenlose Erstkopie der Patientenakte kann durch eine nationale Regelung nicht eingeschränkt werden! Datenschutzaufsichtsbehörden sehen konkreten Handlungsbedarf auf Seiten der Heilberufskammern"

  https://www.datenschutzkonferenz-online.de/media/en/2024-09-11_Entschliessung_DSK_Patientenakte.pdf

  Kurzlink: *https://uldsh.de/tb43-2-1i*

- 11.09.2024: Positionspapier „DS-GVO privilegiert wissenschaftliche Forschung"

  https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_DSK_Positionspapier%20_Wissenschaftliche_Forschungszwecke.pdf

  Kurzlink: *https://uldsh.de/tb43-2-1j*

- 11.09.2024: Beschluss: „Übermittlungen personenbezogener Daten an die Erwerberin oder den Erwerber eines Unternehmens im Rahmen eines Asset-Deals"

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

  Kurzlink: *https://uldsh.de/tb43-2-1k*

- 20.09.2024: Entschließung „Vorsicht bei dem Einsatz von Gesichtserkennungssystemen durch Sicherheitsbehörden"

  https://www.datenschutzkonferenz-online.de/media/en/2024-09-20_Entschliessung_DSK_Gesichtserkennung.pdf

  Kurzlink: *https://uldsh.de/tb43-2-1l*

- November 2024: Orientierungshilfe für Anbieter:innen von digitalen Diensten (OH Digitale Dienste), Version 1.2

  https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf

  Kurzlink: *https://uldsh.de/tb43-2-1m*

- November 2024: Orientierungshilfe zu ausgewählten Fragestellungen des neuen Onlinezugangsgesetzes – Anwendungshilfe für Stellen, die (länderübergreifende) Onlinedienste nach OZG betreiben oder nutzen, Version 1.0

  https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_OZG.pdf

  Kurzlink: *https://uldsh.de/tb43-2-1n*

- 19.12.2024: Entschließung „Menschenzentrierte Digitalisierung in der Daseinsvorsorge sicherstellen!"

  https://www.datenschutzkonferenz-online.de/media/en/2024-12-19_DSK-Entschliessung_Menschenzentrierte-Digitalisierung.pdf

  Kurzlink: *https://uldsh.de/tb43-2-1o*

2.2 Die DSK im Dialog

„Nicht über uns reden, sondern mit uns!" – Das könnte das Motto der 2024 eingerichteten Dialoggruppe der DSK sein, die wir leiten. Ihr Ziel ist eine **verbesserte und vertrauensvolle Kommunikation** beispielsweise mit den Interessenvertretungen der Datenschutzbeauftragten in Organisationen. Dabei trifft sich eine kleine Delegation der DSK mit Repräsentantinnen und Repräsentanten dieser Interessenvertretungen.

So organisiert die Dialoggruppe der DSK zur Förderung des Austausches **Dialogtreffen** mit bundesweit agierenden Organisationen, die einen besonderen Bezug zu Datenschutz und den Aufgaben und Tätigkeiten der DSK aufweisen. Zu diesen Organisationen gehören regelmäßig nur **Interessenverbände von betrieblichen oder behördlichen Datenschutzbeauftragten**. Wenn es von beiden Seiten gewünscht ist, können die Dialogtreffen regelmäßig (z. B. einmal jährlich) stattfinden.

Die bisherigen Treffen, die bislang alle in Präsenz stattfanden, waren ein Informationsgewinn für alle Beteiligten. Die Vorteile liegen auf der Hand: Einerseits erfährt die DSK dabei, welche Themen in der **Datenschutzpraxis vor Ort** besonders dringlich sind, andererseits kann sie auch vermitteln, wann etwa mit Leitlinien auf europäischer Ebene oder Orientierungshilfen auf nationaler Ebene zu rechnen ist. **Missverständnisse** lassen sich so im direkten Gespräch klären. Die Dialoggruppe nimmt auch (möglichst konstruktive) **Kritik** auf, um auf die einheitliche Anwendung des europäischen und nationalen Datenschutzrechts hinzuwirken und Verbesserungen in der **praxistauglichen Umsetzung der Datenschutzanforderungen** zu erreichen.

Die DSK hat die Dialoggruppe zunächst bis zum Herbst 2026 eingesetzt. Dann wird evaluiert, ob sie sich als Instrument bewährt hat und ob und in welcher Form sie gegebenenfalls fortgeführt werden soll.

2.3 Menschenzentrierte Digitalisierung in der Daseinsvorsorge

Dass Deutschland **in Sachen Digitalisierung einigen Nachholbedarf** hat, ist wohl unbestritten. Es kommt aber auf das Wie an – Digitalisierung ist kein Wert an sich. In letzter Zeit erreichen uns und die anderen Datenschutzaufsichtsbehörden immer mehr Beschwerden und Anfragen zu Situationen, in denen Menschen ohne Eröffnung eines digitalen Kontos oder ohne Smartphone und installierter App bestimmte Dienstleistungen nicht mehr in Anspruch nehmen können.

Die Datenschutzkonferenz hat sich mit diesem Effekt, der auch als **Digitalzwang** bezeichnet wird, beschäftigt, soweit Leistungen der Daseinsfürsorge betroffen sind. In einer Entschließung bekennen wir uns zu dem Leitbild einer **menschenzentrierten Digitalisierung** als ein wichtiges politisches Ziel in der Europäischen Union. Zugleich ist uns aber wichtig, dass dabei die Grundrechte gewahrt bleiben und auch die Datenschutzgrundsätze aus Artikel 5 DSGVO beachtet werden. Der menschenzentrierte Ansatz drückt aus, dass es einen Schutz derjenigen geben muss, die nicht digital agieren können oder dies nicht wollen. Diese Menschen sollen nicht von Leistungen der Daseinsvorsorge ausgeschlossen werden. Dazu gehören zentrale Verkehrsdienstleistungen, die Energie- oder Wasserversorgung oder auch öffentlich geförderte kulturelle Dienstleistungen.

Betroffen sind z. B. all diejenigen, die aufgrund körperlicher oder geistiger Beeinträchtigung, ihres Alters (Minderjährige ebenso wie Ältere), wegen fehlender Praxisnähe im Umgang mit digitaler Datenverarbeitung (Technikferne) oder unzureichender Mittel nicht in der Lage sind, die digitale Technik zu nutzen – oder die in Ausübung ihres Grundrechts auf Datenschutz ihre Daten nicht preisgeben wollen, denn in den meisten Fällen, die uns bekannt werden, sind mit den Digitallösungen zusätzliche Risiken verbunden. Hier wird besonders deutlich, dass die **Prin-**

zipien von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Data Protection by Design and Default) nach Artikel 25 DSGVO oft nicht umgesetzt werden. Demnach muss der Verantwortliche bereits bei der Planung von Digitalisierungsprojekten, aber auch bei ihrer Realisierung insbesondere geeignete Maßnahmen zur Datenminimierung, aber auch zu allen anderen Datenschutzgrundsätzen treffen.

Die Datenschutzkonferenz hat in einer Entschließung dargestellt, dass man allein mit Mitteln des Datenschutzes keine befriedigenden Lösungen für die Menschen, die wegen fehlender digitaler Möglichkeiten von wichtigen Leistungen der Daseinsvorsorge ausgeschlossen bleiben, erreichen kann. So würde eine gerichtliche Klärung von Einzelfällen zumeist viel zu lange dauern, um eine Teilhabe effektiv zu ermöglichen. Daher fordert die DSK klare **gesetzliche Leitplanken für eine menschenzentrierte Digitalisierung** im Bereich der Daseinsvorsorge.

Die Entschließung „Menschenzentrierte Digitalisierung in der Daseinsvorsorge sicherstellen!" vom 19.12.2024 ist unter dem folgenden Link abrufbar:

https://www.datenschutzkonferenz-online.de/media/en/2024-12-19_DSK-Entschliessung_Menschenzentrierte-Digitalisierung.pdf

Kurzlink: *https://uldsh.de/tb43-2-3a*

Was ist zu tun?

Die Maxime der menschenzentrierten Digitalisierung sollte insbesondere bei der Daseinsvorsorge leitend sein. Dies betrifft die konkrete Gestaltung von Verarbeitungen personenbezogener Daten. Zu überlegen sind auch gesetzliche Leitplanken.

2.4 Cyberresilienz: Sicherheit by Design

Seit Jahren, nein, sogar **seit Jahrzehnten**, sprechen wir von „Datenschutz by Design", bei dem der Datenschutz in die Produkte und Dienstleistungen eingebaut ist. Mit Geltung der Datenschutz-Grundverordnung kam auch das **Prinzip „Datenschutz durch Technikgestaltung"** (englisch: „Data Protection by Design"), das gemäß Artikel 25 DSGVO umzusetzen ist.

Doch in der Praxis vernehmen wir Klagen von Verantwortlichen, dass die **Hersteller** ihrer Produkte nicht den Artikel 25 DSGVO umsetzen, denn sie sehen sich gar **nicht als Verpflichtete** nach der Datenschutz-Grundverordnung. Ja, es stimmt: Artikel 25 DSGVO richtet sich an die Verantwortlichen selbst, nicht an Hersteller. Den Hersteller trifft also keine unmittelbare Pflicht aus der DSGVO, es sei denn, er wird durch eine eigene Verarbeitung von personenbezogenen Daten zu einem Verantwortlichen (oder im Fall von Artikel 28 DSGVO zum Auftragsverarbeiter).

Artikel 25 DSGVO

(1) […] 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 […], 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.

Tatsächlich kommen die Hersteller nur in Erwägungsgrund 78 der DSGVO vor, in dem es heißt, sie sollten „ermutigt werden, das Recht auf

Datenschutz bei der Entwicklung und Gestaltung der Produkte […] zu berücksichtigen". Man streitet sich, was diese **„Ermutigung"** bedeuten soll – jedenfalls handelt es sich nicht um eine direkte Rechtspflicht des Herstellers.

Erwägungsgrund 78 der DSGVO, Satz 4

In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die **Hersteller** der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.

Es gibt aber andere Rechtsnormen, die vom Hersteller bestimmte Zusicherungen verlangen, welche zumindest **einen Beitrag zur Datenschutzkonformität leisten** können. In diesem Zusammenhang wird das **Cyberresilienzgesetz (Cyber Resilience Act, CRA)** interessant, das im Jahr 2024 verabschiedet wurde. Es handelt sich dabei um die erste europäische Verordnung, die Cybersicherheit für Produkte auf dem EU-Markt verlangt, die digitale Elemente aufweisen. Davon sind ebenso Hardwareprodukte mit vernetzten Funktionen (z. B. Smartphones, Router oder vernetzte Küchengeräte) wie Software (z. B. Apps) umfasst.

Kurzum: Hersteller müssen nun für ihre vernetzten Produkte **„Informationssicherheit by Design"** erfüllen. Wie groß das Maß an Sicherheit ist, das der Hersteller gewährleisten muss, hängt vom Risiko ab. Zum einen muss der Hersteller die Umsetzung der Sicherheitsziele für die vorhersehbaren Einsatzzwecke konzipieren, die notwendigen Maßnahmen treffen und dies auch dokumentieren. Zum anderen gehört zu den Anforderungen auch die Einrichtung eines Systems zum Umgang mit Schwachstellen. Ziel ist das Aufrechterhalten des notwendigen Sicherheitsniveaus über den gesamten Lebenszyklus – einschließlich der Bereitstellung nötiger Software-Updates. Dass der Hersteller seinen Pflichten nachkommt, wird durch eine CE-Kennzeichnung der Produkte bestätigt. Diese Produkte werden nach dem Cyberresilienzgesetz künftig eine umfassende **technische Dokumentation** für die Organisationen, die sie einsetzen, bereithalten. Ein Teil der mitgelieferten Informationen wird sich speziell an Nutzende richten, weshalb auf eine möglichst gute Verständlichkeit geachtet werden muss (siehe auch Tz. 8.3). So wird beispielsweise über zu treffende Maßnahmen nicht nur für eine sichere Verwendung ab der Inbetriebnahme und während der gesamten Lebensdauer, sondern ebenfalls für eine sichere Außerbetriebnahme des Produkts einschließlich der sicheren Löschung von etwa gespeicherten (personenbezogenen) Nutzungsdaten informiert – das betrifft **typische Datenschutzrisiken**.

„Sicherheit by Design" wäre ein großer Schritt vorwärts. Noch besser ist jedoch die Erweiterung zu **„Datenschutz UND Sicherheit by Design"**. Und vielleicht wird es eines Tages für die Verantwortlichen viel einfacher sein, die Vorgaben des Artikels 25 DSGVO zu erfüllen – einfach weil sie alle nötigen Informationen endlich direkt vom Hersteller erhalten und in der Entwicklung bereits Datenschutz- und Sicherheitsanforderungen gleichermaßen eingeflossen sind.

Was ist zu tun?

Wir werden die Synergien zwischen den Vorgaben des Cyberresilienzgesetzes und den Datenschutzanforderungen ausloten. Verantwortliche sollten die technische Dokumentation als Grundlage für Entscheidungen zur Auswahl und zum Betrieb von Hardware- und Softwareprodukten bei der Verarbeitung personenbezogener Daten verwenden.

03

KERNPUNKTE

EuGH-Entscheidung zum parlamentarischen Datenschutz

Datenschutzgremium

Service für Abgeordnete zu Datenschutz und Informationsfreiheit

3 Landtag

Der **parlamentarische Datenschutz** lag bisher außerhalb der Zuständigkeit der Landesbeauftragten für Datenschutz – doch ein Urteil des Europäischen Gerichtshofs (EuGH) aus dem Jahr 2024 wirft Fragen auf (Tz. 3.1). Wie bisher auch war die Landesbeauftragte für Datenschutz Gast bei den Sitzungen des **Datenschutzgremiums** des Schleswig-Holsteinischen Landtages (Tz. 3.2). Zusätzlich weisen wir gern auf unser Angebot für Abgeordnete hin, die sich von uns in konkreten Fällen oder zu allgemeineren Themen beraten lassen können (Tz. 3.3).

3.1 EuGH-Entscheidung zum parlamentarischen Datenschutz

Der EuGH hat in zwei Urteilen zur Anwendbarkeit der DSGVO im parlamentarischen Bereich ausgeführt:

- Mit seiner Entscheidung vom 09.07.2020 – C-272/19 erläuterte der EuGH die Anwendung der DSGVO für den Petitionsausschuss eines Landtages. Der Ausschuss hat demnach die Stellung eines datenschutzrechtlich Verantwortlichen gemäß Art. 4 Nr. 7 DSGVO.
- Mit Urteil vom 16.01.2024 – C-33/22 bejahte der EuGH die Anwendung der DSGVO für die Datenverarbeitung eines von einem Parlament eingesetzten Untersuchungsausschusses. Die DSGVO ist vor allem dann nicht anwendbar, wenn die Verarbeitungen im Rahmen einer Tätigkeit erfolgen, welche nicht in den Anwendungsbereich des Unionsrechts fallen. Tätigkeiten eines vom Parlament eines Mitgliedstaats in Ausübung seines Kontrollrechts der Vollziehung eingesetzten Untersuchungsausschusses, die der Untersuchung der Tätigkeiten einer polizeilichen Staatsschutzbehörde aufgrund des Verdachts politischer Einflussnahme auf diese Behörde dienen, sind nach Auffassung des EuGH nicht als die nationale Sicherheit betreffende Tätigkeiten anzusehen, die außerhalb des Anwendungsbereichs des Unionsrechts liegen.

Das Landesdatenschutzgesetz steht hierzu nicht im Widerspruch. Vielmehr wurde mit § 2 Abs. 3 LDSG in Übereinstimmung mit der nunmehr vorliegenden Rechtsprechung des EuGH verdeutlicht, dass die DSGVO auch im parlamentarischen Bereich Anwendung findet. Die gesetzliche Regelung beinhaltet stattdessen eine Ermächtigung, Einzelheiten zur Verarbeitung personenbezogener Daten in **Wahrnehmung parlamentarischer Aufgaben** abweichend von den Bestimmungen des LDSG in einer Datenschutzordnung zu normieren.

§ 2 Abs. 3 LDSG

(3) Der Landtag, seine Gremien, seine Mitglieder, die Fraktionen und deren Beschäftigte sowie die Landtagsverwaltung unterliegen nicht den Bestimmungen dieses Gesetzes, soweit sie in Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten. Der Landtag beschließt insoweit unter Berücksichtigung seiner verfassungsrechtlichen Stellung sowie der Grundsätze der Verordnung (EU) 2016/679 und dieses Gesetzes eine Datenschutzordnung.

In Schleswig-Holstein hat der Landtag bereits seit vielen Jahren eine Datenschutzordnung, in der **spezifische Datenschutzregeln für das Parlament geregelt** sind (Tz. 3.2). Diese Regelungsmöglichkeit ergibt sich aus Art. 6 Abs. 2 und Abs. 3 DSGVO.

Eine andere Frage betrifft die Frage der Datenschutzaufsicht im parlamentarischen Bereich. In

seinem Urteil vom 16.01.2024 – C-33/22 hat der EuGH in diesem Zusammenhang ausgeführt, welche Stelle für die Entscheidung über datenschutzrechtliche Beschwerden zuständig sein soll, wenn nur eine einzige Aufsichtsbehörde existiert. Demnach sind die Bestimmungen der Art. 77 Abs. 1 und Art. 55 Abs. 1 DSGVO dahin auszulegen, dass „diese Bestimmungen, wenn ein Mitgliedstaat, der im Einklang mit Art. 51 Abs. 1 DSGVO bloß eine einzige Aufsichtsbehörde eingerichtet hat, sie aber nicht mit der Zuständigkeit für die Überwachung der Anwendung dieser Verordnung durch einen vom Parlament dieses Mitgliedstaats in Ausübung seines Kontrollrechts der Vollziehung eingesetzten Untersuchungsausschuss ausgestattet hat, dieser Behörde unmittelbar die Zuständigkeit übertragen, über Beschwerden betreffend von diesem Untersuchungsausschuss durchgeführte Verarbeitungen personenbezogener Daten zu befinden".

Art. 51 Abs. 1 DSGVO sieht vor, dass jeder Mitgliedstaat weitere unabhängige Aufsichtsbehörden einrichten kann, die für die Überwachung und Anwendung der DSGVO zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird. Gerade vor diesem Hintergrund kann die Datenschutzaufsicht im parlamentarischen Bereich von einer eigens hierfür eingerichteten und spezifischen Aufsichtsstelle wahrgenommen werden.

Gemeinsam mit den Landesbeauftragten für Datenschutz aus Baden-Württemberg und aus Hessen haben wir die Anforderungen an eine solche **spezifische Aufsichtsstelle** zusammengestellt, die sich aus Artikel 51 ff. DSGVO ergeben:

- Die Aufsichtsstelle muss völlig unabhängig im Sinn des Artikels 52 DSGVO sein.
- Jedes Mitglied der Aufsichtsstelle muss gemäß Artikel 53 DSGVO vom Parlament gewählt sein und über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen.
- Die Regelungen zur Aufsichtsstelle in den spezifischen Regelungen für das Parlament müssen die Themen des Artikels 54 DSGVO umfassen, wie z. B. Fragen zur Amtszeit, zur Wiederernennung und zu Nebentätigkeiten.
- Die Aufsichtsstelle muss nicht mit allen Aufgaben des Artikels 57 DSGVO betraut sein. Es würde ein Verweis auf Art. 57 Abs. 1 Buchst. a bis i DSGVO genügen. Insbesondere müsste die Aufgabe geregelt sein, Beschwerden von betroffenen Personen nachzugehen.
- Die Stelle müsste nicht über alle Befugnisse nach Artikel 58 DSGVO verfügen, jedoch zumindest mit vergleichbaren Befugnissen wie in Art. 58 Abs. 1 (Informationsbefugnisse) und Abs. 2 (Abhilfebefugnisse) DSGVO ausgestattet sein.

Außerdem haben wir überlegt, welche Konzepte sich für die **Ausgestaltung einer Aufsicht für den parlamentarischen Bereich** anbieten könnten. Das könnte eine Person oder ein Kollegialorgan sein: So käme ein internes Modell zur Selbstkontrolle – also ein Gremium aus gewählten Abgeordneten – ebenso infrage wie ein externes Modell, bei dem als Aufsicht eine oder mehrere Personen gewählt würden, die nicht aus den Reihen der aktuellen Abgeordneten stammen, aber das Vertrauen des Parlaments genießen. Derartige honorige Persönlichkeiten könnten im Prinzip auch von mehreren Parlamenten – wenn dies so beabsichtigt und durch Wahl bestätigt ist – als Aufsicht eingesetzt werden, sodass dann eine Zuständigkeit für mehrere Landtage bestünde. Es gibt mehrere Möglichkeiten – die Aufgabe der Ausgestaltung kommt jedenfalls **dem Parlament** zu.

3.2 Datenschutzgremium

Seit vielen Jahren bewährt: das **Datenschutzgremium** des Schleswig-Holsteinischen Landtages. Mehrfach im Jahr tagt das Datenschutzgremium, um Datenschutzthemen im parlamentarischen Bereich zu diskutieren, etwaige Beschwerden zu bearbeiten und sich mit neuen Entwicklungen zu beschäftigten. Die Landesbeauftragte für Datenschutz ist Gast in diesem Gremium.

Das **Datenschutzgremium des Schleswig-Holsteinischen Landtages** überwacht die Einhaltung der datenschutzrechtlichen Bestimmungen, nimmt Beschwerden und Beanstandungen Betroffener entgegen, geht Vorgängen nach, die Anlass zu einer Überprüfung geben, und unterrichtet den Ältestenrat über festgestellte Verstöße. Jede Fraktion ist durch ein Mitglied vertreten, die Beratungen sind vertraulich.

Webseite des Datenschutzgremiums:

https://www.landtag.ltsh.de/parlament/datenschutz-im-parlament/

Kurzlink: *https://uldsh.de/tb43-3-2a*

Basis für die Arbeit des Datenschutzgremiums ist die Datenschutzordnung:

https://www.gesetze-rechtsprechung.sh.juris.de/perma?a=DSO_SH

Kurzlink: *https://uldsh.de/tb43-3-2b*

Die Datenschutzordnung mit spezifischen Datenschutzregeln für den parlamentarischen Bereich stammt aus dem Jahr 1998 und wurde seitdem mehrfach angepasst, zuletzt im Februar 2018. **Geplante Novellierungen**, die aus praktischen Erwägungen und aus einem Anpassungsbedarf an die DSGVO resultieren, sollten die Entscheidungen des EuGH zum parlamentarischen Datenschutz (Tz. 3.1) berücksichtigen. Gerne bietet die Landesbeauftragte für Datenschutz ihre Unterstützung an.

3.3 Service für Abgeordnete in Fragen zu Datenschutz und Informationsfreiheit

Wie jedes Jahr erneuern wir unsere Werbung in eigener Sache: Zusammen mit ihrem Team bietet die Landesbeauftragte für Datenschutz an, dass sich **jede und jeder Abgeordnete vertrauensvoll an das ULD wenden** kann, um Beratung oder Hilfestellung in Fragen des Datenschutzes oder der Informationsfreiheit zu erhalten.

Nach unserer Erfahrung sind die Aufgaben der Abgeordneten vielfältig. Es besteht die tägliche Herausforderung, die anstehenden Themen in ihrer Breite und Tiefe zu durchdringen. Das kann Praxisfragen aus dem Wahlkreis ebenso betreffen wie Ideen für gesetzgeberische Vorschläge. Querschnittsmaterien wie Datenschutz oder der Bereich von Transparenz und Informationszugang hat nicht jede und jeder sofort im Blick. Mit dieser Perspektive können wir in unserer Rolle als **Ansprechstelle für Datenschutz und Informationsfreiheit** dienen.

§ 62 Abs. 1 Nr. 3 LDSG

(1) Die oder der Landesbeauftragte hat neben den in der Verordnung (EU) 2016/679 genannten Aufgaben die Aufgaben, […]

3. den Landtag, die Landesregierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten; […]

Im Vorwort zu diesem Bericht haben wir beschrieben, wie die noch jungen europäischen Digitalrechtsakte mit Leben gefüllt werden müssen und heute insbesondere in Bezug auf Schnittmengen mit der Datenschutz-Grundverordnung noch nicht alles austariert ist. Die europäische Gesetzgebung betrifft auch Schleswig-Holstein und seine Bürgerinnen und Bürger, die Wirtschaft und die Verwaltung unmittelbar. Nun gilt es, bei der Umsetzung der jeweiligen Anforderungen unerwünschte Effekte zu vermeiden. Das wird nach unserer Überzeugung nur dann gut funktionieren, wenn die **verschiedenen Disziplinen und Perspektiven zusammenkommen** und man miteinander kommuniziert.

Unser Interesse ist es, im Austausch mit den Abgeordneten Chancen und Risiken verschiedener Handlungsoptionen zu verstehen und konstruktiv zu praxistauglichen Lösungen für die diskutierten Sachverhalte beizutragen. So werden wir weiterhin alle Fragen der Abgeordneten zu Datenschutz und Informationsfreiheit mit **unserer juristischen und auch informationstechnischen Expertise** sowie auf Basis unserer Erfahrung in der Anwendung der Rechtsnormen beantworten und dem Beratungsbedarf im Rahmen unserer Ressourcen nachkommen.

Was ist zu tun?

Bei Fragen zu Datenschutz und Informationsfreiheit sind die Abgeordneten des Schleswig-Holsteinischen Landtages eingeladen, den Service der Landesbeauftragten für Datenschutz und ihres Teams in Anspruch zu nehmen.

04

KERNPUNKTE

Digitalpaten

INPOL-Abfrage als Standardmaßnahme

Sicherer Transport von Dokumenten

WhatsApp und private Smartphones bei Pflegediensten

Datenpannen im Medizinbereich

Datenschutz- und Medienkompetenz

4 Datenschutz in der Verwaltung

4.1 Allgemeine Verwaltung

4.1.1 Fahrerlaubnisrecht: Vom Löschen, Tilgen und Verwerten

Zugunsten eines Beschwerdeführers konnte in einem Fall vermittelt werden, in dem diesem der Verlust des Führscheins drohte.

Aufgrund eines Fahrradunfalls unter Alkoholeinfluss im Jahr 2022 ermittelte ursprünglich die Staatsanwaltschaft, stellte das Verfahren jedoch bald ein. Ein Jahr später nahm die örtliche zuständige Führerscheinstelle den Vorfall zum Anlass, die Fahreignung des Beschwerdeführers in Zweifel zu stellen, und ordnete ihm an, sich einer **medizinisch-psychologischen Untersuchung (MPU)** zu unterziehen – so weit ein „normaler" Vorgang, den er nicht infrage stellte. In einem solchen Verfahren müssen Betroffene sich eine unabhängige Begutachtungsstelle aussuchen, an die die Behörde ihre Führerscheinakte (oder eine Kopie davon) schickt. Auf Grundlage der darin enthaltenen Vorgeschichte und der Untersuchungen vor Ort geben Gutachterinnen oder Gutachter ihre Stellungnahme zur Fahreignung ab.

Auslöser der Beschwerde waren nun die Aktenvermerke, mit denen der Betroffene im Rahmen der Gutachtenerstellung konfrontiert wurde: Das jüngste Verfahren ging zurück auf die Jahre 2005 und 2006. Selbst eine Trunkenheitsfahrt im Jahr 1992 wurde ihm im Gutachten vorgehalten, das letztlich zu einem negativen Schluss kam. Weswegen die Führerscheinstelle der Begutachtungsstelle so alte Vorgänge mitteilte, war dem Beschwerdeführer unverständlich – zumal er bereits im Jahr 2010 für den Erwerb eines Lkw-Führerscheins zugelassen worden war und dementsprechend von einem „sauberen" Register ausging, was er auch anhand einer aktuellen Auskunft des Kraftfahrtbundesamtes in Flensburg belegen konnte.

Dies war schlüssig, da die meisten Einträge im zentralen Fahreignungsregister, etwa zu Ordnungswidrigkeiten oder Verkehrsstraftaten, nach zweieinhalb oder fünf Jahren getilgt werden. Bei schweren Verstößen kann dies auch zehn Jahre dauern, unter besonderen Umständen sogar 15 Jahre (vgl. § 29 Straßenverkehrsgesetz (StVG)).

Wie ferner die örtlichen Fahrerlaubnisbehörden solche Informationen nutzen dürfen, regelt § 2 StVG. Die **Löschung von Inhalten aus der Führerscheinakte** hat sich dabei an den **Tilgungsfristen für das zentrale Fahreignungsregister** (Tz. 4.2.3) auszurichten:

> **§ 2 Abs. 9 StVG**
>
> Die Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse dürfen nur zur Feststellung oder Überprüfung der Eignung oder Befähigung verwendet werden. Sie sind nach spätestens zehn Jahren zu vernichten, es sei denn, mit ihnen im Zusammenhang stehende Eintragungen im Fahreignungsregister oder im Zentralen Fahrerlaubnisregister sind nach den Bestimmungen für diese Register zu einem früheren oder späteren Zeitpunkt zu tilgen oder zu löschen. […]
>
> Anstelle einer Vernichtung der Unterlagen ist die Verarbeitung der darin enthaltenen Daten einzuschränken, wenn die Vernichtung wegen der besonderen Art der Führung der Akten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Letzterer Satz stellt eigentlich eine Ausnahme vom Grundsatz der Speicherbegrenzung des Art. 5 Abs. 1 Buchst. e DSGVO dar, die das deutsche Verkehrsrecht den Verwaltungen einräumt. Die Vorschrift zielt auf **fortlaufend geführte Papierakten** ab, aus denen sich Inhalte mit jeweils **unterschiedlich langen Löschfristen** eventuell nicht problemlos herausfiltern und entfernen lassen. Nachforschungen bei der zuständigen Führerscheinstelle ergaben, dass man dort teilweise noch mit genau solchen traditionellen Papierakten arbeitete.

Zur Durchführung einer MPU kennt die **Fahrerlaubnisverordnung (FeV)** allerdings für diese besondere Problemstellung eine Lösung:

§ 11 Abs. 6 Satz 4 FeV

Die Fahrerlaubnisbehörde teilt der untersuchenden Stelle mit, welche Fragen im Hinblick auf die Eignung des Betroffenen zum Führen von Kraftfahrzeugen zu klären sind, und übersendet ihr die vollständigen Unterlagen, soweit sie unter Beachtung der gesetzlichen Verwertungsverbote verwendet werden dürfen.

Spätestens beim Versand der Führerscheinakte an eine Begutachtungsstelle muss diese also bereinigt werden. Letztlich wird dadurch ein **Gleichlauf von Tilgungsfristen, Löschregeln und Verwertungsverboten hergestellt**. Welche Folgen ein Versäumnis der Verwaltung an dieser Stelle hat, lässt sich der Rechtsprechung entnehmen (siehe Urteil vom 22.05.2013 im Kasten rechts).

Streng genommen hätte demnach nicht nur die Behörde, sondern auch die Begutachtungsstelle eine **Verfristung** der allermindestens 16 Jahre alten Akteneinträge **eigenständig prüfen und beachten müssen**.

Der Beschwerdeführer konnte eine Lösung jedoch mit Verweis auf die dargestellten Rechtsgrundlagen selbsttätig bei der Führerscheinstelle erwirken. Noch bevor der Anhörungsbescheid des ULD die Verwaltung erreichte, hatte man Abhilfe geschaffen: Der Betroffene bekam eine Fristverlängerung für die Absolvierung der MPU und seine Kosten für das erste, unbrauchbare Gutachten wurden ihm erstattet.

Oberverwaltungsgericht Greifswald, Urteil vom 22.05.2013 (1 M 123/12)

Bleiben versehentlich nicht verwertbare Unterlagen bei der der Untersuchungsstelle übermittelten Akte, ist dies schlicht rechtswidrig bzw. steht in Widerspruch zu § 11 Abs. 6 Satz 4 FeV. Derartige Fehler gehen grundsätzlich ohne Weiteres zulasten der Behörde, mittelbar dadurch, dass sie – wie vorliegend – die Nichtverwertbarkeit des auf der Grundlage solchermaßen fehlerhafter Unterlagen erstellten Gutachtens nach sich ziehen. […]

Das gesetzliche Verwertungsverbot […] greift auf jeder Stufe des Verfahrens betreffend die Beurteilung der Eignung des Antragstellers: Auch der Gutachter darf die betroffene Tat und Entscheidung dem Betroffenen nicht mehr vorhalten bzw. zu seinem Nachteil verwerten.

Im Nachgang gestand die Behörde den Fehler dem ULD gegenüber unumwunden ein. Aufgrund mangelnder Sorgfalt war in der Sachbearbeitung eine Bereinigung der Unterlagen unterblieben, obwohl die Rechtslage eigentlich bekannt war. Mit der gegenwärtig laufenden **Umstellung auf elektronische Akten** konnte die **Führerscheinstelle** aber auch eine positive Perspektive aufzeigen: Durch Hinterlegung von Löschfristen zu jedem einzelnen Dokument werde man eine **überlange Aufbewahrung von nicht mehr verwertbaren Bestandteilen der Führerscheinakten** in Zukunft **technisch ausschließen**.

Was ist zu tun?

In bestimmten Rechtsgebieten kann an die Stelle einer Löschung unter Umständen ein Verwertungsverbot treten. Beim Umgang mit solchen Daten ist besondere Vorsicht geboten, da deren Nutzung leicht zu einer unrechtmäßigen Benachteiligung Betroffener führen kann.

Wo immer sich eine vollständige Löschung umsetzen lässt, ist diese grundsätzlich vorzuziehen.

4.1.2 Stilllegung eines Fahrzeugs aufgrund einer Verwechslung

Ähnlich dramatisch stellte sich ein weiterer Beschwerdefall mit verkehrsrechtlichem Bezug dar, wenn auch nicht im ersten Moment. Diesmal ging es nicht um eine Fahrerlaubnis, sondern um eine **Fahrzeugzulassung**. Auch für diesen Zweck greifen die örtlichen Behörden auf ein zentrales Register zurück:

§ 32 Abs. 1 StVG

Die Fahrzeugregister werden geführt zur Speicherung von Daten

1. für die Zulassung und Überwachung von Fahrzeugen nach diesem Gesetz oder den darauf beruhenden Rechtsvorschriften,

2. für Maßnahmen zur Gewährleistung des Versicherungsschutzes im Rahmen der Kraftfahrzeughaftpflichtversicherung,

3. für Maßnahmen zur Durchführung des Kraftfahrzeugsteuerrechts,

4. […]

Die Beschwerdeführerin bemängelte zunächst lediglich, einen falschen Bescheid erhalten zu haben: So war sie zwar Adressatin der förmlichen Zustellung. Inhaltlich richtete sich der Bescheid über die zwangsweise Stilllegung eines Fahrzeugs jedoch an einen völlig Fremden, mit Angaben zu dessen Auto und abgelaufenem Versicherungsschutz. Insoweit hätte es sich – schlimm genug – nur um eine Offenbarung an eine Unbefugte gehandelt, also um eine Verletzung des Schutzes personenbezogener Daten. Auf den Hinweis des Fehlers durch die Adressatin per E-Mail habe die Zulassungsstelle beim Landkreis nicht reagiert.

Auf telefonische Nachfrage des ULD bei der Meldenden stellte sich heraus: Die Verwechslung hatte für sie noch ganz andere Folgen. Die Zulassungsstelle hatte das Ordnungsamt der Amtsverwaltung vor Ort beauftragt, das Kennzeichen der Beschwerdeführerin zu entsiegeln und somit **das Fahrzeug stillzulegen**. Grundsätzlich können die **Zulassungsstellen** zur Durchführung von Maßnahmen auch Daten an örtliche Behörden übermitteln (vgl. § 35 Abs. 1 Nr. 1 StVG). Nur wurden hier anscheinend die völlig falschen Daten übermittelt. Weder von dem fehlerhaften Bescheid noch von einer Bestätigung der Kfz-Versicherung über den weiter bestehenden Versicherungsschutz hätten die Ordnungskräfte sich beirren lassen. Und auch weitere Versuche, beim Landkreis jemanden zu erreichen, blieben erfolglos.

In der Hauptsache waren hier **zulassungs-, versicherungs- und vor allem verfahrensrechtliche Probleme maßgebend**. Worin bestand also hier der Ansatzpunkt, mit Mitteln des Datenschutzrechts vorzugehen? In Verwechslungsfällen – wie hier geschehen – lässt sich aus der DSGVO der Grundsatz der Richtigkeit heranziehen:

Art. 5 Abs. 1 Buchst. d DSGVO

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit").

Um in der verworrenen Situation Abhilfe zu schaffen, konnte kurzerhand auf die Unterstützung des Datenschutzbeauftragten der Kreisverwaltung zurückgegriffen werden: Denn dieser war in der Lage, unkompliziert den Kontakt zum Fachdienstleiter der Zulassungsstelle herzustellen.

Die Behörde erkannte endlich ihren eigenen Fehler und veranlasste die Rückabwicklung der Folgen: Die Beschwerdeführerin sollte umgehend eine neue Zulassungsplakette erhalten. Eine Benachrichtigung des eigentlichen Adressaten des Bescheids über die unbefugte Offenbarung seiner Daten wurde uns ebenfalls zugesagt.

Was ist zu tun?

Der Grundsatz der Richtigkeit wird von Datenschützerinnen und Datenschützern nicht ganz so häufig bemüht wie etwa die Prinzipien der Zweckbindung, der Datenminimierung oder der Vertraulichkeit. Dieser Fall zeigt jedoch: Manchmal sind es gerade unrichtige Daten, die die ärgerlichsten Folgen nach sich ziehen.

Hinweise auf falsche Angaben müssen von Verantwortlichen gegebenenfalls als Anträge auf Berichtigung nach Artikel 16 DSGVO aufgefasst und unverzüglich untersucht werden.

4.1.3 Digitalpaten und Datensicherheit

Mit dem Projekt einer Digitalpatenschaft hat ein Kreis sich für die **Verbreitung digitaler Kompetenzen** eingesetzt und hierfür **ehrenamtliches Engagement** in der Bevölkerung geweckt. Digitalpaten haben demnach die Aufgabe, Privatpersonen etwa bei der Einrichtung von Apps auf dem Smartphone, der Erläuterung von Programmanwendungen oder der Vornahme von Tablet-Einstellungen zu unterstützen. Hierzu erhielten wir einen Hinweis in Verbindung mit der besorgten Nachfrage eines Bürgers, da es sich bei den ehrenamtlich tätigen Personen auch um solche handeln könne, die unredliche Motive verfolgen. Schnell hat man sich ein fremdes Passwort gemerkt, um dann gerade die fehlende Praxis und die Unkenntnis bei älteren Leuten zu nutzen, um kriminelle Handlungen auszuführen.

Daraufhin hat das ULD bei dem Kreis nähere Auskünfte eingeholt. Zunächst konnte der Kreis klarstellen, dass er für die Datenverarbeitung im Rahmen der Digitalpatenschaft **als datenschutzrechtlich Verantwortlicher** auftritt. Weiterhin erfolgte die Erarbeitung mehrerer Dokumente, welche die ehrenamtlichen Digitalpaten unterzeichnen und zur Kenntnis nehmen müssen. Im Einzelnen:

- In einem Formular soll der Digitalpate eine **Selbstauskunft** geben und erläutern, für welche konkreten Endgeräte und Betriebssysteme eine Beratung übernommen wird. Hierzu zählen auch Angaben zur beabsichtigten Einrichtung, Installation und Nutzung von Apps oder Näheres zur Einrichtung eines Internetzugangs. Weiterhin sind in dem Formular etwa die Einrichtung von E-Mail-Konten, die Teilnahme an Videokonferenzen und das Onlinebanking erwähnt. Schließlich sollte der Digitalpate auf dem Formular versichern, dass allgemein **keine Vorstrafen bestehen und kein Straf- oder Ermittlungsverfahren anhängig ist**.
- Zu unterzeichnen ist eine **Verpflichtung auf Vertraulichkeit, Verschwiegenheit und die Einhaltung des Datenschutzes**.
- Digitalpaten müssen ferner eine Verpflichtung zur Einhaltung von Datenschutzgrundsätzen unterschreiben. In einem beigefügten Merkblatt wird näher ausgeführt, was Digitalpaten beachten sollen.

Auf unsere Nachfragen und Hinweise hin hat der Kreis im Rahmen der Selbstauskunft Anpassungen vorgenommen. Hinsichtlich laufender Strafverfahren ist zu berücksichtigen, dass zunächst die Unschuldsvermutung gilt. Bezüglich der Vorstrafen wird im Rahmen der Digitalpatenschaft mehr von Bedeutung sein, ob eine Person wegen Vermögens- oder Eigentumsdelikten in Erscheinung getreten und daher für die Beratung ungeeignet ist. Bezüglich der Einrichtung von Konten, etwa einem E-Mail-Konto, und der Unterstützung beim Onlinebanking versicherte der Kreis, dass die Digitalpaten hierzu **sensibilisiert** werden, dass zum Schutz der Hilfe suchenden Personen als auch zu deren Eigenschutz **keine schutzbedürftigen Informationen abgefragt, eingesehen oder eingegeben werden dürfen**. Dies gelte gerade bezüglich der Eingabe von Passwörtern, PINs oder sonstigen sensiblen Informationen. Speziell beim **Onlinebanking** beziehe sich die Hilfestellung durch die Digitalpaten darauf, erforderliche Grundfertigkeiten zu vermitteln und dabei zu erläutern, welche Geräte und welche Informationen für eine Teilnahme und Nutzung erforderlich sind. Auch die Einrichtung soll begleitet werden. Die Dateneingabe müsse aber von den Hilfesuchenden eigenständig und allein bewältigt werden. Den Digitalpaten sei demnach nur eine **Moderatorenrolle** zugewiesen. Auch die Hilfesuchenden selbst wolle der Kreis im Umgang mit den Digitalpaten sensibilisieren und auf Vorsichtsmaßnahmen, wie etwa den Umgang mit Zugangsdaten, hinweisen.

Dem Kreis wurde insbesondere geraten, die Einrichtung des Onlinebankings **nicht durch ehrenamtliche Digitalpaten** erledigen zu lassen. Empfohlen wurde auch die **Gestaltung von Hinweisblättern für die Digitalpaten und die Hilfesuchenden** mit der Auflistung des Leistungs- und Unterstützungsumfangs, um auch eine Abgrenzung zu ermöglich, was im Einzelfall nicht Gegenstand der konkreten Beratung sein soll. Der Kreis hat die Umsetzung der Ratschläge und Empfehlungen zugesagt. Abschließend hat das ULD nochmals darauf hingewiesen, dass der Kreis für eine mögliche Datenverarbeitung der Digitalpaten verantwortlich bleibt. Hierzu zählt vor allem die **Einhaltung aller technischen und organisatorischen Maßnahmen zur Einhaltung der Datensicherheitsvorgaben**, Artikel 32 DSGVO.

Was ist zu tun?

Ehrenamtliches Engagement bei der Vermittlung digitaler Kompetenzen ist wertvoll. Ebenso ist die Gewährleistung der Datensicherheit ein hohes Gut. Im Rahmen der Projektumsetzung für eine Digitalpatenschaft sind geeignete Vorkehrungen zu treffen, damit Hilfesuchende keine sensiblen personenbezogenen Daten preisgeben und damit keine unbefugte Verarbeitung durch Digitalpaten erfolgt.

4.1.4 Dauerhafte Speicherung der Ausleihhistorie in Stadtbücherei

Aufgrund einer Beschwerde prüfte das ULD den Umgang mit Nutzerdaten in einer Bücherei. Im Fokus stand die **Speicherung von Ausleihhistorien**. Entsprechende Daten geben über das Leseverhalten, die Dauer einer Ausleihe und die über ausgeliehene Werke Auskunft und ermöglichen so einen vertieften Einblick in die Lesegewohnheiten und -interessen. Für die Verarbeitung dieser Daten bedarf es einer spezifischen Rechtsgrundlage, welche die Bücherei im eingeleiteten Prüfverfahren nicht vorweisen konnte.

Im laufenden Verfahren hat die Stadtbücherei zunächst Änderungen im Ausleihprozess vorgenommen. Demnach könne die Ausleihhistorie von Nutzenden nicht mehr von den Beschäftigten der Stadtbücherei eingesehen werden. Nutzende erhielten im persönlichen Onlinebereich eine Meldung zur Speicherung der Ausleihhistorie, wobei sie der Speicherung widersprechen könnten. Weiterhin müssten die Nutzenden aber auch aktiv widersprechen, da anderenfalls eine Speicherung der Ausleihhistorie erfolge. Zu berücksichtigen sei, dass viele Nutzende wollen, dass ihre Ausleihhistorie gespeichert wird. Im letzteren Fall würde eine Datenlöschung im Jahresrhythmus durchgeführt.

Losgelöst hiervon gelang es der Kommune nicht, für die Speicherung der Ausleihhistorie eine rechtliche Basis zu benennen. Das ULD hat daher die Stadtbücherei auf folgende Punkte hingewiesen:

- Es darf **keine standardmäßige Speicherung** von nutzerbezogenen Ausleihhistorien erfolgen.
- Es dürfen buchbezogen **keine Benutzerkennungen und Namen vergangener Ausleihen**, mit Ausnahme des Namens des letzten Ausleihers, gespeichert werden. Auf diese Weise kann bei Beschädigung der letzte Ausleihvorgang namentlich nachvollzogen werden. Es dürfen aber für statistische Zwecke Anzahl und Datum der Ausleihvorgänge erfasst werden.
- Eine Ausblendung der Angaben für Nutzer und Bibliothekspersonal reicht nicht aus. Diese Daten dürfen nicht in der Datenbank gespeichert werden.

Abweichungen sind in folgender Form denkbar:

- Daneben können Nutzende **einwilligungsbasiert** eine Speicherung der Ausleihhistorie aktivieren. Dies kann auch die Sichtbarmachung dem Bibliothekspersonal gegenüber, etwa bei einem Service-Check, beinhalten. Standardmäßig, etwa bei der Anlage neuer Nutzerkonten, muss die Speicherung aber **deaktiviert** sein.
- Im Fall, bei der eine Ausleihhistorie bisher noch standardmäßig gespeichert wird, ist es ausreichend, prominent (z. B. über ein Banner beim Log-in) auf die Deaktivierungsmöglichkeit hinzuweisen. Dies gilt für jene Personen, die für die Vergangenheit eine Speicherung der Ausleihhistorie wünschten.
- Entscheiden sich die Nutzenden später für einen Widerruf der Einwilligung, müssen die Ausleihhistorien auch für die Vergangenheit gelöscht werden.

Mit den entsprechenden Hinweisen zur Änderung der Systemeinstellungen konnte das Prüfverfahren gegenüber der Stadtbücherei beendet werden.

4.1.5 Aufforderung einer Gemeinde zur Einholung einer Finanzierungszusage in der Phase der Interessenbekundung

Das ULD wurde um eine datenschutzrechtliche Einschätzung gebeten, ob das Vorgehen einer Gemeinde, eine **Finanzierungszusage in der Phase der Interessenbekundung** bzw. unmittelbar nach deren Einholung anzufordern, zulässig sei. Dazu wurde mitgeteilt, dass die Gemein-

de ein bestimmtes Gebiet als Bauland plane und Bürger Interessenbekundungen für den Erwerb von Grundstücken haben abgeben können, die in diesem Gebiet lägen. Nach Abgabe dieser Interessenbekundungen habe die Gemeinde die Interessenten aufgefordert, eine Finanzierungszusage vorzulegen. Das Gebiet sei zu diesem Zeitpunkt in der Planung gewesen.

Für das ULD ergaben sich auf der Basis des herangetragenen Sachverhalts in Bezug auf die Frage, ob der Zeitpunkt der Abfrage aus datenschutzrechtlicher Sicht zulässig war, folgende Erwägungen:

Bei der Aufforderung, die Finanzierungszusage einzureichen, handelt es sich um eine beabsichtigte **Erhebung von personenbezogenen Daten, die einer Rechtsgrundlage bedarf**. Ob die Erhebung zu einem derartigen frühen Zeitpunkt möglicherweise auf eine kommunale Satzung oder aber auf spezialgesetzliche Regelungen aus dem Bauplanungsrecht o. Ä. gestützt werden konnte, war für das ULD mangels weiterer Sachverhaltsangaben nicht ersichtlich. Aus demselben Grunde war nicht abschließend zu bewerten, ob die unmittelbar nach Abgabe der Interessenbekundung geforderte Beibringung der Finanzierungszusage auf allgemeine datenschutzrechtliche Vorschriften § 3 Landesdatenschutzgesetz in Verbindung mit einer aufgabenzuweisenden Norm bzw. Art. 6 Buchst. c bis e DSGVO in Verbindung mit einer aufgabenzuweisenden Norm zu stützen war. Um die in dieser Phase geplante Erhebung auf eine dieser allgemeinen datenschutzrechtlichen Vorschriften stützen zu können, muss diese erforderlich sein. Aus Sicht des ULD war ohne nähere Kenntnis von den tatsächlichen Umständen nicht ersichtlich, ob die Finanzierungszusage konkret zu dem betreffenden Zeitpunkt erforderlich gewesen ist.

Zum einen kann sich die Situation bis zu dem Zeitpunkt des Abschlusses eines Kaufvertrags über ein konkretes Grundstück ändern und von der ehemals abgegebenen Interessenbekundung muss Abstand genommen werden. Gründe dafür können z. B. in geänderten privaten Lebensverhältnissen oder der finanziellen Situation liegen. Zum anderen kann aufgrund geänderter Umstände ein Erwerb zu einem späteren Zeitpunkt möglich sein, der in der frühen Planungsphase noch nicht möglich war, sodass eine Interessenbekundung damals nicht sinnvoll gewesen wäre. Vor diesem Hintergrund erscheint die Forderung nach der Vorlage einer Finanzierungszusage in dem erwähnten Zeitpunkt **kein geeignetes Mittel**, um die „nicht infrage kommenden" Interessenten gegebenenfalls aus dem Verfahren auszuschließen.

