ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

TÄTIGKEITSBERICHT
2024

ULD – SCHLESWIG-HOLSTEINS ZENTRUM FÜR DATENSCHUTZ UND INFORMATIONSZUGANG

Tätigkeitsbericht 2024
des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

BERICHTSZEITRAUM: 2023

REDAKTIONSSCHLUSS: 31.12.2023

LANDTAGSDRUCKSACHE 20/2039

(42. 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

Fünf Jahre DSGVO

Zahlen und Fakten

Vorsitz der DSK im Jahr 2023

Institutionalisierung der DSK

1 Datenschutz und Informationsfreiheit

Der 42. Tätigkeitsbericht – das ist schon etwas Besonderes! Das Berichtsjahr 2023 war ein Jubiläumsjahr: Das Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983, in dem das Recht auf informationelle Selbstbestimmung aus dem Grundgesetz abgeleitet wurde, feierte 40 Jahre Jubiläum. Die – unberechtigterweise nicht ganz so bekannte – Entscheidung des BVerfG zum Computergrundrecht, also dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, fiel am 27.02.2008, also vor 15 Jahren. Die Datenschutz-Grundverordnung ging am 25.05.2018[1] an den Start und feierte im Berichtsjahr ihr fünfjähriges Jubiläum. Und das erste Landesdatenschutzgesetz Schleswig-Holstein trat am 01.07.1978 in Kraft, also vor 45 Jahren. In dem Jahr gab es auch den ersten Landesdatenschutzbeauftragten in Schleswig-Holstein, Herrn Ernst Eugen Becker, meinen Vorvorvorgänger. Damals war er noch „Der Landesbeauftragte für den Datenschutz beim Innenminister des Landes Schleswig-Holstein" – die Unabhängigkeit von der Regierung kam erst später.

Man würde vielleicht erwarten, dass die Zahl der Tätigkeitsberichte 45 betragen müsste, jedoch erschien der Bericht eine Zeit lang nur zweijährlich, sodass wir in der Zählung „erst" beim 42. Tätigkeitsbericht sind. Die Zahl 42 ist dabei schon wieder etwas Besonderes, denn im Roman „Per Anhalter durch die Galaxis" von Douglas Adams, der längst zur internationalen Popkultur gehört, ist „42" die Antwort, die der Supercomputer auf die „endgültige Frage nach dem Leben, dem Universum und dem ganzen Rest" gibt.

Der 42. Tätigkeitsbericht wird nicht die Antworten auf alle Fragen geben. Er ist auch nicht mit einem Supercomputer erstellt worden, noch nicht einmal mit einem Chatbot. Stattdessen schreiben meine Mitarbeitenden und ich als Menschen über unsere Tätigkeit in den Bereichen Datenschutz und Informationsfreiheit.

Der Bericht gibt auch in seiner 42. Ausgabe einen Einblick in die Tätigkeiten der Behörde der Landesbeauftragten für Datenschutz und, in Personalunion, der Landesbeauftragten für Informationszugang. Mit den ausgewählten Fällen und den behandelten Themen zeigen wir relevante Entwicklungen aus Recht und Technik und geben Hinweise darauf, wie man Fehler vermeidet oder Verbesserungsbedarfe umsetzen kann, um die Anforderungen aus dem Datenschutz- und aus dem Informationszugangsrecht zu erfüllen.

Bestimmt ist in unserer Zusammenstellung für den 42. Tätigkeitsbericht Neues, Interessantes oder auch Spannendes für Sie enthalten. Ich wünsche Ihnen viel Spaß bei der Lektüre!

Dr. h. c. Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein
Landesbeauftragte für Informationszugang Schleswig-Holstein

1.1 Fünf Jahre Datenschutz-Grundverordnung – oder: Leuchttürme, aber für alle

Am 25. Mai 2018 ging es los: Die Datenschutz-Grundverordnung (DSGVO) regelte von nun an die Verarbeitung personenbezogener Daten und damit die Pflichten der Verantwortlichen und die Rechte der betroffenen Personen. In den fünf (oder bei Erscheinen des Berichts fast sechs) Jahren ihrer Geltung hat sich die Datenverarbeitung in Europa verändert: Digitalisierung durchdringt fast alle Lebensbereiche, für viele sind Smartphones und Cloud Computing zur Selbstverständlichkeit geworden, und die Anwendungen der künstlichen Intelligenz übernehmen Aufgaben im Job und im Privatleben.

[1] Der 25. Mai ist übrigens auch als „Handtuchtag" (englisch: „Towel Day") bekannt – eine Referenz auf das Werk „Per Anhalter durch die Galaxis", da der Held, der im Bademantel unterwegs ist, stets ein Handtuch dabeihat. Dies wird im Titelbild dieses Berichts visualisiert.

Das Bewusstsein über die Rechte auf Auskunft, Berichtigung oder auch Löschung von personenbezogenen Daten ist europaweit gestiegen. Die Datenschutzaufsichtsbehörden bearbeiten jedes Jahr Tausende von Beschwerden. Die Verantwortlichen kennen ihre Pflichten. **Das Konzept eines einheitlichen Datenschutzrechts gilt als Erfolgsmodell.** Mit dem Europäischen Datenschutzausschuss wurde ein wichtiges Gremium geschaffen, um durch gemeinsame Leitlinien für die Datenverarbeitung Hilfen zur Rechtsauslegung bereitzustellen. Die Datenschutzbeauftragten in Unternehmen und Behörden spielen eine bedeutende Rolle für den gelebten Datenschutz vor Ort.

Auch im Bereich der Selbstregulierungsinstrumente wie Verhaltensregeln (Codes of Conduct) oder Zertifizierungen sind Fortschritte zu verzeichnen. Wo Auslegungsfragen strittig sind, entscheiden Gerichte – teilweise in mehreren Instanzen bis zur **endgültigen Klärung durch den Europäischen Gerichtshof**.

Unsere Bewertung fällt positiv aus: **Die Datenschutz-Grundverordnung funktioniert.** Sie ist ein probates Mittel, um die Verarbeitung personenbezogener Daten zu ermöglichen und gleichzeitig die Grundrechte zu schützen. So hat sich die DSGVO zu einem bewährten Maßstab entwickelt, der auch international nachgefragt wird.

In der Zeit vor der DSGVO gab es allerdings auch **kein Datenschutz-Vakuum**. Seit 1995 war die EU-Datenschutzrichtlinie 95/46/EG in Kraft, die von den Mitgliedstaaten umzusetzen war. Dies geschah europaweit in verschiedener Art und Weise, auch wenn Grundregeln wie Betroffenenrechte oder Sicherheit – eigentlich ziemlich einheitlich – gesetzt waren. Für Deutschland waren insbesondere das Bundesdatenschutzgesetz (BDSG) und die Landesdatenschutzgesetze (LDSG) gemäß der EU-Datenschutzrichtlinie auszugestalten.

Der Landesgesetzgeber in Schleswig-Holstein hatte sich damals vom Landesbeauftragten für den Datenschutz beraten lassen, wie sich die Vorgaben der EU-Datenschutzrichtlinie in einer innovativen Form umsetzen ließen. So entstand das damalige Landesdatenschutzgesetz Schleswig-Holstein, das u. a. **Begriffe wie Selbstdatenschutz, das Konzept der Pseudonymisierung als Gestaltungsinstrument und Verfahren der Auditierung und Zertifizierung** kannte.

Zugegebenerweise waren nicht alle Personen, die im europäischen Gesetzgebungsprozess aktiv gewesen waren, von diesen **„innovativen Gesetzes-Add-ons“** begeistert. Wäre hier weniger mehr gewesen?

In der Tat kann man sich fragen, warum die möglichst weitgehende Vereinheitlichung der europäischen Datenschutzvorgaben nicht schon früher möglich gewesen war. Das lag nun nicht gerade am schleswig-holsteinischen Gesetz. Vielleicht war die **Zeit noch nicht reif**, und es mussten erst alle Mitgliedstaaten Erfahrungen sammeln und in der Artikel-29-Datenschutzgruppe (dem Vorläufer des Europäischen Datenschutzausschusses) die Zusammenarbeit und einheitliche Bewertung einüben.

Das LDSG Schleswig-Holstein hatte jedenfalls **Maßstäbe gesetzt**, die in der Praxis erprobt werden konnten und – das ist jedenfalls unsere Überzeugung – dadurch wiederum Einfluss auf den Gesetzgebungsprozess der Datenschutz-Grundverordnung hatten. Besonders bei der **Zertifizierung** war der Landesgesetzgeber **Schleswig-Holstein Impulsgeber**, aber auch in anderer Hinsicht – beispielsweise mit stärkerer Orientierung zu Datenschutz durch (Technik-)Gestaltung konnten Regelungen aus dem LDSG Schleswig-Holstein und dem BDSG ein kleines bisschen Vorbild sein.

Doch die Zeiten ändern sich: Das damalige LDSG Schleswig-Holstein war ein Leuchtturm in der Datenschutzgesetzgebung, um einige Instrumente zu zeigen und zu erproben, die möglicherweise für den großen Maßstab sinnvoll sind. Jetzt allerdings muss das **Ziel die Vereinheitlichung** sein. Leuchttürme sind wichtig, doch es ist auch wichtig, dass sie den Weg für alle leuchten.

Übersetzt auf das Datenschutzrecht und die Umsetzung der Verarbeitung in Organisation und Technik bedeutet dies: Wir brauchen eine **Kompatibilität der rechtlichen Grundlagen** – das leistet die DSGVO – und des darauf aufbauenden gelebten Datenschutzes. Das gilt zumindest für alle Verarbeitungen, die Länder- und

Staatengrenzen überschreiten: Abweichungen in den Formulierungen der Normen in den verschiedenen Regionen können es den Rechtsanwenderinnen und -anwendern schwer machen, ihren Pflichten nachzukommen.

Leuchttürme: ja. Aber nach Möglichkeit die Praxisprobleme in Anwendung und Aufsicht mitdenken.

1.2 Zahlen und Fakten zum Jahr 2023

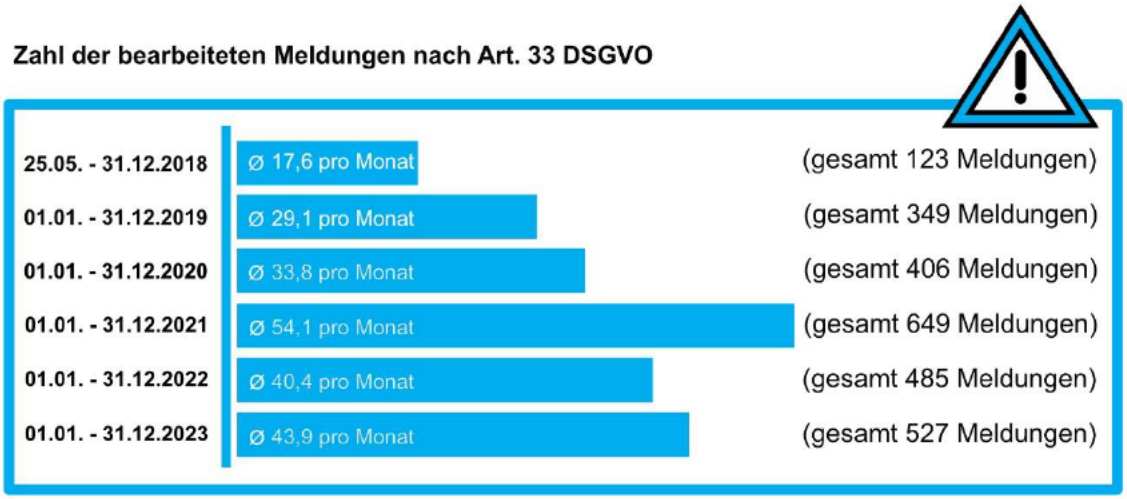
Die Zahl der Beschwerden hat sich im Jahr 2023 auf einem recht hohen Niveau eingependelt, die Zahlen sind denen aus 2022 sehr ähnlich (41. TB, Tz. 1.2). Die Besonderheiten der Corona-Zeit sind nun wohl vorbei. Die Zahl der gemeldeten Datenpannen steigt jedoch wieder, auch wenn der Spitzenwert aus dem Jahr 2021 noch nicht wieder erreicht wurde. Dies liegt nach unserer Beobachtung daran, dass im Jahr 2021 zahlreiche Verantwortliche von gleichartigen Angriffen und Problemen in Bezug auf die von ihnen eingesetzte Technik betroffen waren und es daher zu Massenmeldungen in ähnlichen Konstellationen kam (40. TB, Tz. 6.3.3).

Im Folgenden sind die genauen Zahlen dargestellt:

2023 erreichten uns 1.344 schriftliche **Beschwerden** (Vorjahr: 1.334), von denen 284 (Vorjahr: 259) 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 1.060 (Vorjahr: 1.075) Beschwerden bearbeitet,

Zahl der bearbeiteten Beschwerden im Jahr 2023



davon richteten sich **mehr als zwei Drittel der Beschwerden gegen Unternehmen** und andere nichtöffentliche Stellen (799; Vorjahr: 757), der Rest gegen Behörden (261; Vorjahr: 318). Dazu kamen 570 (Vorjahr: 498) Beratungen für den öffentlichen und den nichtöffentlichen Bereich.

Ohne vorherige Beschwerde wurden eine (Vorjahr: 5) **Prüfung** im öffentlichen und zwei **Prüfungen** (Vorjahr: 5) im nichtöffentlichen Bereich begonnen und neue Verfahren eingeleitet; zahlreiche Prüfungen aus dem Vorjahr wurden **fortgeführt**.

Die Zahl von 527 (Vorjahr: 485) **gemeldeten Verletzungen des Schutzes personenbezogener Daten** nach Artikel 33 DSGVO, § 41 LDSG oder § 65 BDSG in Verbindung mit § 500 StPO (Datenpannen) ist im Vergleich zum Vorjahr wieder gestiegen, hat jedoch nicht den Stand aus dem Jahr 2021 mit den massenhaften Sicherheitsvorfällen aufgrund einiger Angriffswellen erreicht.

Diese Zahl zeigt, dass vielen Verantwortlichen ihre Pflicht zur Meldung des Schutzes personenbezogener Daten bekannt ist. Dennoch gibt es eine Dunkelziffer von Datenpannen, bei denen die Verantwortlichen der Meldepflicht nicht nachgekommen sind. Dies kann mit Unkenntnis oder Fehleinschätzungen zusammenhängen. Manchmal liegt es auch am Auftragsverarbeiter, der selbst seine Pflicht, seinen Auftraggeber – d. h. den datenschutzrechtlichen Verantwortlichen – zu informieren, vernachlässigt hat (Tz. 4.6.5).

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

- 28 Warnungen (Vorjahr: 21),
- 7 Verwarnungen (Vorjahr: 30),
- eine Anordnung zur Änderung oder Einschränkung der Verarbeitung (Vorjahr: 1),
- keine Geldbuße (Vorjahr: 2).

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 zwölf (Vorjahr: 12) neuen Gesetzgebungsvorhaben; einige Themen aus Gesetzgebungsvorhaben des Vorjahres wurden auch im Berichtsjahr weiterverfolgt.

1.3 Schritte zur Evaluation und Anpassung der Gesetze zu Datenschutz und Informationsfreiheit

In den vorherigen Tätigkeitsberichten hatten wir auf die **Evaluierungsklauseln in einigen Gesetzen zu Datenschutz und Informationsfreiheit** hingewiesen (40. TB, Tz. 1.4; 41. TB, Tz. 1.3) und von der Evaluierung zum Bundesdatenschutzgesetz im Jahr 2021 berichtet, die auf die Evaluierung der DSGVO im Jahr 2020 (39. TB, Tz. 1.4) folgte.

Es gibt im Vergleich zum Vorjahr insoweit einen neuen Stand, als wir erfahren haben, dass sich die zuständigen Stellen mit den Anpassungsbedarfen des LDSG und des Informationszugangsgesetzes (IZG-SH) beschäftigen. Während das IZG-SH wohl demnächst einer Evaluierung unterzogen werden soll, wird beim LDSG noch die Reform auf Bundesebene beobachtet und abgewartet. Dies ist auch aus unserer Sicht vernünftig.

Was ist zu tun?

Wir haben unsere Unterstützung beim Herausarbeiten der Anpassungsbedarfe sowohl beim LDSG als auch beim IZG-SH angeboten.

1.4 Alle 17 Jahre …

… übernimmt **Schleswig-Holstein den Vorsitz** in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, auch Datenschutzkonferenz oder DSK genannt. Die DSK besteht aus den unabhängigen Datenschutzbehörden des Bundes und der Länder.

Datenschutzkonferenz

Die Datenschutzkonferenz 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.

Die Reihenfolge des Vorsitzes richtet sich grundsätzlich **nach dem Alphabet** – mit Ausnahmen. So ist die Zahl „17 Jahre“ auch nicht ganz exakt. Das liegt daran, dass bei der Planung der Reihenfolge der Vorsitze berücksichtigt wird, dass der DSK-Vorsitz nicht im Vorsitzjahr aus dem Amt als Landes- oder Bundesbeauftragte(r) scheiden soll. Außerdem sollte sie oder er ausreichende Erfahrung im Zusammenspiel der DSK-Mitglieder (also der Datenschutzaufsichtsbehörden) mitbringen, denn **der Vorsitz vertritt die DSK nach außen**. Und nicht überraschend: Dienststellen ohne gewählte(n) und ernannte(n) Landes- oder Bundesbeauftragte(n) für Datenschutz werden ebenfalls in der Planung ausgespart.

Für das Jahr 2023 war Schleswig-Holstein dran und hat gern den **Staffelstab vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit**, Vorsitz im Jahr 2022, übernommen.

Die Anforderungen an den Vorsitz waren im Jahr 2023 so hoch wie selten zuvor. In Zahlen zu den Aufgaben, die wir erfüllt haben:

- Leitung von neun Konferenzen (zwei Hauptkonferenzen, zwei Vorkonferenzen, drei Zwischenkonferenzen, zwei Austauschtreffen mit den spezifischen Aufsichtsbehörden),
- Leitung von 40 Jour fixes (das sind die beinahe wöchentlich stattfindenden Online-Konferenzen der Leitungen aller DSK-Mitglieder),
- Durchführung von 26 Umlaufverfahren,
- Erarbeitung und Finalisierung von fünf Entschließungen, vier Beschlüssen, zwölf Stellungnahmen und elf Pressemitteilungen der DSK sowie
- Bearbeitung zahlreicher Anfragen zu Auffassungen oder Materialien der DSK.

Die veröffentlichten Ergebnisse haben wir in Tz. 2.1 zusammengestellt. Hinzu kamen zahlreiche fachliche **Gespräche und Austausche** insbesondere mit Parlamentarierinnen und Parlamentariern, den Bund-Länder-Konferenzen in den Bereichen Bildung, Inneres und Justiz sowie Treffen mit Vertreterinnen und Vertretern aus dem BvD (Berufsverband der Datenschutzbeauftragten Deutschlands) e. V., dem DVD (Deutsche Vereinigung für Datenschutz) e. V. sowie dem GDD (Gesellschaft für Datenschutz und Datensicherheit) e. V.

Neu war im Jahr 2023, wie häufig der Vorsitz der DSK von Landes- oder Bundesministerien um unter allen Mitgliedern abgestimmte Positionen zu länderübergreifenden Verarbeitungen – z. B. die Umsetzung des Studierenden-Energiepreispauschalengesetzes (EPPSG) – oder für Deutschland geplanten Gesetzesvorhaben – z. B. das Gesundheitsdatennutzungsgesetz oder die BDSG-Reform – gebeten wurde. Für solche **gemeinsamen Stellungnahmen** ist zumeist nicht viel Zeit, alles muss schnell gehen. Aber diese Gelegenheiten nutzen wir gern.

1.5 Abgestimmte Position der DSK – nur auf Basis derselben Informationen

Für **gemeinsame Positionierungen** ist notwendig, dass alle Datenschutzaufsichtsbehörden über dieselben Informationen verfügen, um auch dieselben Sachverhalte bewerten zu können. Diese Selbstverständlichkeit konnten wir leider zum Start unseres DSK-Vorsitzes nicht voraussetzen:

Wir wurden nämlich im Januar 2023 als Vorsitz der DSK gebeten, zum EPPSG-Verfahren (Umsetzung des Studierenden-Energiepreispauschalengesetzes) eine abgestimmte Position in der DSK herbeizuführen und den Anfragenden mitzuteilen. Dazu erhielten wir in Schleswig-Holstein auch einige Dokumente. Es stellte sich heraus, dass andere Aufsichtsbehörden bereits **früher über Teilinformationen zur geplanten Verarbeitung** verfügten; es gab sogar schon erste Stellungnahmen einzelner Behörden gegenüber ihren zuständigen Ministerien. Andere Aufsichtsbehörden wurden in etwa zeitgleich mit bestimmen Dokumenten über die Verarbeitung versorgt, wieder andere wurden gar nicht angesprochen und hatten auch keinen Zugang zu den Materialien.

Kein Problem, so dachten wir, dann stimmen wir die gemeinsame Positionierung auf Basis der den DSK-Mitgliedern zusammen mit der Bitte um Stellungnahme übersandten und teilweise aktualisierten Informationen ab. Doch das gestaltete sich schwierig, weil diejenigen Aufsichtsbehörden, die von ihren zuständigen Ministerien mit den meisten oder neuesten (?) Materialien versorgt worden waren, die Unterlagen gar nicht weitergeben durften. Diese DSK-Mitglieder informierten die Kolleginnen und Kollegen, dass sie **bedauerlicherweise keine Freigabe zur Weitergabe erhalten hätten, da ihr Ministerium nicht Urheber dieser Dokumente sei und sich damit nicht in der Lage sehe, eine Freigabe zu erteilen**.

Das wäre dann kein Problem gewesen, wenn alle Datenschutzaufsichtsbehörden der Länder einzeln dieselben Dokumente von ihren jeweiligen Ministerien erhalten hätten. Was für ein **Aufwand**! Wir mussten zunächst versuchen, die Dokumente zum zu beurteilenden Stand herauszufiltern und Aktuelles von Veraltetem zu unterscheiden. Dies kann sogar eine unlösbare Aufgabe sein, denn diejenigen mit den aktuellen Dokumenten hatten ja gerade keine Freigabe zum Teilen dieser Materialien innerhalb der DSK und durften daher auch inhaltliche Informationen nicht weitergeben.

Es ist eine unbefriedigende Situation, wenn der DSK-Vorsitz als zentrale Ansprechstelle um eine gemeinsame Stellungnahme der DSK angefragt wird und dies auch gerne leisten möchte, doch **die grundlegenden Dokumente nicht einheitlich zur Verfügung gestellt** werden. In diesem Fall war es sogar noch schwieriger, weil die einzelnen Aufsichtsbehörden anfangs von unterschiedlichen – nämlich so, wie es ihnen gegenüber von den Länderbehörden mitgeteilt worden war – Sachverhalten der Verarbeitung personenbezogener Daten ausgehen mussten. Wo beispielsweise die einen Datenschutzaufsichtsbehörden Lücken in den Konzepten monieren wollten, lagen anderen dazu bereits Texte, teils in verschiedenen Fassungen, vor.

Erst **nach einiger Zeit(verschwendung)** erhielt schließlich eine Landesdatenschutzbehörde die Genehmigung aus dem zuständigen Ministerium ihres Landes, die (jedenfalls zu dem Zeitpunkt aktuellen) Dokumente innerhalb der DSK weiterzuleiten. Mittlerweile waren wohl die Fragen der Urheberrechte auch in Bezug auf die zur Erstellung der Konzepte und Materialien einbezogene Anwaltskanzlei geklärt worden.

Ende gut, alles gut? Nein, denn auch dieser Informationsstand war offensichtlich parallel weitergeschrieben worden, sodass die Stellungnahme der DSK **nicht die allerletzten Änderungen** im Konzept einbeziehen konnte, die zu dem Zeitpunkt durchaus hätten mitgeteilt werden können. Die an die Ministerien abgegebene Stellungnahme war also schon wieder in einigen Teilen überholt.

Wir werden jedenfalls jetzt zur **Bedingung** machen, dass diejenigen, unter denen eine abgestimmte Position herbeigeführt wird, auch **auf dieselben Materialien zurückgreifen** können und denselben Informationsstand erhalten.

Was ist zu tun?

Wenn geplant ist, abgestimmte Positionen von der DSK einzuholen, sollten die dafür benötigten Informationen einheitlich und für alle Beteiligten zu diesem Zweck verwendbar zur Verfügung gestellt werden. Dies ist auch effizienter, als Stellungnahmen einzelner Behörden mit unterschiedlichem Informationsstand einzuholen.

1.6 Die Datenschutzkonferenz wird institutionalisiert

In Tz. 1.4 haben wir berichtet, dass Schleswig-Holstein im Jahr 2023 Vorsitz der Datenschutzkonferenz (DSK) war, und auch die Aufgaben dargestellt. Hier plant der Bundesgesetzgeber eine Änderung: Die **Datenschutzkonferenz soll institutionalisiert** werden. Das war bereits eine Vorgabe im Koalitionsvertrag:

Aus dem Koalitionsvertrag 2021-2025:

Zur besseren Durchsetzung und Kohärenz des Datenschutzes verstärken wir die europäische Zusammenarbeit, institutionalisieren die Datenschutzkonferenz im Bundesdatenschutzgesetz (BDSG) und wollen ihr rechtlich, wo möglich, verbindliche Beschlüsse ermöglichen.

Diese Gesetzesänderung würde dazu führen, dass die Datenschutzkonferenz – anders als bisher – zu einem Gremium mit **„Pflichtmitgliedschaft" der unabhängigen Datenschutzaufsichtsbehörden** wird. Das kann man so regeln. Die Vorgabe einer Geschäftsordnung würde nichts Neues bringen, denn es gibt eine solche schon seit vielen Jahren. Interessant ist vielmehr, was nicht im BDSG-Entwurf geregelt ist, aber aus Sicht der (bisherigen) DSK im Gesetz aufgenommen werden sollte: die dringend nötige organisatorische Unterstützung der Harmonisierungsmaßnahmen im Sinne einer einheitlichen Rechtsanwendung durch eine **Geschäftsstelle**. Diese Geschäftsstelle soll das **organisatorische Fundament** der Datenschutzkonferenz darstellen. Gerade angesichts der steigenden Erwartungen an die DSK wird die Geschäftsstelle benötigt, um eine einheitliche Anwendung des Datenschutzrechts zu erreichen. Die Stellungnahmen der DSK zum BDSG-Entwurf sind hier verfügbar:

https://www.datenschutzkonferenz-online.de/stellungnahmen.html

Kurzlink: *https://uldsh.de/tb42-1-6a*

Vorschlag für einen neuen § 16a im BDSG-Entwurf:

Die Aufsichtsbehörden des Bundes und der Länder im Sinne des § 18 Abs. 1 Satz 1 bilden die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz). Die Datenschutzkonferenz gibt sich eine Geschäftsordnung.

Was ist zu tun?

Als DSK-Vorsitz im Jahr 2023 haben wir einen großen Wunsch für die Zukunft: 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 2023

Datenschutz in der Forschung durch einheitliche Maßstäbe

Anwendungshinweise zum Angemessenheitsbeschluss „EU-US Data Privacy Framework"

Chatkontrolle

2 Datenschutz und Informationsfreiheit – global und national

Datenschutz und Informationsfreiheit sind selbstverständlich nicht nur Landesthemen. Als Sprecherin der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder galt es für die Landesbeauftragte für Datenschutz Schleswig-Holstein, in besonderem Maße auch die nationalen, europäischen und internationalen Entwicklungen im Blick zu haben. Wichtige Ergebnisse der Arbeit über die Landesgrenzen hinweg und kommende Aufgaben werden im Folgenden vorgestellt.