Hinzu kommt, dass sich die Frage stellt, mit welchem Inhalt eine **Finanzierungszusage seitens der Bank** zu diesem frühen Zeitpunkt überhaupt erteilt werden kann. Davon ausgehend, dass in dem geschilderten Fall mangels Erschließung noch keinerlei Preisvorstellungen im Raum standen, hätte die Bank insoweit „wenig Anhaltspunkte" für die Prüfung, ob eine derartige Zusage erteilt werden sollte. In Betracht käme daher allenfalls eine relativ allgemein gehaltene Finanzierungszusage, bei der die Reichweite der rechtlichen Verbindlichkeit angesichts noch ungeklärter Prüfparameter zu klären wäre. Vor diesem Hintergrund stellt sich einmal mehr die Frage nach der Erforderlichkeit, diese Zusage zu dem betreffenden Zeitpunkt abzufordern.

Letztendlich ist auch zu berücksichtigen, dass in ähnlich gelagerten Fallkonstellationen entsprechende Nachweise über die Liquidität erst zu einem wesentlich späteren Zeitpunkt abgefragt werden dürfen. Dies ergibt sich auch aus der Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 24.01.2024 zur Einholung von Selbstauskünften bei Mietinteressenten (Ziffer A., C. 2., 3.), die unter dem folgenden Link abrufbar ist:

https://www.datenschutzkonferenz-online.de/media/oh/2024-01-24_DSK-OH_Mietinteresse_V1.0.pdf

Kurzlink: *https://uldsh.de/tb43-4-1-5a*

Was ist zu tun?

Die Verarbeitung von personenbezogenen Daten bedarf einer Rechtsgrundlage. Der Verantwortliche hat zu prüfen, ob die Anforderungen der gegebenenfalls in Betracht kommenden Rechtsgrundlage zu dem Zeitpunkt der Verarbeitung der personenbezogenen Daten auch tatsächlich vorliegen.

4.1.6 Vollstreckung einer Kommune für Forderungen des NDR

Das ULD wurde von einem Amt um eine datenschutzrechtliche Einschätzung im Zusammenhang mit der **Vollstreckung ausstehender Rundfunkbeiträge** gebeten.

Konkret ging es darum, dass der NDR an das Amt mit der Bitte herangetreten war, wegen ausstehender Rundfunkgebühren zu vollstrecken. Die betroffene Person, der Schuldner, hatte gegen dieses geplante Vorgehen eingewandt, die mit der Vollstreckung einhergehende Verarbeitung seiner personenbezogenen Daten bedürfe seiner Einwilligung.

Die Verarbeitung der personenbezogenen Daten von Schuldnerinnen und Schuldnern zum Zwecke der Durchführung der Vollstreckung bedarf einer Rechtsgrundlage. Sofern sich eine öffentlich-rechtliche Rundfunkanstalt, d. h. eine Anstalt des öffentlichen Rechts, gemäß § 10 Abs. 6 Rundfunkbeitragsstaatsvertrag (RBStV) mit einem Vollstreckungsauftrag an die zuständige Vollstreckungsbehörde wendet, führt diese die Vollstreckung in Wahrnehmung eigener Aufgaben durch (vgl. die gemäß § 263 Abs. 1 LVwG i. V. m. § 1 Abs. 1 Ziffer 4 Landesverordnung über die zuständigen Vollstreckungsbehörden übertragene Zuständigkeit), vgl. auch den Sachstandsbericht des Wissenschaftlichen Dienstes des Deutschen Bundestages 2024 „Vollstreckung von Rundfunkbeitragsforderungen", abrufbar unter dem folgenden Link:

https://www.bundestag.de/resource/blob/994364/f7ab5df9acb5a01c8708b553031d0119/WD-7-001-24-pdf.pdf

Kurzlink: *https://uldsh.de/tb43-4-1-6a*

Die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten durch die zuständige Vollstreckungsbehörde ist somit in derartigen Fällen Art. 6 Abs. 1 Buchst. c, e DSGVO i. V. m. § 10 Abs. 6 RBStV i. V. m. § 263 Abs. 1 Nr. 1, 3 bzw. 4 LVwG i. V. m. § 12 LVwG i. V. m. § 1 Abs. 1 Nr. 4 Landesverordnung über die zuständigen Vollstreckungsbehörden i. V. m. §§ 269 ff. LVwG. Die Zulässigkeit der jeweiligen Vollstreckungshandlung unterliegt dabei den gesetzlichen Anforderungen an die konkrete Vollstreckungshandlung gemäß §§ 269 ff. LVwG (vgl. auch die Beschlüsse des Verwaltungsgerichts Schleswig vom 04.02.2019, 4 B 96/18 und vom 05.01.2021, 4 B 45/20, in denen das Gericht feststellt, dass sich die Zulässigkeit der Vollstreckung von Rundfunkbeiträgen (und Säumniszuschlägen) nach den §§ 262 ff. LVwG richtet). **Einer Einwilligung der betroffenen Person bedarf es somit nicht.**

Was ist zu tun?

Die Vollstreckung ausstehender Rundfunkgebühren durch die zuständige Vollstreckungsbehörde bedarf keiner Einwilligung durch den Schuldner. Die damit einhergehende Verarbeitung personenbezogener Daten beruht auf einer gesetzlichen Rechtsgrundlage.

4.1.7 Datenschutzbeauftragte in Kindertagesstätten

Das ULD wurde um die datenschutzrechtliche Einschätzung dahin gehend gebeten, ob für **private Kindertagesstätten** grundsätzlich eine Verpflichtung besteht, einen Datenschutzbeauftragten zu benennen.

Anders als bei Kindertagesstätten in kommunaler Trägerschaft, für die ausnahmslos gemäß Art. 37 Abs. 1 Buchst. a DSGVO die Pflicht besteht, einen Datenschutzbeauftragten zu benennen, besteht für private Kindertagesstätten nur dann die Verpflichtung, einen Datenschutzbeauftragten zu benennen, wenn

- die Kerntätigkeit des Verantwortlichen (in diesem Fall die Kindertagesstätte) in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche und systematische Überwachung von betroffenen Personen erforderlich machen (Art. 37 Abs. 1 Buchst. b DSGVO), oder
- die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht (Art. 37 Abs. 1 Buchst. c DSGVO).

Unabhängig von diesen Anforderungen besteht nach § 38 Abs. 1 Satz 1 BDSG für private Kindertagesstätten die Verpflichtung, einen Datenschutzbeauftragten zu benennen, wenn „in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten" beschäftigt sind.

Was die erste Fallgruppe betrifft („Kerntätigkeit"), vertritt das ULD in Abweichung zu der noch im Jahre 2018 (37. TB, Tz. 5.4.3) dargelegten Einschätzung nunmehr die Auffassung, dass die in Kindertagesstätten über die Kinder ausgeübte Aufsicht in der Regel **nicht mit einer umfangreichen, systematischen und regelmäßigen (digitalen) Verarbeitung/Überwachung verbunden ist**.

Diese Bewertung trägt den von der (früheren) Artikel-29-Datenschutzgruppe in Bezug auf Datenschutzbeauftragte entwickelten Leitlinien (WP 243) Rechnung: Die in diesen Leitlinien unter Ziffer 2.1.3, 2.1.4 (Seite 9, 10) aufgeführten Beispiele zeigen auf, dass die unter Art. 37 Abs. 1 Buchst. b DSGVO fallende umfangreiche und systematische Verarbeitung/Überwachung eine andere Eingriffstiefe aufweist als die, die mit der üblichen Aufsichtstätigkeit in Kindertagesstätten einhergeht. In Kindertagesstätten werden Kinder beaufsichtigt; gewöhnlich ist damit jedoch keine umfangreiche, regelmäßige und systematische (digitale) Überwachung verbunden. Eine andere Bewertung ergibt sich auch nicht unter Berücksichtigung der frühkindlichen Entwicklung der Kinder (gegebenenfalls durch Heilpädagogen). Erfahrungsgemäß ist auch insoweit in der Regel keine ständige, regelmäßige bzw. umfangreiche Dokumentation der frühkindlichen Entwicklung zu verzeichnen, sondern anlassbezogen (bei „Auffälligkeiten") und/oder punktuell (z. B. um Entwicklungsfortschritte festzuhalten).

In Übereinstimmung mit anderen Aufsichtsbehörden ist davon auszugehen, dass in privaten Kindertagesstätten, in denen in der Regel unter 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, gewöhnlich kein Datenschutzbeauftragter zu benennen ist.

Die private Kindertagesstätte ist gehalten zu prüfen, ob unter Berücksichtigung der zuvor aufgezeigten Anforderungen ein Datenschutzbeauftragter zu benennen ist. Ferner sollte zur **Einhaltung der Rechenschaftspflicht** (Art. 5 Abs. 2 DSGVO) Folgendes dokumentiert werden:

- die Tatsache, dass in Anlehnung an die Anforderungen nach Art. 37 Abs. 1 Buchst. b, c DSGVO und § 38 Abs. 1 Satz 1 BDSG geprüft wurde, ob ein Datenschutzbeauftragter benannt werden muss, und
- die Gründe, die in Anlehnung an die Anforderungen nach Art. 37 Abs. 1 (gegebenenfalls) gegen eine Benennungspflicht sprechen (vgl. Art. 5 Abs. 2 DSGVO).

Was ist zu tun?

Für private Kindertagesstätten ist in der Regel kein Datenschutzbeauftragter zu benennen. Zur Einhaltung der Rechenschaftspflicht sollten sowohl die Prüfung, ob ein Datenschutzbeauftragter zu benennen ist, als auch die (gegebenenfalls) dagegensprechenden Gründe dokumentiert werden.

4.1.8 Ganztagsbetreuung: Datenverarbeitungen auf Grundlage kommunaler Satzungen

Unmut zog eine Kommune auf sich, die sich im Rahmen der Ganztagsbetreuung von Kindern an ihren städtischen Grundschulen entschloss, die Eltern **zur Einholung einer Bescheinigung über ihre Berufstätigkeit** von deren Arbeitgebern aufzufordern.

Zum Hintergrund: Der Rechtsanspruch auf Ganztagsbetreuung für Kinder im Grundschulalter wurde bereits zum Ende der letzten Legislaturperiode vom Bundesgesetzgeber beschlossen, wird aber erst ab 2026 schrittweise eingeführt werden (Art. 7 Abs. 4 Ganztagsförderungsgesetz). Zwar können Schulträger in Schleswig-Holstein für entsprechende Betreuungsangebote auch heute schon Fördermittel des Landes beantragen (vgl. Richtlinie „Ganztag und Betreuung" des Bildungsministeriums), aber die Entscheidung, ob sie diese einrichten oder nicht, liegt gegenwärtig noch bei ihnen selbst.

Zugleich sind die Schulträger mit einer steigenden Nachfrage nach solchen Angeboten konfrontiert, sodass es nicht überall gelingt, allen an einem Betreuungsangebot interessierten Eltern einen Platz zuzusagen. Die betreffende Kommune hatte in der Vergangenheit freie Plätze nach dem Zeitpunkt der Anmeldung vergeben (sogenannte „Windhundverfahren") und dies auch so in einer Benutzungs- und Gebührensatzung im Sinne von § 4 Abs. 1 Gemeindeordnung festgehalten. Man sah sich nach dieser Verfahrensweise aber zunehmend schlechter in der Lage, dem eigens formulierten Anspruch einer Vereinbarkeit von Beruf und Familie gerecht zu werden. So entschied sich die Stadt, die Platzvergabe fortan von der **Berufstätigkeit der Eltern abhängig zu machen** (gewissermaßen **eine Form der „Sozialauswahl"**) und diese auch zu kontrollieren.

Ein betroffener Vater erhob angesichts des weitreichenden Umfangs von Daten, die ihm nunmehr sein Arbeitgeber bestätigen sollte, Beschwerde. Gefordert wurden z. B. Detailangaben zu täglichen Arbeitszeiten oder einer etwaigen Befristung. Es stellte sich die Frage nach der Rechtsgrundlage für diese Erhebungen.

Öffentliche Stellen müssen eine Verarbeitung personenbezogener Daten in den allermeisten Fällen auf ihre spezifischen gesetzlichen Pflichten oder allgemeiner gefasste Ermächtigungen zur Erledigung ihrer Aufgaben (Art. 6 Abs. 1 Buchst. c bzw. Buchst. e DSGVO) stützen können. Die entsprechenden Vorschriften können im europäischen Recht selbst verankert sein, finden sich aber viel häufiger im sogenannten „Recht der Mitgliedstaaten". Dabei ist Folgendes zu beachten:

Das **„Recht der Mitgliedstaaten"** bestimmt sich nach Erwägungsgrund 41 der DSGVO. Demnach genügt eine verbindliche Regelung, die kein von einem Parlament angenommener Gesetzgebungsakt sein muss. Ausreichend sind z. B. auch Rechtsverordnungen und kommunale Satzungen. Die Rechtsgrundlage des Mitgliedstaats muss mit den jeweiligen verfassungsrechtlichen Vorgaben übereinstimmen. Sie muss hinreichend klar, präzise und bestimmt sein, sodass für die betroffene Person die Datenverarbeitung eindeutig vorhersehbar ist.

Auch eine kommunale Benutzungs- und Gebührensatzung kommt damit grundsätzlich als Rechtfertigung für eine sonst nirgends geregelte Erhebung personenbezogener Daten infrage, soweit die Angelegenheit dem Kompetenzbereich der Gemeinde zugeordnet werden kann.

Im vorliegenden Fall erlaubte der Satzungstext dem Schulträger die Verarbeitung der „für die Abwicklung der Betreuung erforderlichen personenbezogenen Daten der Personensorgeberechtigten". Solche allgemein gefassten Vorschriften können je nach Anwendungsfall durchaus ausreichen. Auch z. B. § 3 Abs. 1 Landesdatenschutzgesetz ist keinesfalls präziser formuliert. Das funktioniert aber nur, solange die betreffenden Datenkategorien eher trivialer Natur sind, wie etwa bei bloßen Stamm- oder Kontaktdaten.

Was die Gemeinde hier forderte, war deutlich konkreter und umfangreicher. Vor allem jedoch sah der übrige Satzungstext in seiner damaligen Form eine Sozialauswahl gar nicht vor. Und damit fehlte es eindeutig an der erforderten Erwartbarkeit bzw. Vorhersehbarkeit für die Betroffenen. Eine solche gebietet u. a. der **Grundsatz der Transparenz** gemäß Art. 5 Abs. 1 Buchst. a DSGVO. Von diesem rein datenschutzrechtlichen Problem abgesehen hätte man auch aus gemeinderechtlicher Sicht hinterfragen können, ob die Angelegenheit nicht ohnehin eines ordentlichen Beschlusses der Gemeindevertretung bedurfte.

Die Stadtverwaltung konnte in der Anhörung durch das ULD die Beweggründe für die veränderte Verfahrensweise ohne Weiteres ausführlich darlegen, musste aber eingestehen, dass es an der notwendigen Legitimation mangelte.

Die Gemeinde setzte die Verwendung der strittigen Bescheinigungen zunächst aus. In einer Neufassung der Benutzungs- und Gebührensatzung wurde schließlich die bisherige Platzvergabe nach dem Zeitpunkt der Anmeldung durch ein **kriterienbasiertes Auswahlverfahren** ersetzt.

Auf Anraten des ULD erweiterte die Gemeindevertretung den Passus zur Datenverarbeitung in diesem Zuge um eine Auflistung konkret benannter **Datenkategorien**: Neben Informationen zur Berufstätigkeit der Kindeseltern tauchen hier nunmehr auch Zahlungsdaten oder Angaben zu einem etwaigen Bezug von Sozialleistungen auf. Für Betroffene bedeutet dies einen **deutlichen Gewinn an Rechtsklarheit** und für die Verwaltung eine **Erleichterung bei der Erfüllung ihrer datenschutzrechtlichen Informationspflichten**.

Was ist zu tun?

Die besten und vernünftigsten Absichten stellen per se noch keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten dar, erst recht nicht bei öffentlichen Stellen. Dabei sind Gemeinden oder Kreise aber nicht allein auf das beschränkt, was die Gesetzgeber in Land und Bund regeln. Im Rahmen der Selbstverwaltung können bzw. müssen sie Leerstellen füllen. In jedem Falle müssen die Grundlagen für eine Datenverarbeitung bestimmt genug – also ausreichend konkret geregelt – sein, abhängig von Umfang und Sensibilität der benötigten Datensätze.

4.1.9 Ausstellung von Gästekarten und Informationspflichten

Beim ULD ging eine Beschwerde ein, in der vorgetragen wurde, dass eine Gemeinde mittels ausgehändigter „Gästekarten" in nicht transparenter Weise personenbezogene Daten verarbeiten würde. Die ausgehändigten Gästekarten seien mit einem Barcode versehen und dieser werde bei jeder Nutzung der Karte, z. B. beim Betreten des Strandbereichs, eingescannt. Es sei jedoch nicht ersichtlich, welche Daten beim Einscannen übertragen und gespeichert werden.

In dem daraufhin eingeleiteten Anhörungsverfahren stellte sich u. a. heraus, dass der Gast die Wahl hat, neben einer gedruckten Papiergästekarte auch eine **elektronische Gästekarte** anzufordern. Die im Zusammenhang mit der digitalen Gästekarte erfolgende Verarbeitung wurde auf eine Einwilligung gestützt, die im Rahmen des online ablaufenden Registrierungsprozesses abgegeben wurde. Die erhobenen Daten wurden in einem **„Cardsystem"** verarbeitet.

Die Prüfung der dem ULD zur Verfügung gestellten Unterlagen, vor allem zum Prozess der Registrierung, ergab, dass die abrufbaren Informationen weder den Anforderungen nach Artikel 13 DSGVO noch den Anforderungen nach Artikel 7 DSGVO für die Erteilung einer wirksamen Einwilligung genügten. Auch ergab sich Klärungsbedarf im Hinblick auf eine mögliche Zusammenführung der personenbezogenen Daten des kurabgabepflichtigen Gästekarteninhabers, die im Cardsystem gespeichert sind, mit den pseudonymisiert erfassten Daten zur Kontrolle der Eintrittsberechtigung, die in „begründeten Fällen" erfolgten, sowie im Hinblick auf die Speicherdauer.

Die insoweit von dem ULD erteilten Hinweise wurden vollständig umgesetzt; die Informationstexte wurden sowohl hinsichtlich der Einwilligung als auch der nach Artikel 13 DSGVO zu erteilenden Informationen nachgebessert. Das Verfahren wurde daraufhin eingestellt.

Was ist zu tun?

Bei der Verarbeitung personenbezogener Daten sind die Informationspflichten nach den Artikeln 13, 14 DSGVO sowie die Anforderungen nach Artikel 7 DSGVO bei der Einholung von Einwilligungen einzuhalten. Der Informationsinhalt nach Artikel 13, 14 DSGVO und nach Artikel 7 DSGVO ist nicht vollkommen identisch. Es kann sich anbieten, die jeweiligen Informationspflichten durch einen gemeinsamen Hinweistext zu erfüllen.

Die Informationen sind gemäß Art. 12 Abs. 1 Satz 1 DSGVO in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" zu übermitteln.

4.1.10 Erhebung von Kundendaten für das neue Gebührenmodell eines Zweckverbandes

Beim ULD ging eine Beschwerde ein, in der vorgetragen wurde, dass ein Zweckverband zur Umsetzung eines neuen Gebührenmodells im Bereich der Abfallwirtschaft personenbezogene Daten von Kunden erheben und weiterverarbeiten würde. Konkret verhielt es sich so, dass die Kunden anlässlich der geplanten Umsetzung des neuen Gebührenmodells von dem Zweckverband angeschrieben und mittels eines beigefügten Rückantwortformulars um grundstücksbezogene Angaben (Straße, Hausnummer, PLZ, Ort, Anzahl der Haushalte sowie Personenzahl zu den

jeweiligen Haushalten) und auf die Eigentümer bezogene Angaben (Nachname, Vorname, Straße, Hausnummer, PLZ, Ort) gebeten worden sind.

Die Informationen über die so beabsichtigte Verarbeitung der personenbezogenen Daten nach Artikel 13 bzw. Artikel 14 DSGVO, die dem Schreiben beigefügt waren, enthielten keine Angabe zu der konkreten Rechtsgrundlage.

Da aus Sicht des ULD keine Rechtsgrundlage für die Verarbeitung der abgefragten personenbezogenen Daten für die Umsetzung des neuen Gebührenmodells erkennbar war, wurde ein Beschwerdeverfahren eingeleitet. Der Zweckverband erließ nach dieser Verfahrenseinleitung eine neue **Abfallgebührensatzung sowie eine neue Abfallwirtschaftssatzung** und stützte die mit der geplanten Umsetzung des Gebührenmodells einhergehende Verarbeitung der personenbezogenen Daten auch auf Regelungen in diesen überarbeiteten Satzungen. Im Laufe des Beschwerdeverfahrens stellte sich heraus, dass der Zweckverband auf sein Anschreiben, mit dem er die Angaben von den Kunden erbeten hatte, über 41.000 Rückmeldungen erhalten hatte.

Rechtlich war aus Sicht des ULD festzustellen, dass sowohl vor der Änderung der Satzungen als auch nach deren Änderung weder eine Rechtsgrundlage für die Erhebung der personenbezogenen Daten der Kunden noch für deren Speicherung vorlag. So war beispielsweise für das ULD nicht ersichtlich, dass die Umstellung eines bestehenden Gebührenmodells von dem sachlichen Anwendungsbereich der maßgebenden Satzung erfasst war. Zusammenfassend war festzustellen, dass die Erforderlichkeit der im Einzelnen mit dem Anschreiben des Zweckverbandes abgefragten personenbezogenen Daten aus Sicht des ULD fehlte.

Nach umfassendem Austausch der unterschiedlichen Rechtsauffassungen, vor allem zur Rechtsgrundlage und Löschverpflichtung, zwischen dem ULD und dem Zweckverband in dem Beschwerdeverfahren löschte der Zweckverband ohne Anerkennung einer Rechtspflicht die mit dem Anschreiben erhobenen personenbezogenen Daten. Die früher von dem Zweckverband erhobenen, etwaig identischen personenbezogenen Daten der Kunden, die im Rahmen der gesetzlichen Aufgabenzuweisung des Zweckverbandes auf der Grundlage entsprechender gesetzlicher Regelungen verarbeitet werden, waren davon zulässigerweise nicht erfasst. Die **Löschung** umfasste nach Angaben des Zweckverbandes sämtliche in Papierform sowie digital gespeicherte Daten, die aus den Rückmeldungen übernommen worden waren. Dabei handelte es sich den Angaben des Zweckverbandes zufolge um die Angaben, wie viele Haushalte auf dem jeweiligen Grundstück vorhanden waren und wie viele Personen in dem jeweiligen Haushalt lebten. Weitere Angaben seien aus den Rückmeldungen nicht digital gespeichert worden. Der Zweckverband reichte sowohl für die Vernichtung der Papierunterlagen (Rückmeldungen) als auch für die Löschung der digital gespeicherten Daten entsprechende Bescheinigungen ein, sodass die Löschung als belegt anzusehen war.

Gegenüber dem Zweckverband wurde aufgrund des mit der rechtsgrundlosen Erhebung der Daten und deren (bis zur Löschung dauernden) Speicherung einhergehenden Verstoßes gegen die Vorgaben des Art. 5 Abs. 1 Buchst. a i. V. m. Art. 6 Abs. 1 DSGVO eine Verwarnung gemäß Art. 58 Abs. 2 Buchst. b DSGVO ausgesprochen.

In die Abwägung hinsichtlich der Verhängung einer Verwarnung wurde entlastend berücksichtigt, dass das Beschwerdeverfahren zum Anlass für die Neufassung der Satzungen genommen worden war. Ferner wurde ebenfalls entlastend im Hinblick auf die Schwere des Verstoßes berücksichtigt, dass es sich bei den betreffenden Daten nicht um Daten mit besonderem Schutzbedarf (Artikel 9 DSGVO) gehandelt hat. Berücksichtigt wurde auch, dass die betreffenden personenbezogenen Daten sowohl in Papierform als auch die digital gespeicherten Daten den Angaben des Zweckverbandes zufolge vollumfänglich gelöscht und entsprechende Bestätigungen eingereicht worden waren. Im Rahmen der Gesamtabwägung war jedoch maßgebend die Quantität zu berücksichtigen. Mit über 41.000 Rückmeldungen hat es eine entsprechend hohe Anzahl von betroffenen Personen gegeben. Dies begründete eine erhebliche Schwere des Verstoßes.

Was ist zu tun?

Die Verarbeitung von personenbezogenen Daten bedarf einer Rechtsgrundlage. Der Verantwortliche hat zu prüfen, ob der sachliche Anwendungsbereich der in Betracht kommenden Regelungen eröffnet ist und deren Anforderungen (z. B. die Erforderlichkeit, die betroffenen Daten zu verarbeiten) erfüllt sind.

4.1.11 Die „gezielte Entgegennahme" von E-Mails

Einen stets wiederkehrenden Anlass zu Anfragen und Beschwerden beim ULD bildet die Übermittlung personenbezogener Daten per E-Mail. Eine dieser Beschwerden richtete sich gegen eine Behörde, die in größerem Umfang ärztliche Unterlagen von Betroffenen verarbeitet und diese über verschiedene Wege entgegennimmt, u. a. auch per E-Mail. Ein Bürger, der sich um die Sicherheit seiner Dokumente sorgte, entschied sich nun dafür, diese als passwortverschlüsselte PDF-Dokumente im E-Mail-Anhang bei der Verwaltung einzusenden.

Das Ansinnen war verständlich, handelte es sich schließlich um **Gesundheitsdaten**, die dem Begriff der „besonderen Kategorien personenbezogener Daten" nach Artikel 9 DSGVO unterfallen. Mit Blick auf die Erwägungsgründe 75 und 76 zur DSGVO ist dies stets ein starkes Indiz, dass mit deren Verarbeitung ein „hohes Risiko" für die Rechte und Freiheiten der betroffenen Person einhergeht. Dem muss die verantwortliche Stelle – hier als Empfängerin – bei der sicheren Ausgestaltung ihrer Verfahren Rechnung tragen:

Art. 32 Abs. 2 DSGVO

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch […] unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Stattdessen erhielt der Beschwerdeführer die Antwort, dass verschlüsselte Dateien „aus sicherheitstechnischen Gründen" nicht angenommen werden könnten, und wurde um erneuten Versand in einem unverschlüsselten Dateiformat gebeten. Ein Hinweis mit ähnlichem Sinngehalt fand sich auch auf dem Webauftritt der Behörde. Der Betroffene fasste dies als direkte Aufforderung, einen unsicheren Kommunikationsweg zu nutzen, auf und wandte sich hiermit an das ULD. Tatsächlich können passwortverschlüsselte Dateien ein Sicherheitsproblem darstellen, da sie etwa die Prüfung von Eingängen durch Virenscanner zumindest erschweren. Jedoch hätte die Verwaltung in dieser Situation eine **ausreichend sichere Alternative zur Übermittlung der ärztlichen Nachweise anbieten müssen**. In diesem Sinne wurde die Behörde auf die Empfehlungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu der Thematik aufmerksam gemacht:

DSK-Orientierungshilfe vom 16.06.2021: „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail"

Wer jedoch gezielt personenbezogene Daten per E-Mail entgegennimmt, ist verpflichtet, die Voraussetzungen für den sicheren Empfang von E-Mail-Nachrichten über einen verschlüsselten Kanal zu schaffen. […]

Können die Anforderungen an eine sichere Übermittlung per E-Mail nicht erfüllt werden, so muss ein anderer Kommunikationskanal gewählt werden.

Diese Hinweise stellen klar, dass eine verantwortliche Stelle ihre Schutzmaßnahmen nicht nur beim Versand von E-Mails, sondern auch bei deren Empfang prüfen muss. Als eine „gezielte Entgegennahme" betrachtet die Datenschutzkonferenz dabei beispielsweise den E-Mail-Empfang aufgrund „expliziter Vereinbarung" oder „Aufforderung auf der Homepage". Unschädlich wäre es demgegenüber nur, wenn Bürgerinnen und Bürger auf ein gebotenes Sicherheitsniveau aus freien Stücken und trotz Alternativen verzichten.

Im konkreten Fall konnte uns die Behörde glücklicherweise auf bestehende alternative Kommunikationswege verweisen: nämlich auf **einen Ende-zu-Ende-verschlüsselten Datei-Upload oder aber den altmodischen Postversand**. Das Problem bestand also lediglich in der missglückten Darstellung nach außen, was die verantwortliche Stelle auch ohne Weiteres einsah.

Entsprechend änderte man die internen Textvorlagen und die Ausführungen auf der Behörden-Webseite ab: Die Einsendung sensibler Unterlagen per einfacher E-Mail wird zwar weiterhin akzeptiert. Aber die Anleitungen hierzu wurden um einen Hinweis auf das geringere Sicherheitsniveau und einen Verweis auf den sichereren Upload ergänzt. Ihren Sorgfaltspflichten kommt die Verwaltung mit dieser Lösung nach Auffassung des ULD ausreichend nach.

Die genannte Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail" der Datenschutzkonferenz ist abrufbar unter dem Link:

https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf

Kurzlink: *https://uldsh.de/tb43-4-1-11a*

Das Dokument im Volltext erläutert auch eingehender die technischen Hintergründe, insbesondere welche Anforderungen an eine „obligatorische" und „qualifizierte" **Transportverschlüsselung** einerseits oder an eine **Ende-zu-Ende-Verschlüsselung** andererseits jeweils zu stellen sind. Werden diese Erfordernisse alle erfüllt, kommt auch mittels E-Mail eine datenschutzrechtlich einwandfreie Übermittlung sensibler personenbezogener Daten in Betracht.

Was ist zu tun?

Verantwortliche Stellen, die im Rahmen von Anträgen oder Untersuchungen regelmäßig Unterlagen mit sensiblem Inhalt entgegennehmen, müssen hierfür Kommunikationskanäle, die einen erhöhten Schutz dieser Daten bieten, zumindest vorhalten und anbieten. Eine Übermittlung mittels E-Mail erfüllt die notwendigen Voraussetzungen oft nicht bzw. nur dann, wenn umfangreichere Vorkehrungen getroffen werden.

4.1.12 Urlaub und Updates

Eine Kommune stellte für ihre eigenen Systeme fest, dass über den Virenscanner auf einem Terminalserver eine Gefahr erkannt wurde. Die zugrunde liegende PowerShell-Aktivität erfolgte dabei durch einen nicht berechtigten Nutzer. Daraufhin deaktivierte die Kommune den Zugang dieses Nutzers. Nach vertiefter Recherche konnte der NetScaler als Schwachstelle identifiziert werden, der umgehend vom Netz genommen wurde. Der externe Angreifer hatte so Zugriff auf das interne Netz der Kommune. Zunächst war der Kommune die Anzahl betroffener Personen unbekannt. Nach einer vorläufigen Prüfung der Kommune seien aber „nur" Daten

von Beschäftigten, im Kern Profil- und Anmeldedaten, zugänglich gewesen.

Etwa einen Monat später stellte die Kommune einen zweiten externen Angriff auf das eigene Verarbeitungssystem fest, wobei das Muster des Angriffsszenarios exakt dem entsprach, was vor einem Monat bereits als Ergebnis der Analyse feststand. Da bestehende Sicherheitsrisiken sich innerhalb kurzer Zeit innerhalb der Kommune wiederholten und auch der analysierte Fehler sich als identisch erwies, leitete das ULD ein Prüfverfahren ein.

Im Prüfverfahren zeigte sich, dass die Kommune zwar vier Administratoren beschäftigt. Allerdings waren für diese keine spezifischen Zuständigkeiten festgelegt. Demnach nahm jeder Administrator alle Aufgaben wahr.

Weiterhin konnte die Kommune **keine Verfahrensbeschreibung für das Patchmanagement** vorlegen. Hierzu existiere bisher nur ein Entwurf. Ferner bestand **keine Beschreibung für ein Notfallmanagement**. Auch hierzu sei nur ein Entwurf vorhanden. Grundsätzlich sei der Prozess zum Patchen des NetScalers folgendermaßen gestaltet: Ein Administrator informiert sich regelmäßig über mögliche Veröffentlichungen von Patches und Aktualisierungen, lädt diese manuell herunter und spielt sie dann ein. Es wird vonseiten der Kommune eingeräumt, dass die seit August 2023 bereitgestellten Patches (BSI – Schwachstelle in Citrix NetScaler ADC und NetScaler Gateway, Version 1.1 vom 23.11.2023) versehentlich aufgrund der Urlaubszeit nicht eingespielt wurden. Für die Urlaubszeit im August 2023 war allerdings eine Vertretung für die IT-Administration vorgesehen. Ungeklärt blieb, weshalb die Vertretung die Einspielung des Patches nicht vornahm und warum ab September, nach Ende der Urlaubszeit, weiterhin die Einspielung des Patches unterblieb. Offen blieb auch, wann konkret die Einspielung des Patches erfolgte, da nach dem ersten Sicherheitsvorfall die Sicherheitslücke offenbar noch existierte. Zudem bestehe in der Kommune keine zentrale Bereitstellung der Protokolldaten für eingespielte Patches.

Hinweis des BSI: Aktive Ausnutzung einer Schwachstelle in Citrix NetScaler ADC und NetScaler Gateway

Am 10.10.2023 hat der Hersteller Citrix ein Advisory zu Schwachstellen in den Produkten NetScaler Application Delivery Controller und NetScaler Gateway veröffentlicht. Angreifende können mit authentifizierten Sessions weitere Zugangsdaten sammeln und sich somit möglicherweise höhere Rechte verschaffen und im System sowie Netzwerk ausbreiten. Näheres kann nachgelesen werden unter:

https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2023/2023-275276-1032.pdf

Kurzlink: *https://uldsh.de/tb43-4-1-12a*

Das ULD hat fehlende Unterlagen nachgefordert und geprüft. Die Kommune sagte zu, vorhandene technische und organisatorische Mängel im Zusammenhang mit dem Patchmanagement zu beseitigen. Dies gilt auch für die Überarbeitung und Finalisierung der Konzepte zum Patch- und Notfallmanagement.

Was ist zu tun?

Kommunen müssen dafür Sorge tragen, dass ein angemessenes Patchmanagement besteht. Identifizierte Sicherheitslücken sind umgehend zu schließen. Die Urlaubs- und Vertretungsplanung ist in der Form umzusetzen, dass im Falle von Gefährdungsmeldungen zeitnah reagiert werden kann. Erforderlich ist auch eine klare Verteilung von Zuständigkeiten im Bereich der technischen Administration, ein regelmäßiges Reporting gegenüber der Dienststellenleitung und eine angemessene Protokollierung vorgenommener Maßnahmen zur Gewährleistung der Datensicherheit, wozu auch das Einspielen von Patches zählt.

4.1.13 Meldepflicht gegenüber der Aufsichtsbehörde oder Mitarbeiterexzess

An das ULD wurden in der Vergangenheit wiederholt Sachverhalte herangetragen, bei denen zunächst fraglich war, ob der Arbeitgeber oder aber der einzelne Beschäftigte als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO anzusehen war.

Die Handlungen der Beschäftigten sind dem Arbeitgeber grundsätzlich zuzurechnen, mit der Folge, dass der Arbeitgeber als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO zu erachten ist. Maßnahmen der Aufsichtsbehörde, etwa die Einleitung eines Anhörungsverfahrens, sind daher regelmäßig gegen den Arbeitgeber als Verantwortlichen der Datenverarbeitung gerichtet. Hat die Handlung der Beschäftigten beispielsweise eine Verletzung des Schutzes personenbezogener Daten zur Folge, begründet diese Handlung **für den Arbeitgeber eine Meldepflicht gegenüber der Aufsichtsbehörde** nach Artikel 33 DSGVO und gegebenenfalls auch **Benachrichtigungspflichten gegenüber den betroffenen Personen** nach Artikel 34 DSGVO. Etwas anderes gilt dann, wenn ein **Mitarbeiterexzess des Beschäftigten** vorliegt. In diesem Fall ist der Beschäftigte selbst Verantwortlicher gemäß des Art. 4 Nr. 7 DSGVO.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat in ihrer Entschließung der 97. Konferenz am 03.04.2019 Mitarbeiterexzesse als Handlungen von Beschäftigten definiert, „die bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden können".

Hinsichtlich der Frage, welche konkreten Voraussetzungen für die Annahme eines Mitarbeiterexzesses sprechen, bestehen mehrere Erwägungen.

Ein Ansatz für die Verantwortung des Arbeitgebers könnte darin bestehen, dass dieser verantwortlich ist und bleibt, wenn der Beschäftigte verschuldensunabhängig normative – insbesondere organisatorische – Vorgaben nicht beachtet oder technische Vorkehrungen überwindet, die der Arbeitgeber jeweils nach den Artikeln 5, 24 und 32 DSGVO getroffen hat. Raum für einen Mitarbeiterexzess und damit für die Verantwortung des Beschäftigten bestünde demnach dann, wenn der Beschäftigte bei seiner Handlung die Vorgaben des Arbeitgebers nach den Artikeln 5, 24 und 32 DSGVO außer Acht gelassen hat. Allerdings blieben dann Fragen einer zweckändernden Verarbeitung durch Beschäftigte außer Betracht, die für Mitarbeiterexzesse häufig charakteristisch sind.

Aus Sicht des ULD sollte daher die Frage, ob die Handlung des Beschäftigten einen Mitarbeiterexzess darstellen könnte, insbesondere danach beurteilt werden, ob der Beschäftigte die dienstlich erlangten Daten, gegebenenfalls von seinem Arbeitsplatz aus und unter Einsatz der zur Verfügung stehenden Arbeitsmittel, nicht in Aus-

übung seiner dienstlichen Tätigkeit, sondern ausschließlich für eigene private Zwecke oder Zwecke eines Dritten verwendet. Bei dieser Betrachtungsweise kommt es für die Beurteilung, wie die Handlung des Beschäftigten zu werten ist, nicht primär darauf an, ob der Beschäftigte subjektiv eigene Interessen verfolgt; maßgebend ist vielmehr, ob die fragliche Handlung objektiv der Zweckbestimmung der ihm zugewiesenen Aufgaben entspricht.

Vor diesem Hintergrund bestehen aus Sicht des ULD Anhaltspunkte für einen Mitarbeiterexzess, wenn sich der Beschäftigte **über die dienst- und arbeitsrechtlichen Anweisungen des Arbeitgebers hinwegsetzt** und eigenmächtig dienstlich erlangte Daten ausschließlich **für eigene private Zwecke oder für Zwecke eines Dritten und damit betriebsfremd verarbeitet**. In diesem Fall ist nicht der Arbeitgeber Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO, sondern der betreffende Beschäftigte.

Was ist zu tun?

Für die Bewertung, ob ein Mitarbeiterexzess vorliegt, ist insbesondere zu prüfen, ob sich der Beschäftigte über die dienst- und arbeitsrechtlichen Anweisungen des Arbeitgebers hinwegsetzt und eigenmächtig dienstlich erlangte Daten ausschließlich für eigene private Zwecke oder für Zwecke eines Dritten verarbeitet.

4.2 Polizei und Verfassungsschutz

4.2.1 Auskunftsrecht betroffener Personen bei der Polizei

Haben Sie sich schon einmal gefragt, welche Daten die Polizei über Sie speichert und wie Sie darauf Zugriff erhalten können? Ob nach einem Verkehrsverstoß, einer Anzeige oder anderen polizeilichen Vorgängen – es kann Situationen geben, in denen Sie wissen möchten, welche Informationen zu Ihrer Person bei der Polizei gespeichert sind. Die gute Nachricht: Sie haben ein Recht darauf, Auskunft zu erhalten. Aber wie genau funktioniert das? Welche Hürden müssen überwunden werden? Und worauf sollten Sie achten?

Worauf stützt sich Ihr Recht auf Auskunft?

Mittlerweile sind viele Menschen damit vertraut, bei Unternehmen und öffentlichen Stellen **auf Grundlage der Datenschutz-Grundverordnung (DSGVO)** Auskunft über ihre personenbezogenen Daten zu beantragen. Was viele nicht wissen: Daten, die zur Gefahrenabwehr oder zur Strafverfolgung verarbeitet werden, sind vom Anwendungsgebiet der DSGVO ausgenommen. Der Anspruch auf Auskunft ergibt sich in diesem Fall aus § 33 Landesdatenschutzgesetz (LDSG). Bei Daten, die von der Polizei zu anderen Zwecken verarbeitet werden (z. B. für Arbeitsverhältnisse), greift jedoch wieder die DSGVO.

In beiden Fällen gilt: Sie haben das Recht zu erfahren, ob und welche Daten die Polizei über Sie gespeichert hat.

Wer kann Auskunft beantragen?

Jede betroffene Person kann einen Antrag stellen. Dazu gehören:

- Sie selbst,
- eine von Ihnen bevollmächtigte Person (z. B. ein Anwalt),
- Ihre gesetzlichen Vertreter (bei Minderjährigen).

Wichtig: Bei Minderjährigen ab 14 Jahren kann die Auskunft direkt an die betroffene Person erteilt werden, sofern die Einsichtsfähigkeit gegeben ist.

Wie stellen Sie einen Antrag auf Auskunft?

Ein Antrag auf Auskunft ist formlos möglich. Es wird jedoch empfohlen, ihn schriftlich zu stellen. In Schleswig-Holstein werden alle Anträge auf Auskunft zentral durch das LKA in Kiel bearbeitet. Anträge, die auf anderen Dienststellen eingehen, werden dorthin weitergeleitet.

Was sollten Sie in den Antrag schreiben?

- Ihren Namen, Ihre Anschrift und Ihr Geburtsdatum.
- Einen Hinweis darauf, dass Sie eine Auskunft über Ihre gespeicherten Daten beantragen.
- Wenn Sie spezifische Informationen wünschen, die sich z. B. auf bestimmte Daten, Vorgänge oder Ereignisse beziehen, ist es hilfreich, diese ebenfalls im Antrag zu benennen.

Tipp: Sie müssen nicht begründen, warum Sie die Informationen haben möchten. Die Polizei ist verpflichtet, Ihnen Auskunft zu erteilen.

Wie weisen Sie gegenüber der Polizei Ihre Identität nach?

Die Polizei muss sicher sein, dass sie die Informationen an die richtige Person herausgibt. Häufig wird daher eine Kopie des Personalausweises verlangt.

Wichtige Hinweise zur Ausweiskopie:

- Sie können nicht notwendige Daten schwärzen, z. B. die Seriennummer oder das Lichtbild.
- Erforderliche Angaben sind: Vorname, Name, Anschrift, Geburtsdatum, Gültigkeitsdauer und Geburtsort.

Gut zu wissen: Die Kopie darf nur für die Bearbeitung des Antrags genutzt und muss danach gelöscht werden.

Welche Informationen erhalten Sie?

Sie haben Anspruch auf alle personenbezogenen Daten, die bei der Polizei gespeichert sind. Dazu gehören auch:

- eine Übersicht aller Vorgänge und Dateien zu Ihrer Person

sowie Informationen zu:

- dem Zweck der Datenverarbeitung,
- dem Zeitpunkt der Speicherung und Löschfristen,
- Übermittlungen an andere Stellen.

Einschränkend gilt: Daten Dritter, die mit Ihren Informationen verknüpft sind, werden geschwärzt oder ausgeschlossen.

Besonderheiten bei Verbunddateien

Personenbezogene Daten, die in Verbunddateien gespeichert sind wie beispielsweise **INPOL (das Informationssystem der Polizei) oder PIAV (Polizeilicher Informations- und Analyseverbund)**, können bundesweit abgerufen werden. Auch solche Daten sind von Ihrem Auskunftsrecht umfasst. Hierbei gibt es jedoch eine Besonderheit:

Die Landespolizei muss Ihnen Auskunft über Daten geben, die sie selbst in solche Systeme eingestellt hat. Für Daten, die von anderen Behörden gespeichert wurden, sind diese zuständig.

Gut zu wissen: Falls Daten aus Verbunddateien für Sie relevant sind und Sie die einspeichernde Behörde nicht kennen, können Sie zusätzlich beim Bundeskriminalamt (BKA) darüber Auskunft beantragen.

Wie lange dauert die Bearbeitung eines Antrags?

Anders als in der DSGVO nennt das LDSG keine Frist für die Beantwortung des Auskunftsersuchens. Die Polizei sollte Ihren Antrag daher grundsätzlich so bald wie möglich beantworten. Natürlich ist der Aufwand von Fall zu Fall sehr unterschiedlich. In der Regel sollte eine Antwort

innerhalb eines Monats möglich sein. In komplexeren Fällen kann die Bearbeitung auch bis zu drei Monaten in Anspruch nehmen.

Tipp: Sollten Sie nach Ablauf dieser Fristen keine Antwort erhalten, fragen Sie bitte bei der Polizei direkt nach. Bei Problemen können Sie sich an den behördlichen Datenschutz der Landespolizei (siehe Kasten) oder an uns als zuständige Aufsichtsbehörde wenden.

Was passiert, wenn die Auskunft verweigert wird?

In bestimmten Fällen kann die Polizei die Auskunft einschränken oder sogar verweigern. Dies ist beispielsweise dann der Fall, wenn die Erteilung der Auskunft die öffentliche Sicherheit oder ein Ermittlungsverfahren gefährden würde.

Wenn die Auskunft ganz oder teilweise verweigert wird, müssen Sie im Regelfall darüber informiert und die Entscheidung muss Ihnen gegenüber begründet werden. Die Unterrichtung und die Begründung dürfen jedoch unterbleiben, wenn bereits diese Information eine Gefährdung darstellt.

Sollten Sie Zweifel an der Rechtmäßigkeit der Entscheidung haben, können Sie sich an uns wenden. Wir dürfen Ihnen zwar auch nicht mehr mitteilen als die Polizei, können aber prüfen, ob das Zurückhalten der Informationen rechtmäßig erfolgt ist. Daneben besteht natürlich auch die Möglichkeit, die Einschränkung der Auskunft gerichtlich überprüfen zu lassen.

Transparenz und Verständlichkeit: Datenverarbeitung einfach erklärt

Die Polizei muss Ihnen die Informationen in verständlicher Sprache und in einer klaren Form mitteilen. Dazu gehört auch, dass Fachbegriffe oder Verweise auf Systeme (wie z. B. INPOL oder PIAV) erklärt werden. Falls Sie Fragen zu bestimmten Informationen haben, zögern Sie nicht, diese zu stellen!

Fallen Kosten für Auskunftsersuchen an?

In der Regel ist die Erteilung einer Auskunft kostenfrei. Ausnahmen können in seltenen Fällen gemacht werden, etwa wenn ein Antrag offensichtlich unbegründet oder exzessiv gestellt wird. Dies könnte beispielsweise der Fall sein, wenn wiederholt ähnliche Anfragen eingereicht werden, die keinen neuen Informationsgewinn bieten. Sollte die Polizei in einem solchen Fall Gebühren erheben wollen, muss sie Sie im Voraus darüber informieren.

Fazit: Ihr Recht auf Auskunft – nehmen Sie es wahr!

Die Polizei speichert Daten zu Ihrer Person aus verschiedenen Gründen. Als betroffene Person haben Sie ein Recht darauf zu wissen, welche Informationen vorliegen. Ein Antrag auf Auskunft ist unkompliziert und ohne große Hürden möglich.

Nutzen Sie Ihr Recht und sorgen Sie für Klarheit. Falls Probleme auftreten, stehen Ihnen die behördlichen Datenschutzbeauftragten der Polizeibehörden und die Datenschutzaufsichtsbehörden als Ansprechpartner zur Seite.

Ansprechpartner bei der Landespolizei

LKA 122 (Bearbeitung von Auskunftsersuchen)

Mühlenweg 166
24116 Kiel

Behördliche Datenschutzbeauftragte

Mühlenweg 166
24116 Kiel
Tel.: 0431 160-0
E-Mail: StSt1.Kiel.LPA@polizei.landsh.de

4.2.2 INPOL-Abfrage

Sind polizeiliche Standardmaßnahmen in Form von Abfragen im Informationssystem der Polizei (INPOL) datenschutzrechtlich völlig unproblematisch? Nein! Doch genau dies war die Auffassung einer Polizeidirektion, nachdem sich eine Person über eine Abfrage in INPOL beschwert hatte.

Der INPOL-Abfrage vorausgegangen war der Versuch, auf einer Polizeidienststelle Anzeige zu erstatten. Weil die Anzeige nicht aufgenommen wurde, reagierte die Person aufgebracht und sehr emotional. Sie verließ sogar kurzzeitig die Dienststelle, um dann kurze Zeit später noch einmal dort vorzusprechen – mit unverändertem Ergebnis. Knapp zwei Wochen später erschien sie noch einmal kurz auf der Wache, weil sie eine Beschwerde vorbereiten wollte. Dazu erkundigte sie sich nach der Dienstnummer des Beamten, mit dem sie gesprochen hatte. Bei diesem Besuch wurde sie gebeten, sich auszuweisen. Kurz nach Verlassen der Dienststelle wurden die Daten der Person in INPOL abgefragt.

Durch ein Auskunftsersuchen bei der Landespolizei erhielt sie später Kenntnis von dieser Abfrage. Auf ihre Beschwerde hin teilte man ihr lediglich mit, dass sich die Abfrage auf § 195 Landesverwaltungsgesetz (LVwG) stützt und die Voraussetzungen dafür vorgelegen hätten. Weil sie diese Auskunft nicht nachvollziehen konnte, beschwerte sie sich beim ULD.

§ 195 LVwG (siehe Kasten) erlaubt den Abgleich personenbezogener Daten mit polizeilichen Dateien für bestimmte Personengruppen zu verschiedenen Zwecken. Die Antwort der Polizei auf die Beschwerde enthielt keine Hinweise darauf, welcher Fall des § 195 LVwG vorgelegen hat noch warum die Voraussetzungen dafür gegeben waren. Sie war damit für die betroffene Person tatsächlich nicht nachvollziehbar.