2.1 Die Ergebnisse der DSK im Jahr 2023 im Überblick

Wir waren als Vorsitz der DSK für die Abstimmung und Veröffentlichung zahlreicher Positionierungen der Datenschutzkonferenz zuständig. Die folgende Liste umfasst die veröffentlichten Ergebnisse und illustriert damit die **Vielfalt der Themen**:

- 18.01.2023: Stellungnahme zu Grundsatzfragen zur Sanktionierung von Datenschutzverstößen von Unternehmen – EuGH-Rechtssache C-807/21

  https://www.datenschutzkonferenz-online.de/stellungnahmen.html

  Kurzlink: *https://uldsh.de/tb42-2-1a*

- 03.02.2023: Beschluss „Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten"

  https://www.datenschutzkonferenz-online.de/media/dskb/20230206_DSK_Beschluss_Extraterritoriale_Zugriffe.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1b*

- 27.03.2023: Stellungnahme zum Europäischen Gesundheitsdatenraum bei der Nutzung von Gesundheitsdaten

  https://www.datenschutzkonferenz-online.de/media/st/2023-03-27_DSK-Stellungnahme_EHDS.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1c*

- 29.03.2023: Beschluss „Bewertung von Pur-Abo-Modellen auf Websites"

  https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1d*

- 10.05.2023: Relaunch von YoungData, dem Jugendportal zum Thema Datenschutz und Informationsfreiheit (Tz. 4.8.1)

  https://youngdata.de/

  Kurzlink: *https://uldsh.de/tb42-2-1e*

- 11.05.2023: Stellungnahme „Daten der Verbraucherinnen und Verbraucher beim Einsatz von Smart Meter zur Erfassung des Kaltwasserverbrauchs durch einheitliche Regelungen schützen"

  https://www.datenschutzkonferenz-online.de/media/st/2023-05-11_DSK-Stellungnahme_Funkwasserzaehler.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1f*

- 11.05.2023: Stellungnahme „Handlungsempfehlungen an die Bundesregierung zur Verbesserung des Datenschutzes bei Scoringverfahren"

https://www.datenschutzkonferenz-online.de/media/st/DSK-Handlungsempfehlungen_Verbesserung_des_Datenschutzes_bei_Scoringverfahren.pdf

Kurzlink: *https://uldsh.de/tb42-2-1g*

- 11.05.2023: Entschließung „Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz!" (Tz. 2.3)

  https://www.datenschutzkonferenz-online.de/media/en/2023-05-11_DSK-Entschliessung_Beschaeftigtendatenschutz.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1h*

- 11.05.2023: Entschließung „Verfassungsrechtliche Anforderungen bei automatisierter Datenanalyse durch Polizei und Nachrichtendienste beachten"

  https://www.datenschutzkonferenz-online.de/media/en/2023-05-11_DSK-Entschliessung_Datenanalyse-Polizei.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1i*

- 11.05.2023: Positionspapier „Kriterien für Souveräne Clouds" (Tz. 6.2.4)

  https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kriterien-Souv-Clouds.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1j*

- 21.06.2023: Stellungnahme zum politischen Targeting

  https://www.datenschutzkonferenz-online.de/media/st/23-06-21_DSK-Stellungnahme_Politisches-Targeting.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1k*

- 21.06.2023: Stellungnahme zum politischen Targeting (English Version)

  https://www.datenschutzkonferenz-online.de/media/st/23-06-21_DSK-Opinion_Political-Targeting_EN.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1l*

- 11.07.2023: Stellungnahme zum Referentenentwurf des BMDV zur Rechtsverordnung nach § 26 Abs. 2 TTDSG

  https://www.datenschutzkonferenz-online.de/media/st/23-07-11_DSK-Stellungnahme_Einwilligungsverwaltung_TTDSG.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1m*

- 10.08.2023: Stellungnahme der unabhängigen Datenschutzaufsichtsbehörden der Länder zu Artikel 5 des Referentenentwurfs eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten

  https://www.datenschutzkonferenz-online.de/media/st/23_08_10_Datenschutzaufsicht-Laender-zu-Art_5_GDNG-E.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1n*

- 14.08.2023: Stellungnahme der DSK zum Referentenentwurf des Bundesministeriums für Gesundheit: Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten

  https://www.datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1o*

- 01.09.2023: Stellungnahme der DSK zum Entwurf der Europäischen Kommission: Verordnung des Europäischen Parlaments und des Rates zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679 COM(2023) 348 final

  https://www.datenschutzkonferenz-online.de/media/st/2023_09_01_DSK_Stellungnahme_KOM_E_VVO.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1p*

- 04.09.2023: Übermittlung personenbezogener Daten aus Europa an die USA – Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023 (Tz. 2.4)

  https://www.datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1q*

- 06.09.2023: Stellungnahme der DSK zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes mit Stand 9.8.2023

  https://www.datenschutzkonferenz-online.de/media/st/23_09_06_DSK_Stellungnahme_BDSG.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1r*

- 06.09.2023: Stellungnahme der unabhängigen Datenschutzaufsichtsbehörden der Länder zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes mit Stand 9.8.2023

  https://www.datenschutzkonferenz-online.de/media/st/23_09_06_Laender_Stellungnahme_BDSG.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1s*

- 27.09.2023: Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten

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

  Kurzlink: *https://uldsh.de/tb42-2-1t*

- 17.10.2023: Entschließung „Geplante Chatkontrolle führt zu einer unverhältnismäßigen, anlasslosen Massenüberwachung!" (Tz. 2.5)

  https://www.datenschutzkonferenz-online.de/media/en/20231017DSK EntschliessungChatkontrolle.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1u*

- 06.11.2023: Positionspapier zu cloudbasierten digitalen Gesundheitsanwendungen

  https://www.datenschutzkonferenz-online.de/media/dskb/2023_11_06_Beschluss_cloudbasierte_digitale_Gesundheitsanwendungen.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1v*

- 23.11.2023: Entschließung „Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register"

  https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_medRegister.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1w*

- 23.11.2023: Entschließung: „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken" (Tz. 2.2)

  https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_DS.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1x*

- 23.11.2023: Anwendungshinweise „Kernelemente der Überwachungsaufgaben von Überwachungsstellen für Verhaltensregeln nach Artikel 40 DS-GVO"

  https://www.datenschutzkonferenz-online.de/media/ah/2023-11-23_DSK_Anwendungshinweise_CoC-Ueberwachungsstellen.pdf

  Kurzlink: *https://uldsh.de/tb42-2-1y*

2.2 Datenschutz in der Gesundheitsforschung – besser mit einheitlichen Maßstäben

Forschung braucht den Austausch, Forschung endet oft nicht an den Grenzen eines Bundeslands. Gerade im Medizinbereich sind **länderübergreifende Verbundforschung und multizentrische Studien** keine Seltenheit. Doch zurzeit müssen je nach Forschungsstandort **unterschiedliche datenschutzrechtliche Anforderungen** beachtet werden. Das macht es für alle Beteiligten schwierig und kann sogar zu Nachteilen für die betroffenen Personen führen.

Von Vorteil für alle wären **aufeinander abgestimmte gesetzliche Regelungen auf hohem Datenschutzniveau** (siehe auch Tz. 1.1 zur Kompatibilität der rechtlichen Grundlagen). Dadurch ließe sich der Datenschutz in der länderübergreifenden Forschung stärken – und die Forschenden sähen sich keiner für sie oft unverständlichen Komplexität ausgesetzt.

Weil das Thema so wichtig ist, hatte sich die DSK bereits im Jahr 2022 damit beschäftigt, wie sich die **Anforderungen der Forschung mit dem Datenschutzrecht verbinden** lassen (41. TB, Tz. 2.4). Die Ergebnisse sind hier bereitgestellt worden:

Entschließung der DSK vom 23.03.2022: **„Wissenschaftliche Forschung – selbstverständlich mit Datenschutz“:**

https://www.datenschutzkonferenz-online.de/media/en/DSK_6_Entschliessung_zur_wissenschaftlichen_Forschung_final.pdf

Kurzlink: *https://uldsh.de/tb42-2-2a*

Entschließung der DSK vom 24.11.2022: **„Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung“:**

https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf

Kurzlink: *https://uldsh.de/tb42-2-2b*

Im Jahr 2023 hat die Datenschutzkonferenz die **bestehenden Forschungsregelungen** in den Landeskrankenhausgesetzen sowie den Datenschutzgesetzen von Bund und Ländern **ausgewertet** und auf dieser Basis **Eckpunkte** erarbeitet, um eine weitgehende Nutzung von Gesundheitsdaten zu Forschungszwecken im Einklang mit den Grundrechten zu normieren. Dazu müssen konkrete Garantien und Maßnahmen gesetzlich festgelegt werden.

Es gilt der Grundsatz:

Je höher der Schutz der betroffenen Personen durch geeignete Garantien und Maßnahmen, desto umfangreicher und spezifischer können die Daten zu Forschungszwecken genutzt werden.

In den erarbeiteten Eckpunkten weist die Datenschutzkonferenz darauf hin, dass zwischen den **verschiedenen Datenarten** unterschieden werden solle (z. B. personenbezogenen Daten (Art. 4 Nr. 1 DSGVO), Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) oder genetischen Daten (Art. 4 Nr. 13 DSGVO)). Soweit für besondere Forschungsgegenstände eine ausreichende Anonymisierung nicht gewährleistet werden kann (etwa für radiologische Bilddaten), sollten spezifische Regelungen getroffen werden, um einen angemessenen Schutz der Grundrechte der betroffenen Personen zu gewährleisten, z. B. durch **zusätzliche technische und organisatorische Maßnahmen**.

Darüber hinaus sind die Regelungen des Art. 9 Abs. 2 Buchst. j in Verbindung mit Art. 89 Abs. 1 DSGVO zu beachten. **Im Gesetz selbst** müssen **angemessene und spezifische Maßnahmen** zur Wahrung der Grundrechte und Interessen der betroffenen Personen festgelegt werden. Angemessene und spezifische Maßnahmen in diesem Sinne können etwa sein:

- Vorgaben für die Datenschutz-Folgenabschätzung (z. B. Betrachtungstiefe, Aufgabenzuweisungen für die Durchführung),
- die Schaffung weiterer, über die in Artikel 15 ff. DSGVO hinausgehender Betroffenenrechte (z. B. spezifische Widerspruchsrechte, Vernichtung von Bioproben),
- die Festlegung angemessener Sperrfristen, die den betroffenen Personen ermöglichen, ihre Rechte auszuüben, bevor mit ihren Daten geforscht werden darf (z. B. bei einem Widerspruchsrecht),
- die Einbindung einer unabhängigen Treuhandstelle insbesondere zur Verschlüsselung, Anonymisierung oder Pseudonymisierung der Daten,
- die Einrichtung von Datenintegrationszentren oder Forschungsplattformen, soweit konkrete, der DSGVO entsprechende Anforderungen an deren Ausgestaltung formuliert werden,
- die Verpflichtung beteiligter Stellen zur Verschwiegenheit und die Schaffung korrespondierender Prozessrechte wie ein Beschlagnahmeverbot und Zeugnisverweigerungsrechte,
- konkrete Festlegungen zur Ausgestaltung und Gewährleistung der Datenminimierung.

In bestimmten Fallkonstellationen unterliegen medizinische personenbezogene Daten dem **absoluten Schutz des Kernbereichs privater Lebensgestaltung**. Die DSK weist darauf hin, dass die Verarbeitung solcher menschenwürderelevanten Daten selbst zu Forschungszwecken nicht auf Grundlage einer gesetzlichen Regelung legitimiert werden kann.

Wesentlich ist zudem eine **uneingeschränkte Datenschutzaufsicht** in dem sensiblen Bereich der Verarbeitung von Gesundheitsdaten.

All dies sind Eckpunkte, mit denen sich rechtssicher ein hohes Datenschutzniveau in der medizinischen Forschung erreichen lässt – und zwar durch eine aufeinander abgestimmte zeitnahe rechtsklare und systematische Neustrukturierung der entsprechenden rechtlichen Regelungen.

Die Datenschutzaufsichtsbehörden bieten an, in Wahrnehmung ihrer Beratungsfunktion die Gesetzgeber vor und bei entsprechenden Gesetzesvorhaben zu unterstützen.

Entschließung der DSK vom 23.11.2023:

„Datenschutz in der Forschung durch einheitliche Maßstäbe stärken“:

https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_DS.pdf

Kurzlink: *https://uldsh.de/tb42-2-2c*

Was ist zu tun?

In der Gesundheitsforschung wäre eine Vereinheitlichung der rechtlichen Anforderungen auf hohem Datenschutzniveau von Vorteil. Ebenso wie die anderen Datenschutzaufsichtsbehörden in der DSK stehen wir gern zur Beratung und Unterstützung des Gesetzgebers zur Verfügung.

2.3 Beschäftigtendatenschutz – Fortschritte bisher nur hinter den Kulissen?

Kommt es oder kommt es nicht, das **Beschäftigtendatenschutzgesetz**? Die Datenschutzkonferenz hatte dies immer wieder gefordert und dem Gesetzgeber auch Unterstützung angeboten. Schließlich war das Thema auch im Koalitionsvertrag der Bundesregierung behandelt worden.

> **Aus dem Koalitionsvertrag 2021-2025 auf Bundesebene (Seite 17):**
>
> Wir schaffen **Regelungen zum Beschäftigtendatenschutz**, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen.

Wir berichteten bereits über die Entwicklungen der letzten Jahre (41. TB, Tz. 2.2), z. B. über die beim Bundesministerium für Arbeit und Soziales (BMA) zur Fortentwicklung des Beschäftigtendatenschutzes eingerichtete **unabhängige und interdisziplinäre Expertenkommission**, die im Januar 2022 Thesen und Empfehlungen vorgelegt hatte (40. TB, Tz. 2.6). Die Landesbeauftragte für Datenschutz Schleswig-Holstein hatte als vom Bundesarbeitsminister berufenes Beiratsmitglied an den Ergebnissen mitgearbeitet (39. TB, Tz. 2.4).

Thesen und Empfehlungen der Expertenkommission (Januar 2022):

https://www.bmas.de/SharedDocs/Downloads/DE/Arbeitsrecht/ergebnisse-beirat-beschaeftigtendatenschutz.pdf

Kurzlink: *https://uldsh.de/tb42-2-3a*

Im Jahr 2023 war ein wenig Bewegung wahrnehmbar. Zum einen hatte der **EuGH** am 30.03.2023 in der Rechtssache C-34/21 über die Anforderungen an eine europarechtskonforme Umsetzung des Beschäftigtendatenschutzrechts in Hessen entschieden. Zum anderen legten im April 2023 **das BMAS und das Bundesministerium des Innern und für Heimat (BMI) gemeinsam ein Eckpunktepapier** mit Vorschlägen zum modernen Beschäftigtendatenschutz vor:

BMAS/BMI: Vorschläge für einen modernen Beschäftigtendatenschutz (April 2023):

https://www.denkfabrik-bmas.de/fileadmin/Downloads/Publikationen/Vorschlaege_fuer_einen_modernen_Beschaeftigtendatenschutz.pdf

Kurzlink: *https://uldsh.de/tb42-2-3b*

In Dialogrunden, die BMAS und BMI mit mehreren Stakeholdern führten, waren auch DSK-Mitglieder eingeladen gewesen, um diese Eckpunkte weiter zu diskutieren. Eigentlich war die Rede davon gewesen, dass bis Ende 2023 ein Entwurf für ein Beschäftigtendatenschutzgesetz vorgelegt würde. Dies scheint nun **auf 2024 verschoben** worden zu sein.

Daher soll an die letzten Entschließungen der DSK zum Beschäftigtendatenschutz erinnert werden:

Entschließung der DSK vom 29.04.2022: **„Die Zeit für ein Beschäftigtendatenschutzgesetz ist ‚Jetzt'!":**

https://datenschutzkonferenz-online.de/media/en/Entschliessung_Forderungen_zum_Beschaeftigtendatenschutz.pdf

Kurzlink: *https://uldsh.de/tb42-2-3c*

Entschließung der DSK vom 11.05.2023: **„Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz!":**

https://www.datenschutzkonferenz-online.de/media/en/2023-05-11_DSK-Entschliessung_Beschaeftigtendatenschutz.pdf

Kurzlink: *https://uldsh.de/tb42-2-3d*

Wir werden weiter berichten.

Was ist zu tun?

In unserer Praxis der Datenschutzaufsicht spielen Fragen des Beschäftigtendatenschutzes immer wieder eine Rolle. Ein Beschäftigtendatenschutzgesetz könnte insgesamt zur Rechtssicherheit für die Arbeiter- und für die Beschäftigtenseite beitragen. Wir nehmen gerne Stellung zu vorgelegten Gesetzentwürfen oder auch zu weiteren untergesetzlichen Ansätzen im Bereich des Beschäftigtendatenschutzes.

2.4 Anwendungshinweise zum Angemessenheitsbeschluss „EU-US Data Privacy Framework"

Wer erinnert sich noch an **„Safe Harbor"**? Oder an den **„Privacy Shield"**? Unter diesen Begriffen waren Angemessenheitsbeschlüsse der EU-Kommission für die USA bekannt. Dazu muss man wissen, dass ein Verantwortlicher nicht einfach so personenbezogene Daten ins Ausland transferieren darf. Zunächst einmal ist – wie üblich – eine Rechtsgrundlage nötig. Doch zusätzlich ist nötig, dass aufseiten der Empfänger der Daten ein gleichwertiges Datenschutzniveau garantiert wird. Dafür gibt es verschiedene Instrumente, beispielsweise den Angemessenheitsbeschluss.

> Die EU-Kommission kann in einem **Angemessenheitsbeschluss** für einen Staat die Gleichwertigkeit des Datenschutzniveaus mit Europa feststellen.

Der Transfer von personenbezogenen Daten aus Europa in die USA konnte auf diese Angemessenheitsbeschlüsse gestützt werden, bis der **EuGH** „Safe Harbor" im Jahr 2015 bzw. den Nachfolger „Privacy Shield" im Jahr 2020 **für ungültig erklärte**. Großer Kritikpunkt waren die weitreichenden Befugnisse für US-Sicherheitsbehörden, auf die übermittelten personenbezogenen Daten zuzugreifen.

Der Datentransfer in die USA war nach diesen Urteilen immer noch möglich, aber nur unter besonderen Bedingungen (39. TB, Tz. 2.5). Daher hatten die EU-Kommission und die USA die Verhandlungen erneut aufgenommen, um einen **neuen Angemessenheitsbeschluss** zu erreichen, der nun endlich den Kriterien des Datenschutzrechts und weiteren Gerichtsverfahren vor dem EuGH standhalten sollte.

Nach mehreren Jahren war es am 10.07.2023 so weit: Es gibt seitdem einen neuen Angemessenheitsbeschluss zum Datentransfer in die USA, der sich auf dem **„EU-US Data Privacy Framework"** gründet. Dazu erhielten wir ebenso wie die anderen Datenschutzaufsichtsbehörden in Deutschland viele Fragen von öffentlichen und nichtöffentlichen Stellen. Aus diesem Grund hat die Datenschutzkonferenz am 04.09.2023 **Anwendungshinweise** zu dem Angemessenheitsbeschluss zum EU-US Data Privacy Framework veröffentlicht:

https://datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf

Kurzlink: *https://uldsh.de/tb42-2-4a*

Diese Anwendungshinweise geben zunächst Informationen zum Datenschutz bei Drittlandsübermittlungen. Es folgen Informationen für die Datenexporteure, also die Verantwortlichen und Auftragsverarbeiter, die Daten in die USA übermitteln. In einem weiteren Teil der Anwendungshinweise erfahren betroffene Personen, welche Rechtsschutz- und Beschwerdemöglichkeiten sie haben.

Bleibt denn der Angemessenheitsbeschluss „EU-US Data Privacy Framework" gültig oder kann nun dasselbe passieren wie mit den Vorgängern „Safe Harbor" und „Privacy Shield"? Das ist eine offene Frage. Bei dem neuen Angemessenheitsbeschluss handelt es sich um **aktuell geltendes EU-Recht**. Aber das ist nicht in Stein gemeißelt: Neben den vorgesehenen Evaluationen durch die EU-Kommission, aus denen Anpassungen oder eine Aufhebung resultieren können, bestehen Möglichkeiten für eine gerichtliche Überprüfung des neuen Angemessenheitsbeschlusses.

2.5 EU-Pläne zur Chatkontrolle – Gefahr einer anlasslosen Massenüberwachung

Wieder einmal gibt es Vorschläge, die **Kommunikation im Internet überwachen** zu lassen und dafür die technischen Gegebenheiten zu schaffen, die insbesondere zu einer **Aufhebung von Ende-zu-Ende-Verschlüsselung** führen würden (38. TB, Tz. 2.3; 39. TB, Tz. 2.2). Dieses Mal war das Argument der Kinderschutz: Im Mai 2022 hat die EU-Kommission einen Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern – in Kurzform: „Chatkontrolle" – vorgelegt.

Chatkontrolle

Nach dem Vorschlag der EU-Kommission würden Anbieter von E-Mail-, Messenger- oder Chat-Diensten dazu verpflichtet, die Verbreitung von bekannten oder neuen Darstellungen sexuellen Kindesmissbrauchs oder die Kontaktaufnahme zu Kindern anhand bestimmter Indikatoren zu erkennen.

Selbstverständlich müssen Kinder vor sexuellem Missbrauch geschützt werden. Das hier **gewählte Mittel ist aber kritisch**, denn die digitale Kommunikation sämtlicher Nutzender wäre unterschiedslos und verdachtsunabhängig von einer Überwachung betroffen – und das über alle Lebensbereiche.

Das Gesetzesvorhaben würde von Anbietern verlangen, dass die mittlerweile für private Kommunikation weitgehend etablierte Ende-zu-Ende-Verschlüsselung aufgebrochen wird. Die **Sicherheit zu schwächen** ist aber keine gute Idee. Vor dem Einbauen absichtlicher Bruchstellen in die technischen Infrastrukturen ist zu warnen!

Wir haben gemeinsam mit den anderen DSK-Mitgliedern deutlich gemacht, dass es sich bei der vorgesehenen Chatkontrolle um eine **anlasslose Massenüberwachung** handelt, die nicht mit den Grundrechten auf Achtung des Privat- und Familienlebens, der Vertraulichkeit der Kommunikation und zum Schutz personenbezogener Daten vereinbar ist.

Entschließung der DSK vom 17.10.2023: **„Geplante Chatkontrolle führt zu einer unverhältnismäßigen, anlasslosen Massenüberwachung!":**

https://www.datenschutzkonferenz-online.de/media/en/20231017DSKEntschliessungChatkontrolle.pdf

Kurzlink: *https://uldsh.de/tb42-2-5a*

Nachtrag von Anfang 2024: Der Europäische Datenschutzausschuss hat sich am 13.02.2024 in einer Stellungnahme kritisch zu gesetzlichen Entwicklungen im Bereich der Chatkontrolle geäußert:

EDSA: **Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse:**

https://www.edpb.europa.eu/system/files/2024-02/edpb_statement_202401_proposal_regulation_prevent_combat_child_sexual_abuse_en.pdf

Kurzlink: *https://uldsh.de/tb42-2-5b*

Was ist zu tun?

Ende-zu-Ende-Verschlüsselung darf nicht torpediert werden. Zum Schutz der Kommunikation müssen die Infrastrukturen weiter abgesichert werden, statt die Sicherheit auszuhöhlen. Wo gesetzliche Eingriffe geplant werden, müssen diese verhältnismäßig sein – das ist bei einer anlasslosen Massenüberwachung eindeutig nicht der Fall.

2.6 Die neuen europäischen Digitalrechtsakte – und die DSGVO „bleibt unberührt"?

Es gab **so viele neue Gesetze mit Datenschutzbezug,** die im Jahr 2023 auf europäischer Ebene diskutiert und verhandelt wurden! Die Debatten waren wichtig, um noch rechtzeitig vor der Europawahl im Juni 2024 die Rechtsakte beschließen zu können.

Zu den neuen europäischen **Digitalrechtsakten** gehören insbesondere:

- Daten-Governance-Gesetz (**Data Governance Act – DGA**): am 23.06.2022 in Kraft getreten, anwendbar ab 24.09.2023,
- Gesetz über digitale Märkte (**Digital Markets Act – DMA**): am 01.11.2022 in Kraft getreten, anwendbar ab 02.05.2023,
- Gesetz über digitale Dienste (**Digital Services Act – DSA**): am 16.11.2022 in Kraft getreten, anwendbar ab 17.02.2024,
- Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (**NIS-2-Richtlinie**): am 16.01.2023 in Kraft getreten, in den Mitgliedstaaten umzusetzen bis zum 17.10.2024,
- Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen (Critical Entities Resilience Directive, **CER-Richtlinie**): am 16.01.2023 in Kraft getreten, in den Mitgliedstaaten umzusetzen bis zum 17.10.2024,
- Datengesetz (**Data Act – DA**): am 11.01.2024 in Kraft getreten, anwendbar ab 12.09.2025,
- **KI-Verordnung** (**Artificial Intelligence Act – AIA**): voraussichtlich im Frühjahr 2024 in Kraft, anwendbar zwei Jahre später (2026),
- Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (**Cyber Resilience Act – CRA**): voraussichtlich im Frühjahr 2024 in Kraft, anwendbar zwei Jahre später (2026),
- Europäischer Gesundheitsdatenraum (**European Health Data Space, EHDS**): voraussichtlich im Frühjahr 2024 in Kraft, zur Anwendbarkeit lagen zum Redaktionsschluss noch keine Informationen vor.

All diese Rechtsakte wirken sich auf die Digitalisierung aus. Die europäischen Verordnungen stehen **neben der DSGVO**. Die gute Nachricht: Damit ist klargestellt, dass die Datenschutz-Grundverordnung nicht verdrängt wird. So heißt es beispielsweise in neuen Regelungen: „Die Verordnung (EU) 2016/679 bleibt unberührt."

Aber es ist keine Überraschung, dass die **Komplexität für die Verarbeiter und für deren Datenschutzbeauftragte** steigt, wenn sie dafür einen Nachweis erbringen können sollen, dass sie nicht nur die datenschutzrechtlichen Anforderungen, sondern ebenfalls die zusätzlichen gesetzlichen Regelungen erfüllen. Auch die Datenschutzaufsichtsbehörden sind gefordert, wenn sie das Gesamtbild im Blick haben wollen.

Für die kommenden Monate und Jahre ist viel zu tun, um Verarbeitungen (auch) personenbezogener Daten zu prüfen und zu gestalten sowie die Verantwortlichen dahin gehend zu beraten, wie sie **rechtssichere Lösungen** erreichen können, die allen gesetzlichen Anforderungen gerecht werden.

Was ist zu tun?

Für die Datenschutzaufsichtsbehörden wird nicht nur die Abstimmung in der Datenschutzkonferenz weiterhin vonnöten sein, sondern es ist zumindest empfehlenswert, sich im Kreis der für verschiedene Aspekte der digitalen Verarbeitungen zuständigen Aufsichtsbehörden auszutauschen. Der nationale Gesetzgeber sollte dafür Sorge tragen, dass – wo nötig – die gebotene Zusammenarbeit auch gesetzlich abgesichert wird.

03

KERNPUNKTE

Datenschutzgremium

Service für Abgeordnete zu Datenschutz und Informationsfreiheit

3 Landtag

Die Landesbeauftragte für Datenschutz war im Berichtsjahr zu Gast bei den Sitzungen des Datenschutzgremiums des Schleswig-Holsteinischen Landtages (Tz. 3.1). Zusätzlich haben, wie auch in früheren Jahren, einige Abgeordnete den direkten Weg zur Landesbeauftragten für Datenschutz oder ihrer Dienststelle genutzt, um sich in konkreten Fällen oder zu allgemeineren Themen beraten zu lassen (Tz. 3.2).

3.1 Datenschutzgremium

Wie funktioniert Datenschutz im parlamentarischen Bereich? Im Schleswig-Holsteinischen Landtag gibt es seit vielen Jahren das Datenschutzgremium, das mehrfach im Jahr zusammenkommt, um eine Reihe von jeweils aktuellen Tagesordnungspunkten rund um den Datenschutz abzuarbeiten. 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/tb42-3-1a*

Basis für die Arbeit des Datenschutzgremiums ist die Datenschutzordnung:

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

Kurzlink: *https://uldsh.de/tb42-3-1b*

Die Datenschutzordnung wurde bereits im Jahr 1998, also lange vor Geltung der Datenschutz-Grundverordnung, erlassen. In dieser Zeit wurde die erste europäische Datenschutzreform mit der Datenschutz-Richtlinie 95/46/EG in nationales Recht umgesetzt. Über die Zeit gab es noch mehrere kleinere Änderungen, zuletzt im Februar 2018.

Wie bereits im Vorjahresbericht ausgeführt (41. TB, Tz. 3.1), könnte zu den Aufgaben des Datenschutzgremiums auch gehören, einen Vorschlag für eine Anpassung der rechtlichen Grundlagen auszuarbeiten, um die aufgrund der DSGVO veränderten Gegebenheiten zu berücksichtigen. So könnten Änderungen an der Datenschutzordnung durch den Landtag beschlossen werden.

Bei allen Änderungsvorschlägen sollten auch die Entscheidungen des EuGH und etwaige Auswirkungen auf den parlamentarischen Datenschutz in den Ländern im Blick behalten werden. Gerne bietet die Landesbeauftragte für Datenschutz ihre Unterstützung an.

3.2 Service für Abgeordnete in Fragen zu Datenschutz und Informationsfreiheit

Abgeordnete haben Bedarf an vielerlei Informationen zu allen möglichen Themen, die politisch relevant sind oder es werden können. Zwar verfügen die meisten Abgeordneten über ein Team und können sich auf bestimmte inhaltliche Bereiche spezialisieren, doch wenn dann noch die Querschnittsmaterien Datenschutz oder Informationsfreiheit hinzukommen, wünschen sich einige Abgeordnete kompetente Unterstützung. Aus diesem Grund steht die Landesbeauftragte für Datenschutz mit ihrem Team bereit, um den Abgeordneten als **Ansprechstelle für Datenschutz und Informationsfreiheit** zu dienen. Jede und jeder Abgeordnete kann sich vertrauensvoll an uns wenden und sich beraten lassen.

Die Fragen, die an uns herangetragen werden, sind vielfältig und ergeben sich aus der parlamentarischen Tätigkeit, aus Erlebnissen als Privatperson oder auch in Bezug auf die Fragen, Beschwerden oder Hinweise, die Bürgerinnen und Bürger an sie gerichtet haben.

Stets versuchen wir, zeitnah alle Fragen der Abgeordneten zu Datenschutz und Informationsfreiheit mit unserer juristischen oder auch informationstechnischen Expertise sowie auf Basis unserer Erfahrung in der Anwendung der Rechtsnormen zu beantworten und dem Beratungsbedarf im Rahmen unserer Ressourcen nachzukommen. Aus unserer Sicht ist dieser Austausch auch deswegen fruchtbar, weil er dazu beiträgt, Chancen und Risiken verschiedener Handlungsoptionen zu verstehen und vor allem praxistaugliche Lösungen für die jeweiligen Sachverhalte zu entwickeln.

§ 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; [...]

Was ist zu tun?

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

04

KERNPUNKTE

Luftbilder zur Gebührenberechnung

Veröffentlichung von Namen auf Websites der Verwaltung

Filmen von Polizeibeamten im Einsatz

Datenpannen in der Justiz

Patientendaten außer Kontrolle

Schülerakten auf dem Schulhof

4 Datenschutz in der Verwaltung

In diesem Kapitel werden Einzelfälle und sonstige Themen von herausgehobener Bedeutung im Jahr 2023 dargestellt, die den Bereichen „Allgemeine Verwaltung“ (Tz. 4.1), „Polizei“ (Tz. 4.2), „Justiz“ (Tz. 4.3), „Soziales“ (Tz. 4.4), „Schutz des Patientengeheimnisses“ (Tz. 4.5), „Datenpannen im Medizinbereich“ (Tz. 4.6), „Bildung“ (Tz. 4.7) sowie „Datenschutz- und Medienkompetenz“ (Tz. 4.8) zuzurechnen sind.

4.1 Allgemeine Verwaltung

4.1.1 Luftbilder zur Gebührenberechnung für die Niederschlagswasserentsorgung

Kommunen erheben für die Beseitigung von Niederschlagswasser Gebühren. Gebührenmaßstab für laufende Benutzungsgebühren ist die **Größe überbauter und befestigter Grundstücksflächen, etwa bituminöse Decken, Betondecken oder Pflasterungen**, von welchen das Niederschlagswasser in die öffentliche Abwasseranlage gelangt. Bei der Ermittlung der Größe von entsprechend versiegelten und abflussarmen Flächen berücksichtigen die Kommunen z. B. vorhandene Bauzeichnungen. Fehlen belastbare Angaben, so erwägen die Gemeinden zunehmend eine Beauftragung von Dienstleistern, welche eine **Befliegung des Gemeindegebietes** vornehmen und dabei Luftaufnahmen der maßgeblichen Grundstücke anfertigen.

Wir erhielten in diesem Kontext Beratungsanfragen, ob und unter welchen Voraussetzungen die Anfertigung und Weiterverarbeitung solcher **Luftaufnahmen nach datenschutzrechtlichen Gesichtspunkten** zulässig sind. Im Ergebnis sind insbesondere folgende Punkte zu beachten:

1. Bei den Aufnahmen zu den Grundstücken, bei welchen die Eigentümer natürliche Personen sind, handelt es sich um **personenbezogene Daten**. Eine Identifizierung der Grundstückseigentümer ist auch gewollt, um die Beitragsschuldner zu ermitteln.
2. Eine **gesetzliche Rechtsnorm** im Sinne einer rechtlichen Verpflichtung, personenbezogene Daten als Luftaufnahmen zum Zweck der Beseitigung von Niederschlagswasser zu erheben und weiterzuverarbeiten, ist **nicht ersichtlich**. Insbesondere fehlen damit Anhaltspunkte für eine Anwendung von Art. 6 Abs. 1 Buchst. c DSGVO, wonach die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich sein müsste, welcher die verantwortliche Kommune unterliegt.
3. Als Rechtsgrundlage könnte gegebenenfalls Art. 6 Abs. 1 Buchst. e DSGVO in Verbindung mit § 4 Abs. 1 der Gemeindeordnung Schleswig-Holstein in Verbindung mit einer **kommunalen Satzung** in Betracht kommen. Die Satzung müsste die Anforderungen nach Art. 6 Abs. 3 DSGVO erfüllen, einschließlich einer konkreten Bezeichnung des Verarbeitungszwecks, der Art der Daten, der Speicherdauer und gegebenenfalls auch Hinweisen zum Widerspruchsrecht betroffener Personen. Es sollte darin u. a. festgelegt werden, **welche Auflösung** die Aufnahmen zur Erreichung des verfolgten Zwecks haben sollen und welche weiteren **organisatorischen Maßnahmen** veranlasst werden.
4. Wir gehen davon aus, dass es sich bei der Anfertigung der Luftaufnahmen um eine Erhebung bei den betroffenen Personen handelt, sodass die Erfüllung der Informationspflichten nach Artikel 13 DSGVO sicherzustellen wäre. Dabei würde das Anliegen des Verordnungsgebers auch dann beachtet, wenn die betroffenen Personen **im Vorfeld einer Befliegung angemessen unterrichtet** würden, etwa durch parallele Veröf-

fentlichungen im Webauftritt der Kommune und in geeigneten Zeitungen, Anzeigern, anderen Medien oder durch Postwurfsendungen. Die Pflichtinformationen müssen vor allem einen Hinweis auf das Widerspruchsrecht und Angaben dazu, unter welchen Kontaktdaten man dieses Recht ausüben kann, aufweisen, Art. 13 Abs. 1 Buchst. a, Abs. 2 Buchst. b DSGVO.

Art. 6 Abs. 3 Satz 2 und 3 DSGVO

[2]Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Abs. 1 Buchst. e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. [3]Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, u. a. Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX der DSGVO.

5. Im Falle der Durchführung der Befliegung und der Anfertigung der Aufnahmen durch einen Dienstleister kommt der Abschluss eines Vertrags nach Art. 28 Abs. 3 DSGVO zur **Verarbeitung im Auftrag** in Betracht. Die Kommune bleibt infolge der Hoheit über die Zwecksetzung für die Datenverarbeitung die allein Verantwortliche. Der Dienstleister muss die sonstigen Anforderungen nach Artikel 28 und 29 DSGVO erfüllen.

Art. 28 Abs. 3 Satz 1 DSGVO

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.

6. Die Erstellung eines **Verzeichnisses von Verarbeitungstätigkeiten** ist sowohl von der Kommune (Art. 30 Abs. 1 DSGVO) als auch von dem Dienstleister (Art. 30 Abs. 2 DSGVO) zu erfüllen.

Vor allem hinsichtlich der Vermeidung von vertieften Eingriffen in die Privatsphäre betroffener Personen müssten Regelungen getroffen werden, die auch der Dienstleister einzuhalten hat. Dazu gehören z. B. Festlegungen zur **Auflösung der Aufnahmen** und der **Flughöhe** für die Überfliegung und der **Ausschluss einer Erfassung von identifizierbaren Personen** sowie des **Abfilmens von Privatbereichen wie Sonnenterrassen**.

Was ist zu tun?

Die Anfertigung von Luftaufnahmen von Grundstücksflächen in einer Kommune zur Bemessung der Gebühren für die Beseitigung von Niederschlagswasser bedarf einer Rechtsgrundlage. Näheres kann dabei in einer kommunalen Satzung geregelt werden.

4.1.2 Fragebogenaktion für Projektzwecke

Bei dem ULD ging eine Beschwerde ein, in der vorgetragen wurde, dass eine Kommune „zusammen" mit einer universitären Einrichtung personenbezogene Daten der Bürgerinnen und Bürger dieser Kommune im Rahmen einer **Sportstättenentwicklungsplanung** verarbeite.

Konkret verhielt es sich so, dass die Adressaten angeschrieben und auf freiwilliger Basis um die Beantwortung eines beigefügten Fragebogens gebeten wurden. Neben **Alter, Geschlecht und betreffendem Ortsteil** wurden auch Angaben zum **Sportverhalten**, zur Art der Sportstätte, in der der Sport ausgeübt wird, zum Namen der Sportstätte und zur Mitgliedschaft in einem Sportverein erbeten. Den Schreiben war nicht eindeutig zu entnehmen, ob diese von der kommunalen oder der universitären Einrichtung an die Bürgerinnen und Bürger übersandt und aus welcher Quelle Vor- und Nachnamen sowie Anschriften zum Zwecke des Anschreibens bezogen worden sind. Eine Information über die Verarbeitung der personenbezogenen Daten nach Artikel 13 bzw. Artikel 14 DSGVO war den Schreiben nicht beigefügt.

Die im aufsichtsbehördlichen Verfahren von uns um Stellungnahme gebetene Kommune erläuterte, dass sie mit Beschlüssen der entsprechenden kommunalen Fachausschüsse beauftragt worden sei, eine Sportstättenentwicklungsplanung zu initiieren. Die universitäre Einrichtung sei mit der Umsetzung des Projekts beauftragt worden. Im Rahmen einer **Gruppenauskunft gemäß § 46 Bundesmeldegesetz (BMG)** seien der universitären Einrichtung die personenbezogenen Daten der Adressaten übermittelt worden, um von dort aus das Anschreiben und den Fragebogen versenden zu können. Die mittels der Fragebögen erhobenen Daten würden von der universitären Einrichtung statistisch ausgewertet und das Ergebnis der Auswertung an die Kommune übermittelt werden. Bei der Erhebung der Angaben mittels des Fragebogens sei **davon ausgegangen** worden, **dass es sich bei den erbetenen Angaben nicht um personenbezogene Daten handele**; die Fragebögen würden alle gleich aussehen und anonym gestaltet sein.

Rechtlich war zunächst festzustellen, dass die Übermittlung der personenbezogenen Daten der Bürgerinnen und Bürger im Rahmen der Gruppenauskunft nach § 46 BMG datenschutzrechtlich nicht zu beanstanden war. § 46 BMG stellte für diese Übermittlung die Rechtsgrundlage dar. Nach § 46 Abs. 1 Nr. 4, Abs. 2 Nr. 1 und 2 BMG sind davon auch der Vor- und Nachname sowie die derzeitige Anschrift erfasst. Die **Gruppenauskunft** gemäß § 46 Abs. 1 BMG darf jedoch nur erteilt werden, wenn sie **im öffentlichen Interesse** liegt. Für die Annahme eines öffentlichen Interesses sprach die Beschlussfassung der kommunalen Fachausschüsse.

Was die Verarbeitung der Antworten aus den Fragebögen betraf, bestand hinsichtlich der Auffassung der verantwortlichen Kommune Klärungsbedarf, es handele sich gänzlich um die Erhebung anonymer Angaben. Zumindest **für einen Teil der Angaben** bestanden Anhaltspunkte für einen möglichen **Personenbezug**. Gemäß der in Art. 4 Nr. 1 DSGVO enthaltenen Definition handelt es sich bei personenbezogenen Daten um alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. In dem Fragebogen wurden zwar weder die Namen noch die Anschriften der Adressaten abgefragt. Allerdings war zu prüfen,

ob die betreffenden Personen im Einzelfall aufgrund der erbetenen Antworten identifizierbar waren. Die Kommune musste etwa prüfen, ob eine derartige **Rückschlussmöglichkeit** bei einer kumulativen Betrachtung der Antworten in Bezug auf das Geschlecht, das Alter, Fragen nach dem Ortsteil, nach der Mitgliedschaft in einem konkret zu benennenden Sportverein und nach dem Austritt aus dem Verein besteht.

Das ULD hat vor diesem Hintergrund zunächst einen **Hinweis in Bezug auf die Reichweite des Personenbezugs** erteilt. In diesem Kontext hat das ULD ausdrücklich darauf hingewiesen, dass sich ein **Personenbezug insbesondere auch aus der kumulativen Betrachtung von bestimmten Einzelangaben** ergeben kann.

Ferner wurde auf das Erfordernis einer **Rechtsgrundlage** bei der Verarbeitung von personenbezogenen Daten hingewiesen, sollte sich ein Personenbezug aus den Antworten des Fragebogens ergeben. In diesem Zusammenhang erfolgte der Hinweis, dass in dem Fall, in dem keine gesetzliche Rechtsgrundlage vorliegt, die Verarbeitung nur auf eine den Anforderungen des Artikels 7 DSGVO entsprechende, **freiwillig, in informierter Weise und unmissverständlich erteilte Einwilligung** der betroffenen Personen gestützt werden kann.

Abschließend hat das ULD darauf hingewiesen, dass die betroffenen Personen im Falle der Erhebung personenbezogener Daten **gemäß Artikel 13 bzw. Artikel 14 DSGVO zu informieren** sind und dass im Falle der Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen die für einen **Auftragsverarbeiter** bestehenden Anforderungen nach Artikel 28 DSGVO einzuhalten sind.

Was ist zu tun?

Bei der Erhebung von Daten für Projektzwecke auf Grundlage eines Fragebogens ist von der öffentlichen Stelle für die einzelnen erbetenen Angaben genau zu prüfen, ob diese einen Personenbezug aufweisen. Ist das der Fall, sind die Vorgaben der DSGVO bei der Verarbeitung der Angaben einzuhalten.

4.1.3 Nachweis der Elternschaft – Adoptionsurkunden gibt es nicht

Mit dem **Gesetz zur Unterstützung und Entlastung in der Pflege (PUEG)** erhöhten sich im Sommer 2023 die Beitragssätze für die gesetzliche Pflegeversicherung. Zur Umsetzung des Beschlusses des Bundesverfassungsgerichts vom 7. April 2022 (1 BvL 3/18) anlässlich der Benachteiligung von Eltern war es zudem notwendig geworden, eine **Differenzierung der Beitragssätze nach der Anzahl der Kinder** der Versicherten in das Gesetz aufzunehmen.

Den **Pflegekassen** war die Information hierüber jedoch bislang nicht in allen Fällen bekannt. Ein vorgesehenes digitales Verfahren zum Nachweis der berücksichtigungsfähigen Kinder muss zunächst noch entwickelt werden, spätestens bis zum 31. März 2025. Bis dahin müssen Arbeitgeber und Kassen die Daten gegebenenfalls auf andere Weise erheben.

Klärungsbedarf entstand in einem dem ULD vorgetragenen Fall eines Elternpaares mit adoptiertem Kind. Unterlagen zur Adoption sollten einem Arbeitgeber vorgelegt werden, was den betroffenen Personen unnötig und allzu sensibel erschien. Auf dem verwendeten Vordruck wurde namentlich eine **„Adoptionsurkunde“ als möglicher Nachweis** aufgeführt. Tatsächlich existiert eine solche Urkunde nach deutschem Recht gar nicht. Adoptionen lassen sich zwar im Geburtenregister des Standesamts nachvollziehen. Auf

neu ausgestellten Geburtsurkunden werden jedoch ausschließlich die Adoptiveltern aufgeführt.

§ 55 Abs. 3a SGB XI

Die Elterneigenschaft sowie die Anzahl der Kinder unter 25 Jahren müssen gegenüber der beitragsabführenden Stelle, bei Selbstzahlern gegenüber der Pflegekasse, nachgewiesen sein, sofern diesen die Angaben nicht bereits bekannt sind. Der Spitzenverband Bund der Pflegekassen gibt Empfehlungen darüber, welche Nachweise geeignet sind. Die beitragsabführenden Stellen und die Pflegekassen sind berechtigt, entsprechende Nachweise anzufordern.

Daneben schränkt das Personenstandsrecht den Zugriff auf das **Geburtenregister** in solchen Konstellationen besonders ein:

§ 63 Abs. 1 Satz 1 PStG

Ist ein Kind angenommen, so darf abweichend von § 62 ein beglaubigter Registerausdruck aus dem Geburtseintrag nur den Annehmenden, deren Eltern, dem gesetzlichen Vertreter des Kindes und dem über 16 Jahre alten Kind selbst erteilt werden.

Das Versicherungsrecht macht hier dementsprechend keinen Unterschied. Für den Begriff der Elternschaft verweist § 55 Abs. 3 Satz 3 SGB XI auf den Allgemeinen Teil des Sozialgesetzbuches:

§ 56 Abs. 3 SGB I

Als Eltern im Sinne des Abs. 1 Satz 1 Nr. 3 gelten auch

[…]

2. Stiefeltern,

3. Pflegeeltern (Personen, die den Berechtigten als Pflegekind aufgenommen haben).

Während auch Stief- und Pflegeeltern ausdrücklich von den verminderten Beitragssätzen erfasst sind, führt das Gesetz die Kategorie der Adoptiveltern gar nicht erst ausdrücklich auf. Sinngemäß haben sie ganz **selbstverständlich als „Eltern"** zu gelten.

Den betroffenen Personen im konkreten Fall wurde geraten, sich auf die **Geburtsurkunde als Nachweis** zu beschränken. Um die Elterneigenschaft in der beschriebenen Situation rechtlich nachvollziehbar zu machen, reicht diese aus. Gegebenenfalls könnte der Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO herangezogen werden.

Die Vorlage einer „Adoptionsurkunde" – im Sinne eines Nachweises einer Adoption – könnte in anders gelagerten, sehr speziellen Fällen mit Auslandsbezug notwendig sein, in diesem Fall jedoch nicht.

4.1.4 Datenverarbeitung bei Schuleingangsuntersuchungen – standardisiertes Verfahren

Im Berichtszeitraum war die Landesbeauftragte für Datenschutz im Rahmen einer Beratung des Ministeriums für Justiz und Gesundheit und einiger Gesundheitsämter mit Fragen der Datenverarbeitung im Zusammenhang mit Schuleingangsuntersuchungen befasst. Ferner erhielten wir auch Anfragen von Eltern, die in Erfahrung bringen wollten, ob bestimmte **Fragen zum Gesundheitszustand, zur Ermittlung etwaiger Förderbedarfe und Angaben zu Impfnachweisen bei einer schulärztlichen Untersuchung** erhoben werden dürfen.

Das ULD ließ sich im Folgenden die Datenverarbeitung bei Schuleingangsuntersuchungen in einem Gesundheitsamt vor Ort erläutern und erörterte mit den beteiligten Behörden den Sachverhalt. Das Beratungsverfahren, das von Vertretern des Ministeriums für Gesundheit und

Justiz sowie von einigen Schulärztinnen der Kreise und kreisfreien Städte sehr konstruktiv begleitet wurde, konnte mit der abgestimmten Überarbeitung eines **standardisierten Einladungsschreibens für schulärztliche Eingangsuntersuchungen und erforderlicher Pflichtinformationen** nach der DSGVO zügig zum Abschluss gebracht werden. Einige Punkte aus dem Einladungsschreiben werden im Folgenden genannt:

- Vor Beginn des Grundschulbesuchs ist eine schulärztliche Untersuchung gesetzlich vorgesehen. Diese Untersuchung entscheidet nicht darüber, ob das Kind die Schule besuchen darf oder nicht. Es geht darum, den **Entwicklungsstand des Kindes besser einordnen** und gegebenenfalls eine individuelle Förderung einleiten zu können. Die Schule erhält nur das Ergebnis dieser Untersuchung. Sollten bei der Untersuchung Entwicklungsauffälligkeiten und/oder gesundheitliche Störungen festgestellt werden, die **Auswirkungen auf den Schulbesuch** haben können, werden diese Informationen ebenfalls **an die Schule übermittelt**.
- Bezüglich der im beigefügten Fragebogen mit einem (*) gekennzeichneten Angaben besteht eine **gesetzliche Auskunftspflicht nach § 27 Abs. 3 des Schulgesetzes**. Die Übermittlung des Ergebnisses der Untersuchung sowie **etwaiger Entwicklungsauffälligkeiten und gesundheitlicher Beeinträchtigungen**, die **im Einzelfall** für die Beschulung von Bedeutung sind, einschließlich Förderbedarfe an die Schule, beruht auf § 27 Abs. 4 des Schulgesetzes.
- Weiterhin ist die Vorlage des Vorsorgeheftes zur Durchführung der schulärztlichen Untersuchung des Kindes erforderlich. Die übrigen Angaben im Fragebogen sind **freiwillig**.
- Beim Untersuchungstermin erhalten die Eltern einen zusätzlichen Erhebungsbogen (**Fragebogen zu Stärken und Schwächen – SDQ**). Die Angaben in diesem Erhebungsbogen sind freiwillig. Die Erhebung der Angaben im Fragebogen zu Stärken und Schwächen dient der **Beurteilung des Sozial- und Emotionsverhaltens** des Kindes im Alltag und der Ermittlung von **Förderbedarfen** sowie der Gesundheitsberichterstattung. Rechtsgrundlage für die Erhebung und Anonymisierung zwecks Weitergabe zur Gesundheitsberichterstattung ist die Einwilligung der Eltern.
- Die Vorlage des Impfausweises ist freiwillig. Jedoch ist der Kinder- und Jugendgesundheitsdienst gesetzlich **verpflichtet, den Impfstatus zu erheben**. Die Eltern werden daher gebeten, diesen ebenfalls vorzulegen. Die Daten werden in anonymisierter Form an das Robert-Koch-Institut übermittelt. Die Erhebung des **Impfstatus** beruht auf § 34 Abs. 11 des Infektionsschutzgesetzes. Gemäß § 20 Abs. 9 des Infektionsschutzgesetzes sind die Eltern gesetzlich verpflichtet, gegenüber der Schule **Nachweise zum Masernschutz** vorzulegen. Zusätzlich ist es auch möglich, den Impfnachweis im Rahmen der ärztlichen Untersuchung vorzulegen. Die Information über ausreichenden Impfschutz wird dann an die Schule übermittelt. Rechtsgrundlage hierfür ist die Einwilligung der Eltern. Die Teilnahme an diesem alternativen Verfahren ist für die Eltern freiwillig.
- Seit 1999 wird in Schleswig-Holstein jährlich ein Kinder- und Jugendgesundheitsbericht erstellt (Gesundheitsberichterstattung). Er verschafft Gesundheitsbehörden und Parlament einen Überblick über den Gesundheitszustand der Einschulungskinder. Zum Zweck der **Gesundheitsberichterstattung** werden die im Rahmen der schulärztlichen Untersuchung erhobenen Angaben zusammen mit den bei der Untersuchung festgestellten Befunden sowie den empfohlenen ärztlichen Maßnahmen anonymisiert an das Universitätsklinikum Schleswig-Holstein Campus Lübeck und das Ministerium für Justiz und Gesundheit zur zentralen Auswertung auf Grundlage von § 6 und § 7 des Gesundheitsdienst-Gesetzes und § 5 der Landesverordnung über die schulärztlichen Aufgaben weitergeleitet.

Das Ministerium für Gesundheit und Justiz hat darüber hinaus weitere sachdienliche Informationen zur **schulärztlichen Eingangsuntersuchung** veröffentlicht. Die Informationen, einschließlich eines Videos dazu, wie eine Schuleingangsuntersuchung abläuft, sind unter den folgenden Links abrufbar:

www.schleswig-holstein.de/DE/fachinhalte/S/schuleingangsuntersuchungen/Ablauf.html

Kurzlink: *https://uldsh.de/tb42-4-1-4a*

www.schleswig-holstein.de/DE/landesregierung/themen/bildung-hochschulen/schuleingangsuntersuchungen/schuleingangsuntersuchungen_node.html

Kurzlink: *https://uldsh.de/tb42-4-1-4b*

4.1.5 Aufbewahrungsfristen für abgeschlossene Personalakten im öffentlichen Dienst

Anlässlich einer Beschwerde leitete das ULD ein Anhörungsverfahren gegen den ehemaligen Dienstherrn des Beschwerdeführers als datenschutzrechtlich Verantwortlichen ein. In diesem Verfahren stellten sich Fragen zur **Aufbewahrungsfrist für Personalaktendokumente**.

Die Aufbewahrungsfristen für die abgeschlossenen Personalakten von Beschäftigten des öffentlichen Dienstes in Schleswig-Holstein richten sich grundsätzlich nach § 15 Landesdatenschutzgesetz (LDSG) in Verbindung mit § 91 Abs. 1 Landesbeamtengesetz (LBG). Demnach sind für die Beamtinnen und Beamten Personalakten nach ihrem Abschluss von der personalaktenführenden Behörde **fünf Jahre** lang aufzubewahren. Das LBG bestimmt explizit, wann eine Personalakte als abgeschlossen gilt, und setzt damit einen Zeitpunkt fest, ab welchem die fünfjährige Frist beginnt. Als solche Zeitpunkte gelten z. B. das Ausscheiden der Beamtin oder des Beamten aus dem Beamtenverhältnis auf Widerruf nach Ablauf des Vorbereitungsdienstes oder der Ablauf des Todesjahres, wenn die Beamtin oder der Beamte ohne versorgungsberechtigte Hinterbliebene verstorben ist.

Abweichungen von der genannten Regelfrist ergeben sich aus § 91 Abs. 2 und 3 LBG für Unterlagen über Beihilfen, Heilfürsorge, Heilverfahren, Unterstützungen, Erholungsurlaub, Erkrankungen, Umzugs- und Reisekosten sowie Versorgungs-, Altersgeld- und Hinterbliebenenaltersgeldakten.

Ausgehend von § 91 Abs. 1 LBG bestehen dem Wortlaut nach für die Personalakten von im öffentlichen Dienst **Tarifbeschäftigten keine klaren Vorgaben**, aus denen sich ein Zeitpunkt ableiten lässt, ab welchem eine fünfjährige Aufbewahrungsfrist laufen soll. Anwendbar sind für die Tarifbeschäftigten im öffentlichen Dienst hingegen Vorgaben nach § 91 Abs. 2 LBG, die sich auf Unterlagen zu Erholungsurlaub, Erkrankungen und Reisekosten beziehen.

Im Übrigen wird für die Grundakte und Teilakten der Personalakten von im öffentlichen Dienst Tarifbeschäftigten **gesondert zu entscheiden** sein, welche spezifischen Aufbewahrungsvorgaben – etwa nach anderen gesetzlichen Vorschriften – gelten oder ob sich die Erforderlichkeit einer Aufbewahrung nachvollziehbar begründen lässt. Entfalten Unterlagen in bestimmten Teilakten steuerrechtliche Relevanz, so richtet sich speziell deren Aufbewahrung nach steuerrechtlichen Vorgaben der Abgabenordnung und anderen fachgesetzlichen Bestimmungen des Steuerrechts. Weiterhin kann sich die Erforderlichkeit der Aufbewahrung für bestimmte Teile der Personalakte aus den Vorgaben zur regelmäßigen Verjährung ergeben, sofern noch Ansprüche aus dem Beschäftigtenverhältnis bestehen können, §§ 195, 199 des Bürgerlichen Gesetzbuches (BGB).

Im eingeleiteten aufsichtsbehördlichen Verfahren passte der Verantwortliche die Aufbewahrungsfristen für die von ihm vorgehaltenen Personalakten der im öffentlichen Dienst Tarifbeschäftigten an.

Was ist zu tun?

Öffentliche Stellen haben gemäß den geltenden Regelungen für die jeweiligen Dokumente aus der geschlossenen Personalakte einzelfallbezogen zu prüfen, wie lange diese aufzubewahren sind. Für die Tarifbeschäftigten im öffentlichen Dienst können auch Vorgaben außerhalb des Landesbeamtengesetzes von Bedeutung sein.

4.1.6 Fragen zur Veröffentlichung dienstlicher Kontaktdaten von Beschäftigten des öffentlichen Dienstes

Das ULD wurde um eine rechtliche Einschätzung zu der Frage gebeten, ob **dienstliche Kontaktdaten auf der Homepage** des Dienstherrn, bei dem es sich um eine öffentliche Stelle handelte, veröffentlicht werden dürfen. Konkret ging es um die namentliche Nennung der Beschäftigten auf der Homepage.

Dabei ergibt sich für die Bewertung der Veröffentlichung der dienstlichen Kontaktdaten der Beschäftigten, einschließlich des Namens, auf der Homepage des Dienstherrn Folgendes:

- Die **Veröffentlichung der dienstlichen Kontaktdaten**, bei denen es sich um personenbezogene Daten handelt, bedarf wie jede Verarbeitung personenbezogener Daten einer Rechtsgrundlage.
- Die Verarbeitung der personenbezogenen Daten der Beschäftigten für öffentliche Stellen in Schleswig-Holstein richtet sich nach § 15 des Landesdatenschutzgesetzes (LDSG) in Verbindung mit § 85 des Landesbeamtengesetzes (LBG). Danach darf der Dienstherr diese Daten verarbeiten, soweit dies zur Durchführung organisatorischer, personeller und sozialer Maßnahmen erforderlich ist oder eine Vereinbarung nach dem Mitbestimmungsgesetz Schleswig-Holstein dies erlaubt.
- Die Veröffentlichung der dienstlichen Kontaktdaten der Beschäftigten des öffentlichen Dienstes im Internet, im Engeren: Name, Vorname, dienstliche E-Mail-Adresse und dienstliche Telefonnummer, ist **zulässig, wenn sie zur Durchführung organisatorischer Maßnahmen und in diesem Zusammenhang zur ordnungsgemäßen Aufgabenerfüllung der öffentlichen Stelle erforderlich** ist. Im Einzelfall kann dies zu bejahen sein, um den Bürger darüber zu informieren, welche der Beschäftigten die richtigen Ansprechpartner für die jeweiligen Anliegen sind. Zu berücksichtigen ist jedoch, dass dies lediglich für Beschäftigte gilt, die eine Funktion mit Außenwirkung innehaben und daher im regelmäßigen Kontakt mit Bürgerinnen und Bürgern stehen.
- Vorzunehmen ist daher eine **umfassende Interessenabwägung**. In die Entscheidung über die Veröffentlichung ist auch einzubeziehen, ob nur einzelne der dienstlichen Kontaktdaten veröffentlicht werden sollten. Eine andere Bewertung kann sich im Einzelfall etwa ergeben, wenn sich für die Beschäftigten durch die Veröffentlichung dienstlicher Kontaktdaten generell eine Gefährdungslage ergeben könnte oder wenn in bestimmten Arbeitsbereichen eine sinnvolle Aufgabenerledigung durch die Veröffentlichung der Daten, etwa durch permanentes Klingeln des Telefons, nicht mehr möglich erscheint.

Was ist zu tun?