Erst im Rahmen der Überprüfung durch das ULD wurde mitgeteilt, dass die betroffene Person als „Verhaltensstörer" nach § 218 LVwG abgefragt worden sei. Die Abfrage sei rechtmäßig gewesen und „insgesamt als polizeiliche Standardmaßnahme als völlig unproblematisch zu bewerten".

§ 195 LVwG – Datenabgleich

(1) Die Polizei kann personenbezogene Daten der in den §§ 218, 219 sowie § 179 Abs. 2 Nr. 2 Buchst. a genannten Personen mit dem Inhalt polizeilicher Dateien im Rahmen der Zweckbindung dieser Dateien abgleichen. Personenbezogene Daten anderer Personen kann die Polizei abgleichen, wenn Tatsachen dafür sprechen, dass dies zur Erfüllung polizeilicher Aufgaben erforderlich erscheint. Die Polizei kann ferner im Rahmen ihrer Aufgabenerfüllung erlangte personenbezogene Daten mit dem Fahndungsbestand abgleichen. Ein Abgleich der nach § 179 Abs. 4 erlangten personenbezogenen Daten ist nur mit Zustimmung der betroffenen Person zulässig.

Doch gerade bei „polizeilichen Standardmaßnahmen", also Maßnahmen, die häufig und relativ niederschwellig durchgeführt werden, besteht die reale Gefahr, es mit den gesetzlichen Voraussetzungen nicht ganz so genau zu nehmen. Für eine Abfrage in Verbindung mit § 218 LVwG muss beispielsweise „die öffentliche Sicherheit durch das Verhalten von Personen gestört oder im einzelnen Fall gefährdet" werden. Dafür wurde jedoch im Rahmen der Überprüfung keine tragfähige und nachvollziehbare Begründung gegeben. Sowohl für die Entgegennahme einer Anzeige als auch für die Bearbeitung einer Beschwerde über einen Beamten war die Landespolizei der richtige Ansprechpartner. Allein der Umstand, dass Gespräche „schwierig" verlaufen und Bürger emotional reagieren, begründet noch keine Gefahr für die öffentliche Sicherheit. Darüber hinaus erfolgte die Abfrage erst knapp zwei Wochen nach dem „schwierigen" Gespräch. Im Ergebnis wurde daher gegenüber der Polizeidirektion eine Verwarnung ausgesprochen.

Was ist zu tun?

Sofern sich Bürgerinnen und Bürger über polizeiliche Maßnahmen beschweren, sollte ihnen neben den Rechtsgrundlagen auch erläutert werden, warum die Voraussetzungen dafür in dem konkreten Fall vorgelegen haben. Dies würde zusätzlich die Kontrolle durch Aufsichtsbehörden und Gerichte erleichtern. Insbesondere bei „polizeilichen Standardmaßnahmen" sollte die Sensibilität für die gesetzlichen Voraussetzungen noch mehr geschärft werden.

4.2.3 Abfrage aus dem Fahreignungsregister (FAER)

Das Fahreignungsregister wird beim **Kraftfahrt-Bundesamt (KBA)** geführt und darin werden Informationen zu Verkehrsverstößen, Punkten in Flensburg und Entziehungen der Fahrerlaubnis gespeichert. Es dient dazu, die Verkehrssicherheit zu gewährleisten und Fahrer zu erfassen, die gegen die Verkehrsregeln verstoßen. Das FAER erfüllt damit einen wichtigen Zweck.

Im Rahmen einer Verkehrsordnungswidrigkeit wollte die zuständige Behörde eines Landkreises wissen, ob der mutmaßliche Fahrer bereits im Fahreignungsregister (FAER) vermerkt ist. Die Daten wurden also kurzerhand abgerufen – noch bevor überhaupt feststand, wer eigentlich am Steuer saß. Ist das zulässig?

Vielleicht fragen Sie sich: Darf eine Behörde nicht einfach nachschauen? Tatsächlich nicht, denn der Zugriff auf solche Daten unterliegt gesetzlichen Regeln. Grundsätzlich gilt:

- **Nur wenn es auch „erforderlich" ist** – Das steht so in § 28 Abs. 2 des Straßenverkehrsgesetzes (StVG). Ein Abruf muss einen klaren Zweck haben und zur Erreichung dieses Zweckes auch erforderlich sein.
- **Nur unter Beachtung datenschutzrechtlicher Grundsätze** – § 47 Nr. 3 des Bundesdatenschutzgesetzes (BDSG) betont die Zweckbindung, die Erforderlichkeit sowie die Verhältnismäßigkeit.

Auch mit Blick auf den **Verhältnismäßigkeitsgrundsatz** werden Abfragen aus dem FAER auch im Rahmen von Ermittlungen regelmäßig erst dann angezeigt sein, wenn sich ein hinreichender Tatverdacht abzeichnet. So werden unnötige Abfragen vermieden.

Anders gesagt: Ohne Klarheit darüber, wer der Fahrer war, ist der Blick ins FAER **voreilig und überflüssig**. Schlimmer noch: Es könnte die Falschen treffen.

Was bedeutet das konkret? Ein Abruf aus dem FAER ist erst **nach dem Abschluss der Ermittlungen zulässig**, wenn unter Berücksichtigung der Äußerung des Betroffenen und etwaiger Zeugenaussagen ein Bußgeldbescheid in Betracht kommt.

Leider kommt es in Schleswig-Holstein immer wieder zu solch verfrühten Abfragen. In der Regel soll dadurch Zeit gespart werden. Durch die hohen Fallzahlen finden viele Arbeitsschritte automatisiert oder zumindest teilautomatisiert statt. Dabei entscheidet jede Ordnungswidrigkeitenbehörde selbst über ihre Arbeitsprozesse.

In anderen Bundesländern wie z. B. in NRW sind Abfragen aus dem FAER vor Abschluss der Ermittlungen durch einen landesweit gültigen Erlass des Innenministeriums ausgeschlossen. So etwas würde auch in Schleswig-Holstein für mehr Klarheit unter den Verkehrs-OWI-Behörden sorgen. Aber auch ohne einen solchen Erlass ist die Rechtslage eindeutig.

Was ist zu tun?

Daten aus dem Fahreignungsregister dürfen erst dann abgerufen werden, wenn die Fahrerin oder der Fahrer hinreichend ermittelt wurde und der Abruf tatsächlich erforderlich ist. Bußgeldbehörden sollten ihre Verfahren daraufhin überprüfen und ihre Mitarbeitenden entsprechend sensibilisieren.

4.3 Justiz

4.3.1 Auskunftsrecht betroffener Personen bei den Staatsanwaltschaften

Durch die Beschwerde einer betroffenen Person waren wir im Berichtszeitraum mit der Erteilung von Auskünften an betroffene Personen über die Verarbeitung ihrer personenbezogenen Daten durch den Generalstaatsanwalt befasst.

Der Beschwerdeführer hatte sich an uns gewandt, nachdem er eine Auskunft durch den Generalstaatsanwalt erhalten hatte. Ein Hinweis in dieser Auskunft ließ ihn allerdings daran zweifeln, dass die Auskunft vollständig war. Der Generalstaatsanwalt hatte den Beschwerdeführer auf die gesetzlichen Regelungen zur Einschränkung der Auskunft hingewiesen und ihm mitgeteilt, dass er ihm – bei Nachweis seiner Identität – mit diesen Einschränkungen Auskunft erteilen werde. Daraufhin erhielt der Beschwerdeführer, nachdem er seine Identität nachgewiesen hatte, in einem zweiten Schreiben eine Auskunft. Darin waren einige Verfahren aufgelistet. Darunter befand sich der Hinweis, dass er sich für den möglichen Fall einer Auskunftsbeschränkung an die Landesbeauftragte für Datenschutz wenden könne. Durch diese Hinweise auf die Möglichkeit, die Auskunft zu beschränken, war sich der Beschwerdeführer unsicher, ob er eine vollständige Auskunft erhalten hatte. Er wandte sich daher an uns; eine Überprüfung beim Generalstaatsanwalt konnte bestätigen, dass die Auskunft vollständig war.

Den pauschalen Hinweis des Generalstaatsanwalts auf die Möglichkeit, eine Auskunft einzuschränken, habe ich kritisiert. Denn dadurch ist für jede auskunftsbegehrende Person nicht ersichtlich, ob die Auskunft abschließend erteilt wurde – unabhängig davon, ob die Voraussetzungen einer Einschränkung der Auskunft in ihrem Fall vorliegen. Der Generalstaatsanwalt hat mir daraufhin mitgeteilt, dass er künftig auf solche generellen Hinweise verzichten werde.

4.3.2 Keine Kontrolle justizieller Tätigkeiten

Bereits im 39. Tätigkeitsbericht hatten wir beschrieben, dass uns viele Beschwerden über justizielle Tätigkeiten der Gerichte erreichen, für die zwar die Datenschutz-Grundverordnung gilt, für die es aber keine Kontrollstelle gibt (39. TB, Tz. 4.3.5).

Dies hat im Berichtszeitraum nun das Schleswig-Holsteinische Verwaltungsgericht bestätigt. Geklagt hatte ein Beschwerdeführer, der uns durch das Gericht verpflichten lassen wollte, in seiner Angelegenheit tätig zu werden. Er hatte sich bei uns darüber beschwert, dass ein Gericht seine Anschrift in ein Gerichtsurteil aufgenommen hatte. Er war an dem dortigen Gerichtsverfahren als Geschädigter einer Straftat und als Adhäsionskläger beteiligt, hat also in diesem Strafverfahren einen zivilrechtlichen Schadensersatzanspruch gegen den Täter geltend gemacht. Da er das Gericht darum gebeten hatte, seine

Anschrift nicht zu nennen, sah er in der Angabe der Anschrift im Urteil einen Verstoß gegen das Datenschutzrecht und wandte sich für eine Überprüfung an uns.

Nach unserer vom Verwaltungsgericht nun bestätigten Auffassung ist die Abfassung von Urteilen Teil der justiziellen Tätigkeit der Gerichte. Die Verarbeitung personenbezogener Daten für solche justiziellen Tätigkeiten unterliegt nicht der Aufsicht durch die Datenschutzaufsichtsbehörden. Dies ist bereits durch Art. 53 Abs. 3 DSGVO geregelt und wird in § 2 Abs. 2 Satz 2 LDSG nochmals klargestellt. Dies habe ich dem Beschwerdeführer mitgeteilt, der daraufhin Klage vor dem Verwaltungsgericht erhoben hat.

Das Gericht hat unsere Auffassung bestätigt. Es hat aber auch erkannt, dass im Bereich der justiziellen Tätigkeiten derzeit eine Kontrolllücke besteht. Denn es gelte zwar die DSGVO, doch die in Erwägungsgrund 20 der DSGVO vorgesehenen justizeigenen Kontrollstellen seien in Schleswig-Holstein nicht eingerichtet.

Was ist zu tun?

Für die Datenverarbeitung im Bereich der justiziellen Tätigkeit gilt zwar die DSGVO, doch es besteht eine Lücke in der Datenschutzaufsicht. Diese muss durch den Gesetzgeber geschlossen werden. Das Schleswig-Holsteinische Verwaltungsgericht führt dazu in seinem Urteil vom 8. Juni 2024 – 8 A 89/22 aus:

„Es ist richtig, dass dort, wo die Zuständigkeit der Aufsichtsbehörden nicht besteht, besondere Stellen im Justizsystem des Mitgliedstaats die Einhaltung der Vorschriften der DSGVO sicherstellen und entsprechende Beschwerden bearbeiten sollen (vgl. Erwägungsgrund 20). Es ist aber Aufgabe des Gesetzgebers, eine datenschutzrechtliche Kontrolle für den Bereich der justiziellen Tätigkeit zu schaffen. Eine solche Regelung ist aber bislang nicht geschaffen worden."

4.4 Soziales

4.4.1 Sicherer Transport von Dokumenten – sicher nicht im Kalender

Bei einem Hausbesuch von Klienten verlor ein Mitarbeiter einer sozialen Einrichtung die Dokumente mit personenbezogenen Angaben einer anderen von der Einrichtung betreuten Person. Die Unterlagen wurden bei dem nächsten Hausbesuch einer Kollegin des verursachenden Mitarbeiters übergeben. Zu dem Verlust der Unterlagen kam es, da der Mitarbeiter diese bei deren Erhalt in seinen Kalender legte. Beim Notieren eines neuen Termins müssen die Unterlagen bei der anderen Familie aus dem Kalender gefallen sein.

Die verantwortliche Stelle führte umgehend Gespräche mit dem Mitarbeiter. Er konnte nicht erklären, warum er die Unterlagen nicht bis zum nächsten Hausbesuch im Büro aufbewahrt hatte. Er gab zudem an, keine Tasche zu nutzen, sondern den Kalender händisch zu transportieren. Es folgte eine deutliche Untersagung dieses Vorgehens durch den Arbeitgeber und eine Abmahnung. Organisatorische Maßnahmen in Form einer **Dienstanweisung zum Transport von Unterlagen** wurden ebenfalls ergriffen. Die Dienstanweisung beinhaltete insbesondere, dass Unterlagen von Klienten die Büroräumlichkeiten

nicht verlassen dürfen. Eine Mitnahme der Unterlagen darf zukünftig nur in Ausnahmefällen in einer verschlossenen Tasche erfolgen. Auf diese Weise soll verhindert werden, dass Daten an unbefugte Dritte gelangen.

Die Dienstanweisung erfolgte zunächst nur mündlich während einer Dienstbesprechung. Zur leichteren Nachschlagbarkeit in zukünftigen Situationen und auch um zu gewährleisten, dass nicht nur die in der Besprechung anwesenden Mitarbeiter Kenntnis von der Dienstanweisung erlangen, **müssen Dienstanweisungen dieser Art jedoch verschriftlicht werden**. Von Bedeutung war in diesem Zusammenhang die Konkretisierung von Ausnahmefällen, in denen eine Mitnahme von Unterlagen doch erlaubt ist. Auf diese Weise schafft der Arbeitgeber für die Beschäftigten die hinreichende Transparenz für die Umsetzung der Dienstanweisung. Maßgebend für Ausnahmefälle ist gegebenenfalls auch das Vorhandensein einer Arbeitsumgebung außerhalb des Büros, in welcher die unbefugte Einsichtnahme durch Bekannte, Familienangehörige oder andere Dritte ausgeschlossen werden kann. Hierzu zählen etwa auch Erwägungen zur Anzahl der mitgeführten Akten, zur Sensibilität der Daten und zum beabsichtigten Zeitraum der Bearbeitung außerhalb der Büroräume. Weiterhin ist es sinnvoll, bei Unsicherheiten bezüglich des Vorliegens von Ausnahmefällen Rücksprache mit den Vorgesetzten zu nehmen.

Das Prüfverfahren konnte mit abschließenden Hinweisen für die Dienstanweisung beendet werden.

Was ist zu tun?

Entscheiden sich Verantwortliche dafür, die Bearbeitung von Unterlagen außerhalb der Büroräume zu erlauben, so haben diese für ihre Mitarbeitenden datenschutzrechtlich angemessene Vorgaben zu treffen, unter welchen Voraussetzungen Unterlagen mit personenbezogenen Daten ausnahmsweise transportiert werden dürfen und unter welchen Rahmenbedingungen eine solche Mitnahme von Unterlagen erfolgen darf.

4.4.2 Unbefugter Datenaustausch zwischen Mitarbeitern im Jugendamt

Einen Fehler zu machen ist verzeihlich, den Fehler aber nicht eingestehen zu wollen eher nicht. Das gilt auch für die Beschäftigten in einem Jugendamt.

Eine Beschwerdeführerin schilderte uns ihre Befürchtung, dass sich zwei Beschäftigte aus unterschiedlichen Fachdiensten eines Jugendamtes unbefugt untereinander über ihre familiäre Situation ausgetauscht hätten. Ihre zwei Kinder erhielten unterschiedliche Leistungen des Jugendamtes und wurden daher jeweils von einem der zwei Beschäftigten aus den jeweiligen Fachdiensten getrennt voneinander betreut.

Nicht immer dürfen sich Beschäftigte eines Jugendamtes untereinander über Betroffene austauschen. Das Sozialgesetzbuch VII (SGB VII) enthält hierzu eine klare Vorgabe. Betroffene Personen haben den gesetzlichen Anspruch darauf, dass Daten, die zur Erfüllung unterschiedlicher Aufgaben der Jugendhilfe erhoben wurden, nur zusammengeführt werden, wenn und solange dies **wegen eines unmittelbaren Sachzusammenhangs erforderlich ist**.

Um prüfen zu können, ob dieser Grundsatz der Zweckbindung bei der Datenverarbeitung beachtet wurde, leiteten wir ein Verwaltungsver-

fahren der Datenschutzaufsicht ein. Das Jugendamt wurde um eine Stellungnahme gebeten. Die erste Stellungnahme, die wir erhielten, war kurz und knapp. Die zwei von der Beschwerdeführerin namentlich benannten Beschäftigten wären befragt worden und hätten glaubhaft versichert, dass es keinen Datenaustausch gegeben habe. Alle Informationen habe man stets von der Beschwerdeführerin erhalten. Die Beschwerdeführerin sei sehr redselig und könne sich vielleicht nicht mehr genau daran erinnern, was sie welchem Mitarbeiter wann erzählt habe. Rums, das hatte gesessen!

Die Beschwerdeführerin war fassungslos und blieb bei ihrer Darstellung. Also wurde das Jugendamt erneut um Stellungnahme gebeten. Wieder lautete die Antwort, dass auch nach erneuter Prüfung kein unbefugter Datenaustausch habe festgestellt werden können. Beide Beschäftigten hätten erneut glaubhaft versichert, dass der befürchtete Datenaustausch nicht stattgefunden habe. Zweifel an den Aussagen der Beschäftigten gebe es nicht. Die Beschwerdeführerin war jedoch verzweifelt und wollte schon aufgeben.

Wir sicherten der Beschwerdeführerin weitere Unterstützung zu und ermutigten diese, die ihr vorliegenden Unterlagen auf Hinweise noch einmal zu überprüfen. Und siehe da, in einem Schreiben, welches der Beschäftigte A an das Familiengericht geschickt hatte, fand sich eine Information, die sie nur dem anderen Beschäftigten B mitgeteilt hatte. Die Beschwerdeführerin hatte bei dem Beschäftigten B einen Antrag gestellt und diesem gegenüber bei einer persönlichen Vorsprache begründet. Entscheidend war der zeitliche Ablauf. Wie konnte der Beschäftigte A von diesem Antrag bei seinem Kollegen B und der Antragsbegründung wissen und wie konnte er diese Informationen in seinem Schreiben an das Familiengericht aufnehmen, wenn doch die Beschwerdeführerin nachweislich erst nach Versand dieses Schreibens bei ihm vorgesprochen hatte?

Mit diesen Informationen hörten wir das Jugendamt ein drittes Mal an. Diesmal kam die Stellungnahme noch später. Und nun wurde eingeräumt, dass sich die zwei Beschäftigten in einem kollegialen Tür- und Angel-Gespräch über die Beschwerdeführerin ausgetauscht hätten, was eine **Datenschutzverletzung** darstelle.

Endlich, nach über acht Monaten, konnten wir der Beschwerdeführerin mitteilen, dass Sie recht hatte. Der Datenschutzverstoß wurde beanstandet.

4.5 Schutz des Patientengeheimnisses

4.5.1 WhatsApp und private Smartphones bei Pflegediensten

Die Beschäftigten eines ambulanten Pflegedienstes sind viel unterwegs. Ein Tourenplan gibt vor, welche Pflegebedürftigen wann welche Pflegeleistungen benötigen. Während die Beschäftigten von Wohnung zu Wohnung fahren, müssen sie trotzdem für die Pflegedienstleitung jederzeit erreichbar sein. Es könnten sich z. B. kurzfristig Änderungen im Tourenplan ergeben, weil Kollegen ausfallen. Auch die Beschäftigten müssen untereinander ihre Einsätze koordinieren.

Was liegt da näher, als WhatsApp oder einen vergleichbaren Messengerdienst zu nutzen? Ein (privates) Smartphone hat heutzutage ja fast jeder. Eine WhatsApp-Gruppe für alle Beschäftigten ist einfach eingerichtet, und schon können Informationen schnell untereinander ausgetauscht werden. Schnell ja, aber nicht sicher. Wenn Patientendaten auf diesem Weg übermittelt werden, besteht eine große Gefahr für das Patientengeheimnis.

Pflegedienste müssen bei der Übermittlung von personenbezogenen Daten, sei es von Patientinnen und Patienten oder Beschäftigten, **geeignete technische wie organisatorische Maßnahmen treffen**, um ein dem Risiko angemessenes Schutzniveau für die Rechte und Freiheiten der natürlichen Personen zu gewährleisten. Dies

gilt gerade und insbesondere wenn **sensible Gesundheitsdaten** übermittelt werden sollen. In dem White Paper der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder finden sich Ausführungen zu den „Technischen Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich":

https://www.datenschutzkonferenz-online.de/media/oh/20191106_whitepaper_messenger_krankenhaus_dsk.pdf

Kurzlink: *https://uldsh.de/tb43-4-5-1a*

Bei Prüfungen mussten wir im letzten Jahr immer häufiger feststellen, dass diese Anforderungen nicht beachtet wurden. Nach entsprechender Beratung haben die Pflegedienste andere und sichere Wege für die Kommunikation genutzt.

Kleiner Funfact: Auf die Nutzung von WhatsApp für die Übermittlung von **Patientendaten** werden wir häufig durch Beschäftigte hingewiesen, die sich im Streit von ihren Arbeitgebern getrennt haben. Zum Beweis werden uns **Screenshots von Nachrichten mit den Patientendaten** gezeigt. Screenshots, von denen wir nur hoffen können, dass sie nicht in falsche Hände gelangen.

Was ist zu tun?

Pflegedienste müssen für den Austausch von Daten ihrer Beschäftigten und Pflegebedürftigen sichere Übermittlungswege nutzen. WhatsApp und vergleichbare Messengerdienste sind nicht die Lösung. Auch die Nutzung von privaten Smartphones stellt eine Gefahr für das Patientengeheimnis dar.

4.5.2 Auskunftsrecht gegenüber Gutachtern?

Wenn medizinische Sachverhalte bewertet werden müssen, beauftragen Sozialleistungsträger externe Gutachterinnen und Gutachter. Diese sollen auf der Grundlage eines schriftlichen Auftrages und der Unterlagen, die ihnen der Sozialleistungsträger übermittelt, ein ärztliches Gutachten erstellen. In einigen Fällen tauschen sich die externen Gutachterinnen bzw. Gutachter zudem mit den behandelnden Ärztinnen und Ärzten der betroffenen Personen über deren gesundheitliche Situation aus. Natürlich nur **wenn die betroffenen Personen ihre Ärztinnen bzw. Ärzte von der Schweigepflicht entbunden haben**. Auch eine persönliche Untersuchung ist möglich. Letztendlich erstellt die Gutachterin bzw. der Gutachter ein schriftliches Gutachten und übersendet dies dem Auftraggeber.

Gutachterinnen und Gutachter erhalten durch ihre Tätigkeit Kenntnis von einer Vielzahl von **sensiblen Gesundheitsdaten** der betroffenen Personen. Diese Daten werden gespeichert und übermittelt. Haben betroffene Personen ein Recht auf Auskunft bezüglich der zu ihrer Person verarbeiteten Daten gegenüber den Gutachterinnen bzw. Gutachtern? Die Datenschutz-Grundverordnung gibt eine klare Antwort. Ja!

Auch wenn die externen Gutachterinnen und Gutachter im Auftrag eines Sozialleistungsträgers tätig werden, so sind sie doch Verantwortliche im Sinne des Datenschutzrechtes. Sie können eigenverantwortlich über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten der betroffenen Personen entscheiden. Der Auftraggeber mag die medizinische Fragestellung vorgeben, aber das Ergebnis der medizinischen Untersuchung kann er nicht vorgeben. Die Gutachterin bzw. der Gutachter entscheidet, welche Fragen gestellt bzw. welche Unterlagen benötigt werden, und sie oder er entscheidet auch, wie diese Informationen aus ihrer bzw. seiner Sicht zu bewerten sind. Auch wenn der Auftraggeber nicht an das Ergebnis der

medizinischen Begutachtung gebunden ist, so kann dieser es nicht vorgeben.

Die Beauftragung einer externen Gutachterin bzw. eines externen Gutachters stellt **keine Auftragsverarbeitung** dar. Gegenstand des Gutachtenauftrages ist gerade nicht eine durch den Auftraggeber verbindlich vorgegebene Datenverarbeitung, sondern die **medizinische Bewertung von Gesundheitsdaten einer betroffenen Person**.

Betroffene Personen haben gegenüber den Verantwortlichen und damit auch gegenüber externen Gutachterinnen und externen Gutachtern ein Recht darauf, Auskunft darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden, und sie haben, sofern dies der Fall ist, ein Recht darauf, Auskunft über diese personenbezogenen Daten zu verlangen.

Die externe Gutachterin bzw. der externe Gutachter kann eine Auskunft nicht mit dem Hinweis, dass die betroffene Person (auch) gegenüber dem auftraggebenden Sozialleistungsträger das Recht auf Auskunft habe, verweigern.

Was ist zu tun?

Externe Gutachterinnen und externe Gutachter müssen als Verantwortliche den betroffenen Personen eigenständig und eigenverantwortlich Auskunft über die zu deren Person verarbeiteten Daten erteilen.

4.5.3 Recht auf Berichtigung von Arztbriefen?

Ärztinnen und Ärzte dokumentieren medizinische Feststellungen u. a. in Arztbriefen, Entlassungs- oder Befundberichten. Mehr oder weniger detailliert können diese neben den Stammdaten der Patientin oder des Patienten auch Angaben zur Biografie, der Anamnese, über bereits gesicherte und vermutete Diagnosen und zu erfolgten und empfohlenen Behandlungen enthalten. Dies sind **sensibelste Gesundheitsdaten**, mithin besondere Kategorien schützenswerter Daten.

Andere Ärztinnen und Ärzte benötigen diese Unterlagen, um entscheiden zu können, wie die Patientin oder der Patient behandelt werden soll. Buchstäblich können diese Unterlagen und die darin enthaltenen Daten für den weiteren Lebens- oder Leidensweg der Patientinnen und Patienten entscheidend sein. Diese Unterlagen müssen daher aussagekräftig und vollständig sein. Und vor allen Dingen sollten diese Unterlagen keine unrichtigen Daten beinhalten.

Nur was ist, wenn Arzt und Patient sich nicht darin einig sind, ob die in den Arztbriefen enthaltenen Daten richtig sind? Was, wenn die Patientin oder der Patient der Einschätzung der Ärztin oder des Arztes z. B. bezüglich einer gestellten Diagnose nicht zustimmt? Hat die Patientin bzw. der Patient ein Recht auf Berichtigung?

Betroffene Personen haben das Recht, von den Verantwortlichen (und dazu gehören auch Arztpraxen) unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. So steht es in der Datenschutz-Grundverordnung. Die Daten müssen jedoch objektiv und nachweislich unrichtig sein. Dies ist z. B. der Fall, wenn Stammdaten wie der Name, die Anschrift oder das Geburtsdatum falsch wiedergegeben werden oder Angaben zu Vorbehandlungszeiten falsch sind.

Anders ist es hingegen, wenn persönliche Wahrnehmungen, Einschätzungen, Wertungen – und

hierzu gehören auch Diagnosen – der Ärztinnen und Ärzte bestritten werden. Selbst wenn eine Ärztin oder ein Arzt eine falsche Diagnose stellt, so können und müssen diese Daten in der Patientendokumentation verbleiben. Es besteht die **Pflicht zur vollständigen Dokumentation der ärztlichen Behandlung**. Alle Entscheidungen, auch falsche Entscheidungen, müssen dokumentiert werden, damit diese für die betroffenen Personen **nachvollziehbar und nachprüfbar sind und bleiben**. Die betroffenen Patientinnen und Patienten haben in diesem Fall jedoch unter Umständen ein Recht auf Einschränkung der Verarbeitung der bestrittenen Daten und die Möglichkeit zur Gegendarstellung.

Was ist zu tun?

Das Recht der Patientinnen und Patienten auf Berichtigung ihrer ärztlich dokumentierten Daten beschränkt sich regelhaft auf nachweislich unrichtige Daten. Bei den Aufzeichnungen der Ärztinnen und Ärzte über deren persönliche Wahrnehmungen und Einschätzungen haben Patientinnen und Patienten unter Umständen ein Recht auf Einschränkung der Verarbeitung und die Möglichkeit zur Gegendarstellung.

4.5.4 (Wiederholte) Versendung von Entlassungsberichten gegen den Willen der Patientin – das wird teuer!

Wenn ein Krankenhaus einen Entlassungsbericht an einen Hausarzt übersenden möchte, dann bedarf es hierfür einer Einwilligung (Schweigepflichtentbindung) von dem Patienten. Bei der Aufnahme werden Patientinnen und Patienten daher gefragt, ob sie damit einverstanden sind, dass ihr Hausarzt einen Entlassungsbericht erhält. Sagt der Patient ja, ist alles ok und der Versand kann erfolgen. Sagt er jedoch nein, dann darf der Entlassungsbericht nicht an den Hausarzt übersandt werden. Eigentlich ganz einfach, oder? Anscheinend aber nicht.

Obwohl Krankenhäuser Aufnahmeverträge bzw. Aufnahmeunterlagen verwenden, die diese Abfrage vorsehen, schildern uns Patientinnen und Patienten immer wieder, dass ein Entlassungsbericht versandt wurde, ohne dass sie vorher gefragt bzw. informiert wurden oder dass sie sogar vorher ausdrücklich einem Versand widersprochen hätten. Ein Dauerbrenner bei den Beschwerden.

Ein besonderer Fall machte uns im letzten Jahr beinahe sprachlos. Bereits 2019 beschwerte sich eine Patientin darüber, dass ihr Hausarzt einen Entlassungsbericht der Klinik erhalten hatte, obwohl sie nicht ihre Einwilligung erteilt hatte. Wir leiteten ein Verwaltungsverfahren der Datenschutzaufsicht ein und erteilten der Klinik einen formellen Hinweis. Die Klinik zeigte sich einsichtig und versprach zukünftig den Willen der Patientin zu beachten. Im **Krankenhausinformationssystem (KIS)** wurde in der Patientenakte ein Sperrvermerk aufgenommen. 2021 beschwerte sich die Patientin erneut über die Klinik. Wieder war ein Entlassungsbericht mit sensiblen Daten an den Hausarzt geschickt worden. Diesmal sprachen wir sogar eine Verwarnung aus. Die Beschwerdeführerin berichtete uns zudem, dass sie sich mit der Klinik außergerichtlich verglichen habe. Ein Schadensersatz in vierstelliger Höhe sei gezahlt worden.

Man glaubt es kaum, aber bei einem weiteren Klinikaufenthalt im Jahr 2024 wurde wiederum ein Entlassungsbericht von der Klinik an den Hausarzt geschickt. Die Beschwerdeführerin war fassungslos. Wir auch.

Unzählige Male hatte die Patientin nunmehr schriftlich und mündlich allen möglichen Personen im Krankenhaus mitgeteilt, dass ihr Hausarzt

keine Informationen über die Krankenhausaufenthalte bekommen soll. Was sollte sie denn noch machen, damit das Krankenhaus ihren Willen beachtet und sich an die datenschutzrechtlichen Vorschriften hält? Wir haben jedenfalls erneut eine Verwarnung ausgesprochen. Die Beschwerdeführerin wird unsere Bewertung zu nutzen wissen. Und wir sind gespannt, wie viel Schadensersatz die Klinik diesmal der Patientin zahlen wird.

Was ist zu tun?

Krankenhäuser und Kliniken müssen beachten, dass Entlassungsberichte grundsätzlich nur dann an die Hausärzte der Patientinnen und Patienten übermittelt werden, wenn diese zuvor hierfür ihre Einwilligung erteilt haben. Diese Einwilligung (Schweigepflichtentbindung) sollte in der Patientenakte dokumentiert werden.

4.6 Datenpannen im Medizinbereich

4.6.1 Notfalldatenordner – Verwendung nur in Notfällen!

Man sollte meinen, dass Daten in einem Notfallordner auch nur für Notfälle eingesetzt werden würden. Das schien eine Mitarbeiterin einer Klinik allerdings anders zu sehen: Sie nutzte die Namen und Telefonnummern aus einem ausgedruckten Notfallordner von Kindern privat, um den Eltern im Anschluss an ihren Aufenthalt in der Klinik Dienstleistungen anzubieten. Der Ordner wurde in einem verschlossenen Raum gelagert, zu dem nur ein begrenzter Kreis an Personen Zutritt hatte. Trotz dieser Sicherheitsvorkehrungen kam der Mitarbeiterin anscheinend nicht der Gedanke, dass die Daten nicht für private Zwecke und eventuelle Nebengewerbe für jedermann zur freien Verfügung gedacht waren. Sie kontaktierte die Eltern, um ihnen Edelmetalle zu verkaufen.

Ein Elternteil beschwerte sich bei der verantwortlichen Stelle – zu Recht. In der anschließenden Befragung der Mitarbeiterin gab sie zu, die Daten entwendet zu haben.

Als wäre das noch nicht genug, wurde auf dem privaten Instagram-Profil der Mitarbeiterin auch noch ein Video mit Bezug zu ihrer Tätigkeit in der Klinik gefunden. Auf dem Video waren verpixelt Kinder zu sehen. Es war ohne Erlaubnis mit dem Privathandy der Mitarbeiterin gedreht und für wenige Stunden veröffentlicht worden. Die Mitarbeiterin wurde aufgefordert, das Video sofort zu löschen. Immerhin – die Löschung erfolgte noch am selben Tag.

Eine fristlose Kündigung der Mitarbeiterin folgte zudem umgehend. Die Mitarbeiterin hatte im Arbeitsvertrag eine Datenschutzunterweisung und eine Verschwiegenheitserklärung unterschrieben. Alle anderen Mitarbeiterinnen und Mitarbeiter wurden aufgrund des Vorfalls nochmals zum Umgang mit sensiblen personenbezogenen Daten geschult.

Die verantwortliche Stelle erhielt von uns einen Hinweis, dass **ergänzende allgemeine Dienstanweisungen zum Thema Datenschutz und dem Umgang mit schriftlichen Gesundheitsdaten** zusätzlich zu arbeitsvertraglichen datenschutzrechtlichen Vorgaben zur **grundsätzlichen Sensibilisierung** der Mitarbeitenden sinnvoll wären und zur Verfügung gestellt werden sollten. Da die ergriffenen Maßnahmen im Übrigen den Anforderungen entsprachen und auch keine systematischen Verstöße feststellbar waren, konnte das Verfahren mit dem Hinweis zur Erstellung der Dienstanweisung eingestellt werden.

Was ist zu tun?

Um den eigenen Verpflichtungen nachzukommen, sollten Verantwortliche ihre Mitarbeitenden regelmäßig zum Umgang mit personenbezogenen Daten sensibilisieren und hierfür auch über entsprechende Sensibilisierungsunterlagen verfügen. Der alleinige Hinweis im Arbeitsvertrag zu Beginn der Tätigkeit, sich an datenschutzrechtliche Regeln zu halten, genügt nicht, um Beschäftigte auf lange Sicht hin zu sensibilisieren.

4.6.2 Verlust von Patientenunterlagen – auch für kurze Strecken reicht die Kitteltasche nicht

Für kurze Strecken schnell die Unterlagen in der Kitteltasche transportieren? Dieses Vorgehen ist nicht zu empfehlen. Gemäß einer bei dem ULD eingegangenen Datenpannenmeldung sind auf diesem Weg Patientenunterlagen verloren gegangen.

Eine Patientin sollte in eine wissenschaftliche Studie aufgenommen werden. Die Patientenaufklärung und die Einverständniserklärung wurden von der Patientin in den Räumlichkeiten eines Gebäudes unterschrieben. Das Büro des Arztes befand sich in einem anderen Gebäude. Neben dem Namen und dem Geburtsdatum ergab sich aus den Dokumenten auch die Gruppenzugehörigkeit zu einer Personengruppe mit einer seltenen Erkrankung. Die Dokumente wurden von dem Arzt zur Ablage im Büro mitgenommen. Auf dem Weg ins Büro kam es zu dem Verlust der Unterlagen.

Aufgrund der örtlichen Gegebenheiten war ein Transport der Unterlagen erforderlich. Wie sich jedoch im Laufe des von uns eröffneten Verfahrens herausstellte, wurden die Unterlagen für den Ortswechsel in der Kitteltasche des Arztes transportiert und sind auf dem Weg aus der Tasche gefallen. Glück im Unglück – die Unterlagen wurden von einem anderen Mitarbeiter gefunden und bei der verantwortlichen Stelle abgegeben.

Wie sich herausstellte, verfügte die verantwortliche Stelle über keine Vorgaben für ihre Mitarbeitenden bezüglich des Transports von Patientenunterlagen. Es wurde nachgebessert und eine Regelung in die Richtlinien für die Mitarbeitenden aufgenommen.

Die Teilnehmerin wurde über den Verlust der Unterlagen informiert. Zukünftig sollte ein Transport von Patientenunterlagen auch für kurze Strecken in geeigneter Art und Weise, also nicht mehr in der Kitteltasche, erfolgen.

Was ist zu tun?

Auch bei kurzen Wegen ist die Datensicherheit zu gewährleisten. Vorgaben seitens der verantwortlichen Stelle, wie ein Transport von Unterlagen zu erfolgen hat, sind von den Beschäftigten zu beachten.

4.6.3 Papiermüll im Papierkorb – aber leider im falschen

In einer Klinik bestand die interne Absprache mit dem Reinigungspersonal, dass Papiermüll, der datenschutzkonform im Schredder entsorgt werden müsste, vorher in einem normalen Papiermüll zwischengelagert wird. Der Papiermüll mit dem Datenmüll wurde unter einem Schreibtisch gelagert und war dort nicht direkt einsehbar. Obenauf befand sich ein Blatt mit der Aufschrift „Datenmüll", sodass dieser Papierkorb normalerweise absprachegemäß nicht von dem Reinigungspersonal in der Papiertonne entsorgt wurde.

Es kam, wie es kommen musste: Es erfolgte eine Reinigung durch eine andere Reinigungskraft außer der Reihe und der Papierkorb wurde – inklusive internem Schriftverkehr, der eigentlich für den zur Verfügung stehenden Papierschredder vorgesehen war – in die Papiertonne entleert.

Trotz der Anfrage beim Reinigungsunternehmen, ob der Papiermüll zurückgeholt werden könnte, und der Suche im Papiermüllcontainer nach dem entsprechenden Müllsack konnte der eigentlich zu schreddernde Papiermüll nicht wiedergefunden werden. Der Papiermüll war bereits von der Entsorgungsfirma abgeholt und weiterverarbeitet worden.

Da nur ein sehr geringer Zeitraum zwischen der Entleerung des Papiermülleimers und der Abholung durch das Entsorgungsunternehmen lag, konnte ein Zugriff durch weitere Personen nahezu ausgeschlossen werden.

Es folgten **Sensibilisierungen** der Mitarbeiterinnen und Mitarbeiter, Datenmüll ausschließlich in entsprechenden „Datenschutzmülleimern" zwischenzulagern, um anschließend den Papierschredder zu nutzen. Das Reinigungsunternehmen wurde trotzdem zusätzlich von der verantwortlichen Stelle gebeten, bei der Entsorgung von Papiermülleimern auf Hinweise zu achten.

Wenn Datenmüll in Papierform nicht unverzüglich geschreddert wird, müssen **abschließbare Behälter als „Datenschutzmülleimer"** zur Zwischenlagerung verwendet werden. Die Zugriffsmöglichkeit auf Unterlagen für unberechtigte Dritte, wie z. B. Reinigungspersonal, wird auf diese Weise datenschutzkonform verhindert.

Was ist zu tun?

Verfügen Verantwortliche über technische und organisatorische Maßgaben für die Entsorgung von Unterlagen mit personenbezogenen Daten, sollten diese zum Schutz der zu entsorgenden Daten auch eingehalten und entsprechende Behältnisse verwendet werden.

4.7 Bildung

4.7.1 Ärztliche Bescheinigung zum Nachweis der Prüfungsunfähigkeit

Das ULD war mit der Frage befasst, welche Anforderungen die Hochschulen an den Nachweis der Prüfungsunfähigkeit bei der Studentenschaft stellen dürfen. So wird in Prüfungsordnungen der Hochschulen geregelt, dass in den Fällen eines Rücktritts vom Prüftermin oder beim Versäumen des Prüftermins die Prüfung als nicht ausreichend bewertet wird, es sei denn, es liegen besondere, von der oder dem Studierenden nicht zu vertretende Gründe vor. Ein solcher

Grund kann darin bestehen, dass **der Prüfungstermin krankheitsbedingt nicht wahrgenommen werden konnte**. Diese krankheitsbedingte Prüfungsunfähigkeit ist wiederum durch ein ärztliches Attest unter Angabe der voraussichtlichen Dauer der Prüfungsunfähigkeit glaubhaft darzulegen.

Auszug aus der Prüfungsordnung einer Hochschule

Tritt eine Kandidatin oder ein Kandidat von ihrer oder seiner Modulprüfung nach Frist der Anmeldung oder nach Beginn der Prüfung zurück oder versäumt sie oder er den Termin der Prüfung, so gilt diese als mit „nicht ausreichend (5,0)" bewertet, es sei denn, es liegt ein triftiger und nicht von der bzw. dem Studierenden zu vertretender Grund vor [...]. Bei Rücktritt oder Versäumnis wegen Krankheit am Prüfungstag ist unverzüglich ein ärztliches Attest unter Angabe der voraussichtlichen Dauer der Prüfungsunfähigkeit [...] vorzulegen [...]. Bei lang andauernder und wiederholter Krankheit kann der zuständige Prüfungsausschuss die Vorlage eines amtsärztlichen Attestes verlangen.

Die Rechtsprechung hat in den vergangenen Jahren hierzu Stellung genommen. Demnach gilt:

- Nicht die Ärztin oder der Arzt, sondern das zuständige Prüfungsamt bzw. ein Prüfungsausschuss entscheidet darüber, ob die nachgewiesenen Gründe einen Rücktritt von der Prüfung rechtfertigen, also ob Prüfungsunfähigkeit vorliegt.
- Die in einem ärztlichen Attest enthaltene Einschätzung, dass Prüfungsunfähigkeit bestehe, bildet nur ein Indiz für das Vorliegen von Prüfungsunfähigkeit.
- Die ärztliche Verpflichtung beschränkt sich darauf, krankhafte Beeinträchtigungen zu beschreiben und darzulegen, welche Auswirkungen diese auf das Leistungsvermögen des Prüflings in der konkret abzulegenden Prüfung haben.
- Die von Hochschulen erbetene Angabe von Befundtatsachen hat die Rechtsprechung nicht beanstandet. Diese beziehen sich auf Krankheitssymptome, die zu einer Verringerung der Leistungsfähigkeit führen können.

Der Nachweis der Prüfungsunfähigkeit ist nach Einschätzung des ULD von einer Bescheinigung über das Bestehen einer Arbeitsunfähigkeit zu unterscheiden. Letzteres wird in § 5 Abs. 1 des Entgeltfortzahlungsgesetzes (EnzFG) geregelt, wonach der Umstand der Arbeitsunfähigkeit und deren voraussichtliche Dauer dem Arbeitgeber mitzuteilen sind. Vorliegend handelt es sich aber um eine Glaubhaftmachung der Prüfungsunfähigkeit, wobei zusätzlich eine **Mitteilung von Befundtatsachen** geboten sein kann.

Aus Sicht des ULD ist jedoch für die Hochschulen eine Kenntnis der ärztlichen Diagnose nicht erforderlich. Maßgebend sind nur Angaben zu den durch die Krankheit hervorgerufenen physischen und psychischen Auswirkungen auf die Leistungsfähigkeit. Hinzu kommt, dass die Hochschulen für die Verarbeitung entsprechend **sensibler Gesundheitsdaten** eine hinreichende gesetzliche Ermächtigung brauchten, etwa im Hochschulgesetz, um im Rahmen des Erlasses eigener Satzungen und Prüfungsordnungen derartige Regelungen treffen zu dürfen. Weiterhin kommt das ULD zu der Einschätzung, dass die Hochschulen die Diagnosedaten nicht auf Grundlage einer Einwilligung des Prüflings bzw. einer Schweigepflichtentbindungserklärung der Ärztin oder des Arztes fordern dürfen, da sich der zulässige Datensatz auf die Befundtatsachen beschränkt. Die Einwilligung kann aber auch nicht auf die Bereitstellung der Angaben zu den Befundtatsachen gestützt werden, wenn bezüglich dieser Daten eine hinreichende rechtliche Grundlage in einer Prüfungsordnung der Hochschule vorhanden ist. Anderenfalls entstünde bei den Prüflingen der Eindruck, dass die Erklärung der Einwilligung freiwillig ist, deren Nichterklärung keine Konsequenzen hat und die Erklärung frei widerruflich ist. Einwilligungen bedürften zu ihrer Wirksamkeit gerade der beschriebenen Wahlfreiheit ohne negative Folgen und eine Belehrung zur jederzeitigen Widerruflichkeit. Besteht aber eine Rechtsgrundlage für die Erhebung der Befundtatsachen, wäre die Verwendung eines Einwilligungsformulars irreführend.

Was ist zu tun?

Die Hochschulen müssen prüfen, ob die Erhebung der Befundtatsachen im internen Hochschulrecht, insbesondere in maßgeblichen Prüfungsordnungen, normiert ist. Besteht eine entsprechende Legitimation, ist die Einholung einer Einwilligung zur Mitteilung von Befundtatsachen entbehrlich. Diagnosedaten dürfen die Hochschulen nicht erheben, um eine Prüfungsunfähigkeit zu untersuchen. Weiterhin müssen die Hochschulen prüfen, ob generell für die Erhebung von Gesundheitsdaten von Prüflingen zum Nachweis der Prüfungsunfähigkeit eine ausreichende gesetzliche Ermächtigung besteht, um Näheres im internen Hochschulrecht, etwa in einer Prüfungsordnung, zu regeln.

4.8 Datenschutz- und Medienkompetenz

Datenschutzkompetenz ist ein zentraler Teil der Medienkompetenz. Ziel ist die Vermittlung des Wissens über einen verantwortungsbewussten Umgang mit personenbezogenen Daten. In der heutigen stark durch Technik geprägten Gesellschaft ist Datenschutzkompetenz – wie auch Medienkompetenz – eine wichtige Fähigkeit.

4.8.1 Mitarbeit AK Datenschutz-/Medienkompetenz

Die Datenschutzbehörden der Länder und des Bundes organisieren ihre Zusammenarbeit in regelmäßig tagenden Arbeitskreisen (AK). Im Bereich Datenschutzkompetenz ist dies der **AK Datenschutz-/Medienkompetenz**. Die Leitung des AK untersteht seit dem Sommer 2024 dem Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern.

Der Fokus in diesem Arbeitskreis liegt auf dem Erfahrungsaustausch und der Abstimmung der Aufsichtsbehörden in den entsprechenden Bereichen der **Datenschutzkompetenzvermittlung**.

Im Jahr 2024 waren die wichtigsten Themen des Arbeitskreises u. a. die aktuellen Entwicklungen und Planungen für den **Internetauftritt des Jugendportals zum Thema Datenschutz und Informationsfreiheit** der Datenschutzkonferenz (DSK). Das Jugendportal mit dem Namen **„YoungData“** richtet sich speziell an Kinder und Jugendliche. Weitere Punkte waren u. a. die Zusammenarbeit mit den anderen Arbeitskreisen und mit der Kultusministerkonferenz (KMK).

4.8.2 Mitarbeit im Netzwerk Medienkompetenz Schleswig-Holstein

Das **Netzwerk Medienkompetenz Schleswig-Holstein** hat sich im Jahr 2010 gegründet und besteht aus derzeit 19 landesweit tätigen Institutionen und Organisationen. Ziel des Netzwerks ist es, die vielfältigen Angebote zur Vermittlung von Medienkompetenz zu bündeln und damit den Bürgerinnen und Bürgern Schleswig-Holsteins die Möglichkeit zu eröffnen, ein angemessenes Maß an Medienkompetenz zu erwerben.

In der von der Staatskanzlei Schleswig-Holstein im Jahr 2023 vorgestellten **Medienkompetenzstrategie** für das Land Schleswig-Holstein nimmt das Netzwerk Medienkompetenz eine wichtige Rolle bei der Medienkompetenzvermittlung im Land ein. Im Jahr 2024 wurde zwischen den Mitgliedern des Netzwerkes diskutiert, wie sich das Netzwerk im Sinne der Medienkompetenzstrategie des Landes weiterentwickeln kann. Dabei wurden verschiedene Optionen unter den Mitgliedern des Netzwerks diskutiert.

Eine zentrale Veranstaltung in jedem Jahr ist das Medienkompetenz-Festival (ehemals Medienkompetenztag) im November. Das ULD war wie in den vergangenen Jahren auch mit einem Informationsstand vertreten und war als Ansprechpartner im Bereich Datenschutz und Datenschutzkompetenz wieder stark nachgefragt.

05

KERNPUNKTE

Falschüberweisungen

Muttizettel

Videoüberwachung

Bußgelder für Datenschutzverstöße

5 Datenschutz in der Wirtschaft

5.1 Interessenkonflikte von Datenschutzbeauftragten

Beim ULD gingen Beschwerden bezüglich zweier Unternehmen ein, die sich auf mögliche Interessenkonflikte der betrieblichen Datenschutzbeauftragten bezogen. In beiden Fällen war der **Datenschutzbeauftragte in Führungspositionen** (Leiter der IT-Abteilung und Leiter der Konzernsicherheit) tätig.

Gemäß Art. 37 Abs. 6 DSGVO kann der Datenschutzbeauftragte andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen. Ein solcher **Interessenkonflikt** liegt in der Regel vor, wenn der Datenschutzbeauftragte **sich selbst kontrollieren** müsste oder in der Lage ist, **Datenverarbeitungsprozesse zu bestimmen** oder wesentlich zu beeinflussen.