Bei der Veröffentlichung der Kontaktdaten der Beschäftigten (beispielsweise auf der Homepage) hat der Dienstherr im Einzelfall zu prüfen, ob dies für die ordnungsgemäße Aufgabenerfüllung erforderlich ist. Durch die Veröffentlichung darf keine Gefährdungslage für die Beschäftigten entstehen.

4.1.7 Veröffentlichung von Spendernamen im Bürgerinformationssystem

Die Veröffentlichung von personenbezogenen Daten in kommunalen Bürger- oder Ratsinformationssystemen führt immer wieder zu Anfragen oder Beschwerden beim ULD.

In einem konkreten Fall bat eine Privatperson um unsere Unterstützung, die sich **mit 100 Euro an einer gemeindlichen Spendenaktion** beteiligt hatte. Damit tauchte sie anlässlich der Sitzungsvorlage zur jährlichen Annahme von Spenden, Schenkungen und Zuwendungen der Gemeinde namentlich in einer Spenderliste auf. Das Bürgerinformationssystem der betreffenden Kommune ist über deren **Webauftritt** für alle **frei zugänglich**.

In der Tat schreibt die **Gemeindeordnung** die Aufstellung solcher Listen ausdrücklich vor.

§ 76 Abs. 4 Satz 5 GO

Über die Annahme oder Vermittlung von Spenden, Schenkungen oder ähnlichen Zuwendungen, die über 50 Euro hinausgehen, erstellt die Bürgermeisterin oder der Bürgermeister jährlich einen Bericht, in welchem die Geber, die Zuwendungen und die Zuwendungszwecke anzugeben sind, und leitet diesen der Gemeindevertretung zu.

Unstrittig ist ferner der **Grundsatz der Öffentlichkeit von Sitzungen der Gemeindevertretung** nach § 35 Abs. 1 GO. Was Art und Ausmaß der Verfügbarkeit von Unterlagen zu Sitzungen der Gemeindevertretung angeht, regelt die Gemeindeordnung lediglich Folgendes:

§ 41 Abs. 3 GO

Die Einsichtnahme in die Niederschriften über die öffentlichen Sitzungen ist den Einwohnerinnen und Einwohnern zu gestatten.

Aus Sicht des ULD **reichen die benannten Vorschriften nicht so aus**, als dass sie **als Rechtsgrundlage** im Sinne von Art. 6 Abs. 1 Buchst. c oder Buchst. e DSGVO für eine Veröffentlichung der Spender im Internet herangezogen werden könnten. Eine Möglichkeit zur **Einsichtnahme über das Internet** durch jede beliebige Person erscheint **zu weitreichend**. Da spezifischere Vorschriften zur Veröffentlichungspraxis oder gar zu Bürgerinformationssystemen im Internet fehlen, bleibt das Verhältnis zwischen Sitzungsöffentlichkeit, Gemeindeöffentlichkeit und Internetöffentlichkeit allerdings zugegebenermaßen vage.

Die betreffende Kommune betonte im Rahmen des Anhörungsverfahrens die Bedeutung der **Transparenz** und der **Korruptionsprävention**, denen die Berichte ohne Zweifel dienen. Auf die Veröffentlichung von Spenderlisten zu verzichten, stünde diesen Zwecken entgegen. Als vorläufige Lösung des Konflikts hat die Gemeinde den **offenen Zugriff auf diese Anlagen letztlich gesperrt**, mit Wirkung für die bisherigen Berichtsjahre. Für zukünftige Berichte wolle man eine **Widerspruchslösung** einführen. Insbesondere beabsichtigte die Kommune, eine grundsätzliche Klärung der Problematik auf Landesebene anzuregen.

Was ist zu tun?

Eine Diskussion der Möglichkeiten und Grenzen der Veröffentlichungspraxis in kommunalen Bürger- oder Ratsinformationssystemen auf übergeordneter Ebene wäre zu begrüßen. Letzten Endes wäre auch zu beleuchten, inwieweit die aktuelle Vorschriftenlage noch geeignet ist, angesichts der Erfordernisse der Zeit und der technologischen Entwicklung rechtlich Klarheit zu gewährleisten.

4.1.8 Veröffentlichung der Adressen von Gemeindevertreterinnen und -vertretern

Während das Gemeinderecht im Hinblick auf die Veröffentlichung personenbezogener Daten von Privatpersonen Lücken aufweist (Tz. 4.1.7), lässt sich die Situation von Gemeindevertreterinnen und -vertretern genauer umreißen (39. TB, Tz. 4.1.4 zum Veröffentlichungsort bzw. -medium und der Veröffentlichung von Angaben zu privaten Anschriften, Telefonnummern und E-Mail-Adressen). Gelegentliche Nachfragen beim ULD betreffen dabei erneut die Angaben von Straße und Hausnummer. Auch hier geht es meist um **frei zugängliche Bürger- oder Ratsinformationssysteme auf den Webauftritten** der Kommunen.

Die einschlägige Vorschrift ist unabhängig vom Medium der Veröffentlichung anwendbar:

§ 32 Abs. 4 Satz 2 GO

Die Mitglieder der Gemeindevertretung, der Ortsbeiräte und der Ausschüsse haben der oder dem Vorsitzenden der Gemeindevertretung ihren Beruf sowie andere vergütete oder ehrenamtliche Tätigkeiten mitzuteilen, soweit dies für die Ausübung ihres Mandats von Bedeutung sein kann. Die Angaben sind zu veröffentlichen. Das Nähere regelt die Geschäftsordnung.

Der Begriff der „ehrenamtlichen Tätigkeit" kann dabei auch eine **Parteizugehörigkeit** einschließen. Was **Ortsangaben** angeht, ist zusätzlich das Wahlrecht heranzuziehen, und zwar vor allem die Vorschrift zur Bekanntmachung von Wahlvorschlägen:

§ 31 Abs. 1 Satz 3 GKWO

Die Bekanntmachung enthält die [im Wahlvorschlag] bezeichneten Angaben; statt des Geburtsdatums ist jeweils nur das Geburtsjahr der Bewerberin oder des Bewerbers, statt der Anschrift ist nur die Postleitzahl und der Wohnort anzugeben.

Im Übrigen kann eine bloße Angabe des Wohnorts schon deswegen als unschädlich angesehen werden, da bereits die Wählbarkeit vom Sitz der Hauptwohnung abhängt. **Ausdrücklich ausgenommen** ist aber die **genaue Anschrift**: Darf diese schon nicht in der zeitweise öffentlichen Wahlbekanntmachung aufgeführt sein, kommt eine dauerhafte Verfügbarmachung ohne expliziten Rechtsgrund erst recht nicht infrage.

Allerdings ist es denkbar, dass Gemeindevertreterinnen oder -vertreter von sich aus wünschen, für andere Bürgerinnen und Bürger unter ihrer privaten Anschrift erreichbar zu sein. In diesem Fall handelt es sich jedoch um eine **freiwillige Angabe**. Das Mittel der Wahl im Datenschutzrecht ist hierfür die Einwilligung nach Art. 6 Abs. 1 Buchst. a DSGVO. Angesichts der leider bestehenden Risiken von Missbrauch oder Belästigung darf die **freie Entscheidung der betroffenen Person nicht übergangen** werden. Dies dient letztlich auch dazu, Interessierte nicht dadurch von einem Einstieg in die Kommunalpolitik abzuhalten, dass die Privatadresse des eigenen Haushalts veröffentlicht werden muss.

Was ist zu tun?

Kommunen sollten prüfen, ob ihre bisherige Verwaltungspraxis die Veröffentlichung von Anschriften der Gemeindevertreterinnen oder -vertreter vorsieht, insbesondere wenn dies über frei zugängliche Bürgerinformationssysteme erfolgt. Zulässig ist dies nur auf freiwilliger Basis.

4.1.9 Behördliche Entscheidungen über die Offenlegung von Identitäten

In verschiedensten Situationen stehen Behörden vor der Herausforderung, dass sie gesetzlich gewährte **Auskunftsansprüche erfüllen** müssen, eine etwaige Offenlegung der Identität dritter Personen dem aber entgegensteht. Eine Beratungsanfrage an das ULD beschäftigte sich beispielsweise mit dem **Kontrollrecht der Mitglieder der Gemeindevertretung** gegenüber der Verwaltung:

§ 30 Abs. 1 Satz 1 GO

Einzelnen Gemeindevertreterinnen oder -vertretern hat die Bürgermeisterin oder der Bürgermeister in allen Selbstverwaltungsangelegenheiten und zu allen Aufgaben zur Erfüllung nach Weisung auf Verlangen Auskunft zu erteilen und Akteneinsicht zu gewähren.

§ 30 Abs. 2 Satz 1 GO

Auskunft und Akteneinsicht dürfen nicht gewährt werden, wenn die Vorgänge nach einem Gesetz geheim zu halten sind oder das Bekanntwerden des Inhalts die berechtigten Interessen Einzelner beeinträchtigen kann.

Vergleichbare Ansprüche gibt es beispielsweise im **Verwaltungsverfahrensrecht** gegenüber Beteiligten (§ 88 Abs. 1 LVwG) oder im **Arbeits- oder Beamtenrecht** gegenüber den Mitarbeitenden (§ 3 Abs. 6 TV-L bzw. § 88 Abs. 1 LBG). Nicht zuletzt besteht im Datenschutzrecht der allgemeine Auskunftsanspruch des Art. 15 Abs. 1 DSGVO, der jedoch gemäß Abs. 4 *„die Rechte und Freiheiten anderer Personen nicht beeinträchtigen“* darf.

In vielen Fällen können die Belange Dritter durch eine **Schwärzung ihrer Namen** in den offengelegten Unterlagen gewahrt werden. Manchmal reicht dies aber nicht aus, weil die Person beispielsweise **anhand der Lage eines Grundstücks oder anhand einer protokollierten Äußerung identifiziert** werden kann. In bestimmten Situationen kann es vorkommen, dass ein Antrag auf Auskunft einzig darauf gerichtet ist, Klarheit über die Urheberin oder den Urheber etwa einer Beschwerde zu erlangen.

Behörden kommen dann nicht umhin, die **Auskunftsinteressen** von Antragstellenden und die **Geheimhaltungsinteressen** von betroffenen Personen gegeneinander **abzuwägen**. Ob eine Offenlegung die Rechte Dritter verletzt, muss im Einzelfall im eigenen Ermessen entschieden werden. Eine **Anhörung** einer Seite oder beider Seiten kann dazu notwendig sein.

Einen Sonderfall stellen Behörden dar, die in ihrer Arbeit auf Hinweisgeberinnen oder Hinweisgeber angewiesen sind. Den **Schutz von Informantinnen und Informanten** erkennt die langjährige Rechtsprechung unter Umständen sogar als eigenes Interesse solcher Stellen an:

Bundesverwaltungsgericht, Beschluss vom 22.07.2010 (20 F 11.10)

Sind Behörden bei der Erfüllung ihrer öffentlichen Aufgaben auf Angaben Dritter angewiesen, dürfen sie zum Schutz des Informanten dessen Identität geheim halten. Denn Behörden werden die für eine effektive Aufgabenerfüllung unentbehrlichen Informationen vonseiten Dritter in der Regel nur erhalten, wenn sie dem Informanten Vertraulichkeit der personenbezogenen Daten zusichern. Nicht jede öffentliche Aufgabe rechtfertigt indes die Annahme, Informationen vonseiten Dritter seien zur Erfüllung einer öffentlichen Aufgabe unerlässlich.

Aber auch die Vereinbarung von Vertraulichkeit schützt nicht jede Hinweisgeberin oder jeden Hinweisgeber. Typischerweise **nicht schützenswert** sind etwa Angaben, die **wider besseres Wissen oder leichtfertig falsch** gemacht worden sind.

Mit ähnlichen Problemen sind regelmäßig auch **Arbeitsgerichte** befasst, vor allem wenn anonyme Beschwerden zu arbeitsrechtlichen Maßnahmen gegen Beschäftigte führen. An diesem Beispiel wird besonders deutlich, dass Verantwortliche nicht nur eine eigene Entscheidung für oder gegen die Offenlegung personenbezogener Daten treffen müssen. Sie müssen auch in der Lage sein, ihre Entscheidung zu erklären:

Landesarbeitsgericht Berlin, Urteil vom 30.03.2023 (5 Sa 1046/22)

Der Verantwortliche hat vorzutragen, welche konkreten personenbezogenen Daten nicht herausgegeben werden können, ohne dass schützenswerte Interessen Dritter tangiert werden. Zu dieser Darlegung müssen nicht schon die personenbezogenen Daten als solche preisgegeben werden.

Entscheidungen über Auskunft und Akteneinsicht **in konfliktträchtigen Situationen** müssen daher nicht nur bewusst und sorgsam vorgenommen werden. Sie müssen auch **nachvollziehbar dokumentiert** werden. So kommt es eventuell dazu, dass Auskunftsberechtigte oder von einer Offenlegung betroffene Personen Beschwerde beim ULD einreichen oder sogar vor Gericht ziehen.

Eine ordentliche Dokumentation dient Verantwortlichen dann dazu, den **Nachweis erbringen zu können**, die Interessen sowohl der einen wie auch der anderen Seite angemessen berücksichtigt zu haben.

4.1.10 Ein Personalausweis halb auf Abwegen

Eine ungewöhnliche Beschwerde erreichte das ULD wegen eines **offenbar unsachgemäß entsorgten Personalausweises**: Die Inhaberin hatte beim örtlichen Bürgerbüro ganz regulär einen neuen Ausweis beantragt und das abgelaufene Exemplar zur Entsorgung dort abgegeben. Wenige Wochen später tauchte eine Hälfte des abgelaufenen Ausweises an unerwarteter Stelle wieder auf. Ein völlig Fremder meldete sich über Social Media bei der betroffenen Person: Er habe das Teil der Karte beim Besuch eines **Festivals in den Niederlanden** entdeckt, und zwar auf dem Campingplatz des Festivalgeländes.

Vermutlich gelang die Identifizierung anhand der gut leserlichen und **in Gänze erhaltenen Unterschrift**. Glücklicherweise war der Finder bereit, den halben Ausweis zurückzuschicken.

Auch die **Entsorgung amtlicher Dokumente** unterliegt datenschutzrechtlichen Bestimmungen. Denn bei der „Vernichtung" handelt es sich um eine Verarbeitung von personenbezogenen Daten im Sinne von Art. 4 Nr. 2 DSGVO. Vor allem zu beachten ist hierbei einer der allgemeinen Grundsätze des Datenschutzrechts:

Art. 5 Abs. 1 Buchst. f DSGVO

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, […]

Im folgenden aufsichtsbehördlichen Anhörungsverfahren musste die zuständige Kommune sich auf Fehlersuche begeben. Ob ein **menschliches Fehlverhalten oder eine besondere Unachtsamkeit** zu dem Vorfall führte, war letzten Endes unmöglich nachzuvollziehen. Wenig wahrscheinlich erschien ein Problem bei dem eingesetzten Dienstleister für die Aktenvernichtung: Dessen Maßgaben etwa zum Transport oder zum abschließenden Schreddern von Dokumenten waren sorgsam ausgearbeitet. Vor allem befand sich das Gelände der Firma innerhalb Schleswig-Holsteins.

Als möglicher **Schwachpunkt** fiel aber der **Umgang mit entwerteten Ausweisen innerhalb des Einwohnermeldeamts** auf. Nach Halbierung der eingezogenen Dokumente wurden diese zunächst in einfachen Kartons in den Büroräumlichkeiten zwischengelagert. Ein Umfüllen in den speziellen Datenmüllcontainer des Entsorgungsunternehmens im Keller des Bürogebäudes sollte dabei „regelmäßig" erfolgen.

Als spezielle Regelung für die ordnungsgemäße Vernichtung von Personalausweisen und Pässen gleichermaßen ist die **Allgemeine Verwaltungsvorschrift zur Durchführung des Passgesetzes** heranzuziehen:

Nr. 6.3.4 PassVwV

Bei Vernichtung von Pässen in der Passbehörde ist ein späterer Zugriff auf die Daten im Speichermedium durch weitestgehende Zerstörung des Passes, am besten in einem geeigneten Schredder, zu verhindern.

[…]

Zum Zwecke der Vernichtung können entwertete Pässe auch in einem besonders gesicherten Verfahren an den Passhersteller oder einen geeigneten Dienstleister übersendet werden. […]

Während es demnach zulässig ist, die Dokumente von Externen schreddern zu lassen, ist damit nicht explizit festgelegt, wie eine etwaige **Zwischenverwahrung** bis dahin aussehen kann oder darf.

Eine abschließende Aufklärung des Hergangs, insbesondere des Weges des halben Ausweises bis in die Niederlande, gelang nicht. So blieb der Kommune schließlich nur, die Gefahr einer Wiederholung möglichst auszuschließen. Hierzu wurde ein **spezieller Ausweisschredder** für den Einsatz im unmittelbaren Arbeitsplatzbereich angeschafft. Die personenbezogenen Daten auf den eingezogenen Dokumenten können damit sofort unkenntlich gemacht werden. Einem Abhandenkommen lesbarer Teile sollte so für die Zukunft vorgebeugt sein, unabhängig davon, wer oder was den konkreten Vorfall verursacht hatte.

Was ist zu tun?

Das Vernichten von Ausweisen ist ein gutes Beispiel für einen Verarbeitungsvorgang, der in mehreren Schritten erfolgt. Zu erkennen ist, dass der gesamte Prozess letztlich nur so sicher sein kann wie das schwächste Glied in dieser Kette. An ebendieser Stelle ist anzusetzen, wenn Sicherheitsrisiken bewertet und behandelt werden sollen.

4.1.11 Rechtsmissbräuchlichkeit eines Auskunftsantrags?

Bei dem ULD ging eine Beschwerde ein, in der dargelegt wurde, dass der Verantwortliche die **Erfüllung von Auskunftsanträgen des Beschwerdeführers nach Artikel 15 DSGVO für die Zukunft verweigere**, da diese von ihm als rechtsmissbräuchlich angesehen werden würden. In dem daraufhin gegen den Verantwortlichen eingeleiteten Anhörungsverfahren teilte dieser dem ULD mit, dass er diese Einschätzung u. a. darauf stütze, dass der Beschwerdeführer Anträge gestellt habe, deren Anzahl weit über das übliche Maß hinausgehe.

Im Ergebnis war zunächst festzustellen, dass **eine auf die Zukunft ausgerichtete Bewertung der Anträge nicht zulässig** ist. Der Prüfung, ob Rechtsmissbräuchlichkeit vorliegt, unterliegen jeweils die konkret gestellten Anträge, wobei die in der Vergangenheit gestellten Anträge durchaus herangezogen werden können.

Ferner ergab die Prüfung, dass dem Beschwerdeführer die **Gründe für die Ablehnung** der Auskunftserteilung, d. h. für die angenommene Rechtsmissbräuchlichkeit, **nicht hinreichend konkret** dargelegt worden sind. Eine solche Verpflichtung ist in Art. 12 Abs. 4 DSGVO aber gerade vorgesehen.

Art. 12 Abs. 4 DSGVO

Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

Wird ein Auskunftsantrag gemäß Artikel 15 DSGVO abgelehnt, ist zu berücksichtigen, dass eine Ablehnung des Antrags aus Gründen der Rechtsmissbräuchlichkeit nur unter den in **Art. 12 Abs. 5 Satz 2 DSGVO** genannten Voraussetzungen zulässig ist. Diese Regelung, die eng auszulegen ist, sieht **zwei Fallkonstellationen** vor, in denen eine rechtsmissbräuchliche Antragstellung möglich sein kann: zum einen den **offensichtlich unbegründeten Antrag**, zum anderen exzessive Anträge.

Ein Antrag ist nicht schon deshalb exzessiv, weil er einen hohen Bearbeitungsaufwand auslöst. Erforderlich ist vielmehr ein rechtsmissbräuchliches Verhalten des Antragstellers. Art. 12 Abs. 5 Satz 2, 2. Alt. DSGVO nennt als Beispiel hierfür die **häufige Wiederholung eines Antrags**. Insoweit ist jedoch zu berücksichtigen, dass die bloßen Wiederholungen für sich genommen noch keine Rechtsmissbräuchlichkeit begründen. Hierfür bestehen nur dann Anhaltspunkte, wenn die Anträge ohne stichhaltigen Grund in so kurz hintereinander geschalteten Zeitintervallen gestellt werden, dass sich die Umstände sowie die rechtlichen Gegebenheiten unmöglich geändert haben können und ein anderer Ausgang daher fernliegend ist. Dann kann die Prüfung im Einzelfall ergeben, dass die Antragstellung lediglich der Behinderung des Verantwortlichen und nicht der Geltendmachung der eigenen Rechte dient.

Aus dem Wortlaut des Art. 12 Abs. 5 Satz 2 DSGVO „insbesondere" lässt sich jedoch folgern, dass der Verordnungsgeber abgesehen von der wiederholten Antragstellung auch weitere Formen von exzessiven Anträgen erfasst sehen möchte. Die einschlägige Rechtsprechung wertet Anträge nach Artikel 15 DSGVO einheitlich dann als rechtsmissbräuchlich, wenn der **Antragsteller mit seinem Begehren von der Rechtsordnung missbilligte Ziele verfolgt, arglistig oder schikanös handelt**. Die bloße hohe Anzahl von Anträgen begründet grundsätzlich aus sich heraus nicht bereits eine Rechtsmissbräuchlichkeit. Es bedarf vielmehr klarer Belege, die darauf schließen lassen, dass die Anzahl der Anträge aus einer bestimmten Motivation heraus – z. B. für eine Bindung von Arbeitskapazitäten – genutzt wird.

Die Angaben des Verantwortlichen im zugrunde liegenden aufsichtsbehördlichen Prüfverfahren des ULD waren **nicht hinreichend konkret**, um

eine **Rechtsmissbräuchlichkeit** der Anträge nachweisbar und begründet darzulegen.

Das ULD hat entsprechende Hinweise gegenüber dem Verantwortlichen erteilt sowie erläutert, dass es gegenüber dem Beschwerdeführer einer Darlegung der konkreten Gründe bedarf, wenn der Verantwortliche an der Einschätzung, die bereits gestellten und noch nicht beantworteten Anträge seien als rechtsmissbräuchlich zu bewerten, festhält – einschließlich der **Aufklärung** über die Möglichkeit, einen **gerichtlichen Rechtsbehelf** einlegen zu können.

Was ist zu tun?

Beruft sich eine öffentliche Stelle auf die Rechtsmissbräuchlichkeit eines Auskunftsantrags, so hat sie die Gründe hierfür konkret darzulegen und zu beweisen. Im Falle einer Ablehnung des Antrags sind der betroffenen Person die konkreten Gründe detailliert darzulegen, und es ist darauf hinzuweisen, dass die Möglichkeit besteht, bei einer Aufsichtsbehörde eine Beschwerde oder beim Verwaltungsgericht einen Rechtsbehelf einzulegen.

4.1.12 Verwendung einer Personalausweiskopie zur Identitätsprüfung bei Auskunftsanträgen gemäß Artikel 15 DSGVO?

Im Rahmen eines Anhörungsverfahrens war das ULD mit der rechtlichen Bewertung befasst, ob **Personalausweiskopien für die Identitätsprüfung** bei Auskunftsanträgen gemäß Artikel 15 DSVO von den Antragstellern angefordert werden dürfen.

Bei Eingang eines Auskunftsbegehrens gemäß Artikel 15 DSGVO ist zu prüfen, ob ein Identitätsnachweis erforderlich ist. Für die Fälle, in denen **„begründete Zweifel an der Identität der natürlichen Person"** bestehen, die den Auskunftsantrag stellt, kann der Verantwortliche gemäß Art. 12 Abs. 6 DSGVO zusätzliche Informationen anfordern, die zur Bestätigung der Identität erforderlich sind. Zweifel an der Identität setzen voraus, dass die vorhandenen Daten auf eine bestimmte Identität zwar hindeuten und somit eine Identifizierung grundsätzlich möglich ist, aber nach den Umständen Zweifel daran bestehen, ob der Antragsteller tatsächlich die identifizierte Person ist. Die Tatsache, dass begründete Zweifel bestehen, ist einerseits gegenüber dem Antragsteller im Einzelfall darzulegen und andererseits für den internen Verfahrensablauf zu dokumentieren.

Für den Identitätsnachweis sind gemäß Art. 12 Abs. 6 DSGVO die erforderlichen Angaben zu erheben. Art. 12 Abs. 6 DSGVO rechtfertigt dagegen **keine routinemäßige Identitätsprüfung**.

Sollte sich im Einzelfall ergeben, dass der Personalausweis zum Identitätsnachweis erforderlich ist, ist zu beachten, dass das Anfertigen bzw. Einholen einer Kopie eines Personalausweises **grundsätzlich der Einwilligung des Ausweisinhabers bedarf**, § 20 Abs. 2 Personalausweisgesetz. In diesem Zusammenhang sind die Anforderungen an eine wirksame Einwilligung nach Artikel 7 DSGVO zu berücksichtigen.

Ferner ist der Grundsatz der **Datenminimierung** zu berücksichtigen. Angaben aus dem Personalausweis, die nicht benötigt werden, dürfen nicht erhoben werden. Bei Abfrage der Kopie ist daher gegenüber dem Antragsteller darauf hinzuweisen, welche Angaben benötigt werden und dass die weiteren Angaben auf der Kopie von dem Antragsteller zu schwärzen sind. Etwa **Augenfarbe, Körpergröße auf der Ausweisrückseite und die sechsstellige Zugangsnummer** auf der Ausweisvorderseite sind dabei zur Identifikation

regelmäßig **nicht erforderlich**. Anderes gilt z. B. für die Angaben zu Name und Vorname, zur ausstellenden Behörde, zum Gültigkeitsdatum für den Ausweis und gegebenenfalls zur Anschrift.

Sofern eine **Kopie des Personalausweises per E-Mail** erbeten bzw. eine Übermittlung per E-Mail den Umständen nach erwartet werden kann, ist zu berücksichtigen, dass auch bei der elektronischen Kommunikation sichergestellt sein muss, dass Dritte keine Kenntnis von den personenbezogenen Daten bekommen können. Zur Gewährleistung der Datensicherheit sind dann effektive Maßnahmen, insbesondere eine angemessene **Ende-zu-Ende-Verschlüsselung**, vorzusehen. Eine bloße Transportverschlüsselung wäre nicht ausreichend.

Werden personenbezogene Daten unverschlüsselt per E-Mail übermittelt, ist nicht sichergestellt, dass Dritte keine Kenntnis nehmen können, da die **unverschlüsselte E-Mail-Kommunikation** ein unsicheres Kommunikationsmedium ist. Im Bedarfsfall ist daher die Möglichkeit anzubieten, dass die Übersendung per E-Mail verschlüsselt erfolgen kann.

Was ist zu tun?

Öffentliche Stellen haben im Einzelfall zu prüfen, welche Daten bei begründeten Zweifeln an der Identität des Antragstellers zu erheben sind. In Betracht kommen auch geschwärzte Kopien von Ausweisdokumenten. Im Falle einer digitalen Kommunikation sind zur Wahrung der Datensicherheit angemessene Verschlüsselungsverfahren einzusetzen.

4.1.13 Verletzung des Schutzes personenbezogener Daten: Risikoprognose unerlässlich

Bei der Prüfung von Meldungen gemäß Artikel 33 DSGVO, die von Verantwortlichen bei **Verletzungen des Schutzes personenbezogener Daten** beim ULD eingegangen sind, war vereinzelt festzustellen, dass keine Risikoprognose von den Verantwortlichen durchgeführt worden ist.

Die Durchführung einer **Risikoprognose ist unerlässlich**, um beurteilen zu können, ob für den Verantwortlichen eine **Meldepflicht** gegenüber der Aufsichtsbehörde gemäß Art. 33 Abs. 1 DSGVO und gegebenenfalls eine **Benachrichtigungspflicht** gegenüber den betroffenen Personen nach Art. 34 Abs. 1 DSGVO besteht.

Im Falle der Verletzung des Schutzes personenbezogener Daten **meldet** der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, sie der zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Hinsichtlich der Schwere des Risikos wird in Art. 33 Abs. 1 DSGVO ausdrücklich nicht auf ein hohes Risiko abgestellt.

Die Risikobeurteilung hat nach den Leitlinien der Artikel-29-Datenschutzgruppe zwei wichtige Gründe: Einerseits kann der Verantwortliche **leichter wirksame Maßnahmen zur Eindämmung und Behebung der Datenschutzverletzung** ergreifen, wenn ihm die Eintrittswahrscheinlichkeit und mögliche Schwere der Folgen für die betroffenen Personen bekannt sind. Andererseits kann er so besser beurteilen, ob die **Meldung an die Aufsichtsbehörde erforderlich** ist und ob die betroffenen Personen gegebenenfalls von der Datenschutzverletzung **benachrichtigt** werden müssen (Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, WP 250 Rev. vom 06.02.2018, Seite 27).

Die Leitlinien der Artikel-29-Datenschutzgruppe sind unter folgendem Link abrufbar:

www.datenschutzkonferenz-online.de/wp29-leitlinien.html

Kurzlink: *https://uldsh.de/tb42-4-1-13a*

Diese Leitlinien sind vom Europäischen Datenschutzausschuss aufgenommen und im Rahmen der „Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten" ergänzt worden. Jene Leitlinien aus dem Jahr 2021 sind unter folgendem Link abrufbar:

https://edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_de.pdf

Kurzlink: *https://uldsh.de/tb42-4-1-13b*

Demgegenüber besteht eine **Benachrichtigungspflicht** gegenüber den betroffenen Personen dann, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich **zu einem hohen Risiko für die Rechte und Freiheiten** der betroffenen Personen führt, Art. 34 Abs. 1 DSGVO, und kein Ausschlussgrund greift, Art. 34 Abs. 3 DSGVO. Bei der Bewertung, ob ein hohes Risiko für die betroffenen Personen anzunehmen ist, ist sowohl die Eintrittswahrscheinlichkeit als auch die Schwere des Schadens zu berücksichtigen. Das Risiko ist anhand einer objektiven Bewertung zu beurteilen, wobei die Erwägungsgründe 75 und 76 der DSGVO heranzuziehen sind.

Sowohl die konkreten Bewertungskriterien, anhand derer die Risikoprognose durchgeführt wird, als auch das Ergebnis müssen zur Erfüllung der Rechenschaftspflicht **dokumentiert** werden, Art. 5 Abs. 2 DSGVO. Darüber hinaus sind Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung stehenden Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen nach Art. 33 Abs. 5 DSGVO **auch unabhängig von dem Bestehen eines Risikos** zu dokumentieren.

Was ist zu tun?

Im Falle einer Verletzung des Schutzes personenbezogener Daten ist u. a. eine Risikoprognose gemäß den Leitlinien der Artikel-29-Datenschutzgruppe für die Meldung und Benachrichtigung bei Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679 durchzuführen. Diese darauf beruhende Bewertung sowie das Ergebnis sind zur Erfüllung der Rechenschaftspflicht zu dokumentieren.

4.2 Polizei

4.2.1 Einsatz von Bodycams künftig auch in Wohnungen?

Im Berichtszeitraum haben wir gegenüber dem Schleswig-Holsteinischen Landtag zu einem **Gesetzentwurf** zur Änderung des Landesverwaltungsgesetzes Stellung genommen, mit dem der Einsatz von Bodycams durch die Polizei auch in Wohnungen ermöglicht werden soll.

Die gegenwärtige gesetzliche Regelung für den Einsatz von Bodycams schließt deren Verwendung in Wohnungen aus. Bereits im Pilotprojekt der Landespolizei zur Erprobung von Bodycams zeigte sich, dass – obwohl ausdrücklich ausgeschlossen – die Bodycams in mehreren Fällen

auch in Wohnungen zum Einsatz kamen (vgl. 37. TB, Tz. 4.2.3). Seitdem haben die politischen Forderungen nach einer gesetzlichen Ermächtigung für den Bodycam-Einsatz in Wohnungen zugenommen. Die **Landesregierung** hat im Berichtszeitraum einen entsprechenden **Gesetzentwurf vorgelegt**. Wir haben dazu schriftlich und in einer mündlichen Anhörung im Innen- und Rechtsausschuss des Schleswig-Holsteinischen Landtages Stellung genommen.

Angesichts der erhöhten Gefährdungslage für die Polizeibeamtinnen und Polizeibeamten bei Einsätzen in Wohnungen mag die Forderung nach Bodycams als Schutzmaßnahme nachvollziehbar sein. Es ist dabei jedoch zu beachten, dass Wohnungen dem besonderen Schutz des Artikels 13 Grundgesetz (GG) unterliegen. Es handelt sich um **persönliche Rückzugsorte**, die die Privatsphäre von Menschen berühren. Auch unbeteiligte Dritte, insbesondere Kinder, können durch die Aufnahmen mit betroffen sein. Das Erstellen von Video- und Tonaufnahmen in diesem besonders geschützten Bereich unterliegt daher hohen verfassungsrechtlichen Schranken. Ob eine mit dem Grundgesetz vereinbare und gleichzeitig praktikable Nutzung von Bodycams in Wohnungen möglich ist, ist fraglich. In der **Rechtswissenschaft** werden **erhebliche Bedenken** geäußert, auf die wir in unserer Stellungnahme hingewiesen haben.

Daneben haben wir, größtenteils unabhängig vom Einsatz in Wohnungen, **weitere Empfehlungen** ausgesprochen:

- Eine im Gesetzentwurf vorgesehene Ausnahme von der Pflicht, betroffene Personen **auf die Aufzeichnung hinzuweisen**, ist nicht nachvollziehbar und sollte gestrichen werden.
- Die Pflicht zum Hinweis auf Aufzeichnungen sollte vielmehr ausdrücklich auch für das **Pre-Recording** geregelt werden.
- Wenn der Einsatz in Wohnungen erlaubt wird, sollte gesetzlich klargestellt werden, dass die Aufzeichnung von Inhalten aus dem **Kernbereich privater Lebensgestaltung** zu unterbleiben hat.
- Aufzeichnungen aus Wohnungen sollten **gekennzeichnet** werden, damit die gesetzlichen Schranken auch bei der Weiterverarbeitung beachtet werden.
- Für die **Verlängerung der Aufbewahrungsfrist** für Bodycam-Aufzeichnungen auf Antrag betroffener Personen sollten nicht zu hohe Anforderungen vorgesehen werden.

Was ist zu tun?

Der Gesetzentwurf zur Änderung des Landesverwaltungsgesetzes zum Einsatz von Bodycams sollte entsprechend angepasst werden. Von dem Einsatz von Bodycams in Wohnungen ist aufgrund der verfassungsrechtlichen Risiken abzuraten.

4.2.2 Filmen und Fotografieren von Polizeibeamten im Einsatz

Nicht nur die Polizei nutzt Videotechnik im Kontakt mit Bürgerinnen und Bürgern bei Einsätzen (siehe oben Tz. 4.2.1). Immer häufiger kommt es vor, dass **Bürgerinnen und Bürger das polizeiliche Handeln bei Einsätzen fotografieren oder filmen**. Als zuständige Ordnungswidrigkeitenbehörde für etwaige von den Bürgerinnen und Bürgern dabei begangene Datenschutzverstöße haben wir im Berichtszeitraum eine Reihe von Ordnungswidrigkeitenanzeigen erhalten.

Teilweise wurden von der Polizei auch die Smartphones beschlagnahmt, mit denen Fotos gefertigt worden waren.

Das Fotografieren oder Filmen von Polizeibeamten im Einsatz verstößt nicht regelmäßig gegen das Datenschutzrecht und ist **nicht per se eine Ordnungswidrigkeit**. Es kommt auf die Bewertung des Einzelfalls an:

- Geprüft werden muss zunächst, ob die **DSGVO** für die fotografierenden oder filmenden Privatpersonen überhaupt **anwendbar** ist. Sie gilt nicht für die Verarbeitung personenbezogener Daten zur Ausübung ausschließlich persönlicher Tätigkeiten.
- Ist die DSGVO anwendbar, etwa weil die Absicht erkennbar ist, dass die Aufzeichnungen an Behörden oder andere Organisationen weitergegeben werden sollen, ist zu prüfen, ob es für die Anfertigung und die weitere Verarbeitung der Aufzeichnungen eine **Rechtsgrundlage** gibt. Die DSGVO erlaubt z. B. die Verarbeitung personenbezogener Daten, soweit diese zur Wahrung eines berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, nicht überwiegen.
- Der Begriff des **berechtigten Interesses** ist weit auszulegen. Jedes ideelle Interesse soll darunterfallen. Die Absicht, die Rechtmäßigkeit polizeilichen Handelns nachträglich überprüfen zu lassen, kann z. B. im Einzelfall ein berechtigtes Interesse sein. Kein berechtigtes Interesse ist hingegen die Absicht, Bildmaterial zu sammeln, um dies für Drohungen oder Einschüchterungen der Polizeibeamtinnen und -beamten zu nutzen. Auch die **Veröffentlichung von personenbezogenen Bildern und Filmen im Internet** kann in der Regel nicht auf ein berechtigtes Interesse gestützt werden.
- Dem berechtigten Interesse sind die **schutzwürdigen Interessen der Polizeibeamtinnen und -beamten** gegenüberzustellen. Das Recht auf informationelle Selbstbestimmung und das Recht am eigenen Bild gelten auch für Polizeibeamtinnen und Polizeibeamte im Dienst. Das Maß des Schutzes unterscheidet sich jedoch bei Funktionsträgern und natürlichen Personen: Polizeibeamtinnen und -beamte sind in ihren Persönlichkeitsrechten geringer betroffen und weniger schutzbedürftig, da sie nicht als Privatpersonen, sondern als Repräsentanten des Staates auftreten. Dies ist in der nach der DSGVO erforderlichen **Interessenabwägung** zu berücksichtigen.

Nach diesen Maßstäben ist **im Einzelfall zu beurteilen**, ob das Filmen oder Fotografieren rechtmäßig ist oder gegen die DSGVO verstößt. Bestehen Anhaltspunkte dafür, dass die Aufnahmen zur Drohung, Einschüchterung oder personenbezogener Veröffentlichung im Internet verwendet werden sollen, kann die Polizei mit den Mitteln der Gefahrenabwehr gegen den Verantwortlichen vorgehen.

Werden **Smartphones** beschlagnahmt, ist zudem die **Verhältnismäßigkeit der Beschlagnahme** besonders zu prüfen. Dabei ist die Bedeutung des Smartphones für das alltägliche Leben der Betroffenen zu berücksichtigen. Ein Verzicht kann für sie im Alltag weitreichende Folgen haben.

Wir haben bislang in keinem der angezeigten Fälle ein Bußgeldverfahren eingeleitet. Ein **hinreichender Verdacht** für eine Ordnungswidrigkeit konnte nach den genannten Maßstäben auf Grundlage des angezeigten Sachverhalts **in keinem der Fälle begründet** werden. Bereits eingeleitete Bußgeldverfahren haben wir aus denselben Gründen eingestellt und in einem Fall ein von der Polizei beschlagnahmtes Smartphone an den Betroffenen aushändigen lassen. Gleichwohl musste der Betroffene während der gesamten Verfahrensdauer von etwa **sechs Wochen auf sein Smartphone verzichten**.

Was ist zu tun?

Film- oder Fotoaufnahmen von Polizeibeamtinnen und Polizeibeamten verstoßen nicht per se gegen das Datenschutzrecht. Hierfür bedarf es einer sorgfältigen Prüfung im Einzelfall. Die pauschale Einleitung von Ordnungswidrigkeitenverfahren wegen etwaiger Datenschutzverstöße ist daher nicht zielführend.

4.2.3 Abruf von Melderegisterdaten im Verkehrsordnungswidrigkeitenverfahren

Verkehrsordnungswidrigkeitenverfahren sind bei den Betroffenen in der Regel nicht sehr beliebt. Sie leisten aber einen wichtigen Beitrag zur Sicherheit und Ordnung im Straßenverkehr. Bei jährlich Millionen von registrierten Verkehrsverstößen fallen bei den zuständigen Ordnungsbehörden große Mengen personenbezogener Daten an.

Bei Geschwindigkeitsverstößen wird in der Regel über das Kfz-Kennzeichen der Halter durch eine **Abfrage beim Kraftfahrt-Bundesamt (KBA)** ermittelt und zum Sachverhalt befragt. Gelegentlich sind weitere Ermittlungen zur Feststellung des Fahrzeugführers erforderlich. Zur Erfüllung dieser Aufgabe sind die zuständigen Ordnungsbehörden mit entsprechenden Ermittlungsbefugnissen ausgestattet. Dazu gehört auch die Möglichkeit, mithilfe von Melderegisterabfragen weitere personenbezogene Daten zu erheben. Dies darf (und sollte) jedoch nicht pauschal oder ohne besonderen Anlass geschehen, wie der folgende Fall zeigt:

Im Berichtszeitraum wurde einem Betroffenen ein Anhörungsbogen wegen eines festgestellten Geschwindigkeitsverstoßes zugestellt. Die **Zustellung** erfolgte jedoch nicht an den beim KBA korrekt gemeldeten Hauptwohnsitz des Betroffenen, sondern **an einen nicht ständig genutzten Nebenwohnsitz**. Dadurch wurde die von der Behörde gesetzte Frist versäumt, was zu weiteren Kosten führte. Der Betroffene beschwerte sich daraufhin zunächst bei der zuständigen Behörde und verlangte in diesem Zusammenhang auch Auskunft darüber, woher die Behörde die Adresse seines Zweitwohnsitzes habe. Die Behörde erstattete daraufhin kommentarlos die durch die Falschzustellung entstandenen Gebühren und Auslagen.

Der Betroffene beschwerte sich daraufhin beim ULD. Im Rahmen der Anhörung teilte die Ordnungsbehörde mit, dass die **Adresse des Zweitwohnsitzes durch eine Melderegisterabfrage ermittelt** worden sei. Durch ein Büroversehen sei der Anhörungsbogen dann nicht an die (durch die KBA-Abfrage bereits bekannte) Hauptwohnung, sondern an die Nebenwohnung zugestellt worden. Die Melderegisterabfrage sei jedoch rechtlich zulässig gewesen. Die Nachfrage des Betroffenen, woher die Behörde die Adresse des Zweitwohnsitzes habe, sei übersehen worden, da sie in ein allgemeines Beschwerdeschreiben eingebettet gewesen sei. Mit der Erstattung der Säumniszuschläge sei die Angelegenheit als erledigt angesehen worden.

Also alles nur eine Unachtsamkeit? Richtig ist, dass die Ordnungsbehörden das Melderegister abfragen dürfen. Aber darf das in jedem Fall und unter allen Umständen geschehen? Das Bundesmeldegesetz erlaubt solche Abfragen nur, wenn sie zur Erfüllung einer öffentlichen Aufgabe „erforderlich" sind. Außerdem ist die Meldebehörde an den Grundsatz der Datenminimierung gebunden. Beide Grundsätze sollen sicherstellen, dass nicht mehr personenbezogene Daten verarbeitet werden, als zur Aufgabenerfüllung erforderlich sind.

Aus dem Sachverhalt ergaben sich keine Anhaltspunkte, die weitere Nachforschungen oder Ermittlungen der Ordnungsbehörde erforderlich gemacht hätten. Der aktuelle Name und die Adresse des Beschwerdeführers waren beim

KBA hinterlegt. Im Übrigen hat die – offensichtlich nicht erforderliche – **Melderegisterauskunft** nur dazu geführt, dass der Bußgeldbescheid an die falsche Adresse zugestellt wurde. Die Abfrage war **nicht erforderlich und daher unzulässig**.

Darüber hinaus haben betroffene Personen das Recht, **Auskunft** darüber zu verlangen, **aus welchen Quellen eine Behörde ihre personenbezogenen Daten erhoben** hat. Auch wenn eine solche Frage in einem allgemeinen Beschwerdeschreiben enthalten ist, muss die Behörde darauf reagieren. Mit der Rückerstattung der Säumnisgebühr wurde zwar der finanzielle Schaden ersetzt, gleichzeitig aber der **datenschutzrechtliche Auskunftsanspruch ignoriert**.

Was ist zu tun?

So viel wie nötig, so wenig wie möglich: Bei der Erhebung personenbezogener Daten sind der Grundsatz der Erforderlichkeit und der Grundsatz der Datenminimierung zu beachten. Pauschale Melderegisterabfragen in Verkehrsordnungswidrigkeitenverfahren sind in der Regel nicht erforderlich.

Wer allgemeine Beschwerdeschreiben bearbeitet, sollte den datenschutzrechtlichen Auskunftsanspruch kennen und diesbezügliche Fragen als entsprechenden Antrag behandeln.

4.2.4 Falsche Auskunft aus dem Melderegister

Ein Bürger wandte sich an uns, weil in einem Polizeibericht als seine vermeintlich aktuelle Meldeanschrift eine Adresse genannt wurde, an der er zu dem damaligen Zeitpunkt bereits **seit zehn Jahren nicht mehr wohnte**. Er prüfte zunächst die Einträge im Melderegister dieses Wohnorts. Dort waren der Auszug aus der Wohnung und die Abmeldung korrekt eingetragen. Daraufhin wandte er sich zunächst ohne Erfolg an die Polizei und im Anschluss daran an uns.

Wir haben daraufhin die Polizei um Stellungnahme gebeten, woher die Information über die Adresse stammte und warum diese als aktuell bezeichnet wurde. Die Polizei konnte anhand von Protokolldaten belegen, dass ihr bei der **Abfrage aus der Spiegeldatenbank** des Melderegisters die alte Anschrift als aktuelle Anschrift angezeigt worden war. Eine Abfrage des Melderegisters durch uns, etwa ein Jahr nach der Abfrage der Polizei, ergab hingegen eine andere Anschrift als aktuelle Anschrift. Die alte Anschrift wurde korrekt als frühere Anschrift angezeigt.

Wir haben uns daraufhin an das Innenministerium gewandt. Dort konnte der Fehler ermittelt werden: Zum Zeitpunkt der Melderegisterabfrage der Polizei war eine **fehlerhafte Softwareversion** im Einsatz. Diese hatte die Reihenfolge mehrerer vorhandener Datensätze in der Spiegeldatenbank bei einer landesweiten Suche **nicht nach ihrer Aktualität sortiert**. Somit war der Polizei der ältere Datensatz einer anderen Gemeinde als aktuell angezeigt worden und nicht der neueste Datensatz der Gemeinde des letzten Wohnorts. Zum Zeitpunkt unserer Melderegisterabfrage war der Fehler behoben, sodass wir eine korrekte Auskunft erhalten haben.

Der Beschwerdeführer hatte gegenüber der Polizei die Berichtigung der Adressangabe im Polizeibericht verlangt. Im vorliegenden Fall bestand ein **Berichtigungsanspruch** nicht. Denn trotz der objektiv falschen Anschrift war der Polizeibericht als solches „richtig", da er die Erkenntnisse der Polizei zu dem damaligen Zeitpunkt zutreffend wiedergab. Der Bericht selbst war deshalb nicht zu berichtigen. Ein Berichtigungsanspruch kann hingegen bestehen, wenn in den allgemeinen Stammdaten in polizeilichen

Verarbeitungssystemen unrichtige Daten gespeichert sind. In einem **polizeilichen Vorgang** kann eine **Berichtigung auch in Form einer Ergänzung in Betracht** kommen. Die Richtigkeit ist auch bei einer Weiterverwendung von besonderer Bedeutung: Der Verantwortliche muss gewährleisten, dass unrichtige oder nicht mehr aktuelle personenbezogene Daten nicht übermittelt oder sonst zur Verfügung gestellt werden (§ 74 Abs. 1 BDSG).

Ob die fehlerhafte Softwareversion zu weiteren unrichtigen Suchergebnissen geführt hat, ist nicht bekannt.

4.3 Justiz

4.3.1 Datenpannen in der Justiz

Im Berichtszeitraum sind aus der Justiz **15 Verletzungen des Schutzes personenbezogener Daten**, sogenannte Datenpannen, an das ULD gemeldet worden:

- In den überwiegenden Fällen bestand die Verletzung darin, dass personenbezogene Daten versehentlich **unbefugten Dritten zur Kenntnis gelangt** sind oder zur Kenntnis gelangen konnten.
- In den meisten Fällen (sechs Meldungen) ist dies durch eine **fehlerhafte Adressierung** beim Versand von Schreiben, Unterlagen oder Akten per Post oder E-Mail geschehen.
- In anderen Fällen lag die Ursache z. B. darin, dass versäumt wurde, eine **Auskunftssperre** im Fachverfahren einzutragen oder der in der Akte dokumentierte Wunsch einer Verfahrensbeteiligten, ihre Anschrift nicht an andere Verfahrensbeteiligte weiterzugeben, übersehen wurde.
- In einem anderen Fall wurde versäumt, aus einer Aufstellung über Beschäftigte die **Hinweise auf eine Schwerbehinderung zu entfernen**, bevor diese Liste an die Personalvertretungen weitergegeben wurde.
- Eine Meldung betraf den **Verlust von personenbezogenen Daten**. Hier wurde festgestellt, dass ein USB-Stick mit sensiblen personenbezogenen Daten sich nicht mehr in der Akte befand und auch sonst nicht auffindbar war.

In allen gemeldeten Fällen haben die Justizbehörden auf den Vorfall reagiert und **Abhilfemaßnahmen** im konkreten Fall sowie häufig auch weitere Maßnahmen ergriffen, um künftige ähnliche Vorfälle möglichst zu verhindern.

(Zu) zurückhaltend waren einige Behörden bei der Benachrichtigung betroffener Personen. Diese ist nach dem Gesetz vorgeschrieben, wenn eine Verletzung des Schutzes personenbezogener Daten voraussichtlich eine erhebliche Gefahr für Rechtsgüter betroffener Personen zur Folge hat. Dies kann insbesondere bei Strafverfahren der Fall sein, da das **Bekanntwerden eines Strafverfahrens für die betroffene Person erhebliche rufschädigende Auswirkungen** haben kann.

Was ist zu tun?

Im Falle einer Datenpanne muss der Verantwortliche prüfen, ob das Risiko für die Rechte und Freiheiten der betroffenen Personen durch gezielte Maßnahmen beseitigt oder zumindest verringert werden kann. Bei erheblichen Risiken ist ebenfalls die Benachrichtigung betroffener Personen erforderlich. Der Verantwortliche muss zudem prüfen, worin die Ursache der Verletzung lag und ob sich daraus Anpassungsbedarf für technische und organisatorische Maßnahmen ergibt, damit ähnliche Vorfälle möglichst vermieden werden. Schließlich ist die Schutzverletzung der Aufsichtsbehörde zu melden. Zu einer Meldung gehört grundsätzlich eine Beschreibung des Vorfalls und des Ergebnisses der vorgenannten Prüfungen.

4.3.2 Grundbucheinsicht durch einen Notar – ohne berechtigtes Interesse?

Eine Bürgerin wandte sich an uns, weil ein **Notar** für seine Mandantin **Einsicht** in ihren Grundbucheintrag genommen und eine **Kopie des Grundbuchauszugs an seine Mandantin** weitergegeben hatte. An der Rechtmäßigkeit der Einsicht habe sie Zweifel. Sie sei alleinige Eigentümerin des Grundstücks und stehe in keinerlei Verbindung zu der Mandantin des Notars. Daher habe die Mandantin kein berechtigtes Interesse an einer Grundbucheinsicht haben können.

Der Grundbuchauszug bestätigt die Angaben der Beschwerdeführerin, dass sie alleinige Eigentümerin ist. Die Mandantin hatte dem Notar gegenüber eine Vermutung über abweichende Eigentumsverhältnisse an dem Grundstück geäußert, sodass nicht festgestellt werden konnte, dass bereits für die Einsichtnahme durch den Notar das vom Gesetz geforderte **berechtigte Interesse an der Einsichtnahme fehlte**. Bei der Einsicht konnte der Notar jedoch erkennen, dass die Vermutung seiner Mandantin über die Eigentumsverhältnisse an dem Grundstück falsch war und sie tatsächlich kein berechtigtes Interesse an der Kenntnis über das Grundstück hat. Für die **Weitergabe des Grundbuchauszugs an seine Mandantin** gab es daher **keine Rechtsgrundlage**.

Da der Notar das **Versäumnis selbst erkannt und von sich aus Maßnahmen ergriffen hat**, konnte das Verfahren mit einem Hinweis an den Notar abgeschlossen werden.

Was ist zu tun?

Die Einsichtnahme in Grundbücher anderer Personen ist nur zulässig, wenn hierfür ein berechtigtes Interesse vorliegt. Nehmen Notare oder Rechtsanwälte für Mandantinnen und Mandaten Einsicht, müssen sie das berechtigte Interesse nicht nur bei der Einsichtnahme selbst prüfen. Vielmehr müssen sie auch nach erfolgter Einsichtnahme prüfen, ob das berechtigte Interesse angesichts der Eintragungen im Grundbuch immer noch besteht. Nur soweit dies der Fall ist, dürfen sie Informationen aus dem Grundbuch an die jeweiligen Mandantinnen und Mandanten weitergeben.

4.4 Soziales

4.4.1 Einmal sensible Sozialdaten für alle – das Problem mit den E-Mail-Verteilern

Eine **goldene Regel** in der Verwaltung lautet, dass zunächst die **Zuständigkeit geprüft** werden muss. Wer ist z. B. in der Kreisverwaltung für die Abrechnung von kieferorthopädischen Behandlungen eines bestimmten Kindes zuständig, wenn die Eltern Sozialleistungen erhalten? Eine Mitarbeiterin fragte per interner E-Mail bei den Kollegen nach. Leider **„verklickte"** sie sich bei der Auswahl des internen E-Mail-Verteilers. So erhielten nicht nur die Kollegen, die für diesen Bereich zuständig sind, sondern **822 Empfänger** aller Fachbereiche bzw. Fachdienste der Kreisverwaltung ihre Nachfrage und damit Kenntnis von dem Antrag der Eltern.

Es existierten Regelungen zum Datenschutz und eine Dienstanweisung zur E-Mail-Kommunikation, die auch allen Beschäftigten der Kreisverwaltung zur Verfügung standen. Zur Entschuldigung führte der Kreis in seiner **Datenpannenmeldung** aus, dass die Kollegin gerade erst ihre Ausbildung beendet habe.

Was ist zu tun?

Gerade neue, noch unerfahrene Kolleginnen und Kollegen müssen ausreichend über die Anforderungen zum Schutz von Sozialdaten geschult werden. Dies gilt auch bzw. gerade für die alltäglichen Arbeitsprozesse z. B. bezüglich der Übermittlung von Sozialdaten.

4.4.2 Auskunft erteilen – aber bitte nicht per Salamitaktik!

Stellen Sie sich vor, Sie bekommen im Jugendamt endlich einen Termin für eine Akteneinsicht – und dann wird Ihnen eine Akte mit inhaltsleeren Seiten vorgelegt. Über **600 Seiten sind komplett geschwärzt**, oder es sind nur noch Ihr **Name und die Seitenzahlen** zu lesen. Sie werden darauf hingewiesen, dass es nicht erlaubt sei, die leeren Seiten zu fotografieren oder zu kopieren. Sie könnten sich ja Notizen machen.

Das können Sie sich nicht vorstellen. Konnten wir auch nicht. Aber genau das schilderte uns ein Beschwerdeführer. Der Mitarbeiter des Jugendamts habe bei dieser Akteneinsicht sichtlich seinen Spaß gehabt, so der Beschwerdeführer.

Das Amt erklärte auf Nachfrage, dass **alle Angaben, die andere Personen, z. B. der Kindesmutter, betreffen würden, geschwärzt** worden seien. Der Beschwerdeführer bezweifelte, dass ausschließlich Unterlagen der Kindesmutter geschwärzt wurden, und fragte, warum z. B. auch Schreiben geschwärzt wurden, die er selbst geschrieben und an das Jugendamt geschickt hatte. Exemplarisch benannte der Beschwerdeführer einige seiner Schreiben. Das Jugendamt räumte daraufhin ein, dass **zu viel geschwärzt** worden sei. Der Beschwerdeführer erhielt die von ihm benannten Unterlagen, aber auch nicht mehr. Der Beschwerdeführer benannte daraufhin weitere Unterlagen, woraufhin das Jugendamt **einräumte, dass auch diese hätten beauskunftet werden müssen**.

Sie ahnen, wie die Geschichte weitergeht. Erneut musste der Beschwerdeführer darauf hinweisen, dass die Akte weitere Unterlagen mit Daten zu seiner Person enthalten müsste. Das Jugendamt **prüfte also ein drittes Mal**, und siehe da, der **Beschwerdeführer hatte recht**. Ihm wurden

weitere Unterlagen ausgehändigt. Seit dem ersten Termin für Akteneinsicht waren **zwei Jahre vergangen**.

Selbstverständlich beanstandeten wir das **Verhalten des Jugendamts** und machten von unseren Abhilfebefugnissen Gebrauch.

Was ist zu tun?

Macht eine betroffene Person von ihrem Auskunftsrecht Gebrauch, so muss der Verantwortliche die geforderten Informationen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung stellen. Diese Frist kann um zwei Monate verlängert werden, wenn dies z. B. aufgrund der Komplexität und der Anzahl von Anträgen erforderlich ist. In einem solchen Fall muss die betroffene Person innerhalb der Monatsfrist zusammen mit den Gründen über die Verzögerung unterrichtet werden.

4.5 Schutz des Patientengeheimnisses

4.5.1 Corona-Testzentren – Zulässigkeit von Abrechnungsprüfungen der KVSH durch ein Inkassobüro

Im Berichtsjahr erhielten wir verschiedene Anfragen von Corona-Testzentren, u. a. von einer Apotheke, ob denn die **Kassenärztliche Vereinigung Schleswig-Holstein (KVSH)** berechtigt wäre, gezielte vertiefte **Prüfungen der ordnungsgemäßen Durchführung und Abrechnung von Corona-Testungen** unter Einbeziehung der lokalen Dokumentation **durch ein privates Unternehmen** durchführen zu lassen.

Ja! Gemäß § 7a Abs. 2 der Coronavirus-Testverordnung ist festgelegt, dass die Kassenärztlichen Vereinigungen der Länder im Rahmen ihrer Abrechnungsprüfungen stichprobenartig oder dann, wenn Veranlassung dazu besteht, gezielte vertiefte Prüfungen vornehmen müssen. Für die Durchführung der Prüfung sind die Leistungserbringer und die sonstigen abrechnenden Stellen **verpflichtet, der Kassenärztlichen Vereinigung auf Verlangen Auskunft zu erteilen und die Dokumentation zu überlassen**, die für die Prüfung erforderlich ist. Hierzu zählt insbesondere die Auftrags- und Leistungsdokumentation. Die Kassenärztliche Vereinigung war somit befugt, die für die Zwecke der Prüfung erforderlichen Daten zu verarbeiten und **geeignete Dritte mit der Prüfung zu beauftragen**.