> **Art. 37 Abs. 6 DSGVO**
>
> Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

In beiden beim ULD eingegangenen Fällen lag ein solcher Interessenkonflikt vor. Sowohl als **Leiter der IT-Abteilung** als auch **als Leiter der Konzernsicherheit** waren die Datenschutzbeauftragten in der Lage, Datenverarbeitungsprozesse zu bestimmen oder wesentlich zu beeinflussen. Zudem erfolgte in der vorliegenden Konstellation eine Kontrolle der eigenen Person, eben nur in einer anderen Funktion.

Die Unternehmen wurden durch das ULD im Rahmen eines aufsichtsbehördlichen Verfahrens zum Sachverhalt angehört. Es wurden zudem die datenschutzrechtlichen Vorgaben in Bezug auf den Interessenkonflikt eines Datenschutzbeauftragten sowie die Rechtsauffassung des ULD umfassend erläutert.

Beide Unternehmen argumentierten in ihren Stellungnahmen damit, dass durch umfassende **organisatorische Regelungen** Interessenkonflikte der Datenschutzbeauftragten ausgeschlossen werden konnten. In einem Fall kam jedoch noch erschwerend hinzu, dass der Datenschutzbeauftragte in seiner Funktion als Leiter der Konzernsicherheit die Abteilung Datenschutz fachlich sowie disziplinarisch führte. Die Aufgabe dieser Abteilung war es u. a., den Datenschutzbeauftragten in der Erfüllung seiner Aufgaben zu unterstützen. Auch hier war keine unabhängige Überwachung möglich. Weiterhin erfolgte eine Aufteilung der Aufgaben nach Artikel 39 DSGVO auf den Datenschutzbeauftragten und die Abteilung Datenschutz. Somit wurden seitens des Verantwortlichen Aufgaben des Datenschutzbeauftragten übernommen, und es kam somit zu einer **unzulässigen Vermengung des Verantwortungsbereichs des Verantwortlichen und der Aufgaben des Datenschutzbeauftragten**.

Die angeführten organisatorischen Regelungen waren daher aus Sicht des ULD nicht geeignet, um einen Interessenkonflikt auszuschließen. In beiden Fällen zeigten sich die Unternehmen einsichtig, und es wurden **neue Datenschutzbeauftragte benannt**.

Aufgrund der Benennung neuer Datenschutzbeauftragter wurden die aufsichtsbehördlichen Verfahren eingestellt. Es wurde abschließend nochmals darauf hingewiesen, dass auch in der jetzt vorliegenden Konstellation gewährleistet bleiben muss, dass es zu keinem Interessenkonflikt der Datenschutzbeauftragten kommen kann.

5.2 Stolperfallen beim Führen einer digitalen Akte

Die digitale Akte findet in immer mehr Bereichen Einzug, was aber bei einigen betroffenen Personen durchaus noch zu Irritationen führen kann.

Im Rahmen eine Beschwerde beklagte sich ein Mann darüber, dass er seine **persönlichen Unterlagen** im Rahmen einer Terminvereinbarung einer Sekretariatskraft **zum Scannen** übergeben sollte. Dies verweigerte er. Im Rahmen eines einige Tage später geführten Beratungsgesprächs beklagte er sich dann darüber, dass der zuständigen Sachbearbeiterin nicht alle Unterlagen vorlagen. Nach seiner Auffassung seien diese dort zwischenzeitlich verschwunden.

Im Rahmen des Verfahrens erläuterte die verantwortliche Stelle, dass sie keine Papierakten mehr führe und alle eingehenden Schriftstücke ausnahmslos durch Scannen digitalisiere, in ihr **elektronisches Aktensystem** überführe und der jeweiligen Vorgangsakte zuordne. Wenn sich betroffene Personen der Erstellung eines elektronischen Doppels für das dort genutzte elektronische Aktensystem verweigern würden, führe dies allerdings dazu, dass die entsprechenden Unterlagen nicht vorliegen und auch nicht bearbeitet werden können.

Da der Betroffene in dem streitgegenständlichen Fall seine Unterlagen zu dem Beratungstermin nicht dabeihatte, seien diese in den darauffolgenden Tagen durch die Ehefrau persönlich eingereicht, dort **in die elektronische Akte überführt** und anschließend wieder zurückgegeben worden.

Da die verantwortliche Stelle abschließend nochmals betonte, dass **keine Unterlagen verschwunden** oder verloren gegangen seien, die übergebenen Schriftstücke ausschließlich elektronisch in der dort geführten Verfahrensakte vorhanden seien und sich die Originale im Besitz des Betroffenen befinden, konnte das Verfahren eingestellt werden.

Was ist zu tun?

Auch für das Abfordern von Unterlagen zum Scannen ist ausreichende Transparenz nötig, warum dies geschehen soll: Der Verantwortliche hat die betroffene Person in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache u. a. auch über den Zweck der Verarbeitung zu informieren.

5.3 Versehentliche Falschüberweisung

Das ULD erreichte eine Beratungsanfrage eines Bürgers. Er nutze Onlinebanking, und dabei sei ihm ein Fehler unterlaufen. Er habe eine Überweisung, die er regelmäßig tätige, an eine **veraltete Bankverbindung** geschickt. Die Bankverbindung sei derweil neu vergeben worden. Nachdem ihm der Fehler aufgefallen sei, habe er sich umgehend mit seiner Bank und der Bank des Falschempfängers in Verbindung gesetzt. Er habe den Falschempfänger ausfindig und zur Erstattung auffordern wollen. Bei der Bank des Empfängers wurde ihm jedoch mitgeteilt, dass aus Gründen des Datenschutzes **keine Angaben** gemacht werden dürften.

Die Aufgabe des ULD war daher, unter Zugrundelegung der zur Verfügung stehenden Informationen zu prüfen, ob eine **Weitergabe der Daten des Falschempfängers** durch die Bank in diesem Fall tatsächlich gegen die Vorgaben der DSGVO verstoßen hätte.

Bei den Kontaktinformationen (Name und Adresse) des Kontoinhabers handelt es sich

zweifellos um personenbezogene Daten. Die Weitergabe dieser Daten stellt eine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO dar.

Art. 4 Nr. 2 DSGVO

„Verarbeitung" beschreibt jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Eine Verarbeitung bedarf für ihre Rechtmäßigkeit einer **Rechtsgrundlage** gemäß Artikel 6 DSGVO. Im konkreten Fall kam eine Verarbeitung aufgrund eines berechtigten Interesses gemäß Art. 6 Abs. 1 Buchst. f DSGVO in Betracht.

Art. 6 Abs. 1 Buchst. f DSGVO

Demnach ist eine Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Verantwortliche war hier die Bank, der Ratsuchende war der Dritte und der Falschempfänger die betroffene Person. Das **Interesse des Ratsuchenden war legitim** und damit berechtigt. Das berechtigte Interesse bestand in der Geltendmachung des Herausgabeanspruchs gemäß § 812 Abs. 1 des Bürgerlichen Gesetzbuches (BGB) gegen den Geldempfänger. Dieser Herausgabeanspruch ergibt sich aus geltendem Recht und steht somit in Einklang mit der Rechtsordnung. Das **Kriterium der Erforderlichkeit** lag ebenfalls vor, da der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden konnte.

Letztlich überwogen die Interessen oder Grundrechte und Grundfreiheiten des Falschempfängers nicht. Aufseiten der betroffenen Person war insbesondere das Grundrecht aus Artikel 8 der Grundrechtecharta (GRCh) zu beachten, wonach jede Person das Recht auf den Schutz ihrer personenbezogenen Daten hat. Allerdings ergibt sich aus Artikel 8 GRCh, dass Eingriffe grundsätzlich möglich sind. Diese Interessen waren jedoch im Ergebnis nicht höher zu werten als das Interesse an der Geltendmachung des Erstattungsanspruchs, denn der Verfolgung eigener Rechtsansprüche gegen die betroffene Person (also dem Geldempfänger) kommt ein besonders hohes Gewicht zu. Immerhin war der **Geldempfänger ungerechtfertigt bereichert**.

Zudem hätte eine Weitergabe der Kontaktdaten auch keine unverhältnismäßigen Folgen für den Kontoinhaber bzw. Geldempfänger gehabt. Dieser hätte lediglich den Geldbetrag erstatten müssen, der ihm ohnehin nie zustand. Von besonderer Bedeutung war letztlich im konkreten Sachverhalt noch, dass die Bank des Falschempfängers **in ihren Allgemeinen Geschäftsbedingungen (AGB) auch keine gegenteilige Regelung** traf. Demnach stand lediglich die Erteilung von Bankauskünften unter einem Einwilligungsvorbehalt. Bankauskünfte waren in den AGB als allgemein gehaltene Feststellungen und Bemerkungen über die wirtschaftlichen Verhältnisse von Kunden, der Kreditwürdigkeit und Zahlungsfähigkeit definiert. Die Kontaktdaten der betroffenen Person waren damit nicht umfasst, und deren Weitergabe stand daher nicht unter dem Einwilligungsvorbehalt.

Zwar bestand im Ergebnis keine Verpflichtung der Bank, die Kontaktdaten der betroffenen Person dem Dritten mitzuteilen. Allerdings hatte diese die Befugnis hierfür. **„Gründe des Datenschutzes" standen dem jedenfalls nicht entgegen.**

Im nächsten Schritt empfahlen wir dem Ratsuchenden, dass er sich mit unserer Einschätzung **an den Datenschutzbeauftragten der Bank wenden** solle, um über diesen eine weitere Klärung der Angelegenheit zu erzielen.

Einige Zeit später erhielten wir einen Anruf von einem sehr erleichterten Ratsuchenden. Er habe sich an den Datenschutzbeauftragten der Bank gewendet. Einige Tage später habe er auf seinem Konto eine Erstattung in Höhe des fälschlich überwiesenen Betrages verzeichnen können. Die Bank sei offenbar auf ihren Kunden zugegangen und habe die Angelegenheit mit diesem regeln können. Letztlich habe sich damit die Sache sogar ohne Weitergabe der Kontaktinformationen aus der Welt schaffen lassen.

5.4 Eintreibung der Schuld um jeden Preis – auch beim Falschen

Ende des Jahres 2023 erreichte uns die „Datenpannenmeldung" eines Inkassounternehmens. Hierin wurde die **Zustellung mehrerer Schreiben an einen falschen Schuldner** gemeldet. Dieser Fehlversand erfolgte nach Angaben der verantwortlichen Stelle aufgrund einer Unachtsamkeit der Sachbearbeitung sowie der falschen Zuordnung der Fallnummer im System. Auf Basis des dargelegten Ablaufs wurde der Sachverhalt detailliert geprüft und von uns als **deutlich weitreichender** eingestuft als von der verantwortlichen Stelle angenommen.

Dem von einem Elektrohandel beauftragten Einzugsverfahren lag eine entsprechende Rechnung zugrunde, welche auf ein Gewerbe sowie eine explizite Person (Schuldner A) ausgestellt war. Nach der systemseitigen Anlage des Inkassoverfahrens wurde der Schuldner allerdings entgegen der Rechnungsadresse auf den Inhaber des benannten Gewerbes und **nicht auf den vom Elektrohandel explizit benannten Schuldner A** geführt. Eine Rücksprache mit dem beauftragenden Elektrohandel bezüglich der Änderung der Schuldnerdaten auf den neuen Schuldner B erfolgte nicht.

In den darauffolgenden Monaten wurden zum Einzug der Schuld mehrere Mahnbescheide an den Schuldner B versendet, wobei es aufgrund von Unzustellbarkeiten immer wieder zu Anpassungen der Adressdaten kam. Durch eine **Anfrage beim Einwohnermeldeamt** konnte schließlich die aktuelle Anschrift des Schuldners B ermittelt und das Mahnverfahren mit der Zustellung des Vollstreckungsbescheids abgeschlossen werden.

Durch die darauffolgende **eingeleitete Zwangsvollstreckung** erlangte der Elektrohandel Kenntnis von den abgeänderten Schuldnerdaten. Daraufhin bat der Elektrohandel das Inkassounternehmen um entsprechende **Korrektur, damit das Verfahren wieder gegen den ursprünglichen Schuldner A geführt werden könne**. Obwohl hiermit auf einen eindeutigen Fehler der Schuldnerdaten hingewiesen und um Berichtigung gebeten wurde, entschied sich das Inkassounternehmen eigenmächtig dazu, das Verfahren weiterhin gegen Schuldner B laufen zu lassen.

Auf Basis dieser vorsätzlichen Entscheidung folgte nun wissentlich der Versand von zwei weiteren Schreiben sowie eines **Mahnbescheids an den falschen Empfänger** – den Schuldner B. Dies wurde seitens des Inkassounternehmens damit begründet, dass von einer bevollmächtigten Vertretung ausgegangen wurde, ohne dies allerdings geprüft zu haben. Zudem wurde aufgrund des fehlenden Einspruchs des Schuldners B gegen den Vollstreckungsbescheid vermutlich davon ausgegangen, dass das Verfahren auf diesem Wege effektiver umgesetzt werden könne.

Erst als auf den falsch zugestellten Mahnbescheid ein **Widerspruch** seitens Schuldner B eingereicht wurde, der nochmals darauf verwies, dass Schuldner A der richtige Adressat des Verfahrens sei, wurde der Auftrag gegen Schuldner B zurückgenommen.

Zwar lag in diesem Fall tatsächlich im Grunde genommen ein Fehlversand von Schreiben und Mahnbescheiden vor, allerdings war unsererseits das grundsätzliche Vorgehen und die **damit verbundenen vorsätzlichen Datenschutzverstöße** zu beanstanden. Im Rahmen des durchgeführten aufsichtsbehördlichen Verfahrens wurde auf die Missstände hingewiesen.

Im weiteren Verlauf der Anhörungen widersprach das Inkassounternehmen seiner eigenen Ursprungsmeldung und teilte uns mit, dass das Verfahren fälschlicherweise und nicht vorsätzlich gegen Schuldner B weitergeführt wurde und dabei die Annahme eines korrekten Empfängers bestand. Dies erschien bei den hier ursprünglich getroffenen Äußerungen der „Datenpannenmeldung“ allerdings nicht glaubhaft. Das Unternehmen wurde aufgrund der hier vorliegenden vorsätzlichen Datenschutzverstöße **verwarnt**. Das Inkassounternehmen hat aufgrund des Vorfalls die Mitarbeiterinnen und Mitarbeiter auf die relevanten Merkmale der Schuldnerzuordnung aus datenschutzrechtlicher Sicht erneut hingewiesen und sensibilisiert.

Was ist zu tun?

Der (mögliche) Erfolg eines unternehmerischen Vorgehens darf nicht über die Einhaltung datenschutzrechtlicher Vorgaben gestellt werden.

5.5 Einführung eines neuen Kontomodells – Anforderungen an eine Einwilligung

Beim ULD gingen mehrere Beschwerden ein, die sich auf die Einführung eines **neuen Kontomodells** bei einem in Schleswig-Holstein ansässigen Kreditinstitut bezogen. Neben den üblichen Leistungen eines Girokontos wurden weitere **Mehrwertleistungen wie Cashback, Reisebuchungsservice sowie Versicherungen** angeboten. Hierzu bediente sich das Kreditinstitut eines externen Dienstleisters, der die Abwicklung der nicht bankspezifischen Leistungen übernehmen sollte. Zur Durchführung dieser Leistungen sollten Kunden dem Kreditinstitut gegenüber eine Einwilligung zur Übermittlung ihrer personenbezogenen Daten an den Dienstleister geben – einschließlich der Erklärung, dass dieser die Kunden zu Angeboten direkt kontaktieren durfte.

Die dem ULD vorliegenden Beschwerden bezogen sich auf den Umstand, dass in der neuen Rahmenvereinbarung für das Girokonto die Einwilligung zur Kontaktaufnahme durch den Dienstleister **bereits angekreuzt** war und es somit keine Möglichkeit gäbe, dies abzulehnen. Weiterhin wäre den Kunden suggeriert worden, dass eine **mögliche Kündigung ihres Girokontos** drohe, wenn diese nicht auf das neue Kontomodell umstiegen und somit der **Weitergabe ihrer Daten** an den Dienstleister und der **Kontaktaufnahme zu Werbezwecken** zustimmten. Die Anforderungen an eine Einwilligung sind in der DSGVO umfassend geregelt.

Art. 4 Nr. 11 DSGVO

Der Ausdruck „Einwilligung“ bezeichnet jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Die betroffene Person muss zudem eine **echte und freie Wahl** haben. Sie muss die Einwilligung zudem jederzeit ohne Nachteile verweigern und zurückziehen können. Zudem gibt der Erwägungsgrund 32 der DSGVO vor, dass **bereits angekreuzte Kästchen keine Einwilligung** der betroffenen Person darstellen sollten. Gemäß Art. 7 Abs. 2 DSGVO sind Teile der Erklärung zudem dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

Erwägungsgrund 32 Satz 3 DSGVO

Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten keine Einwilligung darstellen.

Das Kreditinstitut wurde durch das ULD im Rahmen eines aufsichtsbehördlichen Verfahrens zum Sachverhalt angehört. Es wurden zudem die datenschutzrechtlichen Vorgaben in Bezug auf die Anforderungen an eine wirksame Einwilligung umfassend erläutert.

Seitens des Kreditinstituts folgten daraufhin weitreichende Anpassungen. Es wurde festgelegt, dass **keine werbliche Nutzung der Kundendaten** durch den Dienstleister erfolgen darf. Die Rahmenvereinbarung wurde dahin gehend geändert, sodass zukünftig auch **keine vorher angekreuzten Kästchen** mehr verwendet werden. Die bisher eingeholten **unwirksamen Einwilligungen** wurden fortan nicht mehr als aktive Einwilligung dokumentiert und werden nicht als Rechtsgrundlage für werbliche Maßnahmen genutzt.

Weiterhin wurde angeführt, dass es **alternative Kontomodelle ohne Mehrwertleistungen** und der damit verbundenen Weitergabe der Daten an den Dienstleister geben würde, sodass Kunden keine Nachteile im Falle einer nicht erteilten Einwilligung entstehen. Zusätzlich wurden die Mitarbeitenden hinsichtlich der Kommunikation mit den Kunden **sensibilisiert**, da eine Kündigung der Konten, wie teilweise kommuniziert, nicht vorgesehen war.

Aufgrund der umfangreichen Anpassungen wurde das aufsichtsbehördliche Verfahren mit **Erteilung eines Hinweises** nach Art. 58 Abs. 1 Buchst. d DSGVO eingestellt.

5.6 Erziehungsbeauftragung mittels des Muttizettels

Uns erreichte eine Beschwerde in Bezug auf das Verfahren zur **Alterskontrolle einer Diskothek**. Diese hatte im Rahmen dieser Alterskontrolle Kopien des Personalausweises der Erziehungsberechtigten eingesammelt, deren jugendliche Kinder die Abendveranstaltung mittels des sogenannten **Muttizettels** besuchen wollten. Es konnte seitens der Beschwerdeführerin nicht nachvollzogen werden, aus welchem genauen Grund ein Einsammeln der Kopien erforderlich gewesen war.

Gemäß § 4 Abs. 1 Jugendschutzgesetz (JuSchG) darf **Jugendlichen ab 16 Jahren** der **Aufenthalt in Gaststätten** ohne Begleitung einer personensorgeberechtigten oder erziehungs-beauftragten Person in der Zeit von 24 Uhr und 5 Uhr morgens nicht gestattet werden.

Eine Möglichkeit zur Teilnahme an solchen Veranstaltungen besteht in einer **Erziehungsbeauftragung** nach § 1 Nr. 4 JuSchG. In diesem Fall kann der Erziehungsauftrag an eine volljährige Person übertragen werden. Diese **Erziehungsbeauftragung** wird **umgangssprachlich Muttizettel** genannt und soll als Nachweis im Rahmen einer Alterskontrolle zusammen mit der Kopie des Personalausweises eines Erziehungsberechtigten vorgezeigt werden. Ein **Einsammeln der Personalausweiskopie** ist hierbei jedoch **nicht erforderlich**.

§ 4 Abs. 1 Jugendschutzgesetz

Jugendlichen ab 16 Jahren darf der Aufenthalt in Gaststätten ohne Begleitung einer personensorgeberechtigten oder erziehungsbeauftragten Person in der Zeit von 24 Uhr und 5 Uhr morgens nicht gestattet werden.

§ 1 Nr. 4 Jugendschutzgesetz

Eine erziehungsbeauftragte Person ist jede Person über 18 Jahre, soweit sie auf Dauer oder zeitweise aufgrund einer Vereinbarung mit der personensorgeberechtigten Person Erziehungsaufgaben wahrnimmt.

Der Verantwortliche wurde im Rahmen eines aufsichtsbehördlichen Verfahrens zum Sachverhalt angehört. Dieser gab an, dass die Kopien zum Nachweis der vollzogenen Einlass- und Alterskontrolle gegenüber dem Ordnungsamt eingesammelt worden wären. Man habe jedoch bereits direkt nach der Veranstaltung **Zweifel an dem Einsammeln** gehabt und die **Ausweiskopien datenschutzkonform vernichten lassen**. Es wurde jedoch darauf hingewiesen, dass eine Einsichtnahme in die Personalausweiskopien zwecks eines **Abgleichs der Daten auf dem Muttizettel erforderlich** sei.

Seitens des ULD konnte nachvollzogen werden, dass eine Einsichtnahme in die Personalausweiskopien sowie der Abgleich mit dem Muttizettel erforderlich ist, um zu prüfen, ob tatsächlich eine Erziehungsbeauftragung im Sinne des Jugendschutzgesetzes erfolgt ist. Es wurden verfahrensabschließend noch folgende **Vorgaben an den Verantwortlichen** übermittelt:

- Es darf **kein Einsammeln** der Personalausweiskopien erfolgen.
- Es wird auch keine Erforderlichkeit dafür gesehen, den Muttizettel einzusammeln.
- Der Abgleich ist auf die erforderlichen Daten, die sich auf dem Muttizettel befinden, zu beschränken.
- Es kann eine **Schwärzung der Personalausweiskopien hinsichtlich der nicht relevanten Daten** erfolgen.

5.7 Verkauf von Mitgliederdaten durch Verein zum Zweck der Direktwerbung

Nachdem eine betroffene Person überraschend **Werbung von einer fremden Stiftung** erhielt, bat sie diese zunächst um Auskunft über die Herkunft ihrer Daten. Hierzu wurde ihr mitgeteilt, dass diese von einem Verein stammen, in dem sie Mitglied sei. Ein Vorstandsmitglied des Vereins sei zugleich auch Vorsitzende der Stiftung und hätte in dieser Funktion eine **Vereinbarung zur Nutzung von Mitgliederdaten** zur einmaligen Verwendung für einen postalischen Versand von Unterlagen der Stiftung abgeschlossen. Hierfür habe der Verein von der Stiftung ein im Bereich des Adresshandels marktübliches Entgelt erhoben.

Nach Angabe der betroffenen Person hätten die Vereinsmitglieder **weder** einer entsprechenden Verwendung ihrer Mitgliederdaten zum Zweck der Werbung für einen Dritten **zugestimmt noch** seien sie durch den Verein über eine solche Nutzung und die bestehenden Betroffenenrechte **informiert** worden.

Im Rahmen des aufsichtsbehördlichen Verfahrens erläuterte der Verein zunächst ein aus seiner Sicht bestehendes **berechtigtes Interesse an der Veräußerung der Daten** und die hierdurch bestehende Möglichkeit einer Einnahmeerzielung sowie den Art. 6 Abs. 1 Buchst. f DSGVO als mögliche Rechtsgrundlage.

Grundsatz der Zweckbindung

Nach Art. 5 Abs. 1 Buchst. b DSGVO müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Das ULD wies darauf hin, dass die Nutzung von Daten für eigene Werbezwecke und der Handel mit Daten zwei unterschiedliche Verarbeitungszwecke darstellen, die keinesfalls in dem jeweils anderen enthalten sind. Des Weiteren enthalte der hierbei zu berücksichtigende Erwägungsgrund 47 lediglich eine Aussage zur Direktwerbung als ein mögliches berechtigtes Interesse. Da er darüber hinaus auch keine Vorwegnahme der durchzuführenden Interessenabwägung enthalte, sind auch hierbei die vernünftigen Erwartungen der betroffenen Person und die Beziehung zwischen der betroffenen Person und dem Verantwortlichen maßgeblich. Es entspricht **nicht den allgemeinen Erwartungen eines Vereinsmitglieds**, dass seine Daten gegen Entgelt zum Zwecke von Spendenaufrufen für einen Dritten genutzt werden und er entsprechende **Werbung** hierfür erhält.

Unter Bezugnahme auf die vom Verein ebenfalls erwähnte alte Fassung des bis 2018 geltenden **§ 28 Bundesdatenschutzgesetz (BDSG a. F.)** und die dort enthaltene gesetzliche Privilegierung wurde der Verein des Weiteren darauf hingewiesen, dass diese vom Gesetzgeber **ersatzlos gestrichen** wurde, sodass sich die Zulässigkeit allein nach Art. 6 Abs. 1 DSGVO und dem dazugehörigen Erwägungsgrund 47 der DSGVO richtet. Die Konstellationen nach dem BDSG a. F. sind nach diesen geltenden Maßstäben weder als sozialadäquat anzusehen noch entsprechen sie den vernünftigen Erwartungen betroffener Personen.

Darüber hinaus haben betroffene Personen auch unter dem Gesichtspunkt der Transparenz nach Art. 5 Abs. 1 Buchst. a DSGVO ein überwiegendes und schützenswertes Interesse daran, die **Kontrolle über ihre Daten** zu behalten. Zudem stellt die Erklärung des Widerspruchs bei Werbung fremder Organisationen einen nicht unerheblichen Aufwand für die betroffenen Personen dar, ohne dass diese den Anlass für die Datenverarbeitung selbst gesetzt haben. Dies muss im Rahmen der **Interessenabwägung** ebenfalls berücksichtigt werden, sodass diese im Falle des Handelns mit Daten regelmäßig zugunsten der betroffenen Personen ausfällt.

Da der Verein abschließend mitteilte, dass zukünftige Datenverarbeitungsvorgänge dieser Art – wenn überhaupt – nur noch **nach vorheriger Einwilligung der Mitglieder** erfolgen, konnte das Verfahren eingestellt werden.

5.8 Telefonische Mitgliederbetreuung ohne Einwilligung

Im Rahmen einer weiteren Beschwerde berichtete das Mitglied eines Fitnessanbieters, dass der Anbieter bei Vertragsabschluss seine **Rufnummer** mit der Begründung erhob, dass er diese „**für den Notfall**, wenn Sie etwas vergessen haben oder Ähnliches" benötige.

Umso überraschter war der Kunde, dass der Fitnessanbieter ihn anschließend wiederholt auf seinem Handy anrief, um ihm **Angebote für Personal Trainings oder mögliche Vertragsanpassungen** zu unterbreiten, woraufhin er in jedem Telefonat mitteilte, dass er kein Interesse habe und keine weitere Werbung mehr erhalten möchte. Auf die Aussage „Wir kümmern uns darum" geschah dann allerdings nichts, außer dass er nunmehr zusätzlich Werbung via SMS bekam.

Da das Unternehmen im Rahmen des daraufhin eingeleiteten Verfahrens mitteilte, dass es sich hierbei lediglich um eine **Mitgliederbetreuung** handele, wurde dieses darauf hingewiesen, dass „jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen, einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen, zu fördern" **als Werbung definiert** wird. So sind auch Zufriedenheitsnachfragen bei Kunden nach einem Geschäftsabschluss oder Geburtstags- und Weihnachtsmailings als Werbung anzusehen, wofür der Verantwortliche eine entsprechende Rechtsgrundlage benötigt.

Damit der Fitnessanbieter die bestehenden Verträge mit seinen Mitgliedern erfüllen kann, ist **keine Verarbeitung personenbezogener Daten zum Zweck der fernmündlichen Unterbreitung von Angeboten** für Personal Trainings oder eine beitragsfreie Mitgliedschaft erforderlich. Das vom Anbieter in diesem Zusammenhang verfolgte Bestreben kann beispielsweise auch durch Aushänge und persönliche Ansprachen im Studio erreicht werden. Ferner besteht bei Erfüllung der Vorgaben nach § 7 Abs. 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG) auch die Befugnis, gegebenenfalls E-Mail-Adressen von Bestandskunden entsprechend zu nutzen. Die **Nutzung der Telefonnummer für Werbezwecke** bedarf allerdings auch im Hinblick auf die ebenfalls zu beachtenden Regelungen des § 7 Abs. 2 Nr. 2 UWG einer **Einwilligung**.

Darüber hinaus haben betroffene Personen gemäß Art. 21 Abs. 2 DSGVO auch das Recht, jederzeit **Widerspruch** gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke der Werbung einzulegen. Nach erfolgtem Widerspruch ist eine **Weiterverarbeitung** von

personenbezogenen Daten **für Werbung unzulässig**.

Nach Schilderung des Verantwortlichen hätte dieser die Telefonnummern im guten Glauben einer rechtmäßigen Verarbeitung genutzt und diese Nutzung auch in den allgemeinen Geschäftsbedingungen so aufgeführt. Die vom Beschwerdeführer erteilte Rückmeldung, dass er keine weiteren Anrufe durch das Studio mehr wünsche, sei aus nicht geklärten Umständen **in dem Mitgliederverwaltungssystem übersehen** worden.

Nach entsprechender Aufklärung des Verantwortlichen über die Rechtslage bestätigte dieser, zukünftig auf eine fernmündliche Mitgliederbetreuung und somit auch **auf die Verarbeitung von Telefonnummern im Rahmen der Mitgliederbetreuung zu verzichten**. Hierzu wurden dann auch die Beschäftigten durch einen externen Dienstleister zur DSGVO, zum Gesetz gegen den unlauteren Wettbewerb und zu weiteren einschlägigen Bestimmungen wie dem TDDDG und dem BDSG geschult. Des Weiteren wurden die internen Abläufe entsprechend angepasst, um sicherzustellen, dass keine unzulässigen Kontaktaufnahmen mehr erfolgen. Sofern überhaupt noch eine Kontaktaufnahme erforderlich sei (z. B. Fundsachenmeldung), erfolgt nunmehr auch diese in Zukunft persönlich oder postalisch, sodass auch dadurch sichergestellt ist, dass es zu **keiner unerlaubten Kontaktaufnahme per Telefon** mehr kommt. Nach Umsetzung der Maßnahmen konnte das Verfahren eingestellt werden.

5.9 Lebenshilfe – Teilnehmendenliste zur Raumnutzung

Das ULD erreichte die Beschwerde der Bewohnerin einer Wohneinrichtung für lebensältere Personen. Sie gab an, dass die Bewohnenden einen **Gemeinschaftsraum** zur regelmäßigen Nutzung an den Wochenenden **angemietet** hatten. Der Raum sollte für kleinere Feiern und Zusammenkünfte genutzt werden. Seitens des Verantwortlichen wurde vorgegeben, dass sich **sämtliche Teilnehmenden in eine Liste eintragen** sollten, die den Namen und die Unterschrift beinhalteten. Eine Aufklärung hinsichtlich des Zwecks dieser Liste erfolgte hierbei nicht.

Gemäß Art. 6 Abs. 1 DSGVO ist die Verarbeitung von personenbezogenen Daten nur rechtmäßig, wenn mindestens eine der in der genannten Norm aufgeführten Bedingungen erfüllt ist. Es bedarf also einer Rechtsgrundlage zur Verarbeitung personenbezogener Daten. Im vorliegenden Sachverhalt lag keine Einwilligung der Teilnehmenden vor, und es **war fraglich, zu welchem Zweck** und aufgrund welcher Rechtsgrundlage die Erhebung der Daten mittels der Liste erfolgte.

Der Verantwortliche wurde durch das ULD im Rahmen eines aufsichtsbehördlichen Verfahrens zum Sachverhalt angehört. Er argumentierte dahin gehend, dass die Liste dem Zweck diene, das **Hausrecht** auszuüben sowie mögliche Rechtsansprüche bei Beschädigungen oder Diebstahl geltend machen zu können. Weiterhin wurde auf die rechtliche Verpflichtung nach Art. 6 Abs. 1 Buchst. c DSGVO hingewiesen, eine solche Liste zur Kontrolle und Sicherstellung der Nutzbarkeit von Fluchtwegen sowie zur Kenntnis über anwesende Personen im **Rettungsfall** zu führen.

Dieser rechtlichen Argumentation konnte das ULD nicht folgen, da eine **Teilnehmendenliste kein geeignetes Mittel** darstellt, um die vom Verantwortlichen genannten Zwecke zu erreichen, und es sich bei den Nutzenden des Gemeinschaftsraums um eine geschlossene Gruppe handelt. So bleibt beispielsweise unklar, gegenüber wem genau im konkreten Schadensfall Rechtsansprüche geltend gemacht werden können, wenn dem Verantwortlichen zwar die Liste der Teilnehmenden vorliegt, er aber nicht konkret benennen kann, durch wen der Schaden verursacht wurde. Weiterhin gibt es keine verbindliche rechtliche Verpflichtung, Teilnehmendenlisten zur Sicherstellung der Nutzbarkeit von Fluchtwegen sowie zur Kenntnis über anwesende Personen im Rettungsfall zu führen.

Diese rechtliche Einschätzung des ULD wurde dem Verantwortlichen mitgeteilt. Er sagte daraufhin zu, **zukünftig auf das Erstellen einer Teilnehmendenliste zu verzichten**, und gab zudem an, dass alle bisher erhobenen Daten gelöscht worden seien.

Dem Verantwortlichen wurde abschließend ein **Hinweis** nach Art. 58 Abs. 1 Buchst. d DSGVO **erteilt** und zudem davor **gewarnt**, zukünftig personenbezogene Daten ohne Vorliegen einer Rechtsgrundlage zu verarbeiten.

5.10 Abfrage von Gesundheitsdaten im Leistungssport – weniger ist mehr

Über die Beschwerde eines Vereinsmitglieds erreichte uns ein **Formular zur Abfrage von Gesundheitsdaten der Vereinsmitglieder**. Da es sich bei dem betroffenen Verein um einen Sportverein im Bereich des **Leistungssports** handelte, erschien eine Abfrage der Sportgesundheit grundsätzlich gerechtfertigt. Das hier vorgelegte Formular erfragte allerdings Angaben, die über eine bloße gesundheitliche Eignung zum Leistungssport weit hinausging. Folgende Daten wurden u. a. von den Sportlern abgefragt:

- Information über bestehende Krankheiten, z. B. Asthma, angeborene Herzerkrankungen, Diabetes,
- Information über weitere Einschränkungen, z. B. bekannte Epilepsie,
- Erklärung, ob das teilnehmende Kind gesundheitliche Einschränkungen hat, gegebenenfalls auch unter Vorlage eines ärztlichen Attests,
- Angabe von grundsätzlichen Vorerkrankungen,
- Angabe von Medikamenten, die eingenommen werden.

Eine Teilnahme am Training wurde bis zur Vorlage des Formulars ausgeschlossen. Des Weiteren musste das Formular jährlich aktualisiert von den Vereinsmitgliedern abgegeben werden.

Da dem Beschwerdeführer die anzugebenden Daten zu umfangreich erschienen, reichte er das Formular nicht ein – bei Eingabe der Beschwerde drohte ihm daher der **Ausschluss aus dem Training**.

Im Rahmen der Stellungnahme teilte uns der Verein mit, dass er Mitglied in entsprechenden **Landessport- und auch Bundesverbänden** sei und somit den Satzungen und Ordnungen dieser Verbände unterliege. Die in der Stellungnahme benannten Wettkampfbestimmungen wurden seitens des Vereins auch als Maßstab für das im Verein durchgeführte Training herangezogen, da es ihrer Auffassung nach der **Wettkampfvorbereitung** diene. Unsere Prüfung der von dem Verein benannten Vorgaben der Verbände ergab, dass grundsätzlich nur Angaben zur **Sportgesundheit** von denjenigen gefordert wurde, die an einem Wettkampf teilnehmen. Lediglich ein Bundesverband forderte neben der Angabe zur Sportgesundheit auch einen ärztlichen Nachweis, wobei keine näheren Vorgaben zu Art und Umfang der Untersuchung getroffen wurden. Ob das Vorgehen des Bundesverbandes aus datenschutzrechtlicher Sicht tragfähig war, oblag dabei nicht unserer Beurteilung, da dieser seinen Sitz nicht in Schleswig-Holstein hat.

Bezüglich des örtlichen Sportvereins musste nach unserer Auffassung allerdings zwischen einer **Wettkampfteilnahme** und dem **Training** im jeweiligen Verein **differenziert** werden. Diesbezüglich war der Verein nach den Vorgaben der übergeordneten Verbände nicht verpflichtet, sich für das bloße Training ärztliche Nachweise vorlegen zu lassen. Zudem obliegt die **Beurteilung der konkreten Sportfähigkeit den Sportlern selbst** – hier kann der Verein den Sportlern nicht die Eigenverantwortung abnehmen.

In Absprache mit dem Verein wurde das **Formular entsprechend angepasst** und mit uns final abgestimmt. In dem neuen Formular wird nun lediglich die Bestätigung der Sportgesundheit vom Vereinsmitglied abgefragt.

Was ist zu tun?

Insbesondere bei Gesundheitsdaten ist zu prüfen, welche Daten zur Zweckerfüllung erhoben werden müssen. Es gilt: So viel wie nötig, so wenig wie möglich!

5.11 Übermittlung von Lohnabrechnungen per E-Mail

Eine ehemalige Beschäftigte zeigte im Rahmen einer Beschwerde mehrere mögliche datenschutzrechtliche Verstöße ihres früheren Arbeitgebers an. Unter anderem habe sie ihre **Lohnabrechnungen unverschlüsselt per E-Mail** zugesandt bekommen.

Gemäß Art. 5 Abs. 1 Buchst. f DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Da Lohnabrechnungen teilweise sensible personenbezogene Daten enthalten können (z. B. Religionszugehörigkeit), hat der Verantwortliche **geeignete technische und organisatorische Maßnahmen** zu treffen, um sicherzustellen, dass nur der berechtigte Empfänger davon Kenntnis erhält.

Das Unternehmen gab an, dass es grundsätzlich ein **verschlüsseltes Lohnportal** gebe, worüber die Beschäftigten normalerweise ihre Lohnabrechnungen abrufen würden. Im vorliegenden Fall habe die Beschwerdeführerin vor einiger Zeit ihren Vorgesetzten darum gebeten, ihre Lohnabrechnung per E-Mail zugesandt zu bekommen, da sie sich in dem Portal nicht anmelden könne und sie die Lohnabrechnung dringend benötige. In der Folgezeit habe die Beschwerdeführerin dann wiederholt um eine Zusendung per E-Mail gebeten, die dann auch erfolgte. Es könne im Lohnportal aufgrund von technischen Schwierigkeiten, mitunter wegen zu vieler gleichzeitiger Nutzender oder wegen Wartungsarbeiten, zeitweise zu Einschränkungen beim Log-in kommen. Das Lohnportal sei jedoch nicht dauerhaft „out of order" gewesen.

Laut dem ehemaligen Arbeitgeber habe die Beschwerdeführerin **freiwillig die Kommunikation und den Versand von Lohnabrechnungen per E-Mail** gestattet. Ohnehin sei der Versand einer Lohnabrechnung per E-Mail legitim, da nach § 108 Abs. 1 Satz 1 Gewerbeordnung (GewO) dem Arbeitnehmer bei Zahlung des Arbeitsentgelts eine Abrechnung in Textform zu erteilen sei. Die Lohnabrechnung per E-Mail erfülle das Textformerfordernis.

Auch wenn es richtig ist, dass § 108 Abs. 1 Satz 1 GewO der Erteilung einer Lohnabrechnung per E-Mail nicht entgegensteht, ist zu beachten, dass der Verantwortliche dabei ein angemessenes Schutzniveau für die von ihm verarbeiteten personenbezogenen Daten zu gewährleisten hat. Die Übermittlung von Lohnabrechnungen per E-Mail hat daher **grundsätzlich verschlüsselt** zu erfolgen (z. B. passwortgeschütztes Dokument). In **Ausnahmefällen** kann es zwar möglich sein, dass der Verantwortliche **auf ausdrücklichen, eigeninitiativen Wunsch der informierten betroffenen Person** bestimmte vorzuhaltende technische Maßnahmen ihr gegenüber in vertretbarem Umfang nicht anwendet. Grundsätzlich beruhen die vom Verantwortlichen vorzuhaltenden technischen und organisatorischen Maßnahmen aber auf objektiven Rechtspflichten, die nicht zur Disposition der Beteiligten stehen.

Der Beschluss der DSK zur **Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Artikel 32 DSGVO** auf ausdrücklichen Wunsch betroffener Personen ist unter dem folgenden Link abrufbar:

https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf

Kurzlink: *https://uldsh.de/tb43-5-11a*

Allein die Bitte an den Arbeitgeber, die Lohnabrechnung per E-Mail zugesandt zu bekommen, kann noch keinen ausdrücklichen Verzicht auf die vorzuhaltenden technischen Maßnahmen darstellen.

Da das Unternehmen grundsätzlich ein verschlüsseltes Lohnportal bereitstellt, wurde bezüglich der unverschlüsselten Übermittlung der Lohnabrechnungen per E-Mail eine **Warnung** gemäß Art. 58 Abs. 2 Buchst a DSGVO ausgesprochen.

5.12 Videoüberwachung von Beschäftigten ohne Gefährdungslage

Aufgrund einer Beschwerde wurde die von einem Unternehmen betriebene Videoüberwachung geprüft. Das Unternehmen legte dar, dass elf Kameras im Betrieb seien, die rund um die Uhr aufzeichnen und die Aufnahmen für 72 Stunden speichern. Die Videoüberwachung wurde auf Art. 6 Abs. 1 Buchst. f DSGVO gestützt.

Art. 6 Abs. 1 Buchst. f DSGVO

Aus der Norm ergibt sich, dass eine Videoüberwachung zulässig sein kann, wenn sie zur Wahrnehmung **berechtigter Interessen** des Verantwortlichen für konkret festgelegte Zwecke **erforderlich** ist und die **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen** nicht überwiegen.

Das Unternehmen gab an, dass die **Videoüberwachung zur Wahrung des Hausrechts**, zum **Überfall- und Personenschutz** für Beschäftigte, **Vermeidung von Warendiebstahl und der Beweissicherung** bei Vandalismus und Einbruchsversuchen diene. Grundsätzlich sind dies legitime berechtigte Interessen.

Für eine Videoüberwachung bedarf es jedoch eines Grundes, etwa einer **Gefährdungslage**, die hinreichend durch Tatsachen oder die allgemeine Lebenserfahrung belegt ist. Eine Gefährdungslage muss **über das allgemeine Lebensrisiko hinausgehen**, sodass sich eine solche nur aus tatsächlichen Erkenntnissen ergeben kann. Subjektive Befürchtungen oder ein Gefühl der Unsicherheit reichen nicht aus (vgl. BVerwG, Urteil vom 27. März 2019 – 6 CC 2.18, Rn. 26).

Es wurden zwar zwei Vorfälle geschildert, die unter Umständen zu der Annahme einer aktuellen Gefährdungslage hätten führen können. Allerdings wurde **keine zeitliche Angabe** zu den Vorfällen gemacht. Es hieß lediglich, dass diese vor der Installation der Videoüberwachung passiert seien und es seit der Inbetriebnahme der Kameras keine weiteren Vorfälle gegeben habe.

Aus dem beigefügten Verzeichnis von Verarbeitungstätigkeiten ergab sich, dass das Videokamerasystem im **Jahr 2019** installiert wurde. Wenn es seitdem keine weiteren Vorfälle gab, kann man im **Jahr 2024** nicht ohne Weiteres noch von einer aktuellen Gefährdungslage ausgehen. Auch hat das Unternehmen nicht dargelegt, ob vor der Einführung der Videoüberwachung **andere Sicherheitsmaßnahmen geprüft** oder eingesetzt wurden, die weniger stark in die Rechte der betroffenen Personen eingreifen. Bereits an der Erforderlichkeit der Videoüberwachung bestanden daher erhebliche Zweifel.

Erschwerend kam hinzu, dass von der Videoüberwachung überwiegend die **Beschäftigten betroffen** waren. So erfassten einige Kameras Teile des Büros und Lagers, also **dauerhafte Arbeitsplätze** der Beschäftigten. Die Videoüberwachung stellte daher einen erheblichen Eingriff in das Recht der Beschäftigten auf informationelle Selbstbestimmung dar. Die Videokameras ermöglichten dem Verantwortlichen, das Gesamtverhalten der Beschäftigten reproduzierbar festzuhalten, sodass ein **ständiger Überwachungs- und Anpassungsdruck** entstehen konnte. Die Videoüberwachung während der Arbeitszeit stellte daher einen unverhältnismäßigen Eingriff in die Grundrechte und Grundfreiheiten der Beschäftigten dar.

Das Unternehmen **schaltete** daraufhin die Aufnahmezeiten aller **Kameras während der Arbeitszeit ab** und informierte die Beschäftigten darüber. Aufgrund der bisher erfolgten unrechtmäßigen Videoüberwachung wurde eine **Verwarnung** ausgesprochen.

5.13 Zusendung von Zugangsdaten an die private E-Mail-Adresse

Ein Beschäftigter beschwerte sich darüber, dass ihm an seine private E-Mail-Adresse die **Zugangsdaten** (Benutzername und Passwort) für ein neues im Unternehmen eingesetztes System zugesandt worden waren. Dies sei ohne Rücksprache mit den Beschäftigten erfolgt. Er habe der **Nutzung seiner privaten E-Mail-Adresse** zudem nie zugestimmt.

Im Rahmen des durchgeführten Verfahrens teilte das verantwortliche Unternehmen mit, dass die Einführung des neuen Systems notwendig gewesen sei, um bestimmte Abläufe zu gewährleisten. Dafür mussten für jeden Beschäftigten Nutzungszugänge angelegt werden. Die Übersendung der Zugänge von 59 Beschäftigten an deren private E-Mail-Adressen sei im Rahmen des Beschäftigungsverhältnisses zur ordnungsgemäßen Durchführung der beruflichen Tätigkeit erforderlich gewesen. Die **Bereitstellung einer dienstlichen E-Mail-Adresse** für alle Beschäftigten sei aufgrund des organisatorischen Aufwands **gegenwärtig nicht möglich** gewesen. Man sei bestrebt, allen Beschäftigten eine dienstliche E-Mail-Adresse zur Verfügung zu stellen. Alternativ würden vorübergehend **andere Wege der Übermittlung** von Informationen, beispielsweise in Papierform mit Ablage im jeweiligen persönlichen Fach der Beschäftigten, umgesetzt.

Ob die Verarbeitung und Verwendung von Beschäftigtendaten rechtmäßig sind, bemisst sich in erster Linie am **Maßstab der Erforderlichkeit**. Eine Verarbeitung ist erforderlich, wenn es keine anderen, gleich geeigneten Mittel gibt, die weniger stark in die Rechte der betroffenen Personen eingreifen. Das Unternehmen hat zwar dargelegt, dass es zur Durchführung des Beschäftigungsverhältnisses erforderlich war, dass Nutzungszugänge angelegt werden. Für die Zusendung der Zugangsdaten unter Verwendung der privaten E-Mail-Adresse hat das Unternehmen jedoch in seiner Stellungnahme bereits selbst ein milderes, gleich geeignetes Mittel aufgezeigt: Die Beschäftigten hätten die **Zugangsdaten auch in Papierform durch Ablage in das persönliche Fach** erhalten können. Die Verwendung der **privaten E-Mail-Adressen** war somit schon allein deshalb **nicht erforderlich** und erfolgte ohne rechtliche Grundlage.

Vor diesem Hintergrund haben wir gegenüber dem Unternehmen eine **Verwarnung** ausgesprochen.

5.14 Datenpannen in der Wirtschaft – Meldungen nach Artikel 33 DSGVO

5.14.1 „Ich hab doch schon bezahlt" – manipulierte Rechnungen nach Phishing-Angriff

Eine Datenpannenmeldung Ende des Jahres 2023 war der Anfang vieler ähnlich gelagerter Fälle von **Angriffen auf E-Mail-Konten**, welche teilweise mit der **Manipulation von Rechnungen** fortgeführt wurden. Das hier betroffene Unternehmen meldete uns eine erfolgreiche Cyberattacke auf die von ihm genutzte Software Lexoffice. Dieser Angriff wurde allerdings nicht direkt erkannt, sondern erst aufgrund offener Rechnungsposten aufgedeckt.

Denn das Unternehmen stellte zum Ende des Jahres mehrere **offene Rechnungen mit höheren Beträgen** fest, woraufhin sie die Kundinnen und Kunden telefonisch zur Klärung der offenen

Posten kontaktierten. Im Rahmen dieser Telefonate wurde dem Unternehmen vom ersten betroffenen Kunden mitgeteilt, dass die **Rechnung bereits beglichen** wurde. Diese Aussage konnte allerdings aufgrund eines fehlenden Zahlungseingangs nicht bestätigt werden. Erst auf Basis weiterer Gespräche wurde festgestellt, dass die **Überweisungen auf ein polnisches und ein deutsches Konto** erfolgten, welche beide **nicht dem Unternehmen zugeordnet** waren. Weitere Recherchen zeigten schließlich, dass der Kunde anhand gefälschter Mails über das gehackte E-Mail-Konto neue Rechnungsdaten erhielt. Hierfür wurde seitens der Angreifer mit den in Lexoffice hinterlegten Rechnungsvorlagen gearbeitet, sodass die E-Mail der Angreifer für den Kunden zunächst **nicht als Fälschung erkennbar** war.