Die Kassenärztliche Vereinigung Schleswig-Holstein beauftragte ein Inkassobüro mit der Prüfung. Da dieser Beauftragung ein **Vertrag zur Auftragsverarbeitung** zugrunde lag, waren keine Anhaltspunkte für einen datenschutzrechtlichen Verstoß erkennbar.

4.5.2 Online-Meldung von Corona-Infektionen mit verstecktem Tracking?

Das Infektionsschutzteam einer Kreisverwaltung ermöglichte im Herbst 2022 Personen, die sich mit dem **Coronavirus infiziert** hatten, ihrer zu diesem Zeitpunkt bestehenden Meldepflicht mittels eines online zur Verfügung gestellten **„Kontaktformulars für Positive“** nachzukom-

men. Als besondere Serviceleistung wurden zudem u. a. eine Vorlesefunktion, ein Übersetzungsprogramm und ein Tool für die **Barrierefreiheit** angeboten. Genutzt wurden hierfür die Angebote externer Dienstleister (u. a. ReadSpeaker, Google und DIGIaccess).

Allerdings fehlte eine ausreichende Information über die beabsichtigte Datenverarbeitung (Artikel 13 DSGVO). Zudem wurden die betroffenen Personen nicht darüber aufgeklärt, dass bei Nutzung der Vorlesefunktion, des Übersetzungsprogramms und des Tools für die Barrierefreiheit **personenbezogene Daten an die Dienstleister übermittelt** werden. Die betroffenen Personen waren im Zweifel völlig ahnungslos. Für die Übermittlung der personenbezogenen Nutzerdaten an die Dienstleister lag deren Einverständnis nicht vor.

Die Kreisverwaltung reagierte umgehend auf unsere Nachfrage. Das Online-Meldeportal wurde um die fehlenden **Informationen zum Zweck der Datenverarbeitung ergänzt**. Zudem wurde die Nutzung der Vorlesefunktion, des Übersetzungsprogramms und des Tools für die Barrierefreiheit von dem **Einverständnis der Nutzenden** abhängig gemacht. Es wurde zugesagt, einen eindeutigen Hinweis aufzunehmen, dass die Nutzung der Dienste die Übermittlung personenbezogener Daten an die externen Dienstleister bedingt.

Was ist zu tun?

Nutzen Verantwortliche bei ihren Online-Angeboten externe Dienstleister, so müssen diese ausdrücklich darauf hinweisen, wenn bei der Nutzung dieser Dienste personenbezogene Daten an die Dienstleister übermittelt werden.

4.5.3 Bereitstellung einer Kopie der Patientenakte kostenfrei

§ 630g Abs. 1 und 2 BGB

(1) Dem Patienten ist auf Verlangen unverzüglich Einsicht in die vollständige, ihn betreffende Patientenakte zu gewähren, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Die Ablehnung der Einsichtnahme ist zu begründen. § 811 BGB ist entsprechend anzuwenden.

(2) Der Patient kann auch elektronische Abschriften von der Patientenakte verlangen. Er hat dem Behandelnden die entstandenen Kosten zu erstatten.

Patientinnen und Patienten von Arztpraxen, Kliniken, Pflegeeinrichtungen und anderen Stellen haben ein **Recht auf Einsicht in die eigenen Behandlungsunterlagen**. Vorschriften im Bürgerlichen Gesetzbuch (BGB) sehen darüber hinaus vor, dass elektronische Abschriften verlangt werden können und dem Behandelnden die entstandenen Kosten zu erstatten sind.

Verschiedene **Berufsordnungen** sehen zudem vor, dass den Patientinnen und Patienten auf deren Verlangen **Kopien der ärztlichen Dokumentation gegen Kostenerstattung** herauszugeben sind. Erfasst sind davon etwa Aufzeichnungen über Befunde und Behandlungsmaßnahmen, die zu jeder zu behandelnden Person getrennt zu führen sind. Beispielhaft bestehen etwa solche Regelungen in den Berufsordnungen der Ärzte- und Zahnärztekammer.

§ 10 Abs. 2 Berufsordnung der Ärztekammer Schleswig-Holstein

Ärzte haben Patientinnen und Patienten auf deren Verlangen in die sie betreffende Dokumentation Einsicht zu gewähren, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder erhebliche Rechte des Arztes oder Dritter entgegenstehen. Auf Verlangen sind dem Patienten Kopien der Unterlagen gegen Erstattung der Kosten herauszugeben.

§ 12 Abs. 4 Berufsordnung der Zahnärztekammer Schleswig-Holstein

Der Zahnarzt hat dem Patienten auf dessen Verlangen, Einsicht in die ihn betreffenden zahnärztlichen Dokumentationen zu gewähren. Auf Verlangen sind dem Patienten Kopien der Unterlagen gegen Erstattung der Kosten herauszugeben.

Ein **weiterer Anspruch auf Erhalt einer Kopie der vorhandenen Patientenunterlagen** ergibt sich aus der **DSGVO**. Die erste Kopie ist demnach **kostenfrei** zur Verfügung zu stellen.

Art. 15 Abs. 3 Satz 1 und 2 DSGVO

Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen.

Uns erreichen in diesem Zusammenhang immer wieder Beschwerden über eine **Nichterteilung kostenfreier Auskünfte** aus den Patientenunterlagen oder eine Bereitstellung solcher Unterlagen ausschließlich gegen Kostenerstattung.

Das **Landgericht Dresden** hatte bereits mit Urteil vom 29.05.2020, Az. 6 O 76/20, entschieden, dass die erste Bereitstellung von **Patientenunterlagen nicht von einer Kostenerstattung abhängen** darf, soweit sich die Patientinnen oder Patienten dabei auf den Auskunftsanspruch nach der DSGVO berufen. Nach Überzeugung des Gerichts steht dieser Bewertung nicht entgegen, dass nach nationalem Recht, vor allem nicht auf Grundlage von § 630g BGB, eine Kostenerstattung vorgesehen ist. Dieser Einordnung ist das ULD seither gefolgt und wirkte in Beschwerdeverfahren auf die Bereitstellung kostenfreier Kopien der Patientenunterlagen hin.

Der **Europäische Gerichtshof (EuGH)** hat in einer Entscheidung vom 26.10.2023, Az. C-307/22, nunmehr für weitere Klarheit und Sicherheit in der Rechtsanwendung gesorgt und vor allem folgende Punkte hervorgehoben:

- Ein Arzt, der eine vorgeschriebene Dokumentation für seine Patienten führt, ist als datenschutzrechtlich **Verantwortlicher im Sinne der DSGVO** anzusehen und unterliegt damit den mit dieser Eigenschaft einhergehenden Verpflichtungen, wobei er insbesondere auf Antrag der betroffenen Personen gewährleistet, dass über die personenbezogenen Daten Auskunft erteilt wird.
- Die **unentgeltliche Zurverfügungstellung** einer ersten Kopie der personenbezogenen Daten ist nicht davon abhängig, dass die betroffenen Personen ihren Antrag begründen.
- Aus den Erwägungsgründen der DSGVO ist zu entnehmen, dass das Recht der betroffenen Personen auf Auskunft über ihre personenbezogenen Daten im Hinblick auf ihre gesundheitsbezogenen Daten auch **Daten in ihren Patientenakten**, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten, **einschließt**.
- Angesichts der Bedeutung, die die DSGVO dem garantierten Recht auf Auskunft über die personenbezogenen Daten beimisst, darf die **Ausübung dieses Rechts folglich nicht von Bedingungen abhängig gemacht werden, die der Unionsgesetzgeber**

nicht ausdrücklich festgelegt hat. Nationale Regelungen, die eine **entgeltliche Bereitstellung** der Kopie von Patientenunterlagen vorsehen, haben daher auf einen Auskunftsanspruch nach der DSGVO **keinen Einfluss**.

Was ist zu tun?

Betroffene Personen, die bei den Verantwortlichen unter Berufung auf die DSGVO eine Kopie ihrer Patientenunterlagen begehren, haben ein Recht darauf, dass ihnen die erste Kopie unentgeltlich zur Verfügung gestellt wird. Ärztinnen und Ärzte sowie andere verpflichtete Stellen müssen diese Vorgaben berücksichtigen. Im Falle der Versendung einer digitalen Kopie ist auf eine angemessene Verschlüsselung zu achten.

4.5.4 Erhebung des Corona-Impfstatus von Beschäftigten im Jahr 2023

Die **Coronapandemie** konfrontierte in den vergangenen Jahren auch Datenschützerinnen und Datenschützer mit vielen rechtlichen und praktischen Fragen (39. TB, Tz. 1.1; 40. TB, Tz. 4.1.3; 41. TB, Tz. 4.1.4). Während das Thema immer mehr aus der allgemeinen Berichterstattung gewichen ist, beschäftigt die Infektionskrankheit vor allem das Gesundheitswesen jedoch noch immer.

Eine entscheidende Neuerung zum 01.01.2023 war das Auslaufen der sogenannten **einrichtungsbezogenen Impfpflicht** nach dem nun gestrichenen § 20a Infektionsschutzgesetz. Die Regelung schrieb Beschäftigten von medizinischen oder pflegerischen Einrichtungen die Vorlage eines Immunitätsnachweises vor. Bereits im Vorhinein machte die Datenschutzkonferenz auf den **Verbleib von Datenbeständen** aufmerksam, die auf Grundlage dieser Regelung erhoben worden sind:

DSK-Beschluss vom 13. April 2022

Jedenfalls muss eine Löschung aller auf Grundlage des § 20a IfSG verarbeiteten Daten spätestens mit Ablauf der Rechtsgrundlage am 31. Dezember 2022 erfolgen.

Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 13. April 2022: „Zur Verarbeitung personenbezogener Daten im Zusammenhang mit der einrichtungsbezogenen Impfpflicht“:

https://www.datenschutzkonferenz-online.de/media/dskb/2022_13_04_beschluss_DSK_20a_IfSG.pdf

Kurzlink: *https://uldsh.de/tb42-4-5-4a*

Eine Anfrage an das ULD im Jahr 2023 brachte nun die Frage auf, ob ein Krankenhaus trotz Wegfall der Corona-Impfpflicht **weiterhin den Impfstatus von Bewerberinnen oder Bewerbern für eine medizinische Berufsausbildung erheben** darf. Zur Klärung der Sach- und Rechtslage im konkreten Fall wurde das betreffende Klinikum angehört. Tatsächlich konnte es für die Verarbeitung auf eine andere Rechtsgrundlage aus dem **Infektionsschutzgesetz** verweisen:

§ 23a Satz 1 IfSG

Soweit es zur Erfüllung von Verpflichtungen aus § 23 Abs. 3 in Bezug auf übertragbare Krankheiten erforderlich ist, darf der Arbeitgeber personenbezogene Daten eines Beschäftigten über dessen Impf- und Serostatus verarbeiten, um über die Begründung eines Beschäftigungsverhältnisses oder über die Art und Weise einer Beschäftigung zu entscheiden.

Die hier benannten Verpflichtungen treffen die Leitungen von Gesundheitseinrichtungen wie Kliniken und Krankenhäusern, die einer Weiterverbreitung von Infektionskrankheiten entgegenwirken müssen. Das Gesetz verweist bezüglich der Einschätzung solcher Gefahren auf die veröffentlichten Empfehlungen des **Robert-Koch-Instituts**. Eine **Covid-19-Impfung für Personal in medizinischen Einrichtungen** wird darin noch immer nahegelegt. Die entsprechende Mitteilung war zum Zeitpunkt der Abfassung dieses Beitrags weiterhin aktuell.

Anders als die ausgelaufene einrichtungsbezogene Impfpflicht erstreckt sich diese Regelung **nicht pauschal auf alle Mitarbeitenden in einem Krankenhaus**. Die genannten Empfehlungen zu § 23 Abs. 3 IfSG stellen im Sinne einer Erforderlichkeitsbetrachtung auf den Kontakt verschiedener Berufsgruppen mit Patientinnen und Patienten sowie auf deren Vulnerabilität ab. Außen vor sind damit etwa **Beschäftigte in der Verwaltung oder der Haustechnik** medizinischer Einrichtungen.

Solange sich Infektionsschutzmaßnahmen mit Bezug auf das Coronavirus fachlich begründen lassen, müssen Mitarbeitende, Bewerberinnen und Bewerber bestimmter Berufsgruppen jedoch unter Umständen dulden, dass ihr **Impfstatus erhoben und verarbeitet** wird, um ihre **Einsatzbereitschaft** in verschiedenen empfindlichen Arbeitsbereichen beurteilen zu können. Nicht vorweggenommen wird mit dieser Grundlage zur Datenverarbeitung die Zulässigkeit daran gegebenenfalls ansetzender arbeitsrechtlicher Konsequenzen.

Die Rechtslage entspricht nun wieder der **Situation vor dem 16. März 2022**, als die allgemeine einrichtungsbezogene Impfpflicht wirksam geworden war. Hinzuweisen ist daher auch auf den bereits älteren Beschluss der Datenschutzkonferenz „Verarbeitungen des Datums ‚Impfstatus' von Beschäftigten durch die Arbeitgeberin oder den Arbeitgeber" vom 19. Oktober 2021, der damit anwendbar bleibt:

https://www.datenschutzkonferenz-online.de/media/dskb/20211025_DSK_Beschluss_Impfstatus_von_Besch%C3%A4ftigten.pdf

Kurzlink: *https://uldsh.de/tb42-4-5-4b*

Die Beschlüsse der Datenschutzkonferenz sind, nach Jahrgängen sortiert, u. a. hier abrufbar:

https://www.datenschutzkonferenz-online.de/beschluesse-dsk.html

Kurzlink: *https://uldsh.de/tb42-4-5-4c*

4.6 Datenpannen im Medizinbereich

4.6.1 Sensibles Gespräch unter Ärzten – und der Wartebereich hört zu

Eine schwangere Frau ahnte noch nicht, dass sie ihr **Kind verloren** hatte – doch der Ehemann erfuhr es mal soeben nebenbei.

In diesem traurigen Fall musste eine schwangere Patientin wegen akuter Blutungen ins Krankenhaus. Der Ehemann wurde benachrichtigt und fuhr so schnell wie möglich zum Krankenhaus. Dort angekommen, wurde er gebeten, im **Wartebereich** Platz zu nehmen.

Während er wartete, hörte er, wie sich ein **Oberarzt und eine Ärztin** über eine schwangere Patientin **austauschten**, die gerade ihr Kind verloren hatte.

Auch wenn der **Name der Patientin nicht genannt** wurde, war ihm schnell klar, dass man sich über seine Ehefrau unterhielt. So erfuhr der Ehemann noch vor seiner Frau, dass sie ihr Kind verloren hatte.

Was ist zu tun?

Ärztinnen und Ärzte müssen sensible Gespräche vertraulich führen. Es darf keine unbefugten Zuhörerinnen und Zuhörer geben. Hierzu können auch Angehörige gehören. Warte- und Empfangsbereiche sind für sensible Arztgespräche nicht geeignet. Das ärztliche Personal sollte regelmäßig geschult werden. Es müssen geeignete Räume für vertrauliche Gespräche zur Verfügung stehen.

4.6.2 PC-Diebstahl – ein Einbruch kann auch positive Folgen haben

In einer Beratungsstelle, die Straffällige in gemeinnützige Arbeit vermittelt, wurde eingebrochen. Die Diebe entwendeten u. a. einen Desktop-PC, der für die Dokumentation der Beratungstätigkeit genutzt wurde. Auf dem PC waren **personenbezogene Daten von ca. 500 Betroffenen** gespeichert. Entgegen dem bestehenden Datenschutzkonzept war bei diesem PC **keine Festplattenverschlüsselung** erfolgt. Jetzt hatten Unbefugte Zugriff auf diese sensiblen Daten!

Der Träger dieser Beratungseinrichtung nutzte diese Datenschutzverletzung, um aus dem dabei erkannten Problem zu **lernen**. Er erstellte umgehend einen **Zeit- und Maßnahmenplan**. Zunächst wurden alle Beratungsstellen überprüft. So konnte festgestellt werden, dass auch in 16 weiteren Einrichtungen entgegen den bestehenden Anweisungen lokal personenbezogene Daten **unverschlüsselt** gespeichert wurden bzw. unklare Beschreibungen der Schutzmaßnahme erfolgten.

Alle dezentralen Beratungsstellen wurden angewiesen, ihre lokal gespeicherten Daten in die **neue zentrale Ordnerstruktur** des Trägers zu überführen. Für die Einrichtungen wurde ein **sicherer Kanal** geschaffen, um die Daten in das Unternehmensnetzwerk hochzuladen. Wir begleiteten den Prozess.

Was ist zu tun?

Besonders Verantwortliche mit einer Vielzahl von dezentralen Einrichtungen müssen ihre technischen und organisatorischen Maßnahmen regelmäßig überprüfen. So schlimm Datenschutzverletzungen für die betroffenen Personen sein können, so können (und müssen!) diese doch dabei helfen, Lücken bei Sicherheitsmaßnahmen festzustellen und zu beheben.

4.6.3 Unbefugter Umgang mit Patientendaten → Kündigung einer Krankenhausmitarbeiterin

Patientendaten zählen zu den sensiblen Datenkategorien und bedürfen eines besonderen Schutzes vor unbefugter Kenntnisnahme. Mitarbeiterinnen und Mitarbeiter eines Krankenhauses, die mit solchen Daten befugtermaßen Umgang haben, müssen ihre **Verschwiegenheitspflichten** wahren. Mit dieser Verpflichtung nahm es die Mitarbeiterin eines Krankenhauses

wohl nicht so ernst. **Betroffenheit, Interesse und Neugier** liegen oft eng beieinander.

Ein Straftäter wurde medizinisch in einem Krankenhaus behandelt, so wie dies auch vorgesehen war. Nicht vorgesehen ist es jedoch, wenn bei einzelnen Mitarbeiterinnen oder Mitarbeitern private Neugier oder gar **Voyeurismus** die fachliche Aufgabenwahrnehmung überlagert und gefährdet.

In diesem besonderen Fall teilte uns das Krankenhaus mit, dass eine Krankenhausmitarbeiterin aus dem Verwaltungsbereich sehr großzügig mit dem Zugang zu und Zugriff auf personenbezogene Daten von Patienten umgehe, um unberechtigt auf Patientenakten von Kolleginnen und Kollegen zuzugreifen.

Auch die Patientenakte des Straftäters war wohl nicht vor ihr sicher. Diese Mitarbeiterin habe **mit ihrem ergaunerten Wissen geprahlt** und womöglich sogar mit ihrem Handy Fotos von Patientenakten gemacht.

Als die Klinikleitung hiervon erfuhr, reagierte sie schnell und eindeutig. In einem Personalgespräch räumte die Mitarbeitende ihr Fehlverhalten ein. Aufgrund der vorliegenden Rechtsverletzungen und des damit einhergehenden Vertrauensverlustes wurde das **Arbeitsverhältnis beendet**. Die Mitarbeitende wurde aufgefordert, ihre Schlüssel und die Arbeitskleidung zurückzugeben, und musste noch am selben Tag unter Aufsicht das Klinikgelände verlassen.

Die „Orientierungshilfe Krankenhausinformationssysteme (OH KIS)" der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gibt wichtige Hinweise in Bezug auf Berechtigungskonzepte und andere technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Sie ist abrufbar unter dem folgenden Link:

https://www.datenschutzzentrum.de/plugin/tag/klinik/

Kurzlink: *https://uldsh.de/tb42-4-6-3a*

Was ist zu tun?

In Krankenhäusern muss darauf geachtet werden, dass nicht nur im ärztlichen Bereich, sondern auch im Pflege- und Verwaltungsbereich die Mitarbeitenden nur Zugriff auf die Patientendaten haben, die sie für ihre Aufgabe benötigen. Bestehende Berechtigungskonzepte müssen regelmäßig angepasst und eingeräumte Berechtigungen überprüft und aktualisiert werden.

4.6.4 Mutter arbeitet im Krankenhaus – kein Schutz für die Patientendaten der Tochter?

Eine Patientin wurde in einem Krankenhaus psychiatrisch behandelt. Die Mutter arbeitete im Schreibdienst des Krankenhauses und nutzte ihre Zugriffsrechte, um **die Patientenakte ihrer Tochter einzusehen**. Es gab **weder einen fachlichen Grund noch eine Befugnis** für diesen Zugriff. Zusammen mit ihrem Therapeuten entschied sich die Patientin, sich bei der Klinikleitung zu beschweren. Eine mutige und richtige Entscheidung!

Nachforschungen des Datenschutzbeauftragten der Klinik ergaben, dass den Mitarbeiterinnen und Mitarbeitern des Schreibdienstes **abteilungsübergreifende Zugriffsrechte** auf Patientenakten eingeräumt wurden, obwohl nicht jede Schreibkraft für jede Abteilung tätig war.

Umgehend wurden die **Zugriffsrechte beschränkt**. Zukünftig sollen Schreibkräfte nur

noch auf Patientenakten von Abteilungen zugreifen können, wenn sie für diese auch tatsächlich schreiben.

Wieder sei auf die „Orientierungshilfe Krankenhausinformationssysteme (OH KIS)“ der DSK verwiesen (Tz. 4.6.3):

https://www.datenschutzzentrum.de/plugin/tag/klinik/

Kurzlink: *https://uldsh.de/tb42-4-6-4a*

Was ist zu tun?

Bestehende Berechtigungskonzepte müssen regelmäßig angepasst und eingeräumte Berechtigungen überprüft und aktualisiert werden. Nicht ausreichende oder gar fehlende Berechtigungskonzepte können ein Datenschutz-Organisationsverschulden des Verantwortlichen darstellen.

4.6.5 Datenpanne – und der Dienstleister informiert den Auftraggeber nicht?

Ein technisches Problem mit dem Fax? Kein Problem. Schnell den Dienstleister anrufen, der wird den Fehler schon finden. Nur blöd, wenn dem Dienstleister selbst ein Fehler unterläuft und dieser **bei der Fehlersuche ungewollt Arztbriefe an falsche Empfänger versendet**.

Der Fehlversand von Patientenunterlagen stellt unstrittig eine Datenschutzverletzung dar. Sensible Patientendaten gelangen so womöglich in unbefugte Hände. Ein Risiko für die betroffenen Patienten kann dabei nicht ausgeschlossen werden. Aber wer muss diese Datenschutzverletzung der Datenschutzaufsicht melden? Der Auftraggeber oder der Dienstleister? Es ist der **Auftraggeber**. Dieser ist für die Datenverarbeitung verantwortlich.

Arztpraxen können als Verantwortliche externe Dienstleister, sogenannte Auftragsverarbeiter, mit der Verarbeitung von personenbezogenen Daten ihrer Patienten beauftragen (Artikel 28 DSGVO). Grundlage für die Rechtmäßigkeit dieser Auftragsverarbeitung ist insbesondere ein schriftlicher **Auftragsverarbeitungsvertrag**, der u. a. detailliert die Rechte und Pflichten des Auftraggebers und des Auftragsverarbeiters definiert. Hierzu gehört auch, dass der Auftragsverarbeiter als **Dienstleister den Auftraggeber bei der Wahrnehmung seiner Pflicht zur Meldung von Datenschutzverletzungen unterstützt**.

Kommt es also bei dem Dienstleister zu einer Datenpanne, so muss **dieser unverzüglich seinen Auftraggeber informieren**, damit dieser umgehend (und möglichst innerhalb von 72 Stunden) die Datenschutzverletzung der zuständigen Datenschutzaufsichtsbehörde melden und gegebenenfalls die betroffenen Personen benachrichtigen kann.

Was ist zu tun?

Dienstleister müssen beachten, dass die auftraggebende Arztpraxis bzw. das auftraggebende Krankenhaus verantwortlich für die Verarbeitung der Patientendaten ist und bleibt. Wenn es bei der Verarbeitung von Patientendaten durch den Dienstleister zu einer Datenschutzverletzung kommt, so muss die Arztpraxis bzw. das Krankenhaus der Meldepflicht gegenüber der Datenschutzaufsichtsbehörde nachkommen. Der Dienstleister muss daher unverzüglich den Auftraggeber über eine Datenpanne informieren.

4.6.6 Fehlerhaftes Update und keine Datensicherung – alle Patientendaten weg!

Ein IT-Dienstleister wollte in einer Arztpraxis ein Update für die Praxissoftware einspielen. Eigentlich Routine. Aber irgendwas funktionierte nicht, das **Update** musste **fehlerhaft abgebrochen** werden. Ärgerlich war jedoch, dass durch diesen Fehler **Patientendaten im IT-System gelöscht** wurden.

Eigentlich kein großes Problem, schließlich wurden doch täglich **Sicherungskopien** der Patientendaten gemacht, oder etwa nicht? Leider nein. Zwar hatte der Dienstleister hinter einer Feuerschutztür in einem Stahlschrank externe Festplatten für die Datensicherung eingerichtet, jedoch **vergessen**, im Programm den entsprechenden Haken zur täglichen Sicherung zu setzen, und dies entgegen der geltenden Vorgaben auch nicht mehr kontrolliert.

Der Dienstleister versuchte, die Patientendaten zu rekonstruieren. Vergeblich, die Daten blieben fehlerhaft und lückenhaft. **Unwiederbringlich** fehlten u. a. Befunde, Ultraschallbilder, Aufzeichnungen für verschriebene Medikamente, Therapiepläne und Laborberichte. Betroffen waren ca. **2.500 Patientinnen** dieser Arztpraxis für Frauenheilkunde. **Die betroffene Ärztin stellte ihren Praxisbetrieb ein.**

Auch wenn die Patientendaten zwar **nicht in falsche Hände** gekommen sind, so können die Patientinnen nun nicht mehr ihre Daten anfordern. **Die Patientendaten sind weg.**

Was ist zu tun?

IT-Dienstleister sind u. a. aufzufordern,

- Maßnahmen zur Qualitätssicherung des Einspielens von Updates zu ergreifen (Test der einzuspielenden Updates, Sicherung des Datenbestands, Rollback-Funktionalitäten für Software-Updates, temporäre Sicherheitskopien des Gesamtsystems usw.),
- Maßnahmen zur Qualitätssicherung der Back-up-Prozesse (Controlling der Back-up-Konfiguration, der Ausführung einzelner Sicherungsaufträge und der Wiedereinspielbarkeit von Back-ups) zu ergreifen und
- Maßnahmen zu ergreifen, um bei den wiederhergestellten Patientendaten zumindest erkannte Integritätsfehler (Vollständigkeitslücken, Inaktualität von Daten usw.) erkennbar zu machen.

4.6.7 Patientendaten bei TikTok und SnapChat

Videos aufnehmen und online austauschen – ganz einfach mit dem **Smartphone**. So war es auch in unseren beiden Fällen zu TikTok und SnapChat:

Im ersten Fall stellte ein **Praktikant** ein Video von seiner **Arbeit als Pfleger** in einem Krankenhaus bei TikTok online. Das Video bekam umgehend 91 „Gefällt mir", fünf Kommentare und wurde achtmal geteilt. Leider waren in dem **Video auch Daten von Patienten** zu sehen, die nicht ihre Einwilligung erteilt hatten.

Im zweiten Fall hatte ein **FSJler Videos von Pflegeheimbewohnern per SnapChat verschickt**. Eine Empfängerin reagierte fassungslos und stellte den FSJler zur Rede. Wie kann man ungefragt **hilflose Patienten** mit dem privaten Handy filmen, die nicht sprechen oder sich bewegen können? Der FSJler reagierte auf die Kritik mit Unverständnis. Er fand das Ganze **„witzig"**.

Der Praktikant und auch der FSJler wussten, was sie taten. Beide waren zu Beginn ihrer Tätigkeit über den Datenschutz aufgeklärt worden. Die Nutzung privater Handys, das Filmen von Patienten waren ausdrücklich verboten. Es folgten **personalrechtliche Konsequenzen**.

Was ist zu tun?

Verantwortliche stehen in der Pflicht, ihre Beschäftigten über die Anforderungen an den Schutz des Patientengeheimnisses zu unterrichten. Gerade neue und unerfahrene Beschäftigte müssen zu Beginn ihrer Tätigkeit geschult und sensibilisiert werden. Der eigene Datenschutzbeauftragte kann hierbei unterstützen.

4.7 Bildung

4.7.1 Tonne auf dem Schulhof mit alten Schülerakten

Über die **Tücken der Vernichtung von Dokumenten** wurde zuvor bereits berichtet. Eine ordnungsgemäße Zerkleinerung vor Ort mag umsetzbar sein, solange es sich um einzelne Stücke handelt (wie ein Ausweis, Tz. 4.1.10.). Für ganze Aktenbestände ist eine solche Lösung aber kaum vorstellbar, gerade wenn es sich bei der aktenführenden Stelle um eine kleine Einrichtung handelt. Der Aufbewahrung und dem Transport auszusondernder Datenbestände muss dann **besondere Sorgfalt** zukommen.

Eine in dieser Hinsicht unangenehme Datenpanne hatte eine Grundschule zu melden: Eine **Tonne mit alten Schülerakten** hatte – zur Abholung durch ein Entsorgungsunternehmen am nächsten Morgen – über Nacht auf dem **Schulhof** gestanden. Ein denkbarer Zugriff Unbefugter auf die Unterlagen war zu befürchten.

Tatsächlich erreichte das ULD zu dem Vorfall auch die Nachricht eines Hinweisgebers, dem der Behälter in der Nacht aufgefallen war. Soweit nachvollzogen werden konnte, handelte es sich bei dem fraglichen Hof um eine Fläche, die **Passanten frei zugänglich** ist.

Der Hinweisgeber lieferte zusätzliche problematische Details: Die Tonne soll so **überfüllt** gewesen sein, dass einzelne **Unterlagen sich sogar daneben** befunden hätten. Zwei Schülerakten,

die der Finder der Polizei übergab, gehörten offenbar zum **Abgangsjahrgang 2018**. Dass diese nun erst im Jahr 2023 ausgesondert werden sollten, wäre bereits an sich als Missstand zu werten gewesen, da die Schul-Datenschutzverordnung hierfür **ausdrücklich kürzere Fristen** vorsieht:

> **§ 10 Abs. 1 Nr. 1 SchulDSVO**
>
> Schulen haben personenbezogene Daten nach Ablauf der folgenden Fristen zu löschen. Sie betragen zwei Jahre bei Schülerakten und sonderpädagogischen Akten einschließlich Lern- und Förderplänen, kompetenzorientierten Entwicklungsberichten oder Schulübergangsempfehlungen und sonderpädagogischen Gutachten; […]

Erschwerend kommt hinzu, dass die Inhalte von Schülerakten aus vielerlei Gründen naturgemäß als **sensibel** einzustufen sind: Mit Blick auf Erwägungsgrund 75 zur DSGVO lässt sich etwa aufführen, dass es sich um die Daten von Kindern handelt, deren „persönliche Aspekte bewertet werden".

Im Anhörungsverfahren wollte die Schule u. a. mildernd geltend machen, der Hausmeister sei in Rente gegangen und nun nicht angemessen vertreten. Dieser sei in der Vergangenheit mit der Organisation der regelmäßigen Aktenvernichtung und auch mit der Aufsicht über das Gelände betraut gewesen. Hierauf erteilte das ULD einen klaren Hinweis auf die **Gesamtverantwortung der Schulleitung**:

> **§ 2 Abs. 1 SchulDSVO**
>
> Die Schulleiterin oder der Schulleiter trägt mit Ausnahme der Datenverarbeitung durch Elternvertretungen die Verantwortung für die Beachtung des Datenschutzes. Sie oder er hat die Abläufe in der Schule entsprechend zu organisieren und die Einhaltung der Bestimmungen zu überwachen. […]

Positiv hervorheben ließe sich lediglich, dass der **Datenschutzbeauftragte schnell und umfangreich in die Aufarbeitung des Vorfalls eingebunden** wurde. Ein Besuch des Datenschutzbeauftragten und eine Nachschulung des Schulpersonals zum Datenschutz erfolgten zeitnah.

4.7.2 Praktikumsbesprechung in der Schulstunde – Klasse entdeckt sensible Lehrernotizen

Die Offenlegung hochsensibler Angaben unter denkbar unglücklichen Umständen veranlassten eine Schülerin zur Beschwerde beim ULD. Im Vorjahr waren persönliche Gespräche einer Lehrkraft mit den Mitgliedern der Schulklasse vorausgegangen. Die betroffene Person berichtete in diesem Rahmen von schwerwiegenden Vorfällen in ihrem belasteten familiären Umfeld. Nach eigenen Angaben nahm die Lehrkraft diese Informationen als „**persönliche Randnotizen** für eine Teamsitzung" auf.

Zwar führt das Schulgesetz sogar eine eigene rechtliche Grundlage für persönliche Notizen über Schülerinnen und Schüler auf, weist aber auch auf die **Schutzwürdigkeit** solcher Daten ausdrücklich hin:

> **§ 30 Abs. 10 SchulG**
>
> Für persönliche Zwischenbewertungen des allgemeinen Lernverhaltens und des Sozialverhaltens in der Schule sowie persönliche Notizen der Lehrkräfte über Schülerinnen, Schüler und Eltern bestehen die Rechte der betroffenen Personen gemäß Artikel 12 bis 21 der Verordnung (EU) 2016/679 nicht. Die Lehrkraft hat durch geeignete Maßnahmen sicherzustellen, dass diese Daten vor dem Zugriff unbefugter Dritter geschützt werden. […]

Ohnehin wäre ein Schutz der Vertraulichkeit auch nach dem allgemeinen Grundsatz des Art. 5 Abs. 1 Buchst. f DSGVO geboten, und zwar ausgerichtet an den möglichen Folgen eines unbefugten Zugriffs.

Dieser Schutz war letztlich nicht ausreichend gegeben. Die Lehrkraft wählte eine denkbar ungeeignete Art der Speicherung: Sie legte die **Notizen, auch zu anderen Klassenmitgliedern, gesammelt als Tabelle** an. In ebendieser Datei legte sie zu einem späteren Zeitpunkt ein weiteres Tabellenblatt zur **Planung von Praktikumsplätzen** der Klasse an. Zusammen mit der Praktikumsplanung landeten die sensiblen Notizen, zunächst noch unbemerkt, auf der **Lernplattform** der Schule.

Während des Unterrichts geschah es, dass **die Klasse die Aufzeichnungen entdeckte**, wodurch immerhin zeitnah eine Löschung und Gespräche mit den Schülerinnen und Schülern über den Vorfall stattfinden konnten. Ausgerechnet die Beschwerdeführerin war an diesem Tag jedoch nicht anwesend. Sie erfuhr, auch bedingt durch Ferien, erst zweieinhalb Wochen später von dem Geschehen. Während die Lehrkraft zunächst beabsichtigte, die Schülerin unmittelbar zu kontaktieren, entschied die Schule anders – in Widerspruch zur Pflicht der unverzüglichen Benachrichtigung:

Art. 34 Abs. 1 DSGVO

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

Daneben **versäumte die Schule eine Meldung** an die Aufsichtsbehörde nach Art. 33 Abs. 1 DSGVO. Solche organisatorischen Verfehlungen führten im Zusammenwirken mit individueller Unachtsamkeit dazu, den **Kontrollverlust, der der betroffenen Person entstand, zu verschlimmern**.

Zwar geschah die Offenlegung zweifellos unbeabsichtigt, das Schulpersonal hatte die Schwere des Vorfalls wohl erkannt, und die Schule hat im Anhörungsverfahren transparent an der Aufklärung des Sachverhalts mitgewirkt. Jedoch entschuldigt dies nicht die tiefgreifende Schädigung und Verunsicherung der betroffenen Schülerin. Das ULD hat daher eine **Verwarnung** ausgesprochen.

Was ist zu tun?

Gerade Aufzeichnungen mit sensiblem Charakter bedürfen einer sorgsamen und gesonderten Speicherung bzw. Aufbewahrung. Sie im Sinne der Speicherbegrenzung nach Art. 5 Abs. 1 Buchst. e DSGVO nicht länger als unbedingt nötig zu behalten, ist besonders wichtig. Mit Blick auf das Gebot der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO sollte man sich auch stets fragen, ob manche Notizen nicht gänzlich unterbleiben können.

4.8 Datenschutz- und Medienkompetenz

Datenschutzkompetenz ist ein zentraler Teil der Medienkompetenz und beschäftigt sich damit, das Wissen, das für einen verantwortungsbewussten Umgang mit personenbezogenen Daten notwendig ist, zu vermitteln. In der heutigen stark durch Technik geprägten Gesellschaft ist Datenschutzkompetenz ein sehr wichtiger Aspekt.

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 dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI).

Ein zentraler Aspekt des AK sind der Erfahrungsaustausch und die Abstimmung der Aufsichtsbehörden in den entsprechenden Bereichen der **Datenschutzkompetenzvermittlung**.

Im Jahr 2023 wurde der Webauftritt des **Jugendportals zum Thema Datenschutz und Informationsfreiheit** der Datenschutzkonferenz (DSK, Tz. 2.1) komplett überarbeitet. Das Jugendportal mit dem Namen „YoungData" richtet sich mit dem Thema Datenschutz an Kinder und Jugendliche und ist ein Baustein im Bereich der Vermittlung von Datenschutzkompetenz. Die Website ist grafisch und inhaltlich auf die **Zielgruppe** zugeschnitten.

Sie erreichen das Jugendportal YoungData unter:

https://www.youngdata.de

Kurzlink: *https://uldsh.de/tb42-4-8-1a*

4.8.2 Mitarbeit im Netzwerk Medienkompetenz Schleswig-Holstein

Das **Netzwerk Medienkompetenz Schleswig-Holstein** hat sich im Jahr 2010 gegründet und besteht aus derzeit 16 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.

Das Netzwerk Medienkompetenz trifft sich regelmäßig und dient dem Erfahrungsaustausch und der Koordination von gemeinsamen Aktivitäten.

Eine zentrale Veranstaltung in jedem Jahr ist das **Medienkompetenz-Festival** (ehemals Medienkompetenztag) im November. Im Jahr 2023 trafen sich 500 Teilnehmende aus Kita, Vorschule, Schule und Jugendarbeit auf der zweitägigen Veranstaltung in Kiel. Das ULD war wie in den vergangenen Jahren auch mit einem Informationsstand vertreten und war als Ansprechpartner im Bereich Datenschutz und Datenschutzkompetenz stark nachgefragt.

05

KERNPUNKTE

Verwendung von E-Mail-Adressen nach dem Einkauf

Unangepasste Muster-Datenschutzerklärungen

Verantwortlichkeit bei Schulfotografie

Screenshots bei Videobewerbungsgesprächen

Datenpannen durch Wind und Wetter

Immer mehr Beschwerden zur Videoüberwachung

5 Datenschutz in der Wirtschaft

In diesem Kapitel steht Datenschutz in der Wirtschaft im Vordergrund. Da geht es um die Verwendung von Personalausweisdaten, um Weitergaben von E-Mail-Adressen, um die Gestaltung von Websites, die Veröffentlichung von Fotos oder Videos und um Beschäftigtendatenschutz.

Wir berichten weiterhin über einige Datenpannen. Die Bearbeitung der zahlreichen Beschwerden über eine Videoüberwachung hat sich zu einem „Massengeschäft" entwickelt, doch nicht für alle Fallkonstellationen sind wir zuständig oder der richtige Ansprechpartner.

5.1 Offenlegung einer Personalausweiskopie eines Wohnungskäufers im Internet

Zum Beginn des Jahres 2023 wurde das ULD auf eine im Internet veröffentlichte Immobilienanzeige aufmerksam gemacht, in deren **Bildergalerie eingescannte Kopien des Personalausweises eines Kaufinteressenten** veröffentlicht wurden. Einige Tage später benannte der Verantwortliche einen externen Datenschutzbeauftragten, der den Vorfall anschließend auch im Rahmen einer Meldung nach Artikel 33 DSGVO anzeigte.

Auf entsprechende Nachfrage erläuterte der nunmehr neu benannte Datenschutzbeauftragte, dass der Verantwortliche eine speziell für die Immobilienvermittlungsbranche entwickelte Branchensoftware nutzen würde. Zur Gewährleistung des Schutzes vor unbefugter oder unrechtmäßiger Offenlegung von Dokumenten gegenüber Dritten habe die Software alle einem Objekt zugeordneten PDF-Dokumente immer **als interne Dokumente klassifiziert**, da diese regelmäßig nicht für die Veröffentlichung in Anzeigen bestimmt seien.

Sämtliche einem Objekt zugeordneten Fotodateiformate konnten allerdings **durch lediglich einen Klick veröffentlicht** werden. Bei Einführung der Verfahrensweise sei nicht in Erwägung gezogen worden, dass auch Ausweisdokumente von Kaufinteressenten oder andere nicht für die Veröffentlichung bestimmte Dokumente in einem Fotodateiformat bereitgestellt würden.

> Personenbezogene Daten sind in einer Art und Weise zu erheben und zu verarbeiten, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Offenlegung gegenüber Dritten und vor unbeabsichtigtem Verlust.

Nach Schilderung des Datenschutzbeauftragten sei der Vorfall seit Einführung der Software vor mehreren Jahren der erste dieser Art gewesen.

Der Vorfall hat aber gezeigt, dass die bisher genutzte automatisierte Zuordnung von Dateien aufgrund des Dateiformats zu falschen – und vor allem zu unrechtmäßigen – Ergebnissen führen kann. Als Folge hat der Verantwortliche die Verfahrensweise nunmehr dahin gehend angepasst, dass die zu veröffentlichenden Dateien nicht mehr anhand des Dateiformats zugeordnet, sondern **explizit selektiert** werden müssen und eine **Veröffentlichung nur noch durch den Geschäftsführer selbst** erfolgt.

Was ist zu tun?

Zur Gewährleistung einer angemessenen Sicherheit und um den Nachweis dafür erbringen zu können, dass die Verarbeitung datenschutzkonform erfolgt, hat der Verantwortliche geeignete technische und organisatorische Maßnahmen umzusetzen. Dazu gehören auch eine entsprechende Konfiguration der eingesetzten Software und organisatorische Vorgaben.

5.2 Kopieren von Personalausweisen durch Kreditinstitute

Das ULD erhielt mehrere Beschwerden und Anfragen, die sich auf das **Kopieren von Personalausweisen durch Kreditinstitute** bezogen.

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. Für das Kopieren von Personalausweisen in Banken kommt die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 Buchst. c DSGVO in Betracht. Bei dieser Bestimmung handelt es sich allerdings nicht um eine für sich allein stehende Rechtsgrundlage. Vielmehr setzt die Vorschrift eine solche Rechtsgrundlage im Unionsrecht oder im nationalen Recht voraus.

Art. 6 Abs. 1 Buchst. c DSGVO

Die Verarbeitung personenbezogener Daten ist gemäß Art. 6 Abs. 1 Buchst. c DSGVO rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt.

Verpflichtungen für Kreditinstitute, erforderliche Angaben zur Identifikation von Kunden zu erfassen, ergeben sich aus dem **Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz (GwG))**. Gemäß § 2 Abs. 1 GwG sind die verpflichteten Stellen aufgelistet. Zu diesen zählen etwa:

- Kreditinstitute nach § 1 Abs. 1 des Kreditwesengesetzes, mit Ausnahme der in § 2 Abs. 1 Nr. 3 bis 8 des Kreditwesengesetzes genannten Unternehmen, und im Inland gelegene Zweigstellen und Zweigniederlassungen von Kreditinstituten mit Sitz im Ausland,
- Finanzdienstleistungsinstitute nach § 1 Abs. 1a des Kreditwesengesetzes, mit Ausnahme der in § 2 Abs. 6 Satz 1 Nr. 3 bis 10 und 12 und Abs. 10 des Kreditwesengesetzes genannten Unternehmen, im Inland gelegene Zweigstellen und Zweigniederlassungen von Finanzdienstleistungsinstituten mit Sitz im Ausland sowie Wertpapierinstitute nach § 2 Abs. 1 des Wertpapierinstitutsgesetzes und im Inland gelegene Niederlassungen vergleichbarer Unternehmen mit Sitz im Ausland und
- Zahlungsinstitute und E-Geld-Institute nach § 1 Abs. 3 des Zahlungsdiensteaufsichtsgesetzes und im Inland gelegene Zweigstellen und Zweigniederlassungen von vergleichbaren Instituten mit Sitz im Ausland.

Von den Verpflichtungen für diese Kreditinstitute ist auch die Identifizierung von Vertragspartnern durch die Kreditinstitute umfasst. Hierzu sind Angaben wie der Name, das Geburtsdatum oder die Staatsangehörigkeit zu erheben und zu überprüfen. Die Überprüfung der Angaben hat bei natürlichen Personen u. a. **anhand eines gültigen amtlichen Ausweises** zu erfolgen, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird.

Gemäß § 8 Abs. 2 GwG haben die Verpflichteten, wozu auch die Kreditinstitute zählen, **das Recht**

und die Pflicht, Kopien dieser Dokumente oder Unterlagen anzufertigen oder sie optisch digitalisiert zu erfassen.

Eine **Rechtsgrundlage für das Anfertigen von Kopien von Personalausweisen** ergibt sich somit aus Art. 6 Abs. 1 Buchst. c DSGVO in Verbindung mit dem Geldwäschegesetz.

5.3 Rechtmäßigkeit des Versands von Newslettern an Bestandskunden

Regelmäßig erreichen uns Anfragen und Beschwerden, in denen sich die Empfänger von elektronisch versandten Newslettern darüber beklagen, dass sie **keine Einwilligung für die Verarbeitung ihrer E-Mail-Adressen zum Versand von Newslettern** erteilt hätten.

Wie unter Tz. 5.2 des 39. TB bereits erläutert, erkennt der Erwägungsgrund 47 zur Datenschutz-Grundverordnung die Verarbeitung personenbezogener Daten zum Zweck der **Direktwerbung** zwar als eine **einem berechtigten Interesse dienende Verarbeitung** an, in der nach Art. 6 Abs. 1. Buchst. f DSGVO erforderlichen Interessenabwägung sind **allerdings auch die „vernünftigen Erwartungen der betroffenen Person"**, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in den Abwägungsprozess einzubeziehen.

Im Falle von **potenziellen Neukunden**, die bisher noch keine Beziehung zu einem Unternehmen hatten, können diese nicht davon ausgehen, dass die E-Mail-Empfänger entsprechende Newsletter erwarten. Des Weiteren überwiegen die schutzwürdigen Interessen der betroffenen Person in der Regel immer dann, wenn nach den Vorschriften des Gesetzes gegen den unlauteren Wettbewerb (UWG) eine **unzumutbare Belästigung** anzunehmen ist.

In mehreren Anfragen und Beschwerden handelte es sich allerdings um **Bestandskunden**, die ihre E-Mail-Adresse dem werbenden Unternehmen im Rahmen einer Geschäftsbeziehung übermittelt hatten.

In einem solchen Fall sind überwiegende schutzwürdige Interessen der betroffenen Person nach Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO in der Regel dann nicht gegeben, wenn die in § 7 Abs. 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG) enthaltenen **Vorgaben für elektronische Werbung eingehalten** werden.

Hiernach ist eine **unzumutbare Belästigung** bei einer Werbung unter Verwendung elektronischer Post **nicht anzunehmen**, wenn ein Unternehmer die E-Mail-Adressen im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von den Kunden erhalten hat, wenn es sich um Werbung für eigene ähnliche Waren oder Dienstleistungen handelt, die betroffenen Personen der Nutzung für Werbezwecke nicht widersprochen haben und bei der Erhebung wie auch bei jeder Werbeansprache auf ihr Widerspruchsrecht hingewiesen werden, sodass **in diesen Fällen tatsächlich keine Einwilligung erforderlich** ist.

Art. 21 Abs. 3 DSGVO

Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

Ohne vorherige Geschäftsbeziehung oder ohne Erfüllung der Voraussetzungen des § 7 Abs. 3 UWG bedarf es für die Nutzung von E-Mail-Adressen zu Werbezwecken allerdings immer einer **Einwilligung**.

Was ist zu tun?

Um die personenbezogenen Daten von Bestandskunden auch ohne Erhebung einer Einwilligung für den Versand von Newslettern nutzen zu können, sind die betroffenen Personen zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten u. a. auch über Zweck der E-Mail-Werbung und die Rechtsgrundlage der Verarbeitung transparent zu informieren.

5.4 Weitergabe der E-Mail-Adresse an Paketdienstleister

Das ULD erreichte die Beschwerde eines Kunden, die sich auf die **Übermittlung seiner E-Mail-Adresse durch einen Online-Shop an den beauftragten Paketdienstleister** bezog. Seitens des Paketdienstleisters erfolgte eine Kontaktaufnahme zwecks Mitteilung des Lieferstatus. Eine Einwilligung zur Übermittlung dieses personenbezogenen Datums lag nicht vor.

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 Fall wurde seitens des Kunden eine Bestellung aufgegeben. Um den geschlossenen Vertrag zu erfüllen, war es demnach also erforderlich, bestimmte Daten des Kunden zu verarbeiten. Rechtsgrundlage für die Verarbeitung **der zur Vertragserfüllung erforderlichen Daten**, was auch die **Weitergabe der Adressdaten an den Paketdienstleister** umfasst, war hier demnach Art. 6 Abs. 1 Buchst. b DSGVO. Hiervon war jedoch **nicht die Weitergabe der E-Mail-Adresse** umfasst. Dies wäre nur mit Einwilligung des Kunden möglich gewesen.

Die Thematik war bereits Gegenstand eines Beschlusses der Datenschutzkonferenz (DSK) vom 23.03.2018. Darin wird ausgeführt, dass die Übermittlung von E-Mail-Adressen durch Online-Versandhändler an Postdienstleister **nur bei Vorliegen einer Einwilligung** der Kunden in ebendiese Übermittlung rechtmäßig ist.

Die Praxis hat gezeigt, dass es vielen Online-Händlern möglich ist, die Zustellinformationen selbst an den Kunden weiterzugeben bzw. einen Link zur Sendungsverfolgung in die eigene Bestellbestätigung einzubinden. Dies stellt jedenfalls eine **objektiv zumutbare Alternative** dar. Aus dem gleichen Grund wird auch die Erforderlichkeit im Rahmen des Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO verneint.

Der DSK-Beschluss **„Übermittlung von E-Mail-Adressen durch Online-Versandhändler an Postdienstleister“** vom 23.03.2018 ist unter folgendem Link abrufbar:

https://www.datenschutzkonferenz-online.de/media/dskb/20180323_dskb_mail_adressen.pdf

Kurzlink: *https://uldsh.de/tb42-5-4a*

Das verantwortliche Unternehmen gab auf Nachfrage dem ULD gegenüber an, dass im vorliegenden Fall eine **technische Fehleinstellung im Buchungssystem** für die Übermittlung der E-Mail-Adresse an den Paketdienstleister ursächlich gewesen sei. Diese Einstellung sei so durch einen Mitarbeiter des Unternehmens vorgenommen worden. Standardmäßig würde eine Übermittlung nur mit Einwilligung der Kunden erfolgen.

Durch den Verantwortlichen wurde der Vorfall zum Anlass genommen, die Mitarbeitenden nochmals auf die datenschutzrechtlichen Bestimmungen im Zusammenhang mit Kundendaten aufmerksam zu machen. Das aufsichtsbehördliche Verfahren wurde mit einem Hinweis nach Art. 58 Abs. 1 Buchst. d DSGVO eingestellt.

5.5 Unangepasste Muster-Datenschutzerklärungen auf Websites

Das ULD erreichen immer wieder Hinweise und Beschwerden zu **fehlerhaften Datenschutzerklärungen auf Websites**. So gab es einen anonymen Hinweis auf eine Website, die in der Datenschutzerklärung lediglich **Platzhalter „à la Max Mustermann"** bei den Angaben zum Verantwortlichen enthielt.

Viele Website-Betreiber verwenden für ihre Datenschutzerklärungen im Internet bereitgestellte **Muster**. Dabei fällt jedoch oft auf, dass diese **nicht an die individuellen Datenverarbeitungen angepasst** werden. Teilweise wird auf Verarbeitungen hingewiesen, die tatsächlich gar nicht stattfinden. Oder es werden wie im vorliegenden Fall keine zutreffenden Angaben zum Verantwortlichen und zu den Kontaktdaten gemacht.

Auf einer Website kann u. a. die Einbettung von Kontakt- und Feedback-Formularen sowie von Plugin-Funktionen, etwa zum Abruf von Videos, oder der Einsatz von Cookies zur Erhebung und Verarbeitung von personenbezogenen Daten führen. Zu jedem Punkt sind die **Informationspflichten** einzuhalten, die sich aus **Art. 13 Abs. 1 und 2 DSGVO** ergeben. Auszugsweise gehören dazu beispielsweise Name und Kontaktdaten des Verantwortlichen, Zwecke der Verarbeitung und Angaben der konkreten Rechtsgrundlagen, Angaben zu Empfängern/Empfängerkategorien personenbezogener Daten, Speicherdauer für die personenbezogenen Daten und Angaben zu den Rechten der betroffenen Personen.

Nähere Ausführungen zu den Inhalten der Informationspflichten finden Sie in unserer **Informationsbroschüre** (dort insbesondere unter Punkt Nr. 6):

www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-4-Informationspflichten.pdf

Kurzlink: *https://uldsh.de/tb42-5-5a*

Im vorliegenden Fall wurde der Website-Betreiber auf die **fehlerhafte Datenschutzerklärung** hingewiesen. Dieser reagierte umgehend und passte diese an. Weitere aufsichtsbehördliche Maßnahmen waren daher nicht erforderlich.

Was ist zu tun?

Gar nicht musterhaft ist es, auf der Website Muster-Datenschutzerklärungen bereitzustellen, die mit der Realität gar nichts zu tun haben. Muster und Vorlagen im Datenschutzbereich können gute Hilfestellungen geben und die Erfüllung der Datenschutzpflichten erleichtern – doch ohne Anpassung durch Verantwortliche auf die realen (!) Verarbeitungen personenbezogener Daten und anderen Gegebenheiten ist dies nichts wert und führt möglicherweise sogar in die Irre.

5.6 Veröffentlichung eines Videos über einen Auftritt von Schulkindern im Internet

Im Frühjahr erhielt das ULD von einer Polizeistation einen Bericht, in dem sich eine Mutter darüber beschwerte, dass **Videoaufnahmen einer Musikveranstaltung im Internet veröffentlicht** wurden, an der u. a. die Schulklasse ihres Sohnes teilgenommen hätte. Eine Einwilligung für die Veröffentlichung von Aufnahmen, auf denen auch ihr Sohn erkennbar sei, habe sie nicht erteilt.

Da die Teilnahme an der Veranstaltung **im Rahmen einer schulischen Veranstaltung** erfolgte, habe sie sich zunächst an die begleitende Musiklehrerin gewandt, die ihr auf Nachfrage mitteilte,

dass auch sie einer solchen Aufnahme ebenfalls nicht zugestimmt hätte.

Im daraufhin eingeleiteten Verfahren war zunächst zu klären, wer für die Erstellung und Veröffentlichung von Aufnahmen und die Erhebung von Einwilligungen der sorgeberechtigten Eltern verantwortlich war. Die Aufnahmen wurden **von einem medienschaffenden Dritten erstellt**, der aus diesem Grund zu der Veranstaltung eingeladen war.

Auf Nachfrage teilte dieser mit, dass ihm vom Veranstalter mitgeteilt wurde, dass **die Erstellung von Aufnahmen der Auftritte „in Ordnung"** sei. Daraufhin habe er anschließend zahlreiche Aufnahmen zur Förderung von Musik, Kunst und Kultur ehrenamtlich erstellt, in den folgenden Tagen nachbearbeitet, den Teilnehmenden zur Verfügung gestellt und veröffentlicht.

Nach seiner Schilderung hätte ihn die Beschwerdeführerin auch direkt kontaktiert und sich darüber beklagt, dass er u. a. Aufnahmen ihres Sohnes veröffentlicht habe, woraufhin er sie zunächst auf die erfolgte Genehmigung durch den Veranstalter verwiesen hätte. Nachdem sie ihm mitteilte, damit nicht einverstanden zu sein, sei der **Beitrag umgehend gelöscht** worden.

Zur Verhinderung vergleichbarer Fälle wurde gemäß Art. 58 Abs. 1 Buchst. d DSGVO darauf hingewiesen, dass **Aufnahmen Minderjähriger nur mit Einwilligung der Erziehungsberechtigten veröffentlicht** werden dürfen, da die schutzwürdigen Interessen eines betroffenen Kindes grundsätzlich gegenüber dem Interesse eines Veranstalters an der Berichterstattung überwiegen.

Einwilligung

Art. 4 Nr. 11 DSGVO definiert eine „Einwilligung" als „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".

Ferner wurde darauf hingewiesen, dass die betroffenen Personen bzw. deren Erziehungsberechtigte zum Zeitpunkt der Erhebung nach den Artikeln 13 und 14 DSGVO insbesondere über den Verantwortlichen, den konkreten Zweck der Erhebung, die Rechtsgrundlage, etwaige Empfänger und die bestehenden Betroffenenrechte **zu informieren** sind. Dies könnte gegebenenfalls über entsprechende Informationsblätter für die Schulen und Aushänge am Veranstaltungsort erfolgen.

Was ist zu tun?

Bei mehreren Beteiligten ist vor einer entsprechenden Veranstaltung zu klären, wer Verantwortlicher im Sinne der DSGVO ist und ob gegebenenfalls auch eine gemeinsame Verantwortlichkeit vorliegt. Hierbei ist insbesondere festzulegen, wer welchen Informationspflichten nachkommt, wer die erforderlichen Einwilligungen der betroffenen Personen bzw. ihrer Sorgeberechtigten erhebt und wer die Rechte der betroffenen Personen erfüllt.

5.7 Datenverarbeitung durch Schulfotografinnen und -fotografen

Im Rahmen einer beim ULD eingegangenen Beschwerde erfolgte eine Überprüfung der **Verantwortlichkeit für die Verarbeitung von Fotografien durch Schulfotografinnen und -fotografen**. Im vorliegenden Sachverhalt wurden Klassenfotos angefertigt, welche die Eltern über den Online-Shop des Schulfotografen erwerben konnten. Hierzu wurde zwischen dem Dienstleister und der Schule ein Vertrag geschlossen, der als Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO bezeichnet war. Die datenschutzrechtliche Verantwortlichkeit für die Aufnahme der Fotos durch den Dienstleister hätte demnach bei der Schule gelegen. Lag aber überhaupt die Konstellation einer Auftragsverarbeitung vor?

Bei der Auftragsverarbeitung handelt es sich demnach um eine Form der Aufgabenübertragung bei der Verarbeitung personenbezogener Daten. In der Regel lagert der Verantwortliche hierbei **Teilprozesse an einen externen Dienstleister**, den Auftragsverarbeiter, aus.