In dem hier vorliegenden Fall bestand zudem die Problematik, dass nicht nur die Seite des meldenden Unternehmens, sondern auch teilweise die der Kunden **kompromittiert** wurde. Dies führte dazu, dass **Rückfragen der Kunden**, die die neue Bankverbindung hinterfragten, abgefangen wurden und folglich nicht beim betroffenen Unternehmen eingingen. Als **gefälschte Antwort** erhielt der Kunde allerdings eine nochmalige Bestätigung der scheinbar neuen Bankverbindung sowie regelmäßige Zahlungserinnerungen. Das Unternehmen hat infolge dieser Erkenntnisse alle Kundinnen und Kunden, bei denen offene Angebote oder Rechnungen in Bearbeitung vorlagen, **benachrichtigt**.

Leider konnten auch die darauffolgenden Ermittlungen der vom Unternehmen **hinzugezogenen Kriminalpolizei** keine weiteren hilfreichen Erkenntnisse liefern, da die genutzten IP-Adressen letztendlich nach Nigeria führten und sich die Spur dort verlor. Mithilfe eines neu aufgesetzten Systems, erweiterter **technischer Schutzmechanismen** und der Sensibilisierung aller Beschäftigten zur Erkennung von Phishing-Mails konnte das Unternehmen den Vorfall abschließen. Der entstandene **finanzielle Schaden** aufgrund bereits durchgeführter Überweisungen belief sich für das Unternehmen dennoch auf einen **mittleren fünfstelligen Bereich**.

Im Laufe des Jahres 2024 meldeten im Vergleich der vergangenen Jahre überdurchschnittlich viele Unternehmen erfolgreiche **Phishing-Angriffe auf die E-Mail-Konten mit anschließender Manipulation des E-Mail-Verkehrs**. Durch hinterlegte Regeln im kompromittierten Mailpostfach konnten so Angriffe über längere Zeiträume **verschleiert** werden, indem z. B. eingehende E-Mails bestimmter Absender direkt gelöscht oder in Unterordner verschoben wurden. In manchen Fällen wurde ein ähnliches Vorgehen mit dem Abfangen und Abändern von Rechnungen umgesetzt.

Was ist zu tun?

Phishing-Angriffe auf Unternehmen gehören mittlerweile leider schon fast zum Tagesgeschäft. Die effektivste Maßnahme zur Verhinderung derartiger Vorfälle sind gut geschulte Beschäftigte, die derartige Angriffs-E-Mails erkennen. Bei Unstimmigkeiten im Rechnungsverkehr ist eine besondere Vorsicht geboten.

5.14.2 Hacking-Horror im Weihnachtsgeschäft

Die weihnachtliche Stimmung ist in vielen Unternehmen durch eine Zunahme an Bestellungen geprägt. Dieses saisonal **erhöhte Aufkommen an Bestellungen** führte leider dazu, dass die Vorkommnisse der Meldung, die uns drei Tage vor Weihnachten zuging, seitens des Unternehmens zunächst nicht als ungewöhnlich eingestuft wurden.

Bei dem betroffenen Onlinehändler waren mithilfe eines Brute-Force-Angriffs mehrere Kundenkonten kompromittiert worden. Die Angreifer hatten hierfür pro Benutzername **nur ein Passwort als Log-in-Versuch** eingegeben, wobei bei 40 Accounts die Kombinationen richtig waren. Unsere weiteren Untersuchungen ließen vermuten, dass die Angreifer hierfür eine Liste mit Hunderten oder gar Tausenden von E-Mail/Passwort-Kombinationen verwendet haben, um sich erfolgreich in die Kundenkonten einzuloggen. Dabei war der Angriff nach unserer Einschätzung nicht auf die Erbeutung der Kundendaten innerhalb der Konten gerichtet, sondern diente lediglich der Umsetzung der darauffolgenden Käufe.

Denn infolge des Angriffs wurden über die **kompromittierten Konten Bestellungen auf Rechnung an abweichende Lieferadressen** getätigt. Bei den 40 betroffenen Kunden entstanden somit offene Rechnungsbeträge, obwohl die Ware an die hinterlegten Adressen der Angreifer geschickt wurde.

Das Unternehmen **benachrichtigte die betroffenen Kunden** über den Vorfall und ließ die offenen Forderungen gegen sie fallen. Zur Verhinderung ähnlich gelagerter Vorfälle haben wir dem Unternehmen empfohlen, **spezielle Sicherheitssoftware zur Erkennung und Abwehr** solcher Angriffe zu installieren („Intrusion Detection & Prevention"-Systeme). Dafür kommt beispielsweise die Open-Source-Software Fail2Ban infrage.

Das Fazit: Für das Unternehmen hat sich das auf den ersten Blick gut laufende Weihnachtsgeschäft leider als **böse Weihnachtsüberraschung** herausgestellt.

Was ist zu tun?

Seitens der Unternehmen kann mithilfe einer Einrichtung von Sicherheitssystemen ein Brute-Force-Angriff effektiv abgewehrt werden. Seitens der Kunden ist es ratsam, für unterschiedliche Onlineshops oder Kundenkonten abweichende Anmeldedaten zu verwenden.

5.15 Videoüberwachung

5.15.1 Allgemeine Entwicklungen

Die Beobachtung, dass sich immer mehr Personen durch **Videoüberwachungskameras** beeinträchtigt fühlen, wurde auch in diesem Jahr dadurch bestätigt, dass die Anzahl der diesbezüglich eingegangenen Beschwerden weiter gestiegen ist. Die Anzahl von Beschwerden über Videoüberwachungsanlagen stieg im Vergleich zum Vorjahreszeitraum insgesamt um rund 38 Prozent. **Im Vergleich zum Jahr 2022** hat sich die Anzahl der **Beschwerden nahezu verdoppelt** (Tz. 1.3).

Ein Großteil der Beschwerden richtet sich gegen Videoüberwachungsanlagen, die **durch Privatpersonen** in ihrem privaten häuslichen Umfeld installiert werden. Die Gründe für derartige Installationen liegen häufig darin, das Eigentum zu sichern. Über solche Videoüberwachungsanlagen beschweren sich zumeist die direkten Nachbarn, die sich durch die Installation in ihren Rechten verletzt fühlen (Tz. 1.3). Zumeist ist für Außenstehende nicht klar erkennbar, ob von einer Videoüberwachung auch benachbarte Grundstücke oder öffentliche Flächen mit erfasst werden.

Nicht selten geht derartigen Beschwerden ein **festgefahrener Nachbarschaftsstreit** voraus, sodass sich die Betroffenen direkt an die Landesbeauftragte für Datenschutz wenden, ohne zuvor das Gespräch mit den vermeintlich überwachenden Nachbarn gesucht zu haben. Insbesondere bei bereits verhärteten Fronten ist ein **Verweis auf den Zivilrechtsweg** hilfreich: Neben den datenschutzrechtlichen Aspekten sind hinsichtlich einer Videoüberwachung auch zivilrechtliche Ansprüche nicht zu verkennen. Auch wenn eine Kamera nach datenschutzrechtlicher Bewertung rechtmäßig betrieben wird, kann ein zivilrechtlicher Unterlassungsanspruch bestehen.

Darüber hinaus hat meine Dienststelle eine Vielzahl an Beschwerden erhalten, die sich u. a. auf die **Videoüberwachung in Ladengeschäften, Restaurants, Hotels, auf Campingplätzen, in einem Kleingartenverein und in Fitnessstudios** beziehen. Auch bei diesen Beschwerden zeigt sich die Problematik der fehlenden Transparenz. Für die Beschwerdeführer sind die überwachten Bereiche nicht klar ersichtlich, sodass Unsicherheiten entstehen. Hinzu kommt in vielen Fällen eine nicht ausreichende Hinweisbeschilderung. Grundsätzlich wird hier immer auf eine Erhöhung der Transparenz, z. B. durch eine **korrekte Hinweisbeschilderung**, aus der sich alle nach Artikel 13 DSGVO geforderten Angaben (z. B. Kontaktdaten des Verantwortlichen und Rechtsgrundlagen der Datenverarbeitung) ergeben, hingewirkt. In manchen Fällen reicht die Erhöhung der Transparenz nicht aus, da die Videoüberwachung selbst bereits nicht den Vorgaben entspricht. In solchen Fällen müssen weitere Anpassungen erfolgen, z. B. eine **räumliche oder zeitliche Beschränkung** der Videoüberwachung.

Erfreulich ist, dass die Vielzahl der Verantwortlichen sich **kooperativ** zeigt, die im aufsichtsbehördlichen Verfahren benötigten Informationen und Unterlagen zur Verfügung stellt und auch angeregte bzw. geforderte Änderungsbedarfe bereitwillig umsetzt. Ein Teil der Verantwortlichen zeigt sich jedoch weniger kooperativ, sodass im Berichtszeitraum entsprechende **Anordnungen zur Auskunft** erlassen werden mussten, die zum Teil mit der **Verhängung von Zwangsgeldern** durchgesetzt werden müssen.

5.15.2 Der Kampf gegen die Vermüllung – Videoüberwachung von Müllsammelplätzen

Bereits im vorherigen Berichtszeitraum hat meine Dienststelle eine Beschwerde betreffend eine **Videoüberwachung eines Müllsammelplatzes** in einer Gemeinde in Schleswig-Holstein erreicht. Diese Gemeinde setzt seit dem Jahr 2022 eine Videoüberwachung zur Beobachtung eines Müllsammelplatzes ein, um (illegaler) Vermüllung den Kampf anzusagen. Die Videoüberwachung soll die Gemeinde u. a. davor schützen, hohe Kosten aufwenden zu müssen, um den illegal entsorgten Sperrmüll, Elektrogeräte und Farbeimer fachgerecht zu trennen und zu entsorgen. Der Beschwerdeführer bezweifelte die Rechtmäßigkeit der Videoüberwachung unter datenschutzrechtlichen Aspekten.

Bei einer Videoüberwachung von Müllsammelplätzen werden nicht nur die Personen gefilmt, bei denen es zu einem Fehlverhalten kommt. Vielmehr werden **lückenlos alle Personen erfasst**, die ihren Müll an dem überwachten Müllsammelplatz entsorgen, unabhängig davon, ob der Müll legal oder möglicherweise illegal entsorgt wird. Dieser Umstand greift in die Persönlichkeitsrechte der betreffenden Personen ein.

Für einen derartigen Grundrechtseingriff und die Verarbeitung der personenbezogenen Daten bedarf es einer rechtlichen Grundlage. Für die Videoüberwachung von Müllsammelplätzen

durch Städte und Gemeinden kommt die Generalklausel des § 14 Abs. 1 Nr. 1 LDSG (Landesdatenschutzgesetz) als Rechtsgrundlage in Betracht. Danach ist die **Beobachtung öffentlich zugänglicher Raume mit optisch-elektronischen Einrichtungen** (Videoüberwachung) zulässig, soweit dies zur Aufgabenerfüllung der öffentlichen Stelle erforderlich ist.

In dem vorliegenden Fall sind wir bei unserer Prüfung zu dem Ergebnis gekommen, dass die in Rede stehende Videoüberwachung der Gemeinde auf der Grundlage des § 14 Abs. 1 Nr. 1 LDSG rechtmäßig betrieben wird. Dabei ist von besonderer Bedeutung, dass der Eingriff für die von der Videoüberwachung betroffenen Personen **durch technische Maßnahmen auf das Nötigste beschränkt** wurde.

Abschließend ist darauf hinzuweisen, dass eine Videoüberwachung von Müllsammelplätzen nicht pauschal auf der Grundlage des § 14 Abs. 1 Nr. 1 LDSG als rechtmäßig bewertet werden kann, sondern stets die **Umstände des jeweiligen Einzelfalls zu bewerten** sind.

5.15.3 Haben Sie noch Plätze frei? Livebilder eines Campingplatzes im Internet

Uns haben in diesem Jahr mehrere Beschwerden betreffend Webcams erreicht. **Webcams** erweisen sich für die Verantwortlichen als nützlich, um z. B. Touristen einen **Eindruck über das Urlaubsziel** zu verschaffen. Darüber hinaus sind sie praktisch, wenn man sich in Echtzeit über die aktuellen Wetterbedingungen vor Ort informieren möchte.

Die Vorteile einer Webcam hat sich auch die Eigentümerin eines **autark betriebenen Wohnmobilstellplatzes** in Schleswig-Holstein zunutze gemacht. Aufgrund des autarken Betriebes des Stellplatzes sind keine Reservierungen möglich. Um potenziellen Gästen einen Eindruck über die Auslastung des Platzes zu verschaffen, bedient sich die Eigentümerin einer Webcam. Es wird ein Livestream des Stellplatzes auf der Homepage der Betreiberin übertragen. Die Vorteile der Liveübertragung der Übersichtsaufnahme für die Betreiberin und potenzielle Gäste sind nicht zu verkennen. Es ist jedoch zweifelhaft, ob die Gäste während ihres Aufenthalts live im Internet gezeigt werden möchten, wie sie beispielsweise noch **im Schlafanzug den ersten Kaffee** am Morgen vor dem Wohnmobil trinken.

Diesbezüglich hat das ULD im Berichtszeitraum eine Beschwerde erreicht. Hauptgegenstand der Beschwerde war, dass im vorderen Bereich der im Internet übertragenen Übersichtsaufnahme **Personen identifizierbar** abgebildet werden.

Die Abgebildeten haben ein berechtigtes Interesse an der Wahrung ihrer Persönlichkeitsrechte. Dazu gehört ihr Recht, sich **im öffentlichen Raum zu bewegen**, ohne dass diese Tatsache einem weltweiten Publikum übermittelt wird. Insoweit war vorliegend darauf hinzuwirken, dass die von der Webcam erfassten Personen nicht identifizierbar sind.

Betreiber von Webcams können mit einer geeigneten Konfiguration der Kameras dafür sorgen, dass tiefe Eingriffe in die Privat- oder Intimsphäre vermieden werden. In der Regel genügt es oft schon, den **Blickwinkel der Webcam zu verändern** oder den Vordergrund, in dem Personen identifizierbar sein könnten, z. B. durch **Schwärzung oder Verpixelung** von der Erfassung auszunehmen.

Bei der in Rede stehenden Webcam auf dem Wohnmobilstellplatz wurden die vorderen **Bereiche durch unser Einwirken von der Erfassung ausgenommen**. Somit können sich potenzielle Gäste weiterhin einen Überblick über die aktuelle Auslastung des Platzes verschaffen, und gleichzeitig können die anwesenden Gäste in den vorderen Reihen einen Aufenthalt verbringen, ohne dabei weltweit beobachtet werden zu können.

Was ist zu tun?

Der Betrieb von Webcams muss auf eine Rechtsgrundlage gestützt werden, wenn damit identifizierbare Personen aufgenommen werden. Da für den Zweck der Webcam die Aufnahme von Personen in aller Regel nicht erforderlich ist, sollte der Betreiber durch (technische) Maßnahmen dafür sorgen, dass erfasste Personen nicht identifizierbar sind. Zoomfunktionen, die die Erkennbarkeit von Personen oder Gegenständen, die Personen zugeordnet werden könnten (z. B. Kraftfahrzeuge oder Boote), ermöglichen, sollten generell nicht zur Verfügung gestellt werden.

5.16 Bußgelder für Datenschutzverstöße

5.16.1 Datenschutzbußgelder – europaweiter Gleichklang

Im Jahr 2023 hatte der Europäische Datenschutzausschuss die **Leitlinien 04/2022 für die Berechnung von Geldbußen im Sinne der DSGVO** veröffentlicht:

https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_de

Kurzlink: *https://uldsh.de/tb43-5-16-1a*

Dabei handelt es sich um ein Papier, das die **Methode zur Berechnung von Geldbußen gegen Unternehmen** europaweit harmonisieren soll. Für Geldbußen gegen natürliche Personen gelten die Leitlinien nicht. Die Anwendung dieser Leitlinien konnte im Berichtszeitraum weiter erprobt werden.

Nach den Leitlinien erfolgt die Bemessung der Geldbuße in einem **mehrstufigen Verfahren**. Der Ausgangspunkt für die Berechnung ist die Schwere der jeweiligen Tat. Das Bußgeldkonzept sieht hierfür **drei Schweregrade** vor. Der Schweregrad bestimmt den Bußgeldrahmen. So wird z. B. bei einem geringen Schweregrad der Ausgangswert bei bis zu 10 Prozent des gesetzlichen Höchstmaßes angesetzt. In einem zweiten Schritt kann der Ausgangsbetrag an die wirtschaftlichen Verhältnisse des Unternehmens angepasst werden. Maßgeblich ist hierfür der Jahresumsatz des Unternehmens. Anschließend werden in einem dritten Schritt erschwerende und mildernde Umstände im Zusammenhang mit dem früheren oder gegenwärtigen Verhalten des Unternehmens betrachtet. Der vierte Schritt besteht darin, das einschlägige gesetzliche Höchstmaß für den jeweiligen Verstoß zu ermitteln. In vorhergehenden oder folgenden Schritten vorgenommene Erhöhungen dürfen diesen Höchstbetrag nicht überschreiten. Abschließend wird geprüft, ob der berechnete Betrag den **Anforderungen an Wirksamkeit, Abschreckung und Verhältnismäßigkeit** entspricht. Ist dies nicht der Fall, kann die Geldbuße dann entsprechend angepasst werden.

Es hat sich herausgestellt, dass die Leitlinien ein **handhabbares Werkzeug zur Berechnung von Geldbußen** darstellen. Sie bilden einen Rahmen, an dem sich sowohl Datenschutzaufsichtsbehörden als auch Verantwortliche orientieren können. Sie schaffen **Transparenz** bei der Auslegung der zentralen Bußgeldvorschriften der Datenschutz-Grundverordnung. Eine rein mathematische Berechnung von Geldbußen ist indes nicht vorgesehen – dies würde dem Einzelfall nicht immer gerecht. Dementsprechend lassen die Leitlinien **Spielraum für die Besonderheiten des Einzelfalls**. Die Leitlinien bieten einen großen Mehrwert für die Vereinheitlichung der Geldbußen für Datenschutzverstöße in Deutschland und Europa.

5.16.2 Dashcams im Straßenverkehr – auf die Einstellung kommt es an

Auch in diesem Jahr haben wir mehrere Fälle bearbeitet, bei denen es um den Einsatz sogenannter **Dashcams im Straßenverkehr** ging. In zwei Fällen wurden die nachträglich im Fahrzeug installierten Dashcams auf eine Art und Weise eingesetzt, die eindeutig nicht mit dem Datenschutzrecht vereinbar war.

Dashcam

Dashcams sind werkseitig oder nachträglich im oder am Fahrzeug installierte Kameras, die den Bereich rund um das Fahrzeug im ruhenden und fließenden Verkehr aufnehmen.

In einem Fall filmte die im Fahrzeug hinter der Windschutzscheibe verbaute Dashcam über einen Zeitraum von **40 Minuten ununterbrochen den Parkplatz** eines Supermarktes. In dem anderen Fall waren auf der Speicherkarte der Dashcam **über 500 einzelne Videosequenzen des fließenden Straßenverkehrs** gespeichert. In beiden Fällen waren Personen identifizierbar und Kfz-Kennzeichen lesbar. Die betroffenen Personen hatten keine Kenntnis darüber, dass ihr Verhalten im öffentlichen Verkehrsraum aufgezeichnet wurde. Dadurch entstand ein erheblicher Eingriff in die Grundrechte und Grundfreiheiten der betroffenen Personen.

Ein solcher Eingriff hätte durch **technische Maßnahmen** verringert werden können. Für Dashcams, die ein Unfallgeschehen nachvollziehbar machen sollen, kommen kurzzeitige, anlassbezogene Aufzeichnungen infrage, die erst bei Kollision oder starker Verzögerung des Fahrzeugs durch einen Bewegungssensor ausgelöst werden. Weitere Maßnahmen sind eine Verpixelung von Personen oder ein automatisiertes und dem Eingriff des Verwenders entzogenes Löschen.

Nur wenn eine Dashcam solche (Daten-)Schutzmechanismen aufwiese, käme überhaupt in Betracht, dass die **vorzunehmende Güterabwägung** zugunsten des Dashcam-Betreibers ausfallen könnte (BGH, Urteil vom 15.05.2018 – VI ZR 233/17, Rn. 26). Solche Mechanismen zur Abmilderung des Eingriffs in die Grundrechte und Grundfreiheiten der datenschutzrechtlich betroffenen Personen wurden in beiden Fällen nicht ergriffen. Daher haben wir **in beiden Fällen Geldbußen** verhängt.

Häufig werden wir mit der Argumentation konfrontiert, die durch die Dashcam erstellten Aufzeichnungen seien rein privater Natur. Doch die Aufzeichnung des ruhenden oder fließenden Straßenverkehrs mittels Dashcam erfolgt gerade nicht im Rahmen ausschließlich persönlicher oder familiärer Tätigkeiten nach Art. 2 Abs. 2 Buchst. c DSGVO. Durch Dashcams werden **Personen im öffentlichen Raum gefilmt**, womit der persönlich-familiäre Bereich verlassen und die Datenschutz-Grundverordnung auch für Privatpersonen als Verantwortliche vollumfänglich anwendbar ist. Diese Einschätzung basiert auf der Rechtsprechung im Bereich der Videoüberwachung: Soweit sich eine Videoüberwachung mindestens teilweise auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre desjenigen gerichtet ist, der die Daten auf diese Weise verarbeitet, kann sie nicht als eine ausschließlich „persönliche oder familiäre“ Tätigkeit angesehen werden (EuGH, Urteil vom 11.12.2014 – C-212/13). Zudem werden Dashcam-Aufnahmen gerade zu dem Zweck erstellt, sich für den Schadensfall abzusichern und die Aufnahmen gegebenenfalls weiterzugeben, beispielsweise an Sachverständige einer Versicherung oder die Polizei. Wer eine Dashcam nutzt, muss die Vorgaben der Datenschutz-Grundverordnung einhalten und kann sich **nicht darauf berufen, dass die erstellten Aufnahmen rein privater Natur sind**.

5.16.3 Bußgeld für diffamierende Internetveröffentlichungen über Auszubildende

Durch mehrere Hinweise von Bürgerinnen und Bürgern wurden wir darauf aufmerksam gemacht, dass sich eine Apothekerin in einem **sozialen Netzwerk** über die Verhaltensweisen, den Ausbildungsbeginn und die Ausbildungsdauer, die Arbeitszeiten, die geplanten Urlaube sowie die Krankheitsbilder einer Auszubildenden geäußert hatte. Die Äußerungen waren in einer Art und Weise formuliert, die geeignet war, die **Auszubildende bloßzustellen und zu diffamieren**. Der Name der Auszubildenden wurde zwar nicht explizit genannt, jedoch war sie aufgrund von wenigen Zusatzinformationen, die sehr leicht über die Website der Apothekerin zu erlangen waren, identifizierbar. Die Apothekerin hat durch die **Veröffentlichungen im Internet** personenbezogene Daten verarbeitet, ohne dass diese Verarbeitung auf eine gesetzliche Grundlage hätte gestützt werden können. Da die Datenverarbeitung im Rahmen eines Ausbildungsverhältnisses stattfand und zudem auch **Gesundheitsdaten der betroffenen Person** betraf, war der Eingriff in die Grundrechte und Grundfreiheiten der betroffenen Person besonders intensiv. Dieser Verstoß wurde daher mit einer **Geldbuße** geahndet.

Was ist zu tun?

Vorsicht bei Veröffentlichungen: Äußert man sich im Internet, insbesondere in den sozialen Netzwerken, zu einer bestimmten Person, sollte man immer die möglichen Auswirkungen für diese Person im Blick behalten. Gerade Arbeitgeber trifft hinsichtlich ihrer Auszubildenden eine besondere Schutz- und Sorgfaltspflicht. Keinesfalls sind Arbeitgeber befugt, sich öffentlich zu den Krankheitsbildern und Gewohnheiten ihrer Mitarbeitenden zu äußern.

06

KERNPUNKTE

Technische Verantwortlichkeit in verteilten Verfahren

Personenbezug in KI-Modellen

Frag' für 'nen Freund

Rechenschaftspflicht mit System

6 Systemdatenschutz

Die Pflichten des Verantwortlichen erstrecken sich zu einem großen Anteil auf das Treffen geeigneter **technischer und organisatorischer Maßnahmen**, um das dem Risiko angemessene Schutzniveau zu gewährleisten. Das Recht verlangt eine Gestaltung der Verarbeitung personenbezogener Daten entsprechend der rechtlichen Vorgaben. Aus diesem Grund kommt dem Systemdatenschutz eine besondere Rolle zu.

6.1 Landesebene

6.1.1 Zusammenarbeit mit dem Zentralen IT-Management (ZIT SH)

Wie in den Jahren zuvor war das ULD auch im Jahr 2024 Gast in der **Konferenz der IT-Beauftragten (ITBK)**, in der die IT-Beauftragten der Ressorts zusammen mit dem ZIT über aktuelle und geplante IT-Projekte von zentraler Bedeutung beraten. Durch die Gastrolle in der ITBK, aber auch durch die Teilnahme beim IT-Board in Sankelmark (einem jährlich stattfindenden zweitägigen Workshop der IT-Beauftragten der Ressorts und nachgeordneter Behörden) wird das ULD regelmäßig über viele grundlegende IT-Projekte von zentraler Bedeutung, z. B. im Bereich der Arbeitsplätze (Telefonie, Bürokommunikation, E-Mail, Dateiablage usw.), informiert.

Einen Schwerpunkt bildet im ZIT der zunehmende **Einsatz von Open-Source-Produkten**. In der Vergangenheit betraf dies vor allem Serverprodukte (etwa Datenbankmanagementsysteme oder Webserver) im „Maschinenraum" bei Dataport – dies sind Komponenten, die die Nutzerinnen und Nutzer nur indirekt betreffen. Mittlerweile ist man bei der Umstellung auf Open Source in Bereichen angelangt, die für die Nutzerinnen und Nutzer unmittelbar sichtbar sind, etwa die **Software der Bürokommunikation** („Office", E-Mail, Webbrowser). Dies erfordert Umstellungen auch bei den Beschäftigten, da die Software anders zu bedienen ist.

Der Einsatz von Open Source ist **kein Garant für eine bessere Umsetzung von Informationssicherheit** und bedeutet auch nicht zwingend eine Kostenersparnis. Er ermöglicht jedoch in vielen Fällen eine deutliche Verbesserung der Steuerbarkeit, eine größere Unabhängigkeit von Marktbeteiligten und ihren Betriebsmodellen (Stichwort digitale Souveränität, vgl. 42. TB, Tz. 6.2.4) und langfristig die Möglichkeiten einer eigenen Steuerung von IT-Systemen: Im Zweifelsfall ist man nicht den Entscheidungen Dritter ausgeliefert, sondern kann zumindest auf der Ebene der Software frei agieren und alternative Dienstleister beauftragen. Das Land hält sich so Handlungsoptionen offen.

Im Bereich der zentralen Steuerung der Informationssicherheit war das ULD als Gast in der AG Informationssicherheit beteiligt. In dieser Arbeitsgruppe verzahnen sich die zentrale Steuerung der Informationssicherheit des Landes beim ZIT („Chief Information Security Officer" (CISO)) mit den jeweils Zuständigen in den Ressorts und Behörden. Hier ist erkennbar, dass zusätzliche Ressourcen auf Ebene des ZIT erforderlich sind, um den **gestiegenen Anforderungen** Rechnung tragen zu können.

Anders als in den Vorjahren gab es im Berichtszeitraum keine formelle Einbindung des ULD in konkrete Verfahren oder in Regelwerke, die eine landesweite Bedeutung haben oder die im Rahmen der Mitbestimmung entstanden sind. Beteiligt war das ULD an einem Projekt im Bereich **Veränderungsmanagement** zur Umsetzung der Landesdatenstrategie. Weiter erfolgreich fortgesetzt wurde auch die **Zusammenarbeit** mit anderen IT-Stellen und Datenschutzbeauftragten des Landes, u. a. mit dem Amt für Informationstechnik (AIT), dem Bildungsministerium und dem Sozialministerium sowie einzelnen Bereichen von Ministerien, die eine Datenverarbeitung technisch planen oder umsetzen (siehe auch Tz. 6.1.3).

6.1.2 Zusammenarbeit mit dem ITV.SH

Im Berichtsjahr lag ein Schwerpunkt der Zusammenarbeit mit dem ITV.SH in der Erstellung und Überarbeitung von Dokumenten für das Projekt „SiKoSH" (siehe auch 42. TB, Tz. 6.1.2): Diese fußen auf Texten und Standards, die ihrerseits Anpassungen unterliegen (z. B. den Grundschutzstandards des BSI, die typischerweise jährlich fortgeschrieben und ergänzt werden) und daher regelmäßig angepasst werden müssen.

SiKoSH

SiKoSH (Sicherheit für Kommunen in Schleswig-Holstein) ist ein kommunales Projekt, das beim Aufbau eines Informationssicherheitsmanagementsystems (ISMS) auf Basis des IT-Grundschutzes des BSI (BSI = Bundesamt für Sicherheit in der Informationstechnik) unterstützt.

Als Grundlage wird das BSI-Grundschutzprofil „Basisabsicherung Kommunalverwaltung" verwendet. Ein solches Grundschutzprofil stellt aus den zahlreichen Anforderungen des BSI-Grundschutzes diejenigen zusammen, die für einen bestimmten Anwenderkreis relevant sind – hier eben für den Bereich der Kommunen.

In diese Anpassungen sowie in erstellte Musterdokumente gehen auch Ergebnisse aus unserer Beratung und Aufsichtspraxis ein, beispielsweise in Form von Hinweisen und Blaupausen für Musterrichtlinien und **Regelungen zum Umgang mit Sicherheitsvorfällen**, die Datenschutzkomponenten haben. Denn nicht alle Personen, die im Bereich des Informationssicherheitsmanagements tätig sind, denken an mögliche Meldepflichten gemäß Artikel 33 DSGVO und verwandte Obliegenheiten. Es müssen in der Praxis Regelungen geschaffen werden, die den Informationsfluss innerhalb der Behörden steuern – nicht zuletzt im Hinblick auf die Frist von 72 Stunden bei der Meldung von Datenschutzverletzungen gegenüber der Aufsichtsbehörde.

Ein weiterer Berührungspunkt zwischen dem ITV.SH und dem ULD ergab sich zusammen mit dem Landesarchiv bei einem **Projekt zur kommunalen Archivierung**: Das Landesarchiv arbeitet in einem Verbund mit anderen (Landes-) Archiven zusammen, um digitale Medien zu archivieren. Hierbei bestehen ganz neue Anforderungen, etwa im Hinblick auf die Konvertierung typischer Dateiformate in **archivfähige Formate für die Langzeitspeicherung**. Proprietäre Dateiformate einzelner Softwareanbieter, so bekannt und so verbreitet sie auch heutzutage sein mögen, sind dafür nicht geeignet.

Auch die Speichertechnologie ändert sich ständig – man denke etwa an Tonträger, die allein in den letzten 40 Jahren einen Wandel von Vinylplatte über Kompaktkassetten und CDs bis hin zu heute vorherrschenden Streamingdiensten gemacht haben. Ebenso spielen bauliche Aspekte eine Rolle: **Rechenzentren zur Langzeitspeicherung** digitalen Archivmaterials müssen anders gestaltet sein als solche zur Lagerung von Papierdokumenten.

Mit allen diesen Fragen sind letztlich alle Archive befasst, um die zukünftig ausschließlich digital vorliegenden Verwaltungsdokumente archivieren zu können. Hier setzt das Projekt des Landesarchivs an, über den **ITV.SH als zentrale Stelle** interessierten Kommunalarchiven die technische Plattform, die vom Landesarchiv genutzt wird, ebenfalls zur Verfügung zu stellen.

Aus Datenschutzsicht ist hierbei relevant, welche **Vertrags- und Weisungsverhältnisse** bestehen. Aus technischer Sicht ist bedeutsam, dass der Zugriff auf digitale Archivmaterialien in Bezug auf Sicherheit und Kontrolle keine Einbußen gegenüber der Papierwelt aufweist.

6.1.3 Technische Verantwortlichkeit in verteilten Verfahren

Viele Beratungsanfragen, auch im regelmäßigen Austausch mit IT- und Datenschutzbeauftragten der Ressorts, betreffen die Umsetzung von Verfahren, die auf **landesweit oder bundesweit verfügbarer Software** basieren – oft in Verbindung mit einer Auftragsverarbeitung beim Anbieter. In diesen Fällen gilt es zunächst zu klären, ob solche **Verfahren eigenverantwortlich oder in einem Verbund mit anderen Stellen betrieben** werden sollen. Davon hängt ab, welche **Verantwortlichkeiten** bestehen. Bei Verfahren im Verbund gibt es häufig nur eine Stelle, die gegenüber einem Auftragsverarbeiter als weisungsberechtigt auftritt. Hier stellen sich Fragen der gemeinsamen Verantwortlichkeit.

Bei der Beurteilung solcher Verfahren ist auch zu prüfen, ob und welche bereits bestehenden rechtlichen Bewertungen, Funktionalitäten mit Datenschutzbezug sowie technischen Konfigurationen von anderen Teilnehmenden aus dem Verbund übernommen werden können. Meist gibt es Unterschiede, etwa aufgrund landesrechtlicher Regelungen oder der Verwaltungsorganisation, die eine **differenzierte Betrachtung** notwendig machen. Das betrifft beispielsweise Einsatzszenarien bei Produkten oder Verfahren, die aus anderen Bundesländern übernommen oder auch gemeinsam mit diesen betrieben werden sollen. Hier muss überprüft werden, welche Anpassungen erforderlich sind.

Ein typischer Bereich ist der Bildungsbereich: Zum einen besteht hier die rechtliche Hoheit der Länder, zum anderen unterscheiden sich Organisationsform und Zuständigkeiten zwischen den Ländern oder sogar regional. Denn in Schleswig-Holstein liegt die Verantwortung etwa für Schulgebäude (relevant für technische Fragen wie etwa WLAN-Bereitstellung und Übergang in Landesnetze) und Lernmittel (z. B. Lizenzen für Lernsoftware) in kommunaler Hand, während die Fragen des Schulbetriebs Landessache sind. So ist der Schulbetrieb meist in örtlicher Verantwortung (Schulleitungen) organisiert, es gibt aber auch landesweite Verfahren, etwa die Bereitstellung von Laptops für Lehrkräfte, Angebote des IQSH (Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein) oder eine landesweite Schulverwaltungssoftware.

Ähnliches gilt für Infrastrukturen wie z. B. **Kommunikations- und Datenaustauschplattformen**, die gemeinsam von Land und Kommunen genutzt werden sollen, etwa im Gesundheitsbereich. Wichtig ist in jedem Fall die Klärung der Verantwortlichkeiten und Zuständigkeiten von Anfang an, um damit auch **Klarheit über Rechtsgrundlagen und Pflichten der Verantwortlichen** – einschließlich der Auswahl und Implementierung geeigneter und wirksamer technischer und organisatorischer Maßnahmen – zu erhalten.

Was ist zu tun?

Auch Verfahren, die in anderen Bundesländern oder bei anderen Verantwortlichen im Einsatz sind, lassen sich datenschutzrechtlich nicht immer 1:1 auf die Situation in Schleswig-Holstein übertragen. Eine genaue Betrachtung der Verantwortlichkeiten ist gerade bei gemeinsamen Verfahren erforderlich.

6.2 Deutschlandweite und internationale Zusammenarbeit der Datenschutzbeauftragten

6.2.1 Neues aus dem AK Technik

Der Arbeitskreis (AK) Technik der Datenschutzkonferenz (DSK) beschäftigt sich mit **technischen Fragestellungen**, die in der **Datenschutzberatung und Aufsichtspraxis** aufgeworfen werden. Neben den Datenschutzaufsichtsbehörden des Bundes und der Länder sind auch Vertreter des Datenschutzes aus den Kirchen und dem Rundfunk sowie Datenschutzaufsichtsbehörden im deutschsprachigen Ausland beteiligt. Neu in diesem Kreis ist die Bayerische Landeszentrale für neue Medien.

Schwerpunkte in diesem Jahr waren neben dem Standard-Datenschutzmodell (SDM, Tz. 6.2.2) Beiträge zum Einsatz biometrischer Verfahren auf Flughäfen (Tz. 6.2.3), zu Leitlinien für Anonymisierung und Pseudonymisierung (Tz. 6.2.4) sowie Zuarbeiten im Bereich der künstlichen Intelligenz (Tz. 6.2.5, Tz. 6.2.6). Hier besteht eine enge Kooperation insbesondere mit Task Forces der DSK und mit der **Technology Expert Subgroup** (TECH). Die TECH ist ein Fachgremium des Europäischen Datenschutzausschusses (EDSA), das sich mit technischen Fragestellungen auf europäischer Ebene befasst – sozusagen das **Spiegelbild des AK Technik auf der europäischen Ebene**. Die deutschen Diskussionsbeiträge in diesem Ausschuss stammen u. a. aus dem AK Technik, die Diskussionen werden mit dem AK Technik rückgekoppelt.

Dies ist wichtig, da die Dokumente des EDSA, die auf den Arbeiten seiner Fachausschüsse beruht, in Form von Leitlinien und Stellungnahmen europaweite Bedeutung haben. Sie sind **für die Datenschutzpraxis in Deutschland zu beachten** und haben teilweise bindende Wirkung.

Ein größeres Thema, dessen sich der AK Technik angenommen hat, ist die Betrachtung von **Datenschutzaspekten im 6G-Mobilfunkstandard**. Relevant dabei ist, dass aufgrund der verwendeten Frequenzen nicht nur eine Signalübertragung möglich ist, sondern auch eine Sensorik, etwa durch Analyse von Reflexionsmustern ähnlich wie beim Radar. Bei der Standardisierung geht es darum, dass diese Aspekte nicht bereits auf technischer Ebene vermischt werden. Es sollten beispielsweise bei einer Kommunikation mittels 6G nicht automatisiert Geschwindigkeit und Bewegung sämtlicher dazwischenliegender Objekte erfasst werden, sondern Anwendende (z. B. von Mobiltelefonen) müssen eine solche Sensorik steuern können. Voraussetzung dafür ist aber, dass **in den technischen Protokollen eine Steuerungsmöglichkeit** überhaupt vorgesehen ist.

6.2.2 Standard-Datenschutzmodell – ein Update

Im Jahr 2024 haben die Aktivitäten zur Weiterentwicklung des Standard-Datenschutzmodells (SDM) wieder Fahrt aufgenommen. Dieses Jahr war zum einen davon geprägt, die **Bedeutung des SDM** für die DSK zu klären. Zum zweiten wurde die SDM-Methodik um das Kapitel zu **Betriebsmitteln** ergänzt. Dies mündete in der Version 3.1 des SDM.

Das SDM hat mehrere Schwächen, die länger schon bekannt sind und behoben werden müssen. Unter anderem mangelt es den Bausteinen an Bezügen zum sogenannten **SDM-Würfel** (vgl. 41. TB, Tz. 6.2.2), der die einzelnen Verarbeitungsschritte (wie Erheben, Bearbeiten, Nutzen, Löschen) zu den Gewährleistungszielen des Datenschutzes in Beziehung setzt. Einige der online verfügbaren SDM-Bausteine stammen aus den Frühzeiten der Inkraftsetzung der DSGVO. Darin konnten noch keine Bezüge zum SDM-Würfel hergestellt worden sein, was aber zur Verortung einer Maßnahme im gesamten Gefüge einer Verarbeitung sehr hilfreich wäre.

Noch unbefriedigend ist auch, dass nach wie vor **Bausteine für zentrale Aspekte** fehlen, darunter die wichtigen kryptografischen Themen wie Verschlüsselung und Integritätsschutz. Im SDM wird deshalb übergangsweise auf die Maßnahmenkataloge zum IT-Grundschutz des BSI verwiesen. Diese beschreiben gut die technischen Aspekte der Kryptografie. Benötigt werden aber auch Konzepte für eine datenschutzrechtlich durchdachte Umsetzung, etwa beim Schlüsselmanagement, der sicheren Trennung (insbesondere von Verarbeitungen verschiedener Verantwortlicher in einer Infrastruktur) oder der Abschottung von Protokolldaten, gegebenenfalls auch von der eigenen Administration.

Wir erhalten zum SDM öfter die Rückmeldung, dass es beim Einstieg und für kleine Organisationen zu kompliziert sei. Um dies zu vereinfachen, wollen wir **Lese- und Einstiegshilfen** entwickeln.

Insgesamt ist es der DSK ein Anliegen, das **SDM als Standardmethode** für das Prüfen und Beraten von Verarbeitungen personenbezogener Daten noch **handhabbarer** zu machen. Mit diesem Ziel beauftragte die DSK die Unterarbeitsgruppe SDM (UAG SDM), insbesondere folgende Themen zu bearbeiten:

- Überarbeitung des generischen Maßnahmenkatalogs: jede Maßnahme präziser als bislang gegeneinander konturieren und dann Bezüge zum SDM-Würfel herstellen,
- Überarbeitung der Strukturierung der Bausteine und Bezugnahme auf das Methodikniveau des SDM-V3.1,
- einen vorhandenen Baustein entsprechend aktualisieren, der als Muster für die Arbeiten an weiteren Bausteinen dient; hierbei ist inzwischen die Wahl auf den Baustein „Protokollieren“ gefallen,
- eine SDM-Special-Edition entwickeln, die insbesondere Neulingen dabei hilft, leichter einen Einstieg zu finden,
- die Schnittstelle zum IT-Grundschutz des BSI klarer herausarbeiten,
- Erarbeitung eines Leitfadens für die Anbindung von Autorinnen und Autoren, die nicht im datenschutzbehördlichen Kontext beschäftigt sind.

Neu in der Version 3.1 des SDM ist das Kapitel „D2.2 Mittel einer Verarbeitung“ (Satz 39 f.). In diesem Kapitel werden zunächst **„Mittel der Verarbeitung“ von den „Betriebsmitteln“ unterschieden**. Zu den Mitteln der Verarbeitung (im Sinne der DSGVO) gehören „[...] insbesondere die einschlägige Organisation der verarbeitenden Stelle (Aufbau- und Ablauforganisation), die Unterstützung durch Systeme und Dienste (Betriebsmittel) sowie die konkrete Festlegung des verarbeiteten Datenbestands (Datenmodelle und Datenbasis)“.

Für das SDM sind dabei **die technischen Betriebsmittel** zentral. Dabei wird unterschieden zwischen „unmittelbar unterstützenden“ und „mittelbar unterstützenden“ Betriebsmitteln. Zu den als **unmittelbar** bezeichneten Betriebsmitteln zählen beispielsweise ein IT-gestützter Arbeitsplatz oder ein E-Mail-System. Zu den **mittelbaren** Betriebsmitteln zählen z. B. Maßnahmen im Rahmen einer Verarbeitung, die das Risiko einer Verarbeitung mindern, wie ein Backup-System oder ein Antischadsoftwaresystem.

Die Definition von Betriebsmitteln ist wichtig, um die Verfahren sauber **strukturieren** zu können und **Doppelbetrachtungen von Komponenten zu vermeiden**: Betriebsmittel können miteinander teilweise hierarchisch verbunden und geeignet sein, als mehrfach genutzte Betriebsmittel verschiedene Verarbeitungstätigkeiten zu unterstützen (wie z. B. IT-gestützter Arbeitsplatz).

Das SDM-V3.1 ist unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V3_1.pdf

Kurzlink: *https://uldsh.de/tb43-6-2-2a*

6.2.3 EDSA-Guidelines zur Gesichtserkennung am Flughafen

Im Zuge der Mitarbeit in der Technology Expert Subgroup des Europäischen Datenschutzausschusses (EDSA) beteiligte sich das ULD an der Erstellung einer **Stellungnahme zur Nutzung von Gesichtserkennungstechnologien an Flughäfen**. Die Stellungnahme wurde auf Anfrage der französischen Datenschutzbehörde erstellt und beschäftigt sich mit der zunehmenden Implementierung **biometrischer Systeme zur Optimierung von Passagierkontrollen**.

Die Stellungnahme greift dabei ein hochaktuelles Thema auf: Flughafenbetreiber und Luftfahrtunternehmen stehen vor der Herausforderung, steigende Passagierzahlen bei gleichzeitig erhöhten Sicherheitsanforderungen zu bewältigen. Mit der **Nutzung biometrischer Verfahren** sollen eine effizientere Prozessgestaltung und verbesserte **Sicherheitskontrollen** möglich sein. Gleichzeitig bergen diese Technologien erhebliche **datenschutzrechtliche Risiken**. Eine klare rechtliche Einordnung dieser Verfahren war daher dringend erforderlich.

In seiner Bewertung kam der EDSA zu dem Schluss, dass nur zwei Arten für die Speicherung der biometrischen Daten mit den Grundsätzen der Integrität, Vertraulichkeit und Datensicherheit vereinbar sind: die **Speicherung der biometrischen Daten ausschließlich beim Passagier** selbst oder – alternativ – verschlüsselt in einer zentralen **Datenbank**, bei der sich der **Verschlüsselungsschlüssel allein in der Hand des Passagiers** befindet. Eine zentrale Speicherung ohne Kontrolle durch die betroffene Person wird in der Stellungnahme als unvereinbar mit den Anforderungen des Datenschutzes eingestuft.

Für deutsche Aufsichtsbehörden und Flughafenbetreiber liefert die Stellungnahme wichtige **Klarstellungen zur datenschutzkonformen Ausgestaltung biometrischer Systeme**. Insbesondere wurde festgehalten, dass eine biometrische Verifikation nur dann erfolgen darf, wenn auch eine gesetzliche Pflicht zur Identitätsprüfung besteht. Die Verarbeitung biometrischer Daten setzt zudem in jedem Fall eine aktive Einwilligung der Passagiere voraus.

Die **Stellungnahme 11/2024 zum Einsatz von Gesichtserkennung zur Straffung der Fluggastströme (Vereinbarkeit mit Artikel 5 Absatz 1 Buchstaben e und f, Artikel 25 und Artikel 32 DSGVO)** ist unter dem folgenden Link abrufbar:

https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-112024-use-facial-recognition-streamline_de

Kurzlink: *https://uldsh.de/tb43-6-2-3a*

6.2.4 EDSA-Guidelines zu Anonymisierung und Pseudonymisierung

Die Frage, ob bestimmte Daten **„personenbezogene Daten" im Sinne der DSGVO** sind, ist von großer Bedeutung – schließlich entscheidet sie darüber, ob der Anwendungsbereich der DSGVO bzw. der Datenschutzgesetze eröffnet ist. Für nicht personenbezogene Daten ist die DSGVO nicht anzuwenden. Zwar gibt es auch für solche Daten Regelungen – man denke an Geheimschutz oder Regelungen zu Betriebs- und Geschäftsgeheimnissen –, doch sind diese nicht datenschutzrechtlicher Natur.

Ob Daten personenbezogen im Sinne der DSGVO sind, ist nicht immer einfach festzustellen. Laut Definition in Art. 4 Nr. 1 DSGVO geht es um „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen". Bei Namen und Anschriften, E-Mail-Adressen, Identifikationsnummern usw. besteht daran kein Zweifel.

Aber wie ist das mit **statistischen Daten** oder mit Daten, die das Ergebnis einer **Anonymisie-**

rung personenbezogener Daten sind? Ein einzelnes Datum wie „Mann, 43 Jahre alt" wird man kaum als personenbezogen oder -beziehbar ansehen. Bei der Angabe „Frau, ehemalige Bundeskanzlerin" wird man hingegen auch ohne Angabe eines Namens wissen, wer gemeint ist. Spannend ist wie immer der Zwischenbereich: Wie sieht es mit „Frau, ehemalige Bundesministerin" oder „Mann, ehemaliger Ministerpräsident eines Bundeslandes" aus? Hier werden wohl noch Zusatzinformationen (z. B. zum Zeitpunkt) notwendig sein, um Betroffene eindeutig zu bestimmen.

Für die rechtliche Beurteilung ist relevant, **wer über dieses Zusatzwissen verfügt und für wen es realistischerweise zugänglich** ist, aber auch wie groß der Aufwand für eine Identifizierung einer betroffenen Person ist. Hinweise finden sich im Erwägungsgrund 26 der DSGVO.

Aus dem Erwägungsgrund 26 der DSGVO

[…] Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. […]

Im **konkreten Einzelfall** ist es strittig, was es genau bedeutet, dass „alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern"; es gibt bereits mehrere Urteile des Europäischen Gerichtshofs, in dem dieser Aspekt angesprochen wird.

Dass das **Wegstreichen eines Namens** aus einem Datensatz **zum Anonymisieren nicht ausreicht**, zeigt das oben genannte Beispiel des Berufs „Bundeskanzlerin". Aber wie kann man feststellen, ob Daten anonym sind oder eine Anonymisierung erfolgreich war? Kann man für ein effektives Anonymisieren eine Anleitung oder eine Checkliste erstellen?

Zahlreiche **wissenschaftliche Veröffentlichungen** in diesem Bereich zeigen, dass die Antwort nicht ganz einfach ist: Für viele vorgeschlagene Anonymisierungsverfahren gibt es Untersuchungen über ihre Schwächen. Dies erinnert an das Ringen um die besten Verschlüsselungsverfahren – neue Vorschläge werden auf den Prüfstand gestellt und müssen sich beweisen.

Mit diesen Fragen beschäftigt sich seit mehreren Jahren auch der EDSA und erstellt gerade zwei Dokumente mit Leitlinien (Guidelines), an denen auch wir beteiligt sind. Diese Leitlinien sind in die Bereiche der **Pseudonymisierung** und der **Anonymisierung** aufgeteilt.

Hier geht **Sorgfalt vor Schnelligkeit**, denn Fehler können schwerwiegend sein: Werden (vermeintlich) anonyme Daten veröffentlicht, sind sie für alle zugänglich. Stellt sich später heraus, dass betroffene Personen dennoch (re-)identifiziert werden können, lässt sich die erfolgte Veröffentlichung nicht wieder rückgängig machen – und ein entstandener Schaden kann möglicherweise irreversibel sein. Mit derartigen Fragen beschäftigen wir uns auch im vom BMBF geförderten Projekt AnoMed (Tz. 8.4).

Anfang 2025 wurde vor Drucklegung dieses Berichts die Konsultationsfassung der **Guidelines 01/2025 on Pseudonymisation** fertiggestellt, die unter dem folgenden Link zur Verfügung steht:

https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_de

Kurzlink: *https://uldsh.de/tb43-6-2-4a*

Nach Ablauf der öffentlichen Konsultation wird eine überarbeitete Fassung dieser Leitlinien zur Pseudonymisierung auf der Website des EDSA auf Englisch und in den anderen Sprachen der Mitgliedstaaten abrufbar sein. Mit der Fertigstellung der Leitlinien zur Anonymisierung ist im Jahr 2025 zu rechnen.

Was ist zu tun?

Sollen Daten anonymisiert veröffentlicht werden, sollte man sich sehr sicher sein, dass sie wirklich anonym sind. Die derzeit in Arbeit befindlichen Guidelines des EDSA werden dann eine Hilfe bieten.

6.2.5 Die KI zaubert nicht – Diskussion zu Personenbezug in KI-Modellen

Mit den zunehmenden konkreten Einsatzmöglichkeiten von KI-Systemen und insbesondere großen Sprachmodellen haben sich Aufsichtsbehörden in Deutschland und Europa intensiv mit der **datenschutzrechtlichen Einordnung von solchen Large Language Models (LLMs**) befasst. Ein besonderer Fokus lag ab Frühsommer 2024 dabei auf der grundlegenden Frage, ob in trainierten LLMs personenbezogene Daten im Sinne der DSGVO verbleiben und somit ein **Personenbezug** gegeben ist.

Nach eingehender Analyse vertritt das ULD die Position, dass ein Personenbezug in LLMs jedenfalls nicht pauschal ausgeschlossen werden kann. Bei Modellen, die **mit personenbezogenen Daten trainiert** wurden, ist nach aktuellem Stand der Wissenschaft davon auszugehen, dass **Informationen darüber im trainierten Modell verbleiben**. Diese Einschätzung stützt sich insbesondere auf die komplexe Beschaffenheit der Informationsrepräsentation in diesen Systemen sowie die nachgewiesenen Möglichkeiten zur **Extraktion** (d. h. dem Auslesen oder Abrufen) von Trainingsdaten.

Auch **zusätzliche Schutzmaßnahmen**, etwa durch Alignment-Techniken (Ausrichtung eines KI-Modells an vorgegebene Regeln und Direktiven), können **nach bisherigen Erkenntnissen nicht zuverlässig** verhindern, dass personenbezogene Daten nach dem Training verarbeitet oder ausgegeben werden. Dieser Auffassung entspricht auch die im Dezember veröffentlichte EDSA-Stellungnahme zu personenbezogenen Daten in KI-Modellen (Tz. 6.2.6).

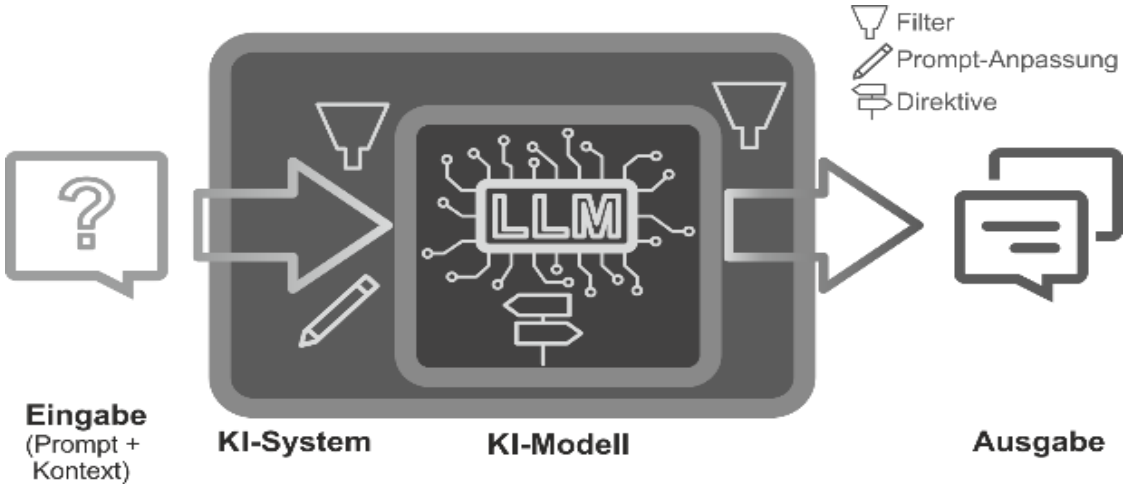

Abb. 3: Das KI-Modell eingebettet in ein KI-System mit Ein- und Ausgabe

Aus dieser Bewertung folgt u. a.: Sowohl der Einsatz als auch die Weitergabe von LLMs müssen unter **Berücksichtigung der datenschutzrechtlichen Vorgaben** erfolgen – selbst wenn der beabsichtigte Einsatz ohne Personenbezug auskommen soll. Da **KI-Modelle eingebettet in KI-Systeme** betrieben werden (siehe Abb. 3), können Filter und andere Maßnahmen ergriffen werden, um die datenschutzrechtlichen Risiken zu verringern, etwaige negative Auswirkungen auszuschließen oder zumindest abzumildern und gegebenenfalls einen datenschutzkonformen Einsatz zu ermöglichen.

Eine besondere Herausforderung stellt für Verantwortliche in jedem Fall die **erforderliche Risikoeinschätzung** dar, da wesentliche Informationen über Trainingsdaten, Optimierungsziele und interne Prozesse der Modelle bzw. Systeme häufig nur den Anbietern vorliegen. Der Verantwortliche, der KI-Modelle oder KI-Systeme einsetzt, bleibt aber datenschutzrechtlich dafür verantwortlich.

6.2.6 Formelles Artikel-64er-Verfahren zu KI – die Antworten des EDSA

Im September 2024 hat sich die irische Datenschutzbehörde an den EDSA gewandt und im formellen Stellungnahmeverfahren nach Art. 64 Abs. 2 DSGVO um die **Beantwortung von einigen wichtigen Fragestellungen zur KI-Entwicklung** gebeten. Diese wurde in den Fachausschüssen des EDSA bis Dezember 2024 entwickelt und veröffentlicht.

Die Stellungnahme zum Einsatz personenbezogener Daten bei der Entwicklung und dem Betrieb von KI-Modellen gibt Hinweise zu grundlegenden Datenschutzaspekten und bietet damit einen **Rahmen für eine datenschutzkonforme Umsetzung von KI-Anwendungen**. Sie betont, dass Datenschutz und verantwortungsvolle KI-Innovation keine Gegensätze darstellen. Die Stellungnahme nennt konkrete Kriterien, unter denen KI-Modelle datenschutzkonform entwickelt und betrieben werden können (zum Unterschied zwischen KI-Systemen und KI-Modellen siehe Tz. 6.2.5 sowie Abb. 3). Der EDSA befasst sich dabei mit drei zentralen Fragestellungen: der **Anonymität von KI-Modellen**, ob und wie **berechtigte Interessen als Rechtsgrundlage** herangezogen werden können sowie den **Auswirkungen rechtswidrig verarbeiteter personenbezogener Daten** bei der Modellentwicklung. Die Stellungnahme schafft damit Rechtssicherheit für die Entwicklung und Anwendung von KI – mit Blick auf den notwendigen Schutz personenbezogener Daten.

Von besonderer praktischer Bedeutung sind die vom EDSA entwickelten **Prüfkriterien zur Bewertung der Anonymität von KI-Modellen** sowie der vorgeschlagene **dreistufige Test zur Prüfung berechtigter Interessen**. Für die Beurteilung berechtigter Interessen werden dabei wichtige Aspekte wie die Erwartungshaltung der betroffenen Personen, der Kontext der Datenerhebung und mögliche risikoeindämmende Maßnahmen berücksichtigt. Bezüglich der Anonymität von KI-Modellen stellt der EDSA klar, dass diese im Einzelfall zu prüfen ist und sowohl die Möglichkeit der Identifizierung betroffener Personen als auch die Extraktion personenbezogener Daten durch Abfragen zu berücksichtigen sind.

Von grundsätzlicher Bedeutung ist zudem die Klarstellung des EDSA zu den Folgen einer rechtswidrigen Verarbeitung personenbezogener Daten bei der Entwicklung von KI-Modellen. Die Stellungnahme macht deutlich, dass sich die Rechtswidrigkeit des Trainings auch auf den späteren Einsatz des Modells auswirken kann – das ist von Fall zu Fall zu prüfen. Eine Ausnahme gilt nur dann, wenn das Modell nachweislich wirksam anonymisiert wurde. Diese Position unterstreicht die Notwendigkeit, **bereits bei der Entwicklung von KI-Modellen auf eine rechtskonforme Datenverarbeitung** zu achten, um keine (möglicherweise unüberwindbaren) Hürden für einen späteren Einsatz zu schaffen.

Die differenzierenden **Kriterien** ermöglichen eine **sachgerechte Einzelfallbetrachtung** und tragen der schnellen technologischen Entwicklung im KI-Bereich Rechnung. Die Stellungnahme verdeutlicht damit, dass die Datenschutzgrundsätze der DSGVO einen geeigneten und

flexiblen Rahmen für die verantwortungsvolle Entwicklung innovativer KI-Systeme bieten.

Die **Stellungnahme „Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models“** ist auf Englisch unter dem folgenden Link abrufbar:

https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

Kurzlink: *https://uldsh.de/tb43-6-2-6a*

6.3 Ausgewählte Ergebnisse aus Prüfungen, Beratungen und Meldungen nach Artikel 33 DSGVO

6.3.1 Typische Beispiele und Erkenntnisse aus Datenpannenmeldungen

Alle Jahre wieder – Meldungen über Datenpannen (genauer: Verletzungen des Schutzes personenbezogener Daten) beschäftigen uns weiterhin in großem Umfang. Auffällig ist, dass **von einigen Organisationen vergleichsweise häufig Meldungen** eintreffen, von anderen gar nicht. Dies lässt mehrere Schlüsse zu: Entweder sind diese Organisationen eher schlecht im Hinblick auf Datenschutz und Datensicherheit aufgestellt. Oder sie sind – im Gegensatz zu anderen Organisationen – besonders sensibel und haben **funktionierende Meldeketten** für Datenschutzverstöße. Oder es liegt schlicht an der Größe einer Organisation: Sind sehr viele Personen mit der Verarbeitung personenbezogener Daten betraut, kommt es mit einer größeren Wahrscheinlichkeit zu Datenpannen.

Auch die **Qualität der Aufarbeitung der Vorfälle** schwankt stark: Ein Teil der Meldungen beschreibt lediglich das aufgetretene Problem (z. B. einen unbefugten Zugriff auf ein E-Mail-Postfach und anschließendem Versand von Spam), was von unserer Seite oft ein mehrfaches Nachfragen nach Ursachen und geplanten Abhilfemaßnahmen erfordert – denn dies gehört zu einer korrekten Bearbeitung eines Artikel-33-Vorfalls. Andere Meldungen sind deutlich präziser; und auch wenn der Sachverhalt oder die genauen Ursachen zum Zeitpunkt der initialen Meldung noch nicht bekannt ist, wird diese Meldung eigeninitiativ ergänzt, der Fall wird aufgearbeitet, und erläuternde Unterlagen werden selbstständig nachgereicht.

Ein Schwerpunkt der Meldungen betrifft „kleinere“ Verletzungen des Schutzes personenbezogener Daten, die beispielsweise auf der **Verwechslung von Unterlagen oder Dateien zweier betroffener Personen** beruhen. In diesen Fällen gibt es kaum technische Gegenmaßnahmen; stattdessen ist erhöhte Aufmerksamkeit und doppelte Kontrolle angesagt. Auch Änderungen von Prozessen können helfen, um die gebotene Sorgfalt zu erreichen.

Weiterhin stark vertreten sind **Angriffe durch Schadsoftware, etwa Verschlüsselungstrojaner**. Auch wenn nicht klar ist, ob Daten wirklich abgeflossen und somit in die Hände Dritter gelangt sind, steht diese Möglichkeit immer im Raum: Wer ein Computersystem so manipulieren kann, dass Schadcode aus dem Internet heruntergeladen wird und Datenspeicher verschlüsselt werden, kann auch Daten über das Internet verschicken.

Dieses Szenario ist auch nicht unwahrscheinlich: Hat man eine funktionierende und aktuelle Datensicherung, so verliert ein Verschlüsselungstrojaner seinen Schrecken. Statt ein „Lösegeld“ für die Entschlüsselung zu zahlen, stellen Verantwortliche die Daten aus der Datensicherung wieder her. Angreifer reagieren darauf mit einer **Doppelstrategie, indem Daten nicht nur verschlüsselt, sondern gleichzeitig auch kopiert** werden – eine sogenannte Exfiltration. Zahlt dann ein Opfer nicht das verlangte Lösegeld, weil es dank Datensicherung nicht auf die Entschlüs-

selung angewiesen ist, so kann man es mit einer zweiten Drohung, **der Veröffentlichung der exfiltrierten Daten**, erpressen.

Schließlich steigt die Zahl der **Angriffe auf E-Mail-Konten**, deren Zugangsdaten mittels **Phishing** erbeutet werden: Die Nutzenden werden verleitet, ihre Zugangsdaten einem Angreifer zur Verfügung zu stellen, z. B. über **nachgemachte Log-in-Fenster oder gefälschte Webseiten**. Dazu reicht es beispielsweise, einem Opfer eine E-Mail mit einem Link zu einer Webseite (unter der Kontrolle des Angreifers) zuzusenden und zur Eingabe des Passworts aufzufordern. Konnte man früher solche E-Mails vergleichsweise leicht an fehlerhaften Formulierungen und logischen Ungereimtheiten erkennen, lassen sich heutzutage die Angreifer unterstützen und solche **E-Mails mittels KI passgenau für das Zielpublikum entwerfen**. Die „erbeuteten" Zugangsdaten werden dann verwendet, um auf E-Mail-Konten zuzugreifen. Im harmlosen Fall werden die Konten zum Versand von Spam genutzt, aber es besteht auch die Gefahr, lesend **auf sämtliche gespeicherte E-Mails und Adressbücher zuzugreifen** oder unbefugt E-Mails im Namen des rechtmäßigen Eigentümers zu versenden. Ein beliebtes Beispiel sind E-Mails der (vermeintlichen) Geschäftsleitung, die **bei der Buchhaltung eine Zahlung auf ein Auslandskonto** beauftragen möchte. Die E-Mail ist dann „echt", wurde aber nicht von der Geschäftsleitung, sondern vom Angreifer verfasst. Sie stammt auch vom korrekten E-Mail-Server und ist daher technisch nur sehr schwer oder gar nicht von einer E-Mail des rechtmäßigen Eigentümers zu unterscheiden.

Angriffe dieser Art nehmen zu, weil der Zugang zu dienstlicher oder geschäftlicher E-Mail anders als früher **nicht mehr das Betreten eines Dienstgebäudes oder Büros** und die Nutzung der dortigen Computer voraussetzt: Viele E-Mail-Systeme sind nämlich mittlerweile ohne besondere Sicherungsmaßnahmen direkt über das Internet mittels Nutzernamen und Passwort und mit jeglicher Hardware zugänglich. Ein Angreifer, der solche Zugangsdaten erbeutet, kann dann ebenso über das Internet auf das E-Mail-Konto zugreifen.

Als Gegenmaßnahme empfiehlt sich in diesem Fall, den **Zugang zu E-Mail-Systemen an einen zweiten Faktor zu koppeln**, der zusätzlich zu Nutzername und Passwort wirkt und sich möglichst schwer kopieren oder entwenden lässt. Ein Beispiel hierfür ist eine zusätzliche **Zwei-Faktor-Authentifizierung**, die einen unbefugten Zugang erschwert. Weitere mögliche Maßnahmen bestehen in der **Bindung an dienstliche Hard- und Software** (z. B. über Gerätezertifikate oder die Bindung an Apps) oder gesicherte Netzzugänge (z. B. VPN), sodass das E-Mail-System nicht direkt aus dem Internet zugänglich ist, sondern nur über eine **gesicherte Netzverbindung**. Eine Verbindung „von jedem PC der Welt im Internetcafé" ist dann nicht mehr möglich – und genau das ist das Ziel der Sicherheitsmaßnahmen.

Was ist zu tun?

Bei Datenpannen ist die Ursache sorgfältig zu ermitteln, damit sie abgestellt wird oder zumindest die Wahrscheinlichkeit von Wiederholungsfällen gesenkt wird.

6.3.2 Frag' für 'nen Freund

Die Integration von künstlicher Intelligenz (KI) in Unternehmen und Behörden nimmt immer weiter zu und stellt sowohl die Organisationen als auch die Aufsichtsbehörden vor Herausforderungen. Häufig bestehen jedoch Hürden auf beiden Seiten: Organisationen befürchten **aufsichtsbehördliche Maßnahmen, wenn sie Fragen stellen**, und dass ihren KI-Projekten Steine in den Weg gelegt werden. Die Aufsichtsbehörden ihrerseits sind darauf angewiesen, die Probleme und Fragen der Organisationen zu kennen, die bei der Planung, Entwicklung und beim Einsatz von KI auftreten. Nur so können sie praxistaugliche Hinweise für die Konzeption, die Implementierung und den Betrieb von KI-Projekten anbieten. Ziel dabei ist, dass Datenschutzanforderungen bereits in der Entwicklungsphase von KI-Anwendungen berücksichtigt werden, statt sie nachträglich mit hohem Aufwand einbauen zu müssen.

Hier setzt das **Konzept „Frag' für 'nen Freund"** an, das einen offenen Rahmen für den Austausch von Wissen und Erfahrungen zwischen Organisationen und Aufsichtsbehörden bietet. Dieses Format schafft eine **vertrauensvolle Gesprächsatmosphäre, in der Teilnehmende Fragen stellen können**, ohne negative Konsequenzen befürchten zu müssen. Zusätzlich fördert diese Form der Veranstaltung das Verständnis zwischen beiden Seiten, kann Missverständnisse ausräumen und bietet einen Rahmen für einen direkten, fachlichen Austausch.

Im November fand in den Räumen des ULD die erste „Frag' für 'nen Freund"-Veranstaltung zum Thema KI statt. Die Teilnehmenden aus Unternehmen, Behörden und Kanzleien diskutierten zu KI-Fragestellungen und brachten ihre Erfahrungen und Fragestellungen ein. In einer abschließenden Feedbackrunde waren sich alle Teilnehmenden einig, dass dieses **Format auch zukünftig genutzt** werden soll, um den Austausch von KI-Expertise zu fördern. Unternehmen, Behörden und Aufsichtsbehörde haben so die Möglichkeit, auf Augenhöhe miteinander zu kommunizieren – ein wichtiger Schritt, um das Verständnis für die praktischen Anwendungen von KI und die damit verbundenen regulatorischen Anforderungen zu stärken.

Unter diesem Link gibt es weitere Informationen:

https://www.datenschutzzentrum.de/artikel/1495-Frag-fuern-Freund-Austausch-rund-um-KI-und-Datenschutz.html

Kurzlink: *https://uldsh.de/tb43-6-3-2a*

Was ist zu tun?

Auf der Website des ULD können sich interessierte Personen auf einer Mailingliste eintragen, um Informationen zu KI & Datenschutz zu erhalten und über zukünftige „Frag' für 'nen Freund"-Veranstaltungen informiert zu werden.

6.3.3 Fragen in der Telefonberatung: Passwörter, E-Mail-Provider und PayPal-Phishing

In der **telefonischen Beratung** begegnen wir regelmäßig technischen Herausforderungen, von denen im Berichtsjahr zwei besonders herausragten: der Verlust von Onlinezugängen und betrügerische PayPal-Anrufe.

Der **Verlust von Onlinezugängen**, sei es durch **Fremdübernahme** oder **selbst verschuldete Aussperrung**, ist ein Dauerbrenner in der telefonischen Beratung. Besonders kritisch ist dabei der Verlust des **E-Mail-Kontos**, da dieses oft als zentrale **Schaltstelle** für viele andere Onlinedienste dient. Haben Unbefugte Zugriff auf das E-Mail-Konto, können sie über die üblichen Passwort-Zurücksetzungsfunktionen schnell weitere Konten des Opfers übernehmen. Die Situation verschärft sich, wenn der E-Mail-Anbieter keinen technischen Support bietet. Dies trifft besonders auf Anbieter kostenloser E-Mail-Dienste (Freemailer) zu, die ihren Support üblicherweise zahlenden Kunden vorbehalten und Gratisnutzer lediglich auf Chatbots oder kostenpflichtige Hotlines verweisen. Wir empfehlen daher, sich bereits bei der **Wahl des E-Mail-Anbieters** über dessen **Supportangebot im Notfall** zu informieren und die möglichen Hilfswege vorab zu kennen.

Die beste Absicherung gegen unerwünschte Kontozugriffe bietet nach wie vor die **Zwei-Faktor-Authentifizierung**. Ist diese aktiviert, reicht ein erbeutetes Passwort allein nicht aus – Angreifer benötigen zusätzlich den Code vom Smartphone oder einen registrierten USB-Stick. Diese **zweite Sicherheitsebene** schützt Onlinekonten selbst dann noch, wenn das eigene E-Mail-Konto bereits kompromittiert wurde.

Ein weiteres aktuelles Phänomen sind **betrügerische Anrufe von angeblichen PayPal-Beschäftigten**. Diese melden sich auf Englisch und behaupten, vom Konto der Angerufenen sei ein größerer Betrag für den Kauf von Bitcoins abgebucht worden. Der Betrug folgt dabei einem wiederkehrenden Gesprächsmuster: Man bietet an, die angebliche Zahlung rückgängig zu machen, besteht aber darauf, zunächst die Kontosicherheit wiederherzustellen. Man führt die Opfer telefonisch auf eine Website, die deren IP-Adresse mit einer Warnung versehen anzeigt, und behauptet fälschlicherweise, die IP-Adresse sei „gehackt" worden (eine Aussage, die technisch natürlich wenig Sinn ergibt). Als **vermeintliche Lösung** fordert man die **Installation einer Fernwartungs-App** über den App-Store. Glücklicherweise wurden die Personen, die sich an das ULD wandten, an dieser Stelle misstrauisch und beendeten das Gespräch, bevor die Betrüger Zugriff auf ihre Smartphones erlangen konnten.

Die PayPal-Anrufe folgen dem klassischen **Betrugsmuster, zunächst eine Stresssituation zu erzeugen**, um die Betroffenen zu schnellen und unüberlegten Reaktionen zu provozieren. Dabei war es in diesem Fall recht leicht, den Betrug zu entlarven: Die angerufene Person fragte einfach nach, um welche PayPal-Adresse es denn eigentlich ginge – prompt legte die Gegenseite auf. **Nachfragen und Präzisierungen** sind dementsprechend ein gutes Mittel, um in vermeintlichen Stresssituationen sowohl ein wenig Zeit zum Nachdenken als auch Klarheit über die Intention der Anrufenden zu erhalten.

Was ist zu tun?

(Vermeintlich) wohlmeinenden Anrufen, die Sicherheitsvorfälle melden, sollte man kritisch begegnen. Rückfragen schaffen Zeit zum Nachdenken und entlarven manchen Betrug.

6.3.4 Modulare Dokumentation – Rechenschaftspflicht mit System

Organisationen müssen sicherstellen, dass sie die Anforderungen der Datenschutz-Grundverordnung (DSGVO) und – soweit einschlägig – des Landesdatenschutzgesetzes in ihren Verfahrensweisen integrieren. Die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO und Artikel 24 DSGVO verlangt, dass nicht nur die **gesetzlichen Anforderungen zu erfüllen sind**, sondern **dies auch jederzeit nachgewiesen werden kann**. Hieraus ergibt sich eine Pflicht zur Dokumentation.

Verantwortliche müssen sicherstellen, dass **alle Grundsätze der DSGVO** – von der Rechtmäßigkeit über die Zweckbindung bis hin zu Integrität und Vertraulichkeit – in jeder Phase der Datenverarbeitung beachtet werden. Darüber hinaus gilt es, die Umsetzung spezifischer Anforderungen zu belegen: von der Sicherstellung von Betroffenenrechten über die Implementierung geeigneter technischer Maßnahmen bis hin zur Einbindung von Datenschutzbeauftragten. Für öffentliche Stellen in Schleswig-Holstein kommen zusätzliche Anforderungen hinzu, z. B. das vom Landesdatenschutzgesetz (LDSG SH) geforderte Test- und Freigabeverfahren für automatisierte Verarbeitungen. Die Komplexität dieser Anforderungen verdeutlicht die Notwendigkeit eines **gut geplanten und strukturierten Ansatzes zur Datenschutzdokumentation**.

Die Herausforderung besteht darin, die **Dokumentationspflichten** nicht als lästige Pflicht, sondern **als Chance zu begreifen**. Eine gut strukturierte Dokumentation bietet die Möglichkeit, Transparenz zu schaffen, Vertrauen aufzubauen und die eigenen Datenschutzprozesse kontinuierlich zu optimieren. Sie bildet das Fundament eines effektiven Datenschutzmanagements und ermöglicht es Organisationen, jederzeit nachzuweisen, dass sie die Datenschutzvorschriften einhalten und die Prüfbarkeit gewährleistet ist.

Wir haben einen Strukturierungsvorschlag entwickelt, um das Datenschutzmanagement zu organisieren. Ziel dieses Vorschlags ist es, einen grundlegenden Rahmen zu schaffen, der es Organisationen ermöglicht, ihre **Dokumentation systematisch und übersichtlich zu gestalten**. Die konkreten Inhalte der einzelnen Dokumentationsbausteine müssen jedoch individuell von jeder Organisation erarbeitet werden, da sie stark von den spezifischen Verarbeitungstätigkeiten, der eingesetzten Technik, den organisatorischen Strukturen und den besonderen Risiken der jeweiligen Datenverarbeitung abhängen.

Der vorliegende Strukturierungsvorschlag unterteilt sich in drei Hauptbereiche, die jeweils einen spezifischen Aspekt der Dokumentation abdecken: **Kerndokumentation, IT-Dokumentation und Dokumentation der Verarbeitungstätigkeiten**. Die gesamte Dokumentation ist hierarchisch auf zwei Ebenen aufgebaut und nutzt einen **modularen Ansatz mit „Was-Bausteinen" und „Wie-Bausteinen"**. Zudem hilft diese Struktur, Redundanzen zu vermeiden, da jede Information nur in einem Baustein dokumentiert wird. Alle anderen Bausteine können dann auf diesen verweisen. Auf diese Weise können Änderungen, Anpassungen oder Fehler in den einzelnen Bausteinen leicht vorgenommen werden, ohne dass die gesamte Dokumentation überarbeitet werden muss.

Die **Verarbeitungsdokumentation** ist **das zentrale Element des Datenschutzmanagements** in Organisationen. Aus diesem Grund stellt das ULD sowohl für die Erfüllung der Rechenschaftspflicht als auch zur Erfüllung der Informationspflichten zusätzliche Dokumentationsvorlagen und Erläuterungen zur Verfügung. Sie können als roter Faden für die Dokumentation angesehen werden.

Der **Strukturierungsvorschlag und die Dokumentationsvorlagen mit ihren Erläuterungen** können auf der Website des ULD unter dem folgenden Link heruntergeladen werden:

https://uldsh.de/doku/

Kurzlink: *https://uldsh.de/tb43-6-3-4a*

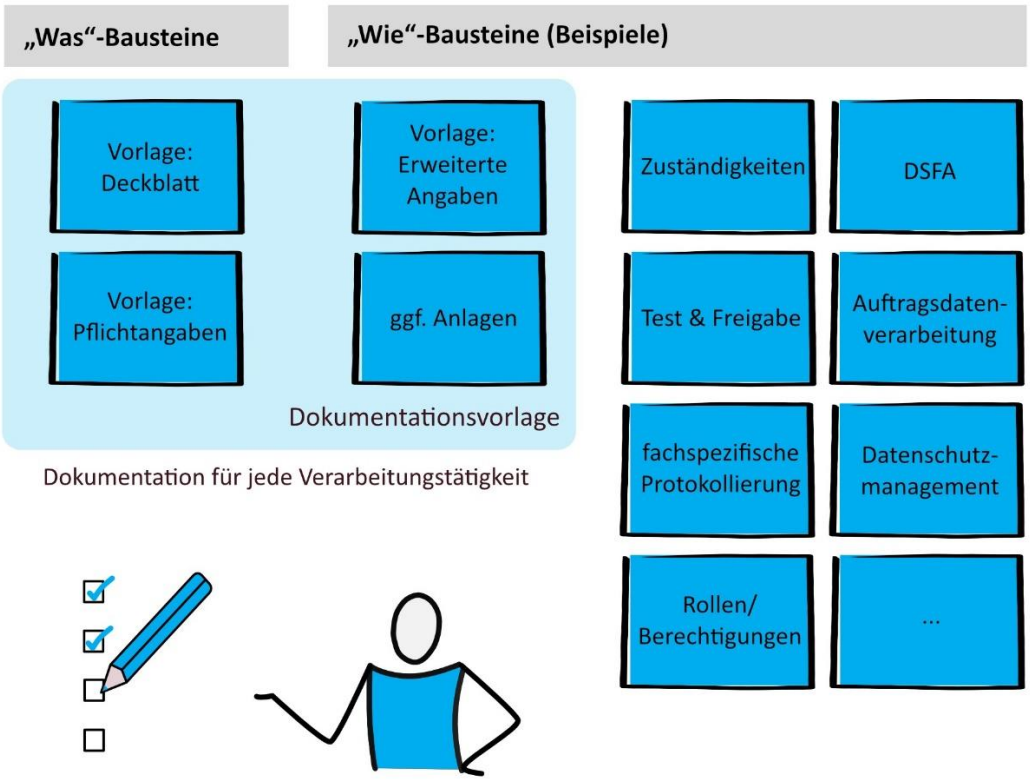

Abb. 4: Verarbeitungsdokumentation

07

KERNPUNKTE

Aktuelles aus dem AK Medien

Orientierungshilfe zu Funkzählern

7 Neue Medien

Unter den „Neuen Medien" versteht man primär digitale und interaktive Medien – also etwas, das gar nicht mehr als „neu" anzusehen ist. Dennoch lohnt sich der Blick auf den **Wandel von der analogen zur digitalen Welt**. In der Datenschutzkonferenz (DSK) beschäftigt sich der Arbeitskreis (AK) Medien, an dem wir uns beteiligen, mit einem bunten Strauß an Themen, über die hier nur ein kurzer Überblick gegeben werden soll.

7.1 Aktuelles aus dem AK Medien

Der AK Medien der DSK beschäftigt sich mit den aktuellen Themen rund um Datenschutz und Medien. Zusätzlich zu den zwei Präsenzsitzungen haben wir im Berichtsjahr an den monatlichen Videokonferenzen teilgenommen. Gegenstand der Sitzungen waren zunächst Berichte aus den europäischen Arbeitsgruppen wie der Technology Expert Subgroup und der Social Media Expert Subgroup. Zu den besprochenen Themen gehört regelmäßig die Nutzung aktueller sozialer Medien, beispielsweise TikTok oder Facebook (41. TB, Tz. 7.1).

Ein Dauerthema im AK Medien ist das **Einwilligungsmanagement** und der Umgang mit **Cookie-Bannern**. Hierzu haben sich die Mitglieder des Arbeitskreises aktuelle Umsetzungen angeschaut. Ebenfalls mit Websites hängt das Thema der sogenannten „**Authentic Consent Service**"-Dienste zusammen, die das Wiedererkennen von Nutzenden über verschiedene Kontexte hinweg erlauben.

Auf nationaler und europäischer Ebene wurde das Konzept der bezahlten Abomodelle diskutiert, mit dem Nutzende vor die Wahl **„Einwilligung (in eine Datenverarbeitung) oder Bezahlung"** (englisch: „Consent or Pay" oder auch „Pay or okay" genannt) gestellt werden. Dahinter steht die Idee, dass Anbieter wie Meta (Facebook) bereit sind, ihre Verarbeitung von personenbezogenen Daten insbesondere zur Profilerstellung bzw. Werbung gegen einen monatlichen Betrag zu verringern. Strittig ist dabei u. a., welche Beträge für ein solches Modell zumutbar wären, damit Nutzende tatsächlich eine sinnvolle Alternative haben. Auch ist in konkreten Fällen oft unklar, in welchem Maße tatsächlich die Anbieter dann die Datenverarbeitung reduzieren oder ob nur die Verwendung der Daten zu Werbezwecken eingeschränkt wird. Die **Stellungnahme 08/2024 des Europäischen Datenschutzausschusses zur Wirksamkeit von Einwilligungen im Kontext von „Consent or Pay"-Modellen großer Onlineplattformen** ist unter dem folgenden Link verfügbar:

https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_de

Kurzlink: *https://uldsh.de/tb43-7-1a*

Überarbeitet werden musste die Orientierungshilfe zu Telemedien. Insbesondere war inzwischen aus dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) geworden. Eine entsprechende Überarbeitung wurde von der DSK am 15.11.2024 als **Orientierungshilfe zu digitalen Diensten** angenommen und veröffentlicht. Die Orientierungshilfe steht unter diesem Link zum Abruf bereit:

https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf

Kurzlink: *https://uldsh.de/tb43-7-1b*

7.2 Orientierungshilfe zur Datenverarbeitung durch funkbasierte Zähler

Die DSK hat im Jahr 2024 eine **Orientierungshilfe zur Datenverarbeitung im Zusammenhang mit funkbasierten Strom-, Heizungs- und Wasserzählern** veröffentlicht. Auf 33 Seiten bietet das Papier eine Einführung zur Funktion der Zählertypen, eine Bewertung zur Verarbeitung von Daten mit Personenbezug und eine aktuelle Übersicht zu den Rechtsgrundlagen der Datenverarbeitung. Weiterhin gibt die Orientierungshilfe Antworten auf Fragen zu Duldungspflichten betroffener Personen beim Einbau der Zähler, zu möglichen Widerspruchsrechten, zulässigen Abruffrequenzen, den technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit, maßgeblichen Speicherfristen und zu bestehenden Informationspflichten.

Bei der funkbasierten Verbrauchsablesung werden die Verbrauchswerte durch elektronisch betriebene Geräte (z. B. Stromzähler, Wasserzähler, Heizkostenverteiler, Wärme- und Kältezähler) erfasst. Die Übertragung an das Unternehmen, das die Verbrauchswerte insbesondere für Abrechnungszwecke verarbeitet, wird per Funk oder sonstiger Netztechnik realisiert. Neben zählerbezogenen Daten oder Angaben zur Durchflussleistung und Temperatur sind auch verbrauchsbezogene Daten Gegenstand der Verarbeitung, wie z. B. der Zählerstand und die Historie der Werte. Eine **Zuordnung zu natürlichen Personen** und damit die Herstellung des Personenbezugs ist etwa über eine Zählernummer, einen Energieliefervertrag oder einen Mietvertrag denkbar. Bezüglich der **Rechtsgrundlagen** für die Datenerfassung und Weiterverarbeitung wird wie folgt ausgeführt:

- **Strom:** Das Messstellenbetriebsgesetz enthält Regelungen zur zulässigen Datenverarbeitung und zur Gewährleistung der Datensicherheit.
- **Heizung und Warmwasser:** Mit § 6b der Verordnung über Heizkostenabrechnung hat der Gesetzgeber den Umfang einer zulässigen Datenverarbeitung normiert.
- **Kaltwasser:** Eine bundeseinheitliche gesetzliche Vorgabe gibt es für diese Verbrauchsart nicht. Nur vereinzelt haben Bundesländer hierfür spezifische gesetzliche Vorgaben geschaffen. Um Rechtssicherheit herzustellen und den als notwendig erachteten Gesetzgebungsprozess zu beschleunigen, hat die DSK bereits in ihrer Stellungnahme vom 11.05.2023 Hinweise für bundesweit einheitliche Regelungen auch für diese Verbrauchsart ausgearbeitet.

Speziell bei **Strom- und Heizkostenzählern** hat der Gesetz- und Verordnungsgeber für die betroffenen Personen eine **Duldungspflicht hinsichtlich des Einbaus** normiert. In diesen Bereichen besteht auch kein Widerspruchsrecht. Die Zulässigkeit der Abruffrequenz bezüglich der Verbrauchswerte orientiert sich an der Erforderlichkeit der Datenverarbeitung im Einzelfall und muss angemessene Sicherheitsmaßnahmen (z. B. Verschlüsselung der Funksignale und Pseudonymisierung der Daten) vorsehen.

Die personenbezogenen Daten sind regelmäßig dann zu **löschen**, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Eine Ausnahme besteht etwa dann, wenn den Verantwortlichen eine anderweitige rechtliche Verpflichtung zur Aufbewahrung trifft. Die Orientierungshilfe gibt in einer tabellarischen Zusammenstellung einen **Überblick über maßgebliche Speicherfristen**. Schließlich wird erläutert, welche Rechte betroffene Personen gegen den Betreiber einer Messstelle geltend machen können.

Die **Orientierungshilfe „Datenverarbeitung im Zusammenhang mit funkbasierten Zählern“**, Version 1.0 vom 16.08.2024, ist unter dem folgenden Link abrufbar:

https://www.datenschutzkonferenz-online.de/media/oh/240816_DSK_OH_Datenverarbeitung_funkbasierte_Zaehler.pdf

Kurzlink: *https://uldsh.de/tb43-7-2a*

Die Stellungnahme der DSK **„Daten der Verbraucherinnen und Verbraucher beim Einsatz von Smart Meter zur Erfassung des Kaltwasserverbrauchs durch einheitliche Regelungen schützen“** vom 11.05.2023, die in der Orientierungshilfe erwähnt wird, steht unter dem folgenden Link zur Verfügung:

https://www.datenschutzzentrum.de/uploads/dsk/2023-05-11_DSK-Stellungnahme_Funkwasserzaehler.pdf

Kurzlink: *https://uldsh.de/tb43-7-2b*

08

KERNPUNKTE

Plattform Privatheit

Transparenz für das Internet der Dinge

AnoMed – Anonymisierung für medizinische Anwendungen

8 Modellprojekte und Studien

Das Unabhängige Landeszentrum für Datenschutz hat als Behörde der Landesbeauftragten für Datenschutz seine **Aktivitäten in drittmittelfinanzierten Projekten und Studien** fortgesetzt. Damit kooperiert das ULD weiterhin aktiv mit der Wissenschaft und kann zusammen mit Wissenschaftspartnern proaktiv an der Erforschung datenschutzspezifischer Fragen und der Gestaltung einschlägiger Technologien mitwirken. Gefördert wurden die im Berichtsjahr laufenden Projekte seitens des Bundesministeriums für Bildung und Forschung (BMBF), teils mit Co-Förderung durch die Europäische Union (NextGenerationEU). Beteiligungen an Projekten erfolgten weiterhin primär dort, wo **datenschutzfördernde Technik** (englisch: „Privacy-Enhancing Technologies", kurz PETs) erforscht, entwickelt oder in die Praxis transferiert wird oder wo **besondere Risiken** für die Rechte und Freiheiten natürlicher Personen bestehen.

Im Jahr 2024 beteiligte sich das ULD an Projekten zu aktuellen Themen in den Bereichen Privatheit und selbstbestimmtes Leben (Tz. 8.1), Überführung von Lösungen des Datenschutzes durch Technikgestaltung in die Praxis (Tz. 8.2) sowie Transparenzprobleme des Internets der Dinge (Tz. 8.3). Zudem setzte das ULD sein Engagement zu Anonymität für Medizinforschung mit Gesundheitsdaten fort (Tz. 8.4).

8.1 Plattform Privatheit: PRIDS – Privatheit, Demokratie und Selbstbestimmung

Über das Verbundvorhaben **„PRIvatheit, Demokratie und Selbstbestimmung im Zeitalter von KI und Globalisierung – PRIDS"** hatten wir schon berichtet (40. TB, Tz. 8.1; 41. TB, Tz. 8.1; 42. TB, Tz. 8.1). In dem von April 2021 bis Mai 2024 laufenden Projekt beschäftigten sich sieben Konsortialpartner aus verschiedenen Perspektiven mit der digitalen Transformation von Gesellschaften. Diese wird u. a. durch soziale Medien, Systeme der künstlichen Intelligenz (KI) und weitere technische Entwicklungen geprägt. Das ULD konzentrierte sich dabei auf den Bereich „Grundrechtsschutz in globalen Technikinfrastrukturen" und beteiligte sich an den interdisziplinären Forschungsarbeiten des Gesamtvorhabens zu Fragen von Datenschutz- und Privatheitsaspekten in Bezug auf Demokratie, künstliche Intelligenz (KI) und verschiedene Situationen im Verlauf der Lebensspanne von Individuen.

Prägend für das Vorhaben war die Vernetzung innerhalb der Plattform Privatheit (vormals: Forum Privatheit) sowie mit Akteuren aus Wissenschaft, Politik, Wirtschaft, Verwaltung und Zivilgesellschaft, um den öffentlichen und fachlichen Diskurs voranzubringen. Zu berücksichtigen war dabei die regulatorische Entwicklung auf europäischer und nationaler Ebene.

Die Weiterentwicklung vom Forum Privatheit (40. TB, Tz. 8.1) zur Plattform Privatheit fiel in die Projektlaufzeit von PRIDS. Es handelt sich dabei nicht um eine Umetikettierung, sondern der Charakter des Projekts hat sich zu einem **Dach für eine Vielzahl von interdisziplinären Projekten** gewandelt. Forschende entwickeln aus unterschiedlichen Perspektiven rechtliche, technische und organisatorische Lösungen, die es ermöglichen, in unserem digitalen Alltag unsere Grundrechte und europäischen Werte zu wahren. PRIDS gehörte zu den Kernprojekten in dieser Phase des Übergangs zu einer Plattform.

Ein großer Teil der im PRIDS-Projekt entstandenen wissenschaftlichen Veröffentlichungen ist über die **Website der Plattform Privatheit** als Open Access verfügbar, beispielsweise die Tagungsbände der jährlichen Konferenz der Plattform Privatheit, an der wir über das Projekt PRIDS maßgeblich mitgewirkt haben. Hinzu kommen White Paper und Policy Paper, die ebenfalls zum Download bereitgestellt werden:

https://www.plattform-privatheit.de

Kurzlink: *https://uldsh.de/tb43-8-1a*

8.2 Projekt DatenTRAFO – Neue Datenschutz-Governance – Technik, Regulierung und Transformation

Im Projekt **„DatenTRAFO"**, das für drei Jahre (2023-2026) geplant ist, untersuchen wir die neuen EU-Datengesetze, insbesondere die Digitale Dienste- und die KI-Verordnung (42. TB, Tz. 8.2). Beide folgen strukturell einem ähnlichen Ansatz wie die DSGVO und verlangen die Bewertung von Risiken für Grundrechte. Dabei müssen bestimmte Anbieter und Anwender Grundrechte-Folgenabschätzungen durchführen und Risikomanagementsysteme einrichten, um die Risiken für Grundrechte wirksam einzudämmen. Eine wichtige Rolle spielt insbesondere das **Grundrecht auf Nichtdiskriminierung**.

Im Zusammenhang mit algorithmischen Systemen, die oft als KI bezeichnet werden, gab es in der Vergangenheit bereits Probleme in den Niederlanden und vor kurzem in Dänemark. Dort wurden im Sozialbereich jeweils Systeme eingesetzt, die Sozialbetrug erkennen sollten. Allerdings zeigte sich, dass immer dann, wenn die **betreffende Person weiblich** war oder einen vom System als **nicht westeuropäisch eingeordneten Namen** aufwies, ein deutlich erhöhter Risikofaktor für Sozialbetrug angegeben wurde. Von einer neutralen, diskriminierungsfreien Berechnung eines derartigen Risikofaktors für die betroffenen Personen konnte keine Rede sein.

Im Projekt DatenTRAFO erforschen wir einen **Ansatz für Grundrechte-Folgenabschätzungen**, der sich am Vorgehen der Datenschutz-Folgenabschätzung orientiert und mit dem Verantwortliche auf bereits vorhandenem Wissen aufbauen können. Auf diese Weise soll gewährleistet werden, dass die Möglichkeit einschneidender Folgen für betroffene Personen, wie es beispielsweise bei einer Diskriminierung der Fall ist, frühzeitig erkannt wird und geeignete Maßnahmen getroffen werden, um gegenzusteuern. Bei einer ergebnisoffenen Herangehensweise kann es auch sein, dass Verantwortliche oder Aufsichtsbehörden zum Ergebnis kommen, dass gewisse Verarbeitungsformen oder der Einsatz von bestimmten (KI-)Systemen zu unterbleiben haben.

Das DatenTRAFO-Projekt beschäftigt sich außerdem mit **datenschutzfördernder Technik** und untersucht, unter welchen Bedingungen bekannte Verfahren der Privacy-Enhancing Technologies in der Praxis Verwendung finden können oder sollten. Weitere Informationen zum Projekt sind unter folgendem Link abrufbar:

https://www.datenschutzzentrum.de/projekte/datentrafo/

Kurzlink: *https://uldsh.de/tb43-8-2a*

8.3 Projekt Unboxing.IoT.Privacy – Transparenz für Datenschutzeigenschaften von IoT-Geräten

Dinge, die sich über das Internet vernetzen und steuern lassen? Na klar, seit einigen Jahren gehören Küchengeräte, Autos oder Hausanlagen, die mit dem Internet verbunden sind, zur Standardtechnik, die auf dem Markt angeboten wird. Das **Internet der Dinge** (englisch: „Internet of Things", IoT) bringt Vorteile und Risiken der Digitalisierung und Vernetzung direkt zu den Menschen (42. TB, Tz. 8.3).

Mit dieser Situation beschäftigt sich das vom BMBF geförderte Projekt „Tool-gestützte, moderierte und bürgerzentrierte Community-Plattform zur Privacy-Einstufung von IoT-Produkten – Unboxing.IoT.Privacy", das seit November 2023 läuft. Das Projekt setzt an dem Umstand an, dass für eine Vielzahl von IoT-Geräten die nötige Transparenz fehlt. Bereits die Tatsache einer Datenerhebung und -verarbeitung ist für betroffene Personen angesichts der geringen Größe und Unauffälligkeit der Geräte oft nicht erkennbar. Aber auch sonst haben die Nutzenden vielfach zu wenig Informationen über die Geräte und die damit verbundenen Onlinedienstleistun-

gen. Zudem mangelt es an einem Bewusstsein dafür, wer beim Einsatz von IoT-Geräten welche Datenschutzpflichten erfüllen muss.

Gegenstand des Projekts Unboxing.IoT.Privacy ist eine zielgruppengerechte zusammenfassende Darstellung von **aus Datenschutzsicht relevanten Informationen über IoT-Geräte** einschließlich der teils zwingend für deren Einsatz erforderlichen Onlinedienste. Diese Informationen sollen Verbraucherinnen und Verbraucher, Unternehmen und Behörden dabei unterstützen, ihre Entscheidung für einen Kauf und Einsatz solcher vernetzten Geräte informiert treffen zu können. Das Projekt baut auf Vorarbeiten der Teams der Universität Göttingen und des ULD zur Aufbereitung und Darstellung der Informationen auf (38. TB, Tz. 8.6). Im Projekt werden Software-Tools zur Analyse von IoT-Geräten entwickelt und bereitgestellt, um nötige Eckdaten über die Geräte erheben und diese darstellen zu können.

Mit dem **Cyberresilienzgesetz** (englisch: „Cyber Resilience Act", CRA) wurde im November 2024 ein europäischer Rechtsakt zur Regelung von Hardwareprodukten mit digitalen Komponenten verabschiedet. Zwar geht es darin um Sicherheit und nicht primär um Datenschutz, doch gehen wir davon aus, dass damit die Informationslage zu Sicherheits- und Datenschutzaspekten für IoT-Geräte deutlich verbessert wird. Nach dem Inkrafttreten im Dezember 2024 werden die Regelungen des CRA bis Dezember 2027 schrittweise umgesetzt. Anders als unter der DSGVO belegt der CRA nicht nur datenschutzrechtlich Verantwortliche, sondern auch Hersteller, Einführer in die EU und Händler mit Pflichten, damit die grundlegenden Anforderungen der IT-Sicherheit erfüllt werden (Tz. 2.4).

Auch wenn die im CRA vorgesehenen Maßnahmen nicht unmittelbar auf Datenschutz ausgerichtet sind, werden die bereitzustellenden Informationen eine deutliche **Erleichterung für Nutzende** und für Verantwortliche und Verarbeiter bei der **Einhaltung ihrer Datenschutzpflichten** bieten. Für die im Projekt zu entwickelnde aufbereitete Informationsdarstellung werden die Daten, die aufgrund des CRA künftig zugeliefert werden müssen, eine wesentliche Rolle spielen. Sie können ein wichtiger Ausgangspunkt für die Analyse und Bewertung sein.

Die Pflichten nach dem CRA können zudem bei der **Konzeption einer Bewertungsmetrik** für Produkte unterstützend einfließen. Dies betrifft beispielsweise Fälle, in denen nach dem CRA verpflichtende Angaben mit Datenschutzbezug fehlen oder das tatsächliche Verhalten der Geräte von der Beschreibung des Herstellers abweicht.

Cyberresilienzgesetz (CRA)

Der Cyber Resilience Act bezweckt, ein Mindestmaß an Cybersicherheit für alle auf dem EU-Markt erhältlichen vernetzten Produkte zu gewährleisten. IoT-Produkte fallen typischerweise in den Anwendungsbereich. Neben Cybersicherheit by Design, Pflichtinformationen und einer Konformitätserklärung, dass die Anforderungen eingehalten werden, wird auch Monitoring von und im Umgang mit Sicherheitslücken geregelt.

Mit Blick auf die künftig bestehenden Dokumentationspflichten des CRA liegt auf der Hand, Herstellern und Importeuren nahezulegen, **ergänzende datenschutzrechtlich wichtige Angaben bereitzustellen**. Dies würde allenfalls einen geringen Mehraufwand aufseiten der Hersteller erfordern, die zur Erfüllung der Pflichten nach dem CRA ohnehin über die Verarbeitungen ihrer Produkte im Bilde sein müssen. Soweit personenbezogene Daten verarbeitet werden, müssten derartige Informationen sonst von Verantwortlichen angefordert werden, um ihrer datenschutzrechtlichen Rechenschaftspflicht nachzukommen. Zu denken wäre hier etwa daran, den verantwortlich Betreibenden von IoT-Geräten Mittel, Anleitungen und Kontaktinformationen zur effektiven und zeitnahen Umsetzung von Betroffenenrechten entlang der Verarbeitungskette an die Hand zu geben.

Weitere Informationen zum Projekt finden Sie unter:

https://www.datenschutzzentrum.de/projekte/unboxingiot/

Kurzlink: *https://uldsh.de/tb43-8-3a*

8.4 Projekt AnoMed – Kompetenzcluster Anonymisierung für medizinische Anwendungen

Das dreijährige Forschungsprojekt **„Anonymisierung für medizinische Anwendungen – AnoMed“** nahm im November 2022 die Arbeit auf. Es wird vom Bundesministerium für Bildung und Forschung sowie der Europäischen Union (NextGenerationEU) als Kompetenzcluster (42. TB, Tz. 8.5) gefördert. Der Fokus liegt auf Pseudonymisierungs- und Anonymisierungsforschung zur Anwendung im Gesundheitsbereich. Im Konsortium von elf Partnern aus Hochschulen, Forschungseinrichtungen und mittelständischen Unternehmen trägt das ULD mit technischer und datenschutzrechtlicher Expertise bei. Das Projekt befasst sich mit vielversprechenden Technologien zum Schutz von Gesundheitsdaten, die insbesondere auf Differential Privacy oder maschinellem Lernen basieren.

Differential Privacy

Bei Differential Privacy handelt es sich um ein Verfahren, mit dem Abfragen aus Datenbanken mit personenbezogenen Daten gezielt verrauscht werden. So lässt sich einerseits eine Nutzbarkeit der Daten, z. B. zum Herausfinden statistischer Werte oder Korrelationen, erhalten und andererseits vermeiden, dass einzelne personenbezogene Datensätze bekannt werden.

Die Gesundheitsforschung ist politisch bedeutend – auch über den medizinischen Bereich hinaus: Mit dem **Europäischen Raum für Gesundheitsdaten** (European Health Data Space, EHDS) soll eine Blaupause für weitere Datenräume geschaffen werden. Die Europäische Datenstrategie sieht weitreichende Sekundärnutzungen von Daten für Gemeinwohl, Wirtschaft und Verwaltung vor. Die Strategie wird in mehreren Datenräumen in Form von Verordnungen umgesetzt. Oftmals sind die benötigten Daten personenbezogen und teils hochsensibel. Um sie für Datenräume nutzbar zu machen, ist es erforderlich, sie zu anonymisieren oder anderweitig ausreichende Schutzmaßnahmen zu treffen.

Zur technischen Umsetzung von Datenräumen bedarf es eines Brückenschlags zwischen dem teils **unterschiedlichen Verständnis von Anonymität** der beteiligten Akteure mit technischem, rechtlichem oder wirtschaftlichem Hintergrund. Aus der Arbeit des AnoMed-Projekts heraus wurde bereits eine differenzierte Terminologie vorgestellt (42. TB, Tz. 8.5). Um nun erfolgreich in Europa die minimalen Anforderungen an Anonymisierung zu diskutieren, festzulegen und zu harmonisieren, ist es sinnvoll, verschiedene Arten und Grade von Anonymität ausdrücken zu können. Dies kann Voraussetzung dafür sein, angemessene Anonymisierungsmethoden passend zum jeweiligen Risiko einer Re-Identifizierung auszuwählen.

Aufbauend auf der **Terminologie zur Anonymität** konnten die verfügbaren Verfahren zur Reduktion des Personenbezugs und zum Erlangen anonymisierter Daten drei wesentlichen Stadien zugeordnet werden. Als Resultat dieser Arbeit ist ein Modell (Zustandsdiagramm) von verschiedenen Arten von Daten mit **Variationen bezüglich des Personenbezugs** entstanden. Dies wird in Abbildung 5 dargestellt. Gemäß dem Modell können Daten prinzipiell in drei Formen vorliegen:

- direkt identifizierte Information,
- Informationen über Individuen ohne direkt identifizierende Kennungen oder
- in aggregierter Form.

In dieser **generalisierenden Darstellung** kommt zum Ausdruck, dass der Personenbezug mit bestimmten Transformationen im Allgemeinen abnimmt (nach rechts ausgerichtete graue Pfeile). Das Entfernen direkt identifizierender Merkmale (d. h. Kennungen) wie Namen oder Patientenkennziffern führt zu Datensätzen, die sich immer noch auf Einzelpersonen beziehen, d. h. eine Individualebene darstellen, aber eine Identifizierung nur noch mit geeigneter Zusatzinformation erlauben. Für einen weiter gehenden Schutz könnte der Datenbestand durch Weglassen oder Generalisierung von Informati-

onen so verändert werden, dass eine Verkettung nur noch mit Gruppen von Individuen möglich wäre und diese Gruppen für den gesamten Datenbestand eine gewisse Mindestgröße nicht unterschreiten. Eine weiter reichende Reduktion des Personenbezugs wird erreicht, wenn Merkmale von mehreren Individuen zu einem einzelnen (z. B. statistischen) Wert aggregiert werden. Eine Umkehrtransformation dazu ist bei Offenlegung mehrerer aggregierter Datensätze möglich; dadurch lassen sich – je nach Informationsgehalt der Informationen – alle oder einige der ursprünglichen Daten auf Individualebene rekonstruieren.

Ein weiteres wichtiges AnoMed-Resultat, das auf dieser Basis ausgearbeitet wurde, ist eine **Taxonomie über denkbare Arten von Anonymität**. Diese Taxonomie ist sowohl technologieneutral als auch trennscharf.

Projektergebnisse und weitere Informationen sind unter folgendem Link abrufbar:

https://www.datenschutzzentrum.de/projekte/anomed/

Kurzlink: *https://uldsh.de/tb43-8-4a*

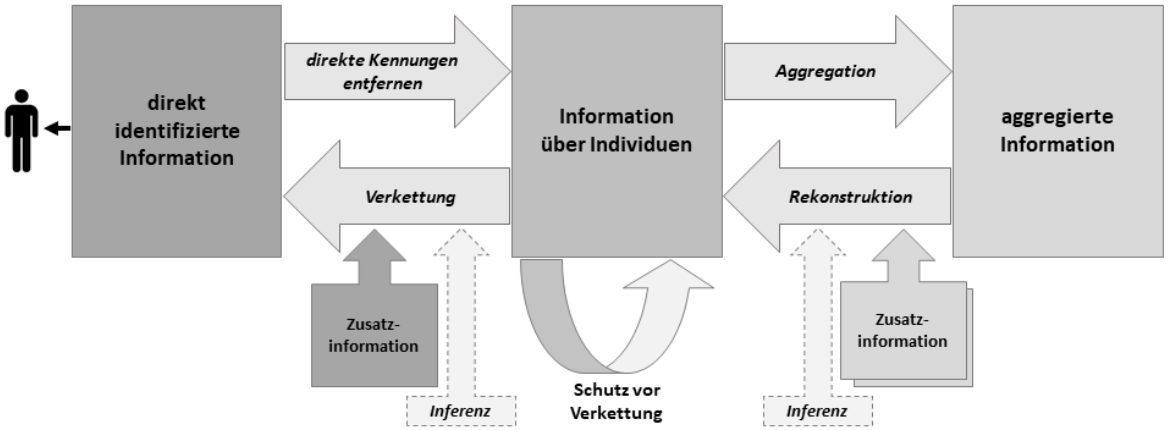

Abb. 5: Zustandsdiagramm über Personenbezug und Anonymisierung

09

KERNPUNKTE

Leitung AK Zertifizierung

Prüfkriterienkatalog

Deutsche und europäische Verfahren zu Akkreditierungen und Zertifizierungen

9 Zertifizierung und Akkreditierung

Seit 2018 besteht durch die DSGVO die Möglichkeit, dass sich im Datenschutzbereich **Zertifizierungsstellen akkreditieren lassen** können, die dann Zertifizierungen an Verantwortliche und Auftragsverarbeiter vergeben. Diese dienen als Nachweis, dass die DSGVO bei den Verarbeitungsvorgängen eingehalten wird. Lange hat es gedauert, bis hierfür die notwendigen Dokumente und Verfahren auf europäischer und nationaler Ebene geschaffen wurden. Doch nun war es 2024 so weit, dass erste Akkreditierungen auch in Deutschland abgeschlossen werden konnten.

9.1 Offene Fragen – der AK Zertifizierung hat viel zu tun

Die Koordinierung zu Zertifizierung und Akkreditierung unter den deutschen Aufsichtsbehörden erfolgt im **Arbeitskreis Zertifizierung der Datenschutzkonferenz** (AK Zertifizierung), den wir leiten. Wie in den Vorjahren haben wir monatliche virtuelle Treffen abgehalten, um uns über aktuelle nationale und internationale Entwicklungen insbesondere bei der **Genehmigung von Kriterienkatalogen und Akkreditierungen** auf dem Laufenden zu halten. Zum ersten Mal seit 2020 haben wir uns auch wieder im Juli 2024 persönlich in Hamburg zu einem zweitägigen Präsenztreffen zusammengefunden. Einen großen Raum nahm dort der Austausch mit der **Deutschen Akkreditierungsstelle (DAkkS)** ein, die in Zusammenarbeit mit den Aufsichtsbehörden die Akkreditierung von Zertifizierungsstellen vornimmt. Flankiert wurde die Arbeit des AK Zertifizierung weiterhin durch den **Unterarbeitskreis Prüfkriterien** (vgl. u. a. 42. TB, Tz. 9.1), der von Nordrhein-Westfalen geleitet wird. In diesem Unterarbeitskreis wird der Prüfkriterienkatalog weiterentwickelt (Tz. 9.4). Außerdem koordinieren sich darüber die Aufsichtsbehörden, die aktuelle Genehmigungs- und Akkreditierungsverfahren betreiben.

Nachdem nunmehr die ersten Kriterienkataloge in Deutschland genehmigt wurden und auch **Akkreditierungen von Zertifizierungsstellen** erfolgten (Tz. 9.2), ist es die Aufgabe des AK Zertifizierung, die sich daraus ergebenden weiteren Herausforderungen zu begleiten und offene Fragen zu klären. Unter anderem sind Zertifizierungsstellen nach Art. 43 Abs. 1 i. V. m. Abs. 5 DSGVO verpflichtet, die zuständige Aufsichtsbehörde **über eine unmittelbar bevorstehende Zertifizierung zu unterrichten**. Durch das föderale System in Deutschland kann das auch eine Aufsichtsbehörde eines anderen Bundeslandes betreffen als jenes, in dem die Zertifizierungsstelle ihren Sitz hat. Zu diesen Punkten ist ein Austausch zwischen den Aufsichtsbehörden nötig. Da die Meldung der Zertifizierungsstelle gegebenenfalls nur sieben Tage vor der Zertifizierung erfolgt, ist Eile geboten, damit es der betroffenen Aufsichtsbehörde noch möglich ist, wirksam Einwände mitzuteilen. Aus diesem Grund führen wir eine Liste der Kontaktmöglichkeiten in den Aufsichtsbehörden, damit die Meldung ohne Verzögerung umgehend von den zuständigen Mitarbeiterinnen und Mitarbeitern bearbeitet werden kann. Auch sollen Zertifizierungsstellen dazu angehalten werden, schon früher als sieben Tage über anstehende Zertifizierungen zu unterrichten. Dies gilt ebenfalls für mögliche Widerrufe von Zertifizierungen.

Diskutiert wurde außerdem, ob ein **deutschlandweites Verzeichnis der erfolgten Zertifizierungen** eingerichtet werden und wer dafür zuständig sein könnte. Diese Diskussion ist noch nicht abgeschlossen.

Besonders beschäftigten den AK Zertifizierung im Berichtszeitraum **Fragen zu grenzüberschreitenden Genehmigungen, Akkreditierungen und Zertifizierungen**. Hierzu wurde zusammen mit Kolleginnen und Kollegen der Datenschutzaufsichtsbehörden für Berlin und Nordrhein-Westfalen sowie der DAkkS ein interner Wegweiser zu Akkreditierungen und Zertifizierungen mit internationalem Bezug erstellt. Hierin wird zunächst der Unterschied zwischen

nationalen Zertifizierungskriterien und europäischen Kriterien dargelegt. Behandelt wird u. a. die Frage, inwieweit alle nationalen und europäischen Kriterienkataloge von deutschen Zertifizierungsstellen genutzt werden können. Eine weitere Frage ist, ob Zertifizierungsstellen auch für Kunden im Ausland tätig werden können. Die Diskussion zu einigen Fragen ist noch nicht abgeschlossen; teilweise ist eine Klärung auf europäischer Ebene erforderlich. Die DAkkS berichtete davon, dass zu Akkreditierungen mit internationalem Bezug auch in ihren europäischen Gremien rege Diskussionen geführt werden.

Es zeigt sich, dass auch auf europäischer Ebene weiterhin viele Fragen offen sind und vor allem sich jetzt mit den ersten erfolgten Akkreditierungen Folgefragen auftun, die nun vertieft außerhalb der regulären Sitzungen der zuständigen Subgroup (Tz. 9.3) behandelt werden sollen. Daher haben wir uns zusammen mit der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bereit erklärt, hierzu einen **Workshop** in Berlin auszurichten. Wie schon bei ähnlichen Workshops in Luxemburg und Madrid stammen die Teilnehmer aus der **Compliance, e-Government und Health Expert Subgroup (CEH Expert Subgroup)**. Der Workshop soll an drei Tagen im Juni stattfinden und auch die Möglichkeit bieten, dass Akkreditierungsstellen (insbesondere die DAkkS) und Zertifizierungsstellen über ihre Erfahrungen und Probleme berichten.

Was ist zu tun?

Die Arbeit im AK Zertifizierung wird fortgesetzt. Insbesondere müssen die noch offenen Fragen zum nationalen und internationalen Umgang mit Akkreditierungen und Zertifizierungen geklärt werden. Der intensive Austausch zwischen den Aufsichtsbehörden zu den Themen Akkreditierung und Zertifizierung hat sich bewährt, um etwa widersprüchliche Ergebnisse in Deutschland zu vermeiden und schnell reagieren zu können.

9.2 Stand der Akkreditierungen und Zertifizierungen in Deutschland und der EU

Im Berichtsjahr verfestigte sich der schon früher festgestellte Trend, dass in einigen wenigen Mitgliedstaaten (Deutschland, Luxemburg, Niederlande) bzw. Ländern (Nordrhein-Westfalen, Bremen, Berlin) gehäuft Anträge auf Genehmigung von Zertifizierungskriterien und Akkreditierung von Zertifizierungsstellen gestellt werden. Zu beobachten war eine **Verbesserung der Qualität** der durch die zukünftigen Zertifizierungsstellen oder Programmeigner erstellten und eingereichten **Zertifizierungsprogramme**.

Ungeachtet dessen ist das Verfahren, das Zertifizierungsstellen für ihre Akkreditierung durchlaufen müssen, aufgrund der **anspruchsvollen Thematik und seiner Mehrstufigkeit** durchaus komplex und zeitintensiv. In diesem Verfahren prüft die DAkkS in enger Zusammenarbeit mit der zuständigen Aufsichtsbehörde die eingereichten Programme auf ihre Anwendbarkeit und Eignung. Die jeweils zuständige Datenschutzaufsichtsbehörde ist für die Prüfung der Zertifizierungskriterien aus fachlicher Sicht zuständig und genehmigt diese – vorbehaltlich der Stellungnahme durch den Europäischen Datenschutzausschuss (EDSA). Dieses Verfahren bedarf daher – sowohl im europäischen als auch im deutschen Kontext – der Klärung etlicher Detailfragen sowie einer **engen Abstimmung aller Beteiligten**.

Im Jahr 2024 haben mehrere nationale und europäische Zertifizierungskriterien das Genehmigungsverfahren erfolgreich abgeschlossen. Zum aktuellen Zeitpunkt gibt es somit **mehrere genehmigte Kataloge mit Zertifizierungskriterien**. Konkret ist nunmehr in Deutschland EuroPriSe aus Bonn akkreditiert. Weitere Akkreditierungsverfahren stehen kurz vor dem Abschluss.

Was ist zu tun?

Um eine einheitliche Bewertung von Kriterienkatalogen und Zertifizierungsprogrammen zu gewährleisten, sollen die von der DSK bereitgestellten Materialien zur Akkreditierung und Zertifizierung entsprechend den jeweiligen Entwicklungen fortgeschrieben werden. Auf diese Weise kann die Qualität der eingereichten Programme weiter gesteigert und das Instrument der Zertifizierung langfristig auf einem fachlich hohen Niveau ganz im Sinne der DSGVO verankert werden.

9.3 Akkreditierung und Zertifizierung in der europäischen Expert Subgroup

Auf europäischer Ebene koordinieren sich die Datenschutzaufsichtsbehörden zu Fragen der Akkreditierung und Zertifizierung in der **Compliance, e-Government und Health Expert Subgroup (CEH Expert Subgroup)**. Wir tragen dazu bei, dass die Erfahrungen und das Know-how des AK Zertifizierung in die dortigen Diskussionen mit einfließen.

Im Jahr 2024 wurde von der CEH Expert Subgroup einerseits die Aufgabe der **Prüfung und Genehmigung konkreter Kriterienkataloge** wahrgenommen, andererseits stand die Abstimmung zu zahlreichen Fragen im Mittelpunkt. Neben Aspekten der **innereuropäischen Zusammenarbeit** unter den Aufsichtsbehörden waren vor allem Bedingungen der Zertifizierung in Bezug auf den **Drittstaatentransfer personenbezogener Daten gemäß Artikel 46 DSGVO** zu klären. Wichtig dafür war die Einbindung weiterer Expert Subgroups wie der International Transfer Subgroup (ITS) sowie der Key Provision Subgroup (KEYP), um die grundlegenden Punkte aus den verschiedenen Perspektiven zu klären und auf eine einheitliche Auslegung der DSGVO hinzuwirken.

Art. 46 Abs. 2 Buchst. f DSGVO – Datenübermittlung vorbehaltlich geeigneter Garantien

(2) Die in Absatz 1 genannten geeigneten Garantien können, ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in […]

f) **einem genehmigten Zertifizierungsmechanismus gemäß Artikel 42** zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.

Für das Jahr 2025 ist in Deutschland ein Workshop zu den Themen Akkreditierung und Zertifizierung geplant. Zu diesem sollen sowohl Vertreterinnen und Vertreter der CEH und gegebenenfalls weiterer Subgroups als auch von Zertifizierungsstellen eingeladen werden, um einen **intensiven und praxisbezogenen Austausch** unter den Teilnehmenden zu fördern (Tz. 9.1).

Was ist zu tun?

Die Zusammenarbeit unter den Datenschutzaufsichtsbehörden in Europa zu Akkreditierung und Zertifizierung ist im Sinne eines europäisch einheitlichen Vorgehens fortzusetzen. Ziel ist es, das Instrument der Zertifizierung stärker in die Praxis zu bringen.

9.4 Überarbeitung des Prüfkriterienpapiers

Das von der DSK verabschiedete Papier **„Anforderungen an datenschutzrechtliche Zertifizierungsprogramme – Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6), Version 2.0"** wurde im Berichtszeitraum durch den Unterarbeitskreis Prüfkriterien des AK Zertifizierung überarbeitet und weiterentwickelt. Die grundlegende Struktur des Dokuments wurde beibehalten; lediglich einige Abschnitte wurden zur besseren Lesbarkeit und Verständlichkeit neu angeordnet.

Inhaltlich konzentrierte sich die Arbeit insbesondere auf umfangreiche Ausführungen zu den Anforderungen der DSGVO **zur datenschutzfreundlichen Technikgestaltung** und zu datenschutzfreundlichen Voreinstellungen (Artikel 25 DSGVO) sowie zur Auftragsverarbeitung (Artikel 28 DSGVO). Sobald die Änderungen von der DSK verabschiedet sind, wird das Papier in neuer Version veröffentlicht.

Die aktuelle Version 2.0 des Papiers hat sich bereits in einigen Akkreditierungsverfahren bewährt und konnte dort seine Praxistauglichkeit unter Beweis stellen. Das Papier ist in der Version 2.0 vom 21.06.2022 unter dem folgenden Link abrufbar:

https://www.datenschutzkonferenz-online.de/media/ah/DSK_Zertifizierungskriterien_V2.0_Stand_21062022.pdf

Kurzlink: *https://uldsh.de/tb43-9-4a*

Mit dem Papier bietet die DSK eine Basis zur einheitlichen Bewertung von Zertifizierungsprogrammen. Für die aktuellen und künftigen Weiterentwicklungen ist es dem AK Zertifizierung ein Anliegen, konkrete Erfahrungen mit dem Papier selbst, seiner Anwendung sowie die Vorgaben der europäischen Ebene einfließen zu lassen und dabei stets auf die Praxisnähe zu achten. Auch weiterhin soll das Papier als **Orientierungshilfe für zukünftige Zertifizierungsstellen** dienen, um sie bei der Erstellung von Zertifizierungsprogrammen und insbesondere der Erarbeitung von Zertifizierungskriterien zu unterstützen.

Was ist zu tun?

Der AK Zertifizierung wird die Entwicklungen auf deutscher und europäischer Ebene weiterverfolgen, um das Papier zu den Anforderungen an datenschutzrechtliche Zertifizierungsprogramme möglichst praxisnah weiterzuentwickeln und auf einem aktuellen Stand zu halten.

10

KERNPUNKTE

Large Language Models und Reproduzierbarkeit

Maßnahmen gegen Spam- und Phishing-E-Mails

Schwärzen von Dokumenten

10 Aus dem IT-Labor

In unserem IT-Labor beschäftigt sich unser Team mit **neuen technischen Entwicklungen**, damit wir uns mit Chancen und Risiken sowie mit den Möglichkeiten zur Risikobeherrschung vertraut machen können. Dies ermöglicht es uns, Empfehlungen zu erarbeiten und an Verantwortliche oder Auftragsverarbeiter weiterzugeben. Wo es passt, verwenden wir die gewonnenen Erkenntnisse in den Kursen der DATENSCHUTZAKADEMIE (siehe Kapitel 13) oder in der Beratung.

Im Berichtsjahr gehörten KI-Systeme wie LLMs (Tz. 10.1), Möglichkeiten zur Abwehr von Spam-E-Mails (Tz. 10.2) und das Problem des sicheren Schwärzens in Dokumenten (Tz. 10.3) zu den Schwerpunkten unserer Untersuchungen.

10.1 Large Language Models: Herausforderung der Reproduzierbarkeit

Beim Einsatz von KI-Systemen müssen – selbstverständlich – die **Anforderungen des Datenschutzrechts** berücksichtigt werden (Tz. 6.2.5 und Tz. 6.2.6). In diesem Beitrag in der Rubrik „Aus dem IT-Labor" konzentrieren wir uns auf den Aspekt der **Reproduzierbarkeit von Ergebnissen**, der wesentlich ist für die Entscheidung, ob man für seine Zwecke der Verarbeitung von Daten ein probabilistisch (d. h. wahrscheinlichkeitsbasiert) arbeitendes KI-System oder ein deterministisches algorithmisches IT-System auswählen soll. Dies betrifft insbesondere generative KI-Systeme wie Large Language Models (LLMs).

Stellt man einem **LLM** fünfmal dieselbe Frage, erhält man im Allgemeinen fünf verschiedene Antworten. Im Normalfall sind die Unterschiede rein sprachlicher Natur; abhängig von verschiedenen Faktoren können sich die Antworten jedoch auch inhaltlich unterscheiden. Das macht die **Reproduzierbarkeit** solcher Ausgaben äußerst schwer. Die Angabe, ein Text sei „mit der KI XY erstellt", ist in dieser Hinsicht wenig hilfreich.

Die **Variabilität der Ergebnisse** hat ihre Wurzeln bereits in der technischen Infrastruktur der LLMs. Abhängig vom Status der Nutzenden stellen die Anbieter verschiedene Modellversionen bereit, die unterschiedlich leistungsfähig sind: Zahlende Nutzende erhalten oft Zugang zu leistungsstärkeren Modellen, während in den Nutzerkonten ohne Geldzahlung mitunter ältere Versionen zur Verfügung gestellt werden, deren Antworten sich dementsprechend unterscheiden. Auch die aktuelle Systemlast beeinflusst die Modellauswahl: Bei hoher Auslastung greifen Anbieter häufig auf ressourcensparende, aber weniger leistungsfähige Modellvarianten zurück.

Eine besondere Rolle spielt dabei das **Kontextfenster**, d. h. die maximale Textmenge, die ein LLM bei der Verarbeitung gleichzeitig berücksichtigen kann. Bei hoher Systemlast reduzieren Anbieter bisweilen die Größe dieses Kontextfensters, wodurch das KI-System frühere Teile der Konversation nicht mehr einbeziehen kann. Diese dynamischen Anpassungen erfolgen für Nutzende meist unmerklich, da sich die Benutzungsoberfläche nicht verändert. Sie haben jedoch erheblichen Einfluss auf die Qualität und Konsistenz der Antworten.

Neben diesen systembedingten Faktoren sind die sogenannten **Inferenzparameter** entscheidend. Im Unterschied zu den grundlegenden Modellparametern, die während des Trainings festgelegt werden, sind Inferenzparameter Steuerungsgrößen, die zur Laufzeit angepasst werden können. Ein besonders wichtiger Inferenzparameter ist die **„Temperatur"**. Sie bestimmt, wie das Modell Wahrscheinlichkeiten bei der Wortwahl gewichtet: Hohe Temperaturwerte führen zu einer breiten Streuung möglicher Antworten und damit zu kreativeren, aber auch weniger vorhersehbaren Ergebnissen. Niedrige Temperaturwerte hingegen erzeugen konstantere, dafür weniger variable Ausgaben.

Parameter

Bei Entwicklung und Nutzung von LLMs unterscheidet man verschiedene Gruppen von Parametern, mit denen sich das LLM steuern lässt:

Hyperparameter: Diese werden vor dem Training festgelegt, um das Lernverfahren selbst zu konfigurieren (z. B. Lernrate, Netzarchitektur oder Anzahl der Schichten in einem neuronalen Netz).

Inferenzparameter: Diese Parameter beeinflussen, wie ein trainiertes Modell während der Inferenzphase (Vorhersagephase) arbeitet. Sie werden nicht während des Trainings optimiert, sondern steuern das Verhalten des Modells bei der Anwendung auf neue Daten (z. B. Temperatur oder Begrenzung der Auswahl der nächsten Tokens auf die wahrscheinlichsten Kandidaten (Top-k-/Top-p-Sampling)).

Diese technischen Charakteristika prägen fundamental die Einsatzmöglichkeiten von LLMs. Im Gegensatz zu klassischen Suchmaschinen, die auf existierende Datenbestände zugreifen und ihre Quellen transparent ausweisen, generieren LLMs neue Texte auf Basis statistischer Muster, die sie während ihres Trainings gelernt haben. Diese grundlegend verschiedene Funktionsweise führt zu zwei separaten Herausforderungen: Zum einen **fehlt die Nachvollziehbarkeit der Quellen**, da LLMs ihre Ausgaben nicht mit Referenzen verknüpfen. Zum anderen neigen sie zu sogenannten **„Halluzinationen"**, d. h., sie produzieren mitunter Aussagen, die zwar sprachlich und kontextuell plausibel erscheinen, aber inhaltlich falsch sind. Dieser Effekt entsteht nicht durch die fehlende Referenzierung, sondern ist eine direkte Folge ihres **probabilistischen Funktionsprinzips**.

Diese Eigenschaften führen zu einem **grundlegenden Spannungsverhältnis in der Anwendung von LLMs**: Je mehr man ihre kreativen Fähigkeiten zur Texterstellung nutzt – etwa durch höhere Temperaturwerte oder komplexere Aufgabenstellungen –, desto größer wird das Risiko von Halluzinationen und unvorhersehbaren Ergebnissen. Umgekehrt führt das Streben nach maximaler Konsistenz und Verlässlichkeit zu einer deutlichen Einschränkung ihrer oft gewollten Variabilität.

Probabilistisches Funktionsprinzip

Das probabilistische Funktionsprinzip basiert darauf, dass LLMs **Wahrscheinlichkeitsverteilungen über Token-Sequenzen** lernen und nutzen, um Text zu generieren oder zu verarbeiten.

Dazu wird der Eingabetext in kleinere Einheiten (**Tokens**) zerlegt, z. B. Wörter, Teile von Wörtern oder Zeichen. Das Modell berechnet für jedes mögliche nächste Token eine Wahrscheinlichkeitsverteilung basierend auf dem bisherigen Kontext (d. h. den vorherigen Tokens) und wählt dann das nächste Token basierend auf der gelernten Wahrscheinlichkeitsverteilung aus. Auf diese Weise setzt es Token zu Ausgabetexten zusammen.

Für Nutzende ergibt sich aus diesen technischen Charakteristika die Handlungsempfehlung, genau zu überlegen, wann (datenschutzgerechte) generative KI-Systeme zur Verarbeitung von Daten eingesetzt werden sollen: LLMs mögen sich als Unterstützung bei kreativen Prozessen eignen, etwa beim Brainstorming zu Argumentationslinien oder bei der Erstellung erster Textentwürfe. Für diese Anwendungen kann die inhärente Variabilität der Systeme vorteilhaft sein. Bei der **Recherche von Fakten**, der Analyse von Rechtsprechung oder der Überprüfung rechtlicher Sachverhalte sollten reine LLMs hingegen nicht als hauptsächliches, sondern **allenfalls als ergänzendes Werkzeug** verwendet werden. Ihre Ausgaben müssen in diesen Fällen stets durch klassische, quellenbasierte Recherche verifiziert werden. Ohnehin sollte man nicht davon ausgehen, dass KI-Systeme die menschliche Kontrolle überflüssig machen.

Was ist zu tun?

Kommt es auf Reproduzierbarkeit von Ergebnissen an, sind generative KI-Systeme zumeist nicht das Mittel der Wahl. Abhängig von verschiedenen Faktoren, die teilweise außerhalb des Einflusses der Nutzenden liegen, können Ergebnisse häufig nicht exakt wiederholt werden. So muss generell Wert auf die Kontrolle der produzierten Ausgaben gelegt werden. Wer diese Tätigkeit übernimmt, muss selbst den nötigen Sachverstand haben; Sorgfalt und ausreichend Zeit zum Prüfen sind essenziell.

10.2 E-Mail: Maßnahmen gegen Spam und Phishing

Unverlangte Werbung per E-Mail, die sogenannte Spammail, ist seit Jahren ein fester Bestandteil des Arbeitsalltags. Nutzerinnen und Nutzer sind der E-Mail-Flut nahezu unentrinnbar ausgesetzt. Dabei ist es wichtig zu verstehen, wie die **Masse an Spamnachrichten** zustande kommt, um langfristige Strategien dagegen zu entwickeln.

Um es vorwegzunehmen: Ist das Kind erst einmal in den Brunnen gefallen und die eigene E-Mail-Adresse kursiert unkontrolliert im Netz, besteht wenig Aussicht, den Erhalt von Spam wieder zu stoppen. Verfügt man jedoch über eine bislang **nicht belastete E-Mail-Adresse**, gibt es Maßnahmen, damit das so bleibt.

Eine E-Mail-Adresse wird üblicherweise im Laufe der Zeit **an zahlreiche Stellen weitergegeben**: an Freundinnen und Freunde, Bekannte, Kolleginnen und Kollegen, Onlinedienste, Shopping-Plattformen und Spiele-Anbieter. Kurz gesagt: Die eigene E-Mail-Adresse macht eine weite Reise und ist mit der Zeit in den Adressbüchern vieler Menschen und Organisationen zu finden. Einige Anbieter erheben Adressdaten direkt zum Zweck und mit dem Ziel der Weitergabe – Gewinnspiele haben diese Klausel oft im Kleingedruckten. Aber auch Schadsoftware kann E-Mail-Adressen aus einem E-Mail-Programm entwenden. E-Mail-Adressen können bei Hackerangriffen auf E-Mail-Konten oder Server „erbeutet" werden. So gibt es viele Wege, über die eine E-Mail-Adresse in die Hände von Spamversendern gelangen kann. Außerdem besteht die Möglichkeit, dass bei einem Angriff gleich fremde Infrastrukturen verwendet werden, um Spamnachrichten zu versenden.

Am besten wäre es daher, die eigene E-Mail-Adresse geheim zu halten, was naturgemäß nicht sonderlich kommunikativ wäre. Aber es gibt weniger drastische **Methoden**:

Parallele E-Mail-Konten: Ein E-Mail-Konto kann man sich bei verschiedenen Anbietern leicht anlegen. Eine effektive Strategie besteht daher in der Nutzung mehrerer E-Mail-Adressen für unterschiedliche Zwecke, z. B.:

- eine Adresse für private Kommunikation mit Freunden und Bekannten,
- eine separate Adresse für Online-Einkäufe und
- eine weitere für Anmeldungen in sozialen Netzwerken.

Sollte eine dieser Adressen von Spam betroffen sein, lässt sie sich ohne Konsequenzen für die anderen Kommunikationsbereiche stilllegen.

Weiterleitungsdienste: Es gibt verschiedene sogenannte Relay-Dienste, bei denen man sich eine bestimmte Zahl an Alternativadressen für die eigene E-Mail-Adresse erzeugen kann. All diese Alternativadressen werden dann auf das eigene Konto umgeleitet. So kann man beispielsweise für Onlinehändler einen separaten Alias einrichten und alle dorthin gesandten E-Mails bequem im echten Konto empfangen. Im Falle der Spamzusendung kann die betroffene Alternativadresse gelöscht und eine neue erzeugt werden. Auch hier müssen Kommunikationspartner informiert und gegebenenfalls Einträge in den eigenen Konten geändert werden.

Catch-all-Accounts: Wer eine eigene Domain besitzt, kann – sofern der Provider dies anbietet – einen Catch-all-Account aktivieren. Dabei werden dann sämtliche Adressbestandteile vor dem @-Zeichen einem einzigen Konto zugeordnet. Besitzt man etwa die Domain „beispiel.de“ und legt sich ein Konto bei einem Onlinedienst an, nutzt man dann einfach die Adresse „onlinedienst@beispiel.de“. Der Telefonanbieter bekommt „telefon@beispiel.de“ und der Fußballverein „fussball@beispiel.de“. Da alle diese Adressen intern im selben Konto landen, kann man weiterhin bequem alle E-Mails lesen, ohne verschiedene Konten bedienen zu müssen. Das Elegante an dieser Methode: Sollte auf einer der Adressen Spam eintreffen, kann man diese Adresse ohne Kollateralschäden für andere Kontakte stilllegen, etwa indem man eingehende Spamnachrichten dann automatisiert filtert. Zusätzlich hat man in diesen Fällen ein starkes Indiz für die Information, an welcher Stelle die Adresse in fremde Hände geraten ist, da jede Adresse genau einem Kommunikationspartner zugeordnet ist.

Auch **Phishing-E-Mails** sind so einfacher zu erkennen: Eine vermeintliche Nachricht der Bank an die Adresse, die ausschließlich der Fußballverein verwendet? Ertappt!

Ein weiterer Vorteil besteht darin, dass sich auf diese Weise nicht nur E-Mail-Adressen, sondern auch Nutzerkonten unterscheiden. Viele Onlinedienste verlangen als Nutzername eine gültige E-Mail-Adresse. Aus technischer Sicht ist dies praktisch: Da E-Mail-Adressen weltweit eindeutig sind, müssen sich Anbieter nicht darum kümmern, eine doppelte Vergabe von Nutzernamen auszuschließen. Wenn für alle Onlinedienste nur eine einzige E-Mail-Adresse genutzt wird, können Anbieter leicht Aktivitäten auf verschiedenen eigenen Plattformen zusammenführen.

Auch **Angriffe auf Onlinedienste** bergen eine weitere Gefahr, wenn nur eine einzelne Adresse verwendet wird: Wurden beispielsweise E-Mail-Adressen und Passwörter bei einem Angriff auf einen Onlinedienst erbeutet, kann ein Angreifer die gleichen Zugangsdaten bei weiteren Onlinediensten ausprobierten. Leider funktioniert dies häufig, denn Menschen neigen dazu, Passwörter wiederzuverwenden.

Verwendet man hingegen **für verschiedene Onlinedienste verschiedene E-Mail-Adressen** als Nutzernamen, so erschwert man zum einen die Nachverfolgung über verschiedene Onlinedienste hinweg. Gleichzeitig kann sich ein Angreifer mit einer erbeuteten Kombination von Nutzername und Passwort nicht bei den anderen Onlinediensten anmelden, selbst wenn das Passwort gleich sein sollte.

Ein vollständiger Schutz vor unerwünschten E-Mails ist heutzutage unrealistisch. Sobald eine Adresse einmal in Umlauf geraten ist, lässt sich der Spamversand kaum noch eindämmen. **Vorbeugende Maßnahmen** bleiben daher der effektivste Ansatz zum Schutz der digitalen Kommunikation. Die beschriebenen Strategien erfordern zwar anfänglichen Aufwand, bieten langfristig jedoch deutlich mehr Kontrolle über die eigene E-Mail-Kommunikation und sind letztlich dem nachträglichen Spamsortieren per Hand im Posteingang deutlich überlegen.

Was ist zu tun?

Im Alltag sollte mehr als nur eine einzige E-Mail-Adresse zum Einsatz kommen. Verschiedene Konzepte ermöglichen dabei unterschiedliche Stufen des Komforts. Da über unverlangte E-Mails nicht nur Werbung, sondern auch Phishing-Versuche versendet werden, sind Maßnahmen dagegen auch ein Sicherheitsgewinn.

10.3 Update: Schwärzen in Dokumenten

Das Thema „Schwärzen in Dokumenten" ist nicht zum ersten Mal Gegenstand des Tätigkeitsberichts (36. TB, Tz. 10.4; 39. TB, Tz. 10.3; 40. TB, Tz. 10.1), sondern spielt als **Dauerbrenner** sowohl in der Beratung als auch bei Meldungen nach Artikel 33 DSGVO über Datenschutzverletzungen eine wichtige Rolle. Daher lohnt es sich, sich bewusst zu machen, wie sich ein sicheres Schwärzen nach aktuellem Stand erreichen lässt.

Sollen **Informationen aus Dokumenten nur in Teilen weitergegeben** werden, so werden typsicherweise in (Original-)Dokumenten diejenigen Textteile geschwärzt, die nicht weitergegeben werden sollen oder dürfen. Dies ist schon in Papierform nicht einfach: Ein schwarzer Stift mag zwar Schrift überdecken, doch im Gegenlicht, auf einem Foto, unter einem Scanner oder auf einer Kopie sind manche Buchstaben dennoch zu erkennen, weil das Papier an diesen Stellen die Farbe anders aufnimmt.

Bei elektronisch vorliegenden Daten, z. B. Bild- oder PDF-Dateien, ist diese Aufgabe noch komplexer: Was **vordergründig wie eine Abbildung** aussieht, ist technisch meist nicht nur eine Grafik, sondern eine **Datenstruktur**, die auch Inhalte (Buchstaben bei Texten), Schichten (übereinandergelegte Grafikelemente) und Überarbeitungsmarkierungen enthalten kann. Sollen aus einer solchen Datei Informationen rückstandsfrei gelöscht werden, so sind alle Informationen zu erfassen.

Die beliebte Methode, ein **schwarzes Rechteck** auf den zu löschenden Textteil zu zeichnen und die Datei abzuspeichern, **reicht nicht**: Auf der Empfangsseite kann das Rechteck wieder entfernt werden. Nötig ist stattdessen, alle grafischen Elemente zu verschmelzen und die an dieser Stelle intern gespeicherte Information, z. B. Buchstaben, zu entfernen.

Zwar bieten zahlreiche **Programme zur PDF-Bearbeitung** mittlerweile die Funktion „Schwärzung" an, doch funktioniert diese nicht immer zuverlässig: Der erste Teil der Aufgabe – zu löschenden Text mit schwarzem Block überdecken – wird gelöst. Hier würde eine Fehlfunktion auch sofort auffallen. Ob der zweite Teil der Aufgabe, die **Löschung der nicht sichtbaren Informationen in der Datei**, tatsächlich erledigt ist, lässt sich nicht mit einem Blick feststellen.

So etwas kann sich auch je nach Version der Software ändern: Für eine frühe Version eines Programms zur PDF-Bearbeitung wurde beispielsweise erkannt, dass noch **Restinformationen in der Datei vorhanden** waren; in einer Folgeversion der Software korrigierte der Hersteller diesen Fehler. Besonders ärgerlich: Einige Versionen später trat der Fehler erneut auf. Zwar ist er mittlerweile – für die aktuelle Version – korrigiert, verlassen möchte man sich auf diese Funktion aber nicht mehr.

Was kann man tun? Das Optimum besteht darin, Dokumente nicht nachträglich zu **schwärzen**, sondern **aus editierbaren Quelldateien**, z. B. einer Textdatei, die fraglichen Informationen zu entfernen und dann ein neues Ausgabedokument (PDF-Datei, Ausdruck) zu erstellen. Dass und an welchen Stellen Informationen entfernt wurden, sollte kenntlich gemacht werden, z. B. durch einen schwarzen Balken; bei barrierefreien Dokumenten ist dies noch zu ergänzen. Auch Software, die Texte analysiert und automatisiert Schwärzungsvorschläge erstellt (z. B. durch die Erkennung von Geburtsdaten, Namen, Kontonummern, Adressen usw.), arbeitet am einfachsten mit Textdateien.

Muss oder will man eine PDF-Datei schwärzen, so sollte man nach der Schwärzung die Datei als neue Datei abspeichern und auf alle Fälle mit einem PDF-Leseprogramm kontrollieren, ob sich schwärzende Rechtecke beiseiteschieben oder die gelöschten Texte oder Buchstaben aus der Datei in editierbarer Form entnehmen lassen.

Wer ganz sichergehen will (oder muss), dass in der PDF-Datei wirklich **keine versteckten Informationen mehr enthalten** sind, muss den optischen Weg gehen: **Ausdruck der digital geschwärzten Datei und erneuter Scan**. Dies mutet zugegebenermaßen absurd an, ist aber eine Lösung für die Fälle, in denen man der eingesetzten Software nicht vertraut.

Was ist zu tun?

Schwärzungen und Anonymisierungen in Dokumenten erfolgen vorzugsweise mithilfe der zugrunde liegenden Originaltexte.

11

KERNPUNKTE

Datenübermittlung in die USA

Europäische Prüfung zum Auskunftsrecht

11 Europa und Internationales

11.1 Beschwerdemöglichkeit bei Datenübermittlung in die USA

Alle europäischen Datenschutzaufsichtsbehörden informieren auf ihren Websites seit 2024 über die Möglichkeit, sich bei **Datenschutzverstößen durch US-Unternehmen oder US-Organisationen** und bei der **Verarbeitung personenbezogener Daten durch US-Nachrichtendienste zu beschweren**. Wir erklären hier auf unserer Website, wie dies funktioniert:

https://www.datenschutzzentrum.de/meldungen/datenuebermittlung_usa/

Kurzlink: *https://uldsh.de/tb43-11-1a*

Zum Hintergrund (siehe auch 42. TB, Tz. 2.4): Am 10. Juli 2023 hat die Europäische Kommission den Angemessenheitsbeschluss für das **„EU-US Data Privacy Framework"** (EU-US DPF) verabschiedet.

Angemessenheitsbeschluss

Es handelt sich dabei um einen Beschluss, der von der Europäischen Kommission gemäß Artikel 45 DSGVO angenommen und durch den festgestellt wird, dass ein Drittland (d. h. ein Land, das nicht an die DSGVO gebunden ist) oder eine internationale Organisation ein angemessenes Schutzniveau für personenbezogene Daten bietet. Im Rahmen dieses Beschlusses werden die innerstaatlichen Rechtsvorschriften des Landes, seine Aufsichtsbehörden und die von ihm eingegangenen internationalen Verpflichtungen berücksichtigt.

Dies führt dazu, dass personenbezogene Daten aus der EU wieder an die USA übermittelt werden dürfen, ohne dass – vorbehaltlich einer Rechtsgrundlage für die Datenübermittlung – weitere Übermittlungsinstrumente (z. B. Standarddatenschutzklauseln) oder zusätzliche Maßnahmen erforderlich sind. Neben den allgemeingültigen Anforderungen der DSGVO an Datenverarbeitungen, insbesondere dem Vorhandensein einer Rechtsgrundlage gemäß Art. 6 Abs. 1 DSGVO, gilt die Voraussetzung, dass der jeweilige US-Datenempfänger unter dem EU-US DPF beim US Department of Commerce zertifiziert ist. Dies müssen Datenexporteure in der EU vorab prüfen.

Anders als bei anderen Zertifizierungen (Tz. 9.2) handelt es sich nicht um eine Prüfung durch Dritte, sondern hier reicht eine **Selbstzertifizierung** aus, die aussagt, dass die Regeln des EU-US DPF beachtet werden. Das US Department of Commerce veröffentlicht eine Liste über alle nach dem EU-US DPF zertifizierten Unternehmen und Organisationen, die unter dem folgenden Link zu finden ist:

https://www.dataprivacyframework.gov/s/participant-search

Kurzlink: *https://uldsh.de/tb43-11-1b*

Wenn eine betroffene Person nun der Meinung ist, dass ein unter dem EU-US DPF zertifiziertes US-Unternehmen, an das personenbezogene Daten übermittelt worden sind, gegen seine Pflichten aus dem EU-US DPF verstoßen hat oder die Rechte, die betroffenen Personen nach dem EU-US DPF zustehen, verletzt hat, kann sie sich mit einer **Beschwerde direkt an das ULD** wenden. Der Europäische Datenschutzausschuss (EDSA) hat dafür ein **Beschwerdeformular** entwickelt:

https://www.datenschutzzentrum.de/uploads/meldungen/eu-us_dpf_beschwerdeformular_gewerbliche_angelegenheiten.pdf

Kurzlink: *https://uldsh.de/tb43-11-1c*

Die Nutzung dieses Formulars wird ausdrücklich empfohlen, damit sichergestellt werden kann,

dass alle für die Bearbeitung wesentlichen Informationen enthalten sind. Je nach Fallgestaltung kann es sodann erforderlich sein, dass das ULD die Beschwerde an das **„Informelle Gremium der EU-Datenschutzbehörden"** oder an US-Unternehmen/US-Organisationen oder die zuständigen US-Behörden weiterleitet. Wie das Informelle Gremium der EU-Datenschutzbehörden arbeitet, ist in einer **Geschäftsordnung** beschrieben:

https://www.datenschutzzentrum.de/uploads/meldungen/eu-us_dpf_geschaeftsordnung_informelles_gremium_der_eu-datenschutzbehoerden.pdf

Kurzlink: *https://uldsh.de/tb43-11-1d*

Es gibt darüber hinaus die Möglichkeit der **Beschwerde** in Bezug auf die **Verarbeitung personenbezogener Daten durch US-Nachrichtendienste** – wenn nämlich eine betroffene Person annimmt, dass US-amerikanische Geheimdienste oder Sicherheitsbehörden auf ihre personenbezogenen Daten für Zwecke der nationalen Sicherheit zugegriffen und dabei die rechtlichen Vorgaben verletzt haben. Dieses Beschwerdeverfahren unterscheidet sich ein wenig vom oben beschriebenen Beschwerdeverfahren in gewerblichen Angelegenheiten: Es beruht auf US-amerikanischem Recht und dient der Untersuchung, ob US-Nachrichtendienste bei einem etwaigen Zugriff auf ihre Daten gegen die hierfür geltenden Vorgaben des US-amerikanischen Rechts verstoßen haben.

Damit Personen in der Europäischen Union dieses neue Beschwerdeverfahren möglichst einfach nutzen können, nehmen die Datenschutzbehörden der EU-Mitgliedstaaten entsprechende Beschwerden entgegen und leiten diese anschließend über das Sekretariat des Europäischen Datenschutzausschusses an die zuständigen Stellen in den Vereinigten Staaten weiter. Dort werden die Beschwerden geprüft und entschieden. Auch für dieses Verfahren gibt es **ein gesondertes Beschwerdeformular**:

https://www.datenschutzzentrum.de/uploads/meldungen/eu_us_dpf_beschwerdeformular_nachrichtendienste.pdf

Kurzlink: *https://uldsh.de/tb43-11-1e*

11.2 CEF-Aktion: Koordinierte Prüfung zum Auskunftsrecht

Das ULD beteiligte sich 2024 neben insgesamt 27 weiteren europäischen Datenschutzaufsichtsbehörden an einer **koordinierten Prüfung im Rahmen des Coordinated Enforcement Framework (CEF)** des Europäischen Datenschutzausschusses (EDSA), die sich auf die Umsetzung des Auskunftsrechts konzentriert.

Art. 15 Abs. 1 DSGVO

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf die in der Norm genannten Informationen.

Das **Auskunftsrecht nach Artikel 15 DSGVO** kann Einzelpersonen eine Überprüfung ermöglichen, ob ihre personenbezogenen Daten von den verantwortlichen Stellen gesetzeskonform verarbeitet werden. Es ist eines der wichtigsten und am häufigsten ausgeübten Rechte und fungiert regelmäßig als eine Art **Türöffner für die Ausübung weiterer Betroffenenrechte**, wie etwa des Rechts auf Berichtigung oder des Rechts auf Löschung. Oftmals münden die entsprechenden Vorgänge in Beschwerden bei den Datenschutzaufsichtsbehörden.

Ziel der koordinierten Aktion im Berichtsjahr war es zu beurteilen, wie Organisationen das **Auskunftsrecht in der Praxis** umsetzen und inwiefern zu konkreten Aspekten Anpassungen oder Klarstellungen der EDSA-Leitlinien oder eine weitere Sensibilisierung von Verantwortlichen

oder betroffenen Personen durch die Datenschutzbehörden sinnvoll sein könnten.

EDSA-Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht, Version 2.1, nach öffentlicher Konsultation angenommen am 28. März 2023:

https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_de

Kurzlink: *https://uldsh.de/tb43-11-2a*

Kernelement der koordinierten Prüfung war ein **strukturierter Fragebogen** zur Umsetzung des Rechts auf Auskunft durch Verantwortliche, den alle teilnehmenden Datenschutzaufsichtsbehörden in den verschiedenen Mitgliedstaaten verwendeten. Seitens des ULD wurden im Rahmen der Prüfung mehrere Stellen aus dem öffentlichen und nichtöffentlichen Sektor angeschrieben. Aus den eingegangenen Antworten der Verantwortlichen konnten Erkenntnisse dahin gehend gewonnen werden, wie mit Auskunftsersuchen umgegangen wird und welche **internen Abläufe und Standards zur Bearbeitung dieser Ersuchen implementiert** wurden. In der Prüfung des ULD konnten keine gravierenden datenschutzrechtlichen Verstöße festgestellt werden. In einem Fall haben wir Hinweise hinsichtlich der Möglichkeit erteilt, die internen Prozesse zur Bearbeitung von Auskunftsersuchen effektiver auszugestalten.

Die koordinierte Aktion zum Auskunftsrecht war die dritte Initiative im Rahmen des CEF, die darauf abzielt, die **Durchsetzung der Datenschutz-Grundverordnung und die Zusammenarbeit zwischen Datenschutzbehörden innerhalb der EU** zu optimieren. Die Ergebnisse der gemeinsamen Initiative werden in einem Bericht des EDSA veröffentlicht.

12

KERNPUNKTE

Beanstandungen nach dem IZG-SH

Top-5-Themen und besondere Fälle

Beschlüsse der IFK

Wünsche an den Gesetzgeber

12 Informationsfreiheit

2024 war ein arbeitsreiches Jahr für uns im Bereich der Informationsfreiheit. In vier Fällen haben wir **Beanstandungen gegenüber öffentlichen Stellen** in Schleswig-Holstein aussprechen müssen (Tz. 12.1). Die Zahl der Beschwerden von Antragstellern aufgrund ihrer Ansicht nach ungenügender Beachtung des IZG-SH durch öffentliche Stellen hat erneut merklich zugenommen. Waren es 2022 noch 37 und 2023 82 Eingaben, so erreichten uns 2024 sogar **128 Eingaben**. Neben den Evergreens, die auch weiterhin einen Großteil der Beschwerden ausmachten (Tz. 12.2), waren auch wieder einige besondere Fälle dabei (Tz. 12.3).

Für eine bundesweite Vernetzung haben wir unsere Arbeit in der **Konferenz der Informationsfreiheitsbeauftragten (IFK)** und dem zugehörigen Arbeitskreis aktiv fortgesetzt (Tz. 12.4). In der anstehenden Evaluation des IZG-SH wollen wir sowohl unsere Erfahrungen aus der schleswig-holsteinischen Informationszugangspraxis als auch aus dem Austausch mit anderen Informationsfreiheitsbeauftragten aus Bund und Ländern als Wünsche an den Gesetzgeber einbringen (Tz. 12.5).

12.1 Beanstandungen

2022 hat der schleswig-holsteinische Gesetzgeber das IZG-SH geändert und damit auch die Befugnisse der/des Landesbeauftragten für Informationszugang erweitert (41. TB, Tz. 12.4; 42. TB, Tz. 12.1). § 14 Abs. 5 IZG-SH regelt, dass für solche Fälle, in denen die oder der Landesbeauftragte für Informationszugang Verstöße gegen das IZG-SH feststellt, sie oder er diese gegenüber der informationspflichtigen Stelle beanstanden kann. Hiervon haben wir im Berichtszeitraum viermal Gebrauch machen müssen. Im Vorfeld einer Beanstandung geben wir jeweils der betroffenen Stelle und anschließend auch der zuständigen Rechts-, Dienst- oder Fachaufsichtsbehörde Gelegenheit zur Stellungnahme.

1. Über die Beanstandung gegenüber der **Apothekerkammer Schleswig-Holstein** hatten wir schon im 42. TB, Tz. 12.1 berichtet.

2. Es wurde festgestellt, dass das **Landeskriminalamt Schleswig-Holstein** den von einer Antragstellerin nach § 4 IZG-SH beantragten Informationszugang ohne nachvollziehbare Gründe an die Mitteilung identifizierender Informationen gebunden und damit gegen § 5 Abs. 1 Satz 1 IZG-SH bzw. § 6 Abs. 1 Satz 3 IZG-SH verstoßen hat.

In diesem Fall beantragte die Antragstellerin nach dem IZG-SH beim Ministerium für Inneres, Kommunales, Wohnen und Sport Schleswig-Holstein Zugang zu bestimmten gespeicherten Daten, insbesondere bei der Landespolizei. Dafür bediente sie sich des Portals Fragdenstaat.de, das den Antrag in Form einer E-Mail sendete. Den Antrag leitete das Ministerium an das Landeskriminalamt weiter, das auch zumindest teilweise die angefragten Informationen beauskunftete.

Allerdings ergaben sich bei der Antragstellerin noch Nachfragen. Das Landeskriminalamt wies darauf hin, dass für die Beantwortung erheblicher Aufwand entstehen und Kosten in Höhe von 200 Euro anfallen könnten. Die Antragstellerin sagte die Zahlung zu und bat um eine Möglichkeit, „die Kosten anonym" begleichen zu können. Das Landeskriminalamt teilte der Antragstellerin mit, dass die Kosten „in Form eines ordentlichen, vollstreckbaren und klagefähigen Gebührenbescheids erhoben" würden und dies nicht **anonym** möglich bzw. eine Anschrift erforderlich sei. Die Antragstellerin verwies aber darauf, dass nach Dokumenten auf der Website des ULD der Antrag bzw. die Bezahlung „auch anonym erfolgen" können müsse, und zitierte hieraus, dass das IZG-SH nicht vorsehe, dass Name und

Anschrift des Antragstellers mitgeteilt werden müssten. Nach Ansicht des Landeskriminalamts handelte es sich hingegen um einen klagefähigen Gebührenbescheid, der auf Grundlage des Verwaltungskostengesetzes erstellt werde – also um einen Verwaltungsakt. Verwaltungsakte unterlägen dem Bestimmtheitsgrundsatz. Hiernach müssten Verwaltungsakte u. a. zustellbar und vollstreckbar sein. Ein anonymer Gebührenbescheid sei weder zustellbar noch vollstreckbar und somit rechtswidrig. Insofern könne eine Bearbeitung der Anfrage erst dann erfolgen, wenn die Voraussetzungen für die Erstellung eines rechtmäßigen Gebührenbescheides gegeben seien bzw. die Identität der Antragstellerin offengelegt werden würde.

Wir konnten die Argumentation des Landeskriminalamtes nicht nachvollziehen. Das IZG-SH sieht gerade **keine Identifikationspflicht** des Antragstellers bzw. der Antragstellerin vor. Eine anonyme Antragstellung ist grundsätzlich möglich und stellt keinen Ablehnungsgrund dar (siehe auch Tz. 12.5). Die Auskunft davon abhängig zu machen, dass die Antragstellerin Kontaktdaten bzw. konkrete Angaben zu ihrer Identität macht, ist dann nicht zulässig, wenn wie hier u. a. eine Vorausleistung möglich ist und angeboten wird. Bei Gebührenbescheiden muss im Einzelfall geprüft werden, ob diese so zugestellt werden können und ob Zahlungen möglich sind, ohne dass Antragsteller Namen nennen und sich identifizieren müssen. Eine Identifizierung der antragstellenden Person ist nicht erforderlich, solange sichergestellt werden kann, dass die informationspflichtige Stelle die begehrten Informationen der antragstellenden Person zukommen lassen kann und z. B. über anonyme Bezahlverfahren die eventuell entstehende Gebührenpflicht durchsetzbar ist.

Dies folgt aus dem Sinn und Zweck des IZG-SH als **Recht für jeden Menschen zur Durchsetzung der Transparenz der Behörden**. Es kommt hier gerade nicht auf die Person der Antragstellerin oder des Antragstellers an, da nicht Zielrichtung des Gesetzes ist, individuelle Rechte zu wahren, die in der Person der Antragstellerin oder des Antragstellers begründet sind. Das unterscheidet dieses Verfahren von vielen anderen Verwaltungsverfahren, in denen eine Antragstellerin bzw. ein Antragsteller etwas beantragt, um eigene Interessen zu wahren. Indem Transparenz der Behörde als ein eigener Wert gesehen wird, der von jeder Person eingefordert werden kann, ist es nicht erforderlich, dass sich diese identifiziert. Dass im Sinne der Ausführungen des Ministeriums nach Artikel 6 DSGVO bzw. § 3 Abs. 1 LDSG die Verarbeitung personenbezogener Daten durch die Behörden grundsätzlich zulässig ist, ändert nichts daran, dass für einzelne Verwaltungsvorgänge die Reduzierung der Kontaktdaten auf ein Minimum nach dem Sinn und Zweck des Gesetzes auch aus Haushaltsinteressen zumutbar und damit geboten ist. Verwaltungsakte sind auch grundsätzlich formfrei. Ein Verwaltungsakt enthält zwar eine Regelung mit Bindungswirkung. Dem steht jedoch eine anonyme Antragstellung nicht entgegen, da es im Rahmen eines Anspruchs nach dem Informationszugangsgesetz gerade nicht auf die antragstellende Person und ihre Interessen ankommt.

3. Es wurde festgestellt, dass die **Gemeinde Heikendorf, vertreten durch das Amt Schrevenborn**, dem von mehreren Antragstellern nach § 4 IZG-SH beantragten Informationszugang nicht fristgerecht entsprochen und teilweise ohne nachvollziehbare Gründe abgelehnt und damit gegen § 3 Satz 1 IZG-SH i. V. m. § 5 Abs. 1 Satz 1 IZG-SH bzw. § 6 Abs. 1 Satz 3 IZG-SH verstoßen hat.

Mehrere Antragsteller hatten bei der Gemeinde Heikendorf Informationen über **Gemeinderatssitzungen und Anwaltsgutachten** im Auftrag der Gemeinde beantragt. Diese Auskünfte waren nur teilweise und mehrfach deutlich nach Ablauf der Monats- bzw. Zweimonatsfrist des IZG-SH erfolgt. Begründet wurde die Verweigerung von Informationen zu Gemeinderatssitzungen u. a. damit, dass die **Gemeindeordnung (GO)** den Regelungen des IZG-SH vorgehen würde und damit Informationen bezüglich nichtöffentlicher Sitzungen versagt werden könnten. Der Informationszugang sei insofern gemäß § 9 Abs. 1 Nr. 3 IZG-SH teilweise abgelehnt worden, da die Bekanntgabe der Informationen nachteilige Auswirkungen auf die Vertraulichkeit der Beratungen in nichtöffentlichen Sitzungen der Gemeinde Heikendorf gehabt hätte. Zudem hätten die entnommenen Sitzungsvorlagen der unmittelbaren Vorbereitung des gemeindlichen Entscheidungsprozesses gedient und fielen daher unter den Schutz des § 9 Abs. 2 Nr. 2 IZG-SH.

Hinsichtlich der Gutachten wurde auf § 9 Abs. 1 Satz 1 Nr. 3 verwiesen, wonach die Vertraulichkeit der Beratungen von informationspflichtigen Stellen geschützt wird. Auch handele es sich um interne Mitteilungen im Sinne des § 9 Abs. 2 Nr. 2 IZG-SH.

Beiden Argumentationen konnten wir nicht folgen. Die **GO** stellt kein Spezialrecht gegenüber dem IZG-SH dar, das diesem vorgehen würde. Dies ist ausdrücklich in § 16a Abs. 4 GO geregelt, wonach die Rechte der Einwohnerinnen und Einwohner nach dem IZG-SH unberührt bleiben. Im Gegensatz zum Vorgänger des IZG-SH, dem Informationsfreiheitsgesetz Schleswig-Holstein (IFG), normiert § 3 Satz 2 IZG-SH keinen grundsätzlichen Vorrang anderer Gesetze. Die Rechte auf Zugang zu Informationen, die andere Gesetze einräumen, bleiben lediglich unberührt. Die Regelungen der GO werden durch das IZG-SH allerdings auch nicht ausgehebelt und sind natürlich in ihrem Sachzusammenhang zu beachten. Eine Sperrwirkung für die Informationen für sonstige Auskunftsrechte bzw. Informationsrechte in der Zukunft (etwa nach dem IZG-SH) ist dem jedoch nicht zu entnehmen. Das IZG-SH ist somit nicht grundsätzlich für Informationen gesperrt, die in einer nichtöffentlichen Gemeindesitzung Thema waren.

Gutachten unterfallen in der Regel nicht den Ausnahmen in § 9 IZG-SH. Nach Kommentaransicht und Rechtsprechung fallen die zur Entscheidung führenden Tatsachen, Sachinformationen und gutachterlichen Stellungnahmen nicht unter die in § 9 Abs. 1 Satz 1 Nr. 3 IZG-SH geschützten Beratungen. Auch handelt es sich nicht um interne Mitteilungen nach § 9 Abs. 2 Nr. 2 IZG-SH. Es kommt somit nicht darauf an, ob das Verfahren bezüglich der Sachverhalte, die die Gutachten betrafen, schon abgeschlossen ist. Zwar kann ein Gutachten Grundlage für die Willensbildung sein und damit auch Teil des Willensbildungsprozesses. Allerdings unterliegt es nicht selbst der Willensbildung, sondern stellt nur eine feststehende Grundlage dar, die wie auch andere Tatsachen von den Beratungsorganen bewertet werden muss. Ein Gutachten nimmt auch keine Beratung vorweg, sondern muss individuell betrachtet werden. Der Inhalt des Gutachtens wird nicht abgewogen, sondern die Abwägung erfolgt im hierauf aufbauenden Beratungsvorgang.

Die Gemeinde Heikendorf bzw. das Amt Schrevenborn haben gegen unsere Beanstandung **Klage beim Verwaltungsgericht** in Schleswig eingelegt. Das Verfahren ist somit **noch nicht abgeschlossen** und wird uns weiter beschäftigen.

4. Es wurde festgestellt, dass das **Amt Schwarzenbek-Land** einem nach § 4 IZG-SH beantragten Informationszugang nicht fristgerecht entsprochen und damit gegen § 3 Satz 1 IZG-SH i. V. m. § 5 Abs. 1 Satz 1 IZG-SH verstoßen hat.

Der Antragsteller hatte im September 2023 Akteneinsicht in ein bestimmtes Verfahren beantragt. Im Folgenden kam es zu mehrfachen Versuchen vonseiten des Antragstellers, für die Akteneinsicht einen Termin zu vereinbaren. Auf diese Schreiben wurde mehrfach sehr **zögerlich reagiert** und mehrfach darauf verwiesen, dass eine zu dem Zeitpunkt abwesende Person, die für den Fall zuständig sei, sich nach ihrer Rückkehr beim Antragsteller melden würde. Ende Oktober 2023 erreichte uns die Beschwerde des Antragstellers, und auch wir bemühten uns, bei der informationspflichtigen Stelle eine Auskunft oder zumindest einen abschließenden Bescheid zu erreichen. Doch auch hierauf wurde selbst nach bewilligter Fristverlängerung nicht zielführend reagiert. Im weiteren Verlauf kam es zwar tatsächlich zu Terminabsprachen zwischen dem Amt und dem Antragsteller für eine Akteneinsicht. Aber auch diese Termine wurden dann wieder vom Amt kurzfristig abgesagt – mit Ausnahme einer ersten Einsichtnahme im Januar 2024. Schließlich erfolgte erst im August 2024 eine Teilauskunft. Weitere Unterlagen wurden zwar in Aussicht gestellt, doch auch die Terminabsprache hierzu wurde nur sehr zögerlich bearbeitet.

Nach § 5 Abs. 2 IZG-SH besteht eine **Frist von einem Monat**, auf einen entsprechenden Antrag zu antworten. Bei umfangreichen und komplexen Sachverhalten kann diese Frist auf zwei Monate erweitert werden, worüber der Antragsteller zu informieren ist. Auch wenn zwischenzeitlich eine Teilauskunft durch die informationspflichtige Stelle getätigt wurde, so wurde nach den uns vorliegenden Informationen auch von dieser nicht bestritten, dass die Auskunftserteilung noch nicht vollständig war. Auch ist nicht ersichtlich, dass vonseiten des Antragstellers

noch eine Konkretisierung des Antrags vom Amt erwartet worden wäre. Selbst wenn die Nachfragen des Antragstellers bei der ersten Einsichtnahme im Januar 2024 als neuer Antrag nach dem IZG-SH angesehen werden würden, wäre die Monatsfrist inzwischen deutlich überschritten.

Die Absagen der Termine erfolgten in den meisten Fällen aus Gründen der Abwesenheit der zuständigen Person. Das IZG-SH sieht keine Verlängerungen der Fristen nach § 5 Abs. 2 IZG-SH vor, sodass die Behörde selbst in der Pflicht ist, **organisatorische Vorkehrungen zu treffen, die Fristen einzuhalten**. Selbst wenn solche besonderen Umstände gegebenenfalls Augenmaß bei dem weiteren Vorgehen verlangen, waren hier kaum Maßnahmen der Behörde erkennbar, die Situation zugunsten des Antragstellers zu klären.

Erschwerend kam hinzu, dass mehrfach neue Termine angekündigt wurden, die dann wieder abgesagt wurden, und zwischen März und August 2024 keine Reaktion mehr gegenüber dem Antragsteller und auch uns erfolgte. Auch danach reagierte das Amt zunächst nicht auf Versuche des Antragstellers für eine Terminfindung zur mittlerweile von der Behörde angebotenen Akteneinsicht. Das Verfahren befindet sich inzwischen in einer gerichtlichen Klärung.

Was ist zu tun?

Das Mittel der Beanstandung ist bei Verstößen gegen das IZG-SH weiterhin zu nutzen, um den informationspflichtigen Stellen nachdrücklich offenzulegen, wenn sie bei der Umsetzung der Informationsfreiheit Fehler machen.

12.2 Top 5 der Themen in Schleswig-Holstein

Nach § 14 Abs. 1 IZG-SH kann eine Person, die der Ansicht ist, dass ihr Informationsersuchen zu Unrecht abgelehnt oder nicht beachtet worden ist oder dass sie von einer informationspflichtigen Stelle eine unzulängliche Antwort erhalten hat, die Landesbeauftragte für Informationszugang anrufen. Einige Beschwerdegründe von Petentinnen und Petenten wiederholten sich auch 2024 mehrfach. Die Top 5 der Beschwerden unterscheiden sich kaum von denen der letzten Jahre (vgl. u. a. 41. TB, Tz. 12.3 und 42. TB, Tz. 12.2). Hinzugekommen ist jedoch noch eine besondere Beobachtung unsererseits.

Der häufigste Beschwerdegrund war erneut, dass die informationspflichtige Stelle nicht **fristgerecht** auf den Antrag auf Informationszugang reagierte. Nach § 5 Abs. 2 Satz 1 IZG-SH sind die Informationen der antragstellenden Person unter Berücksichtigung etwaiger von ihr angegebenen Zeitpunkte sobald wie möglich, spätestens jedoch mit Ablauf eines Monats nach Eingang des Antrags zugänglich zu machen. Nur bei umfangreichen und komplexen Anfragen kann die Frist auf höchstens zwei Monate verlängert werden (§ 5 Abs. 2 Satz 2 IZG-SH). Die Verlängerung ist zu begründen und schon innerhalb des ersten Monats mitzuteilen. Zu beachten ist, dass die Rückmeldung sobald wie möglich erfolgen muss und die Monatsfrist nicht zwingend ausgeschöpft werden sollte. Die Frist beginnt mit Eingang des Antrags und ist grundsätzlich unabhängig von der personellen und organisatorischen Ausgestaltung der informationspflichtigen Stelle (vgl. auch Tz. 12.1 Nr. 4). Auch eine teilweise oder vollständige Ablehnung muss die Fristen einhalten. Eine Sondersituation besteht, wenn der Antrag zu unbestimmt war und noch von der Antragstellerin bzw. dem Antragsteller präzisiert werden muss. Dann muss die Aufforderung zur Präzisierung auch innerhalb eines

Monats erfolgen. Nach Eingang des präzisierten Antrags beginnt die Frist zur Beantwortung des Antrags erneut (§ 4 Abs. 2 IZG-SH).

Nicht immer ist erkennbar, ob die ausstehende Antwort nach Ablauf der Frist darauf beruhte, dass die konkrete Fristenregelung ignoriert wurde oder **gar nicht erkannt worden** ist, dass es sich um einen Antrag nach dem IZG-SH handelte. Das Gesetz schreibt keine besondere Form für den Antrag vor. Auch müssen sich antragstellende Personen nicht konkret auf das IZG-SH berufen. Grundsätzlich kann somit jeder Wunsch nach Informationen bei einer öffentlichen Stelle als Antrag im Sinne des § 4 Abs. 1 IZG-SH gewertet werden. Dies kann auch für mündliche Anträge etwa in Bürgersprechstunden gelten. Bei Unklarheit über den Charakter der Anfrage sollte umgehend nachgefragt bzw. gegebenenfalls um Präzisierung des Antrags gebeten werden.

Nicht immer wird bei (Teil-)Ablehnungen die **Form des § 6 IZG-SH** eingehalten. Der antragstellenden Person sind danach stets die Gründe für die Ablehnung mitzuteilen, auch wenn sie nur einige wenige Schwärzungen betreffen. Auch ist über die Rechtsschutzmöglichkeiten gegen die Entscheidung sowie darüber, bei welcher Stelle und innerhalb welcher Frist um Rechtsschutz nachgesucht werden kann, zu belehren.

Es hat sich in vielen Fällen gezeigt, dass die Beschwerden eventuell hätten vermieden werden können, wenn die informationspflichtige Stelle **frühzeitig den Kontakt** zu dem Antragsteller bzw. der Antragstellerin aufgenommen hätte, um Unklarheiten zu beseitigen und Verständnis für gegebenenfalls bestehende Auskunftsprobleme zu wecken. Gerade auch mit Blick auf den Aufwand bei der Behörde (und damit einhergehend gegebenenfalls die anfallenden Kosten) kann es sinnvoll sein, ins Gespräch zu kommen. Wenn stattdessen die Angelegenheit bis zur Beschwerde liegen gelassen wird, erzeugt das das unangenehme Gefühl bei Antragstellerinnen und Antragstellern, dass die Behörde Anfragen bewusst ignoriert. Bis zur gerichtlichen Auseinandersetzung ist es dann nicht weit. In § 4 Abs. 2 Satz 4 IZG-SH ist ausdrücklich geregelt, dass die informationspflichtige Stelle die antragstellende Person bei der Stellung und Präzisierung von Anträgen zu unterstützen hat. Eine Chance, die zu beiderseitigem Vorteil leider nicht immer genutzt wird.

Eine weitere oft ungenutzte Chance ist, dass die informationspflichtigen Stellen auch **uns um Rat bitten** können. Nach § 14 Abs. 3 IZG-SH berät die oder der Landesbeauftragte für Informationszugang die informationspflichtigen Stellen in Fragen zum IZG-SH. Im Berichtszeitraum ist es jedoch erneut vorgekommen, dass informationspflichtige Stellen, nachdem wir sie aufgrund einer Beschwerde um Stellungnahme gebeten haben, die Angelegenheit an eine Kanzlei abgaben. Dies ist zwar nicht per se zu kritisieren, jedoch haben wir in einigen Fällen den Eindruck gehabt, dass es sinnvoll gewesen wäre, vorab auch den Kontakt zu uns aufzunehmen. Insbesondere in Fällen, in denen die Behörde von uns angeschrieben wurde, da sie zunächst gar nicht auf einen Antrag nach dem IZG-SH reagiert hatte, könnte zunächst geklärt werden, ob tatsächlich ein rechtlicher Dissens der Ansichten vorliegt.

Die Grundlagen zum IZG-SH haben wir in einer Broschüre zusammengefasst, die regelmäßig aktualisiert wird:

https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-7-Informationszugang.pdf

Kurzlink: *https://uldsh.de/tb43-12-2a*

Was ist zu tun?

Wir gehen den Beschwerden von Petentinnen und Petenten nach und weisen informationspflichtige Stellen gegebenenfalls auf Fehler bei der Bearbeitung von Informationszugangsersuchen hin. Damit Fehler gar nicht erst auftreten, werden wir die Schulung bzw. Information über das IZG-SH gegenüber öffentlichen Stellen intensivieren.

12.3 Besondere Fälle und Fragen

Im Berichtszeitraum hatten wir einige besondere Anfragen und Beschwerden, die über die typischen Fragestellungen (Tz. 12.2) hinausgingen.

Auch wenn immer mal wieder juristische Personen des Privatrechts bestreiten, dass sie nach § 2 Abs. 3 Nr. 2 IZG-SH dem IZG-SH unterfallen, und zu keiner Auskunft bereit sind, gab es im Berichtszeitraum ein Positivbeispiel: Einige **Rettungshubschrauber** werden durch die DRF Stiftung Luftrettung gemeinnützige AG in Filderstadt betrieben. Ein Petent hatte dort Informationen zu Einsätzen von Rettungshubschraubern nach dem IZG-SH beantragt. Eine Antwort hatte er jedoch nicht erhalten. Wir wiesen die Stelle darauf hin, dass sie für die Aufgabe beliehen wurde und somit Aufgaben der öffentlichen Verwaltung zur Erledigung in den Handlungsformen des öffentlichen Rechts übertragen bekommen habe. Nach kurzer Diskussion über mögliche Ausnahmegründe kam die Stelle ihren Pflichten nach dem IZG-SH nach.

Soweit natürliche oder juristische Personen des Privatrechts nicht beliehen wurden und daher auf den ersten Blick nicht dem IZG-SH unterfallen, kann dieses bei **Umweltinformationen** anders zu beurteilen sein. So hatten wir im 42. TB, Tz. 12.3 von Stadtwerken berichtet, die nicht dem IZG-SH unterfielen. In einem anderen Kontext wurde nach Intervention durch uns anerkannt, dass Informationen herauszugeben waren. Dies gilt nach § 2 Abs. 3 Nr. 3 IZG-SH bei Umweltinformationen, soweit die natürliche oder juristische Person des Privatrechts im Zusammenhang mit der Umwelt öffentliche Aufgaben wahrnimmt und dabei der Kontrolle des Landes oder einer unter Aufsicht des Landes stehenden juristischen Person des öffentlichen Rechts unterliegt. Kurz gesagt, bei Umweltinformationen reicht es in der Regel aus, dass die juristische Person des Privatrechts von einer öffentlichen Stelle kontrolliert wird. Eine Beleihung ist nicht erforderlich. Ausführlich diskutiert wurde im konkreten Fall dann jedoch, welche Informationen tatsächlich „Umweltinformationen" seien.

Mehrfach beschäftigten uns Anfragen von Antragstellern nach **Datenschutz-Folgenabschätzungen (Artikel 35 DSGVO) und Verzeichnissen von Verarbeitungstätigkeiten (Artikel 30 DSGVO)** bei informationspflichtigen Stellen. Diese Anfragen wurden teilweise sehr pauschal von den informationspflichtigen Stellen abgelehnt. Wir teilten den Stellen daher daraufhin mit, dass auch diese Dokumente grundsätzlich informationspflichtig sind. Insbesondere spielt es in Bezug auf das Verzeichnis von Verarbeitungstätigkeiten keine Rolle, dass im Gegensatz zum alten Verfahrensverzeichnis aus dem BDSG oder LDSG die DSGVO keine Veröffentlichung dieses Verzeichnisses verlangt. Dass darin keine Veröffentlichungspflicht explizit geregelt wird, bedeutet nämlich keinen Ausschluss der Anwendbarkeit des IZG-SH. Auch war für die DSGVO ein anderer Gesetzgeber zuständig, sodass es sich in Artikel 30 DSGVO nicht um eine Nachfolgeregelung vom BDSG handelt. Somit sind beide Dokumente – das Verzeichnis nach Artikel 30 DSGVO sowie der Bericht der Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO – grundsätzlich zunächst einmal auskunftspflichtig. Geprüft werden muss jedoch, ob Ausnahmevorschriften nach §§ 9 und 10 IZG-SH greifen. Bei der Datenschutz-Folgenabschätzung kann dieses insbesondere bedeutende Schutzgüter der öffentlichen Sicherheit im Sinne des § 9 Abs. 1 Satz 1 Nr. 1 IZG-SH betreffen: Die Herausgabe von zugehörigen Dokumenten darf nicht zu Sicherheitsproblemen führen. Dabei ist jedoch zusätzlich neben der entsprechenden Abwägung auch zu untersuchen, ob zumindest Teile des Berichts der Datenschutz-Folgenabschätzung beauskunftet werden können.

In der Regel fragen Antragstellerinnen und Antragsteller Informationen an, die schriftlich bzw. in Textform bei einer Stelle vorhanden sind. Außergewöhnlich war eine Beschwerde, bei der ein Petent den **Tonmitschnitt** einer öffentlichen Ratsversammlung anfragte. Tatsächlich sind nach § 1 Abs. 1 IZG-SH Informationen im Sinne des IZG-SH alle in Schrift-, Bild-, Ton- oder Datenverarbeitungsform oder auf sonstigen Informationsträgern vorhandene Zahlen, Daten, Fakten, Erkenntnisse oder sonstige Auskünfte. Der Tonmitschnitt fiel also darunter. Allerdings waren hierauf auch die Stimmen anderer Perso-

nen zu hören, sodass der Schutz personenbezogener Daten im Sinne des § 10 Satz 1 Nr. 1 IZG-SH geprüft werden musste. Bei der Abwägung musste zwischen unbeteiligten Dritten und Teilen der Ratsversammlung unterschieden werden. Im Endeffekt einigte man sich darauf, dass das Tonprotokoll zwar nicht übermittelt wurde, jedoch angehört werden konnte.

Noch nicht abschließend geklärt ist die Frage, inwieweit **Wahlorgane** vom IZG-SH erfasst sind. Ein Petent beantragte Wahlniederschriften zur Europawahl 2024 bzw. Informationen zu ungültig erklärten Wahlscheinen. Die Stelle führte jedoch aus, dass das IZG-SH nicht auf die Wahlorgane anwendbar sei, da keine Behördenfunktion gegeben sei. Die Wahlorgane seien als eine Art Selbstverwaltungsorgane der Wahlberechtigten ausgestaltet. Ein Ausschluss von Wahlorganen ist dem IZG-SH jedoch unseres Erachtens nicht zu entnehmen. Anwendbar ist das IZG-SH nach § 2 Abs. 3 Nr. 1 IZG-SH nicht nur für Behörden, sondern auch für sonstige juristische Personen des öffentlichen Rechts.

Wir vertreten die Ansicht, dass es sich bei der Vorbereitung und Durchführung der Wahl um Verwaltungshandeln handelt. Für den Bundeswahlleiter wird dieses ausdrücklich in der Kommentarliteratur mit Bezug auf das Informationsfreiheitsgesetz des Bundes (IFG Bund) bejaht. Dies hat der Bundeswahlleiter auch anerkannt. Wir können nicht erkennen, weshalb für die hier infrage stehende Wahl für Schleswig-Holstein etwas anderes gelten sollte. Es liegt im Interesse der Gesellschaft, dass Wahlen transparent durchgeführt werden, weshalb es unseres Erachtens widersinnig wäre, wenn ein Gesetz zur Förderung der transparenten Verwaltung hierauf keine Anwendung finden würde. Einwänden, wie etwa dem Personenbezug einiger der gewünschten Informationen, kann mit den Ausschlussgründen der §§ 9 und 10 IZG-SH begegnet werden. Sie würden somit nicht dazu führen, dass das Wahlgeheimnis in Mitleidenschaft gezogen werden würde.

Unklar war in einem Fall, ob **Vergabekammern** dem IZG-SH unterliegen. Wörtlich ausgenommen sind sie nicht. In einem Beschwerdeverfahren wurde jedoch von einer Stelle ausgeführt, dass das Fehlen der Vergabekammern in den ausgenommenen Stellen nach § 2 Abs. 4 Nr. 3 IZG-SH eine planungswidrige Regelungslücke darstellen würde. Vergabekammern seien Sonderbehörden mit gerichtsähnlicher Stellung, was wenig bekannt sei. Sie gewährten nach dem Gesetz gegen Wettbewerbsbeschränkungen (GWB) Primärrechtsschutz erster Instanz. Der Charakter der Vergabekammer als Gericht ist unseres Erachtens nicht eindeutig geregelt, da sie grundsätzlich Verwaltungsbehörden sind und damit Teil der Exekutive. Allerdings können auch Teile der Exekutive Organe der Rechtspflege sein.

Im Rahmen der Vorlagemöglichkeit von Gerichten beim EuGH nach Artikel 267 des Vertrages über die Arbeitsweise der Europäischen Union hat der EuGH auch die Vorlage einer Vergabekammer als Gericht anerkannt (EuGH, Urteil vom 18.09.2014 – C-549/13). Nach § 168 Abs. 3 GWB hingegen ergeht die Entscheidung der Vergabekammer durch Verwaltungsakt (und somit nicht durch ein Urteil). Das Bundesverwaltungsgericht hatte sich in seinem Beschluss vom 15.12.2020 – 10 C 24.19 – auch zu dem Verhältnis Vergaberecht und Informationsfreiheit (hier: IFG Bund) geäußert und festgestellt, dass die Informationsfreiheit zumindest nach Abschluss des Vergabeverfahrens nicht durch die Vorschriften der Vergabeverordnung verdrängt wird.

Auch schließt § 165 GWB unseres Erachtens das IZG-SH nicht aus. Eine Subsidiaritätsklausel besteht gerade nicht im IZG-SH. Hinsichtlich laufender Verfahren kann die oben genannte Frage in vielen Fällen allerdings gegebenenfalls dahinstehen, da hierbei oftmals Betriebs- und Geschäftsgeheimnisse im Sinne des § 10 Satz 1 Nr. 3 IZG-SH betroffen sein könnten und insbesondere vor einer Entscheidung der Vergabekammer noch die Vertraulichkeit der Beratungen (§ 9 Abs. 1 Satz 1 Nr. 3 IZG-SH) vorliegen könnte.

Was ist zu tun?

Personen, die der Ansicht sind, dass ihre Anträge nach dem IZG-SH nicht ordnungsgemäß beantwortet worden seien, können sich an uns wenden. Zu unserer Aufgabe gehört es, die informationspflichtigen Stellen auf ihre Pflichten nach dem Gesetz hinzuweisen – wenn erforderlich auch in Form einer Beanstandung.

12.4 Beschlüsse der IFK

Im Rahmen des Arbeitskreises Informationsfreiheit (AKIF) und der Treffen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) in Dresden und Leipzig unter dem Vorsitz der Sächsischen Datenschutz- und Transparenzbeauftragten haben wir an mehreren Entschließungen maßgeblich mitgewirkt.

- Entschließung zwischen der 45. und der 46. Konferenz der Informationsfreiheitsbeauftragten in Deutschland vom 4. Juni 2024 in Dresden: **Gut informiert im Superwahljahr 2024!**

  https://www.datenschutzzentrum.de/uploads/ifk/20240604_IFK_Entschliessung_Superwahljahr.pdf

  Kurzlink: *https://uldsh.de/tb43-12-4a*

- Entschließung der 46. Konferenz der Informationsfreiheitsbeauftragten in Deutschland am 05.06.2024 in Dresden: **Pflicht zur Informationsfreiheit und Transparenz auch für Kommunen in Hessen und Sachsen!**

  https://www.datenschutzzentrum.de/uploads/ifk/Entschliessung_Kommunen.pdf

  Kurzlink: *https://uldsh.de/tb43-12-4b*

- Entschließung der 46. Konferenz der Informationsfreiheitsbeauftragten in Deutschland am 05.06.2024 in Dresden: **Gleicher Auftrag – gleicher Informationsanspruch gegenüber öffentlich-rechtlichen Rundfunkanstalten!**

  https://www.datenschutzzentrum.de/uploads/ifk/Entschliessung_Rundfunkanstalten.pdf

  Kurzlink: *https://uldsh.de/tb43-12-4c*

Die **Protokolle und weitere Informationen** zu den Sitzungen der IFK können hier abgerufen werden:

https://www.datenschutzzentrum.de/artikel/1347-.html

Kurzlink: *https://uldsh.de/tb43-12-4d*

Was ist zu tun?

Wir werden uns weiterhin intensiv in die Diskussionen und Entschließungen der IFK und den zugehörigen Arbeitskreis einbringen.

12.5 Wünsche an den Gesetzgeber

Nach § 14 IZG-SH kann eine Person, die der Ansicht ist, dass ihr Informationsersuchen zu Unrecht abgelehnt oder nicht beachtet worden ist oder dass sie von einer informationspflichtigen Stelle eine unzulängliche Antwort erhalten hat, die Landesbeauftragte für Informationszugang anrufen. Dies wurde 128-mal im Berichtszeitraum gemacht. Hierbei und auch schon bei Beschwerden in den Jahren zuvor zeigten sich einige Unklarheiten im IZG-SH, die zu Diskussionen führten. Im Rahmen einer Weiterentwicklung des Gesetzes (Tz. 1.4) wünschen wir uns einige Klarstellungen.

1. Ausweitung auf juristische Personen des Privatrechts, die im Besitz von öffentlichen Stellen sind

Hierzu hatten wir schon im letzten Tätigkeitsbericht Ausführungen gemacht (42. TB, Tz. 12.3). In der Praxis waren es Stadtwerke, die als GmbH ausgestaltet und 100 Prozent Töchter der jeweiligen Stadt sind und sich weigerten, Auskünfte nach dem IZG-SH zu tätigen. Nach § 2 Abs. 3 Nr. 2 IZG-SH können auch derartige juristische Personen informationspflichtige Stellen sein, soweit ihnen Aufgaben der öffentlichen Verwaltung zur Erledigung in den Handelsformen des öffentlichen Rechts übertragen wurden (sogenannte Beleihung). Als Beispiele nennt das Gesetz u. a. Energieerzeugung und -versorgung. Eine solche Beleihung ist jedoch selten und liegt nur in wenigen Fällen bei Unternehmen vor, die vollständig oder überwiegend in der Hand einer Kommune sind, obwohl diese etwa mit staatlichen Kontrahierungszwängen usw. begünstigt sind. Für Bürgerinnen und Bürger ist es kaum nachvollziehbar, weshalb diese Stellen aus der Informationsfreiheit herausgenommen wurden.

In einigen anderen Bundesländern unterliegen solche Unternehmen eindeutig der Auskunftspflicht; es ist dort nicht möglich, sich etwa durch Ausgründungen dieser Pflicht zu entziehen. So stellt etwa das Landesinformationsfreiheitsgesetz Baden-Württemberg in § 2 Abs. 4 darauf ab, ob eine öffentliche Stelle die Mehrheit am Kapital oder der Anteile an dem Unternehmen hält bzw. mehr als die Hälfte der entscheidenden Personen stellt. Eine solche Regelung wünschen wir uns auch.

2. Wann ist zu umfangreich zu unbestimmt?

Das IZG-SH macht bewusst kaum Vorgaben für die Ausgestaltung von Anträgen nach § 4 IZG-SH. Die Hemmschwelle soll gering gehalten werden und das Recht auf Informationszugang jeder Person offenstehen. Wenn der Antrag zu unbestimmt ist, so muss die informationspflichtige Stelle nach § 4 Abs. 2 IZG-SH zur Präzisierung auffordern. In der Praxis kommt es teilweise zu sehr umfangreichen Anfragen. Um dem ausufernden Umfang Herr zu werden, wird auch hier um Präzisierung gebeten und der Antrag als zu unbestimmt angesehen. Die Frage in der Praxis ist jedoch, wann eine informationspflichtige Stelle die vollständige Bearbeitung zunächst ablehnen kann, weil der damit verbundene Umfang zu groß ist. Dabei ist teilweise nicht nur der Umfang der betroffenen Informationen problematisch, sondern es werden auch Fragenkataloge mit dutzenden Einzelposten übermittelt und zu einem Antrag zusammengefasst.

In der Beratungspraxis bemühen wir uns in solchen Fällen insbesondere darum, die Parteien dazu zu bringen, sich persönlich zu dem Antrag auszutauschen. Dies ist auch schon im Gesetz in § 4 Abs. 2 Satz 4 IZG-SH angelegt, wonach die informationspflichtige Stelle bei der Stellung und Präzisierung von Anträgen unterstützen muss. Ab wann eine solche Präzisierung geboten ist, ist dennoch weiterhin im Gesetz unklar. Hierbei kann man sich an der Kostenverordnung zum IZG-SH orientieren. Diese sieht für eine außergewöhnlich umfassende Auskunft eine maximale Gebühr in Höhe von 500 Euro (seit 14.01.2025 700 Euro) vor. Bei der Stufe darunter (umfassende Auskunft) ist eine Gebühr von maximal 250 Euro vorgesehen (seit 14.01.2025 350 Euro). Die Gebühren sind zwar nach § 13 Abs. 2 IZG-SH auch unter Berücksichtigung des Verwaltungsaufwands so zu bemessen, dass das Recht auf Zugang zu Informationen wirksam in Anspruch genommen werden kann. Allerdings kann die

Kostenverordnung auch einen Orientierungsrahmen zum möglichen Aufwand darstellen. Überschreitet die Anfrage der Petentin oder des Petenten diesen Umfang deutlich, kann gegebenenfalls der Antrag als zu unbestimmt angesehen werden. Dies sollte der Gesetzgeber zur Transparenz klarstellen.

3. Anträge unter Pseudonym

Das Urteil des Bundesverwaltungsgerichts vom 20.03.2024 – 6 C 8.22 – gegen den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, wonach nach dem IFG des Bundes anonyme Antragstellung oder Anträge unter einem Pseudonym unzulässig sein können, hat auch bei informationspflichtigen Stellen in Schleswig-Holstein für Irritationen gesorgt. Wir vertreten weiterhin die Ansicht, dass auch anonyme bzw. pseudonyme Anträge zulässig sind, und sehen keine Anzeichen im IZG-SH, die dieser Ansicht widersprechen würden. Bei der Betrachtung des Urteils ist zu beachten, dass es sich auf das IFG des Bundes bezieht und durchaus Abweichungen zu den Regelungen in Schleswig-Holstein bestehen. So nimmt etwa § 5 Abs. 1 Satz 1 IFG Bund direkten Bezug auf die Antragstellerin oder den Antragsteller, was in § 10 Satz 1 Nr. 1 IZG-SH nicht der Fall ist. Auch nimmt das BVerwG Bezug auf die Gesetzesbegründung des IFG Bund, was natürlich nicht für das IZG-SH gelten kann. Hätte der Gesetzgeber in Schleswig-Holstein eine zwingende Identifizierung der Antragstellerin oder des Antragstellers gewollt, so hätte er es spätestens beim Erlass des IZG-SH als Nachfolger des IFG-SH aufnehmen können. Dies ist jedoch gerade nicht passiert. Ein Großteil der Anfragen nach dem IZG-SH erfolgt über Portale, die keinen Nachweis der Identität der Antragstellerin oder des Antragstellers verlangen und in der Regel problemlos bearbeitet werden können.

Das IZG-SH hat auch gerade keine Einschränkungen bezüglich der Antragstellenden vorgenommen (es ist z. B. nicht auf Bürgerinnen und Bürger aus Schleswig-Holstein beschränkt). Für die Gebührendurchsetzung mag es Gründe zur Identifizierung der Antragstellerin oder des Antragstellers geben (Tz. 12.1). Eine pauschale Pflicht zur Identifizierung sehen wir jedoch weder im IZG-SH verankert noch als zweckmäßig an. Um hierzu Klarheit für Antragstellende und informationspflichtige Stellen zu erhalten, sollte dies auch im Gesetz herausgestellt werden.

4. Transparenzbeauftragte

Es zeigt sich, dass in vielen informationspflichtigen Stellen unklar ist, wer für Anfragen nach dem IZG-SH zuständig ist und auch für uns als Ansprechpartner genutzt werden kann. Teilweise werden die Datenschutzbeauftragten zusätzlich mit dieser Aufgabe betreut, teilweise ist es Chefsache und teilweise gibt es gar keine Regelungen. Daher halten wir es für sinnvoll, dass informationspflichtige Stellen eine(n) Beauftragte(n) für Informationszugang bzw. Transparenz benennen. Auch wenn die Informationen an sehr unterschiedlichen Stellen einer Behörde vorliegen können, so erscheint es sinnvoll, eine zentrale Koordinierungsstelle zu haben, die als Ansprechpartnerin für Antragstellende und für uns fungiert. Auch kann eine solche Koordinierungsstelle bei Landesbehörden dafür Sorge tragen, dass die Veröffentlichungspflichten nach § 11 IZG-SH eingehalten werden. Auch wenn wir keine Pflicht zur Benennung einer oder eines behördlichen Beauftragten für Informationszugang bzw. Transparenz vorschlagen wollen, hielten wir es für förderlich, eine Anregung zur freiwilligen Benennung für eine solche Position ins Gesetz aufzunehmen.

Was ist zu tun?

Wir bringen unsere Praxiserfahrungen mit der Umsetzung des IZG-SH in der Diskussion zur Gesetzesevaluierung ein und bieten unsere Unterstützung bei Gesetzesänderungen an.

13

KERNPUNKTE

Fortbildungsveranstaltungen der DATENSCHUTZAKADEMIE

Sommerakademie „Digitale Datenräume und Archive“

13 DATENSCHUTZAKADEMIE Schleswig-Holstein

Die DATENSCHUTZAKADEMIE Schleswig-Holstein ist für die Konzeption und Organisation der Fortbildungsveranstaltungen zu den Themen **Datenschutz und Informationsfreiheit** zuständig. So wird beispielsweise den behördlichen und betrieblichen Datenschutzbeauftragten das Fachwissen der DSGVO und anderer einschlägiger Gesetze vermittelt.

13.1 Fortbildungsveranstaltungen im Programm der DATENSCHUTZAKADEMIE

Im **Schulungsjahr 2024** hat sich die DATENSCHUTZAKADEMIE auf Grundlagenkurse in den folgenden Bereichen konzentriert:

- behördlicher Datenschutz,
- betrieblicher Datenschutz,
- Standard-Datenschutzmodell / Datenschutz-Folgenabschätzung

Die Dauer der Fortbildungskurse lag bei zwei bis drei Tagen. Die Kurse im Bereich behördlicher und betrieblicher Datenschutz unterteilten sich in rechtliche und technische Inhalte. Die Teilnehmenden konnten sich so **das nötige Datenschutz-Know-how erarbeiten**, bestehendes Wissen vertiefen und sich untereinander vernetzen.

Die aktuellen Fortbildungsveranstaltungen finden Sie unter:

https://www.datenschutzzentrum.de/akademie/

Kurzlink: *https://uldsh.de/tb43-13-1a*

13.2 Sommerakademie – jährliche Datenschutzkonferenz in Kiel

Die alljährlich an einem Montag im Spätsommer stattfindende Sommerakademie der DATENSCHUTZAKADEMIE stand im Jahr 2024 unter dem Motto **„Digitale Datenräume und Archive: Brückenschlag zwischen Vergangenheit und Zukunft“**. Die Konferenz wurde im Jahr 2024 in inhaltlicher Kooperation mit dem Landesarchiv Schleswig-Holstein durchgeführt. Teilnehmende aus dem gesamten Bundesgebiet fanden den Weg nach Kiel, um über Datenschutz und Datensicherheit sowie Fragen des Archivrechts oder der Informationsfreiheit zu diskutieren.

Hintergrund der Sommerakademie 2024 war die Entwicklung, dass seit einigen Jahren auf allen Ebenen – von Europa über Deutschland bis hin nach Schleswig-Holstein – **Datenstrategien zum Datenteilen** erarbeitet werden: Daten sollen in größerem Umfang und in besserer Qualität genutzt werden, um Vorteile für die Weiterentwicklung von Staat, Gesellschaft, Wirtschaft und Forschung auszuschöpfen. Es gelten dabei aber weiterhin die gesetzlichen Schutzpflichten, insbesondere das Datenschutzrecht, um die Rechte der betroffenen Personen zu wahren. **Datentreuhänder** können in den Datenstrategien eine wichtige Funktion einnehmen, beispielsweise beim Aufbau von Datenräumen zu Gesundheit oder Mobilität.

Eine ganz besondere Rolle spielen die **Archive im öffentlichen Bereich**: Alle heutigen Daten-

schutzgesetze enthalten weitreichende Ausnahmebestimmungen für die Archive, die sich als verlässliche Datentreuhänder ein besonderes Vertrauen verdient haben. Ein reflektierter Umgang mit Informationen muss sich in der Praxis niederschlagen, in der es Zielkonflikte zwischen informationeller Selbstbestimmung und Erinnerungsauftrag zu lösen gilt. Nicht immer sind die Regelungen eindeutig. Auch in der eigentlich gesetzlich geregelten Zusammenarbeit zwischen Behörden und öffentlichen Archiven sorgt das Thema Datenschutz häufig für Diskussionen.

So widmete sich die Sommerakademie 2024 der Debatte zum Verhältnis von **Datenschutz und Archivierung**, aber auch **Informationsfreiheit**. Die Vorträge der eingeladenen Expertinnen und Experten aus Praxis und Wissenschaft sind unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/sommerakademie/2024/

Kurzlink: *https://uldsh.de/tb43-13-2a*

Index

E

F

G

H

I

ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

Schleswig-Holsteins
Zentrum für Datenschutz
und Informationszugang

https://www.datenschutzzentrum.de/tb/