Art. 4 Nr. 8 DSGVO

Der Begriff „Auftragsverarbeiter" bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Beispiele für eine Auftragsverarbeitung nach Artikel 28 DSGVO sind die Entsorgung (Vernichtung und Löschung) von Datenträgern mit personenbezogenen Daten durch einen Dienstleister oder die Verarbeitung von Kundendaten durch ein Callcenter ohne wesentliche eigene Ermessensspielräume.

Im vorliegenden Sachverhalt handelte es sich jedoch nicht um eine Auftragsverarbeitung nach Artikel 28 DSGVO, da der **Schulfotograf die Fotos nicht im Auftrag der Schule anfertigte**.

Grundsätzlich sind **Schulfotografen** daher als **Verantwortliche** im Sinne des Art. 4 Nr. 7 DSGVO anzusehen, da der Schwerpunkt der Datenverarbeitung in ihrer Tätigkeit, dem Erstellen und Verarbeiten der Fotos, liegt und sie zudem über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Ein weiterer Zweck ist der Verkauf der erstellten Fotos über den Online-Shop der Schulfotografen. Auch hier entscheidet der Schulfotograf alleinig über diesen sowie die Mittel der Verarbeitung. Die Schule hat hinsichtlich der Verarbeitung der personenbezogenen Daten **keine Weisungsbefugnis gegenüber den Schulfotografen**.

Art. 4 Nr. 7 DSGVO

Der Begriff „Verantwortlicher" bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Es ist zwar möglich, dass die **Schule für die Schulfotografen die Einwilligung** der Eltern für die Anfertigung der Bilder sowie die Übermittlung der Schülerdaten an den Schulfotografen einholt und an diese übermittelt. Dies entbindet die Schulfotografen jedoch nicht von den datenschutzrechtlichen Pflichten eines Verantwortlichen.

Der mit der Schule abgeschlossene Vertrag über die Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO spiegelte **nicht die tatsächliche Verantwortlichkeit** im vorliegenden Sachverhalt wider. Seitens des ULD wurden dem Schulfotografen daher die datenschutzrechtlichen Bestimmungen umfassend erläutert. Zudem wurde ein Hinweis nach Art. 58 Abs. 1 Buchst. d DSGVO ausgesprochen.

Weiterhin nahmen wir zum **zentralen Datenschutzbeauftragten des Bildungsministeriums für die öffentlichen Schulen** Kontakt auf, um auch die Schulen hinsichtlich der datenschutzrechtlichen Bestimmungen in Bezug auf die Verantwortlichkeit erneut zu sensibilisieren.

5.8 Erstellen von Screenshots bei Bewerbungsgesprächen per Videokonferenz

In einer Beschwerde berichtete ein Bewerber von einem 30-minütigen **Videointerview**, das er wegen einer zu besetzenden Stelle mit einer Interviewerin aus Indien gehabt hätte. Nach dem Gespräch habe er die Ergebnisse des Vorstellungsgesprächs inklusive eines Screenshots von ihr per E-Mail erhalten. Der Bewerber beklagte, dass er **keine Einwilligung zur Anfertigung des Screenshots** erteilt hätte.

§ 26 BDSG

Arbeitgeber dürfen lediglich personenbezogene Daten über ihre Bewerber verarbeiten, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist.

Im daraufhin gegen das u. a. in Schleswig-Holstein ansässige Unternehmen eingeleitete Verfahren wurde von diesem zunächst eingeräumt, dass in dem vorliegenden Fall **Screenshots** während des per Videokonferenz geführten **Bewerbungsgesprächs** angefertigt wurden. Diese Praxis sei allerdings **unternehmensseitig nicht gestattet**, was sich bereits aus den geltenden internen Vorgaben ergebe, auf die die an den Bewerbungsgesprächen beteiligten Beschäftigten regelmäßig hingewiesen würden.

Des Weiteren würden die beteiligten Beschäftigten auch in der Einladung zur Teilnahme an Bewerbungsgesprächen durch **Einblendung eines entsprechenden Hinweistextes** nochmals explizit darauf aufmerksam gemacht, dass keine Aufnahmen erstellt werden dürfen.

Unternehmensseitig wurde ausdrücklich bedauert, dass in dem geführten Bewerbungsgespräch entgegen den geltenden internen Vorgaben Bildschirmfotos erstellt wurden. Eine interne Untersuchung des Vorfalls hätte ergeben, dass diese Handlung auf ein **individuelles Fehlverhalten einer noch neuen Beschäftigten** zurückzuführen war.

Um sicherzustellen, dass dieser Vorfall ein Einzelfall bleibt, seien gegenüber der den Vorfall verursachenden Beschäftigten **arbeitsrechtliche Maßnahmen** ergriffen worden. In diesem Zusammenhang sei sie nochmals eindringlich auf das **Verbot des Anfertigens von Aufnahmen** während des Bewerbungsgesprächs hingewiesen und dahin gehend sensibilisiert worden.

Nachdem der Betroffene der Interviewerin und der deutschen Personalverantwortlichen mitteilte, dass er keine Zustimmung zur Anfertigung des Screenshots erteilt habe, wurden die **Aufnahmen unverzüglich gelöscht** und dem Betroffenen gegenüber die **Löschung bestätigt**, sodass von etwaigen Maßnahmen gegen das Unternehmen abgesehen werden konnte.

5.9 Unternehmensinterne Bekanntgabe einer Kündigung

Ein Beschäftigter beschwerte sich beim ULD darüber, dass sein **Arbeitgeber** intern bekannt gab, dass er das **Unternehmen zu einem bestimmten Zeitpunkt „auf eigenen Wunsch" verlasse**.

Auch bei den Angaben hinsichtlich der Beendigung einer Tätigkeit bei einem Arbeitgeber handelt es sich um personenbezogene Daten, wenn die beschäftigte Person identifizierbar ist. Folglich war der Arbeitgeber verpflichtet, die datenschutzrechtlichen Vorgaben einzuhalten. So dürfen personenbezogene Daten von Beschäftigten für **Zwecke des Beschäftigungsverhältnisses** verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder

Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Wenn ein Beschäftigter das Unternehmen verlässt, kann es zur **Aufrechterhaltung der internen Prozesse und Abläufe erforderlich sein, den genauen Termin des Ausscheidens im Unternehmen bekannt zu geben**. Je nach Größe des Unternehmens ist jedoch darauf zu achten, dass nur die Bereiche Kenntnis erlangen, für die diese Information tatsächlich erforderlich ist. Unter Beachtung des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) sollten zudem nur die für den angestrebten Zweck erforderlichen Daten verarbeitet werden. Die Information, dass der Beschäftigte **das Unternehmen „auf eigenen Wunsch verlasse**", dürfte dabei regelmäßig **nicht erforderlich** sein.

Das Verfahren wurde mit einem Hinweis und einer Warnung gegenüber dem Verantwortlichen beendet.

5.10 Übermittlung von Beschäftigtendaten ohne Einwilligung

In einer anonymen Beschwerde wurde uns mitgeteilt, dass ein **Arbeitgeber seine Beschäftigten bei einer privaten Krankenversicherung angemeldet** habe. Dabei seien mindestens der Name sowie die Anschrift der Beschäftigten übermittelt worden. Als die Beschäftigten von der Krankenversicherung angeschrieben wurden, konnten sie diesen Brief nicht einordnen, da diese keine Kenntnis von der Übermittlung hatten. Die Beschäftigten hätten **keine Einwilligung** in die Übermittlung der Daten gegeben.

Als wir den Arbeitgeber mit dem Inhalt der Beschwerde konfrontierten, war der Sachverhalt dort bereits bekannt. Der Arbeitgeber habe eine **betriebliche Krankenversicherung einführen** wollen. Um den Versicherungsschutz zum Beginn des neuen Monats sicherzustellen, wurde der Arbeitgeber zwei Tage vorher darum gebeten, die Daten an die Versicherung zu übermitteln. Es sei **eigentlich geplant** gewesen, **Einwilligungserklärungen** der Beschäftigten im Rahmen von Einführungsveranstaltungen einzuholen. Aufgrund der Dringlichkeit und in dem **Glauben, dass „alle" mitmachen würden**, sei dann vorschnell gehandelt und die Daten seien ohne eine vorherige Einwilligung übermittelt worden.

Die Beschäftigten erhielten von ihrem Arbeitgeber zu dem Vorfall umgehend eine Information, und das **Vorgehen wurde bedauert**. Der Arbeitgeber bat schließlich alle Beschäftigten, die nicht an der Zusatzkrankenversicherung teilnehmen wollen, sich zu melden, sodass diese von der Versicherung **wieder abgemeldet und die Daten gelöscht** werden. Im Übrigen seien die betroffenen Beschäftigten aufgefordert worden, ihre Zustimmung nachzureichen.

Gegenüber dem Verantwortlichen wurde deutlich gemacht, dass die Datenübermittlung **nicht durch eine nachträgliche Zustimmung oder Ähnliches rückwirkend rechtmäßig** werden kann. Zudem verdeutlichten wir die Besonderheiten, die bei einer **Einwilligung im Rahmen des Beschäftigtenverhältnisses** zu beachten sind:

Eine Einwilligung muss freiwillig erteilt werden. Für die **Beurteilung der Freiwilligkeit** sind insbesondere die im Beschäftigungsverhältnis bestehende **Abhängigkeit der beschäftigten Personen** sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher **Vorteil** erreicht wird oder Arbeitgeber und beschäftigte Person **gleich gelagerte Interessen** verfolgen.

Da eine betriebliche Krankenversicherung regelmäßig vom Arbeitgeber finanziert wird und jene für die Beschäftigten einen wirtschaftlichen Vorteil bietet, kann in diesem Fall die Einwilligung als Rechtsgrundlage für die Verarbeitung personenbezogener Daten herangezogen werden. Maßgeblich für diese Einschätzung ist auch der Umstand, dass der Arbeitgeber die Erbringung der Arbeitsleistung **nicht an die Erklärung einer Einwilligung zum Abschluss einer Krankenversicherung knüpfte**.

Grundsätzlich sollte die **Einwilligung** im Beschäftigungsverhältnis jedoch nur **in Ausnahmefällen als Rechtsgrundlage** verwendet werden, da der Aspekt der Freiwilligkeit aufgrund des Abhängigkeitsverhältnisses oft nicht gegeben ist.

Da der Arbeitgeber den Vorfall bereits vor unserem Tätigwerden umfassend aufgearbeitet und entsprechende Maßnahmen ergriffen hatte, waren abgesehen von den oben genannten Hinweisen keine weiteren aufsichtsbehördlichen Maßnahmen erforderlich.

5.11 Datenpannen in der Wirtschaft

5.11.1 Meldungen von Datenpannen bei Kreditinstituten

Auch im vergangenen Jahr gingen beim ULD Meldungen von **Datenpannen bei Kreditinstituten** ein. Gemäß Artikel 33 DSGVO meldet der Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Den größten Teil der Meldungen machte der **Fehlversand von Unterlagen**, die personenbezogene Daten und insbesondere Finanzinformationen enthielten, aus. Der Fehlversand erfolgte auf postalischem oder elektronischem Wege und stellt eine unrechtmäßige Offenlegung gegenüber Dritten dar.

Seitens des ULD erfolgte in den vorliegenden Fällen eine Überprüfung, ob sowohl die Vorgaben in Bezug auf die Frist sowie den Inhalt der **Meldung** als auch die datenschutz-rechtlichen Vorschriften in Bezug auf die **Sicherheit der Verarbeitung** eingehalten wurden.

Einer der Grundsätze für die Verarbeitung personenbezogener Daten sieht vor, dass diese in einer Weise verarbeitet werden, die eine **angemessene Sicherheit gewährleistet**, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung („Integrität und Vertraulichkeit“). Hierzu setzt der Verantwortliche gemäß Artikel 24 DSGVO geeignete technische und organisatorische Maßnahmen um.

Art. 24 Abs. 1 DSGVO

Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.

In den vorliegenden Fällen handelte es sich zumeist um **individuelle Fehler von Mitarbeitenden**, die sich teilweise nicht an die bestehenden **Vorgaben** der Kreditinstitute hielten oder durch **Unaufmerksamkeit** einen Fehlversand der Unterlagen verursachten. Der Verantwortliche nahm die Vorfälle zum Anlass, die Mitarbeitenden hinsichtlich der datenschutzrechtlichen Bestimmungen zu **sensibilisieren** und auch – soweit erforderlich – **technische Veränderungen** vorzunehmen, um eine ungewollte Offenlegung der Daten zukünftig zu vermeiden. Hierbei wurde z. B. eine **zusätzliche Plausibilitätsprüfung im Kundensystem** implementiert, die den Versand der Unterlagen an den richtigen Empfänger sicherstellen soll.

Seitens des ULD wurden abschließend Hinweise nach Art. 58 Abs. 1 Buchst. d DSGVO ausgesprochen.

5.11.2 Vom Winde verweht

Eine Meldung bezog sich auf den Verlust von Papierdokumenten und digitalen Datenträgern, die auf einem Transportwagen gelagert und **von einer Sturmbö verweht** wurden. Dabei handelte es sich um **Unterlagen zu einem Planfeststellungsverfahren**. Die darin enthaltenen personenbezogenen Angaben umfassten die Daten zu vier Eigentümern betroffener Grundstücke. Überwiegend waren bei den über 300 Papierseiten und den drei Datenträgern Angaben zu juristischen Personen enthalten, welche keinen Personenbezug aufwiesen.

Die Meldung durch das verantwortliche Unternehmen erfolgte gegenüber der Landesbeauftragten für Datenschutz fristgerecht innerhalb des maßgeblichen Zeitraums von 72 Stunden. Die vier betroffenen Grundstückseigentümer wurden zudem über den Datenverlust benachrichtigt.

Nach der Rekonstruktion der Vorgänge, die zum Verlust einiger Unterlagen führten, konnte das Unternehmen nähere Erläuterungen geben. Demnach war ein Austausch von Dokumenten beabsichtigt. Auf dem **Hinweg** zum Austauschort erfolgte ein **fachgerechter Transport** der Unterlagen in geschlossenen Kartons und in Aktenordnern. Zum Austausch der Dokumente mussten die Kartons geöffnet werden, wobei maßgebliche ausgetauschte Unterlagen dann nicht wieder in Aktenordner geheftet, sondern lose in die Kartons eingeordnet wurden. Weiterhin legte der mit dem Austausch beauftragte Beschäftigte ausgetauschte Datenträger in einen der Kartons.

Noch am Austauschort erfasste eine Windbö einen der zwischenzeitlich wieder verschlossenen Kartons und verteilte die Datenträger auf dem Erdboden. Als der Mitarbeiter diesen Karton nebst Inhalt sichern wollte, **erfasste die Windbö weitere der mit Kartondeckeln verschlossenen Kartons** und verwehte einen Teil der Papierunterlagen. Vor Ort gelang es schließlich, die Papierunterlagen zu sichern. Einer der **Datenträger konnte jedoch nicht mehr aufgefunden** werden.

Bezüglich der Angaben auf dem abhandengekommenen Datenträger existierte eine Kopie, sodass die **Verfügbarkeit** über die Daten weiterhin **gewährleistet** blieb. Auch dieser Umstand war bedeutend hinsichtlich der Einschätzung bestehender Risiken für die Persönlichkeitsrechte betroffener Personen.

Verfügbarkeit

Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen bedeutet, dass diese von den Anwendern stets wie vorgesehen genutzt werden können. Maßnahmen zur Unterstützung der Verfügbarkeit sind z. B. die redundante Auslegung von Systemen, eine unterbrechungsfreie Stromversorgung, Vertretungsregelungen, Speicherungen in RAID-Systemen oder in (mehreren) Clouds sowie Datensicherungen.

Das Unternehmen hat darüber hinaus veranlasst, dass bei künftigen Transporten vergleichbarer Unterlagen **immer zwei Beschäftigte die Dokumentenlieferung** durchführen werden, um eine zusätzliche Sicherung zu gewährleisten. Ferner erfolgte eine Anweisung an alle Beschäftigten, Dokumente, digitale Datenträger und sonstige Datenträger mit personenbezogenen Daten **stets in geschlossenen und gesicherten Behältnissen zu transportieren**, um auch einen Schutz vor Sturmböen zu bieten.

Die von dem Unternehmen vorgeschlagenen und umgesetzten Maßnahmen zur künftigen Sicherung entsprechender Transporte erachteten wir als **hinreichend**, sodass das eingeleitete Prüfverfahren beendet werden konnte.

Was ist zu tun?

Wind und Wetter gehören zu Schleswig-Holstein. Der Transport von personenbezogenen Unterlagen bedarf einer angemessenen Sicherung vor äußeren Einflüssen. Wetterbedingungen wie Niederschlag oder Wind können die Verfügbarkeit von Daten beeinträchtigen und zu Verletzungen der Datensicherheit führen. Die verantwortlichen Unternehmen müssen angemessene Maßnahmen ergreifen, die neben der ordnungsgemäßen Sicherung der Ladung auch die Vorhaltung von Sicherungskopien und die Verschlüsselung von Datenträgern umfassen kann.

5.12 Videoüberwachung

5.12.1 Allgemeine Entwicklungen

Die Entwicklung, dass sich immer mehr Menschen durch Videoüberwachungskameras beeinträchtigt fühlen und daher beim ULD eine Beschwerde einreichen, setzt sich auch in diesem Berichtszeitraum fort. Die **Anzahl von Beschwerden über Videoüberwachungsanlagen** stieg im Vergleich zum Vorjahreszeitraum insgesamt **um rund 34 Prozent** an.

Einen Großteil der Beschwerden machen dabei Videoüberwachungsanlagen aus, die durch Privatpersonen in ihrem privaten Umfeld installiert werden. Über solche Videoüberwachungsanlagen beschweren sich meistens die **direkten Nachbarn**. Oftmals geht solchen Beschwerden ein festgefahrener Nachbarschaftsstreit voraus, sodass sich die Betroffenen direkt an das ULD wenden, ohne das direkte Gespräch mit den vermeintlich überwachenden Nachbarn zu suchen. Im Vergleich zum Vorjahr ist der Anteil derartiger Beschwerden deutlich – **um rund 65 Prozent** – gestiegen. **Knapp die Hälfte** aller im Berichtszeitraum eingegangenen Beschwerden zum Thema Videoüberwachung bezogen sich auf Videoüberwachungsanlagen in der Nachbarschaft.

Die andere Hälfte der Beschwerden im Bereich der Videoüberwachung, die an uns herangetragen wurden, bezog sich u. a. auf Videoüberwachungsanlagen, die in **Restaurants**, auf **Campingplätzen**, an und in **Fahrzeugen** (Dashcams) oder auch im Umfeld von **Pferdehöfen** installiert sind. In den zu prüfenden Fällen war oftmals die **Hinweisbeschilderung** nicht korrekt, einige Betreiber konnten auch die Erforderlichkeit für die Videoüberwachung nicht nachvollziehbar begründen. Auch über Videoüberwachungsanlagen in **Fitnessstudios, Schwimmbädern oder Spa-Einrichtungen** wurde sich im Laufe des Jahres mehrfach beschwert.

Videoüberwachung in der Nachbarschaft

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 keine Anwendung. Erfasst die Videoüberwachung jedoch Bereiche außerhalb des privaten Grundstücks, ist die Datenschutz-Grundverordnung vollumfänglich zu berücksichtigen.

In solchen Fällen wird regelmäßig eine **Prüfung der Rechtmäßigkeit** dieser Videoüberwachungsanlagen eingeleitet. In einigen Fällen wurde sehr

deutlich, dass die Videoüberwachung die Grundrechte und Grundfreiheiten der betroffenen Personen in einem unverhältnismäßigen Umfang beeinträchtigt hat. In solchen Fällen wurde darauf hingewirkt, den Eingriff in die Rechte der Betroffenen abzumildern, indem beispielsweise **Veränderungen der Erfassungsbereiche** oder eine **Erhöhung der Transparenz** gefordert wurden.

Außerdem stach im Berichtszeitraum ein Fall hervor, in dem jemand, der sich von einer **Wildkamera** beeinträchtigt fühlte, kurzerhand ein Schreiben unterhalb der Kamera aufhängte. In diesem Schreiben wurde darauf hingewiesen, dass der Einsatz von Wildkameras nach der Datenschutz-Grundverordnung grundsätzlich unzulässig sei. Das Schreiben enthielt die Aufforderung, die Wildkamera zu entfernen, und die Androhung der Sicherstellung der Kamera, falls der Aufforderung nicht Folge geleistet würde. Unterhalb des Textes wurde die **Anschrift der Dienststelle der Landesbeauftragten für Datenschutz angegeben**. Durch diesen **Aushang** erhielt unsere Dienststelle berechtigterweise eine irritierte Nachfrage des zuständigen Jagdausübungsberechtigten, ob ein solches Schriftstück im Auftrag der Landesbeauftragten unterhalb seiner Kamera angebracht worden sei. Dies war selbstverständlich nicht der Fall. Das Schreiben stammte nicht aus dem ULD.

Schriftliches Auftreten der Landesbeauftragten für Datenschutz

Die Landesbeauftragte für Datenschutz kommuniziert ausschließlich direkt mit einem Verantwortlichen. Aushänge in der Öffentlichkeit erfolgen durch unsere Dienststelle nicht. Zudem sind Schriftstücke, die unsere Dienststelle verlassen, immer von der jeweiligen Sachbearbeiterin oder dem Sachbearbeiter unterschrieben. Im Falle der Kommunikation per E-Mail geht aus der Absenderadresse oder der Signatur eindeutig hervor, ob die Mitteilung aus unserer Dienststelle stammt. Bei Zweifeln empfiehlt sich eine Nachfrage.

5.12.2 Heimlich ein Gespräch belauschen? Audio- und Videoüberwachung im Eingang eines Hostels

Bereits seit dem Jahr 2021 beschäftigt uns eine **Beschwerde über Video- und Tonüberwachung in einem Hostel**, die wir im Berichtszeitraum zum Abschluss gebracht haben. Gäste hatten sich über eine Audio- und Videoüberwachung im Eingangsbereich eines Hostels im Zentrum einer touristisch viel besuchten Stadt beschwert. Danach sollte eine Videobeobachtung im Eingangsbereich erfolgen. Dies war ihnen bekannt. Nicht gerechnet hatten sie allerdings damit, dass der Inhaber des Hostels darüber auch ihre **Gespräche im Eingangsbereich mithören** könne.

Der Verantwortliche bestätigte die Vermutung der Beschwerdeführer: Wenn Gäste sich zum **Einchecken** im Vorraum des Hostels befinden, erhält der **Inhaber** über eine App eine Mitteilung auf seinem Smartphone und kann so **die Gäste sehen und auch hören**. Bei Bedarf könne er so die Gäste ansprechen und **beim Einchecken behilflich** sein. Dieses Verfahren sei wegen der unterschiedlichen Nationalitäten/Sprachen der Gäste erforderlich. Die Überwachung diene außerdem zum **Einbruchschutz**. Auf die Überwachung werde im Eingangsbereich hingewiesen.

Wir haben den Verantwortlichen darauf hingewiesen, dass die Überwachung der Gäste in ihrer konkreten Ausgestaltung zum Teil **nicht ausreichend begründet** und zum Teil **nicht erforderlich und verhältnismäßig** ist. Insbesondere galt dies für die **Tonüberwachung**. Diese greift erheblich in die Rechte der betroffenen Personen ein und kann unter Umständen sogar eine Straftat darstellen.

Als mildere Alternative haben wir vorgeschlagen, eine **Gegensprechanlage zu installieren**, welche die Gäste bei Bedarf beim Einchecken betätigen. Für die optische Überwachung zum

Schutz vor Einbrüchen haben wir eine substanzierte Gefährdungseinschätzung gefordert. Diese hat der Verantwortliche nicht vorgelegt. Er war **nicht bereit, Änderungen vorzunehmen**, um die Video- und Tonüberwachung in Einklang mit den datenschutzrechtlichen Anforderungen zu bringen. Die Installation einer Gegensprechanlage wurde als nicht praktikabel und zu teuer abgelehnt.

Was haben wir dann getan? Es folgten diverse Schritte im Rahmen eines Verwaltungsverfahrens, die schließlich darin mündeten, dass wir **den Verantwortlichen angewiesen** haben, die Video- und Audioüberwachung entweder zu unterlassen oder in der Weise auszugestalten, dass sie erst durch bewusste und gewollte Auslösung der betroffenen Person aktiviert wird. Daraufhin entfernte der Verantwortliche die Kamera mit Tonüberwachung, und das Verfahren konnte eingestellt werden.

Was ist zu tun?

Unbemerktes Abhören von Gesprächen von Gästen im Hotel oder an ähnlichen Orten ist nach dem Datenschutzrecht unzulässig und hat zu unterbleiben. Das ULD wird erforderlichenfalls Untersagungsverfügungen erlassen, wenn Verantwortliche nach einer Datenschutzprüfung an solchen Maßnahmen festhalten.

5.12.3 Der Kampf gegen die Vermüllung – Videoüberwachung von Müllsammelplätzen

Mehrere Millionen Tonnen an illegal entsorgtem Müll landen jährlich auf Deutschlands Straßen oder in den Wäldern. Die Gründe dafür sind verschiedene, die Folgen für Städte und Gemeinden überall gleich: hohe Kosten, um illegal entsorgten Sperrmüll, Elektrogeräte und Farbeimer fachgerecht zu trennen und zu entsorgen. Städte und Gemeinden sehen sich vermehrt gezwungen, der Vermüllung auch **mit technischen Mitteln entgegenzutreten**. Dies spiegeln Beratungsanfragen wider, die das ULD vermehrt erreichen. Städte und Gemeinden wollen sich der Videoüberwachung bedienen, um **Müllsammelplätze vor unberechtigter Müllentsorgung zu schützen** und die Vermüllung präventiv zu vermeiden.

Eine Gemeinde in Schleswig-Holstein setzt seit dem Jahr 2022 eine **Videoüberwachung zur Beobachtung eines Müllsammelplatzes** ein – nach eigener Aussage mit Erfolg. Bezüglich dieser Videoüberwachung hat das ULD Anfang 2023 eine Beschwerde erreicht. Die Rechtmäßigkeit der Videoüberwachung wird von dem Beschwerdeführer unter datenschutzrechtlichen Aspekten bezweifelt.

§ 14 LDSG

Videoüberwachung öffentlich zugänglicher Räume

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit dies

1. zur Aufgabenerfüllung öffentlicher Stellen oder
2. zur Wahrnehmung des Hausrechts erforderlich ist

und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen.

[...]

Bei einer Videoüberwachung von Müllsammelplätzen werden nicht nur die Personen gefilmt, bei denen es zu einem Fehlverhalten kommt. Es werden **im öffentlichen Raum 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 diesen Grundrechtseingriff und die Verarbeitung der personenbezogenen Daten bedarf es einer **gesetzlichen Grundlage**. Die betreffende Gemeinde stützt die Rechtmäßigkeit der Videoüberwachung auf die Generalklausel des § 14 Abs. 1 Nr. 1 LDSG (Landesdatenschutzgesetz). Nach ihrer Stellungnahme sei die Videoüberwachung für die Erfüllung ihrer Aufgaben erforderlich.

Die abschließende datenschutzrechtliche Bewertung und der folgende Abschluss des Verfahrens stehen derzeit noch aus.

5.12.4 Webcams im Hafengebiet

Im Berichtszeitraum waren mehrere **Webcams** Gegenstand von Prüfungen durch das ULD. Besonders in den Sommermonaten gehen Jahr für Jahr Beschwerden über Webcams ein. Webcams werden häufig an Orten wie Strandpromenaden oder Häfen betrieben, um **touristische Zwecke** zu verfolgen. Auch öffentliche Stellen haben den Nutzen von Webcams längst erkannt. Die Möglichkeit, einen Einblick in den Ortskern, das Geschehen an der Strandpromenade oder die tagesaktuelle Wetterlage zu erhalten, nehmen laut den Verantwortlichen auch viele Menschen gern wahr.

Gegenstand einer Prüfung des ULD waren u. a. Webcams an einer **Seeuferpromenade** und in einem **Hafengebiet**. In beiden Fällen war es zunächst möglich, einzelne Personen zu identifizieren. Dass öffentliche Stellen Webcams nutzen möchten, um ihre Attraktivität für den Tourismus zu erhöhen, ist durchaus nachvollziehbar. Wenn **Personen identifizierbar von Webcams erfasst werden**, stellt dies aber in der Regel einen **erheblichen Eingriff in ihre Grundrechte** und Grundfreiheiten dar. Vor allem vor dem Hintergrund, dass die Aufnahmen von Webcams für jeden **frei im Internet zugänglich** sind, wiegt dieser Eingriff besonders schwer. Das touristische oder wirtschaftliche Interesse eines Webcam-Betreibers kann es nicht rechtfertigen, dass Personen auf öffentlichen Flächen von Kameras erfasst und in Echtzeit aus der Ferne beobachtet werden können. Der Betrieb einer Webcam kann daher aus datenschutzrechtlicher Sicht nur dann **zulässig** sein, **wenn Personen nicht identifiziert** werden können.

Insbesondere im Hafengebiet war die **Identifizierung von Personen** auch **anhand der dort liegenden Boote möglich**. Bei der Frage, ob eine Person auf einer Videoaufnahme identifiziert werden kann, kommt es nicht nur darauf an, ob das Gesicht erkennbar ist oder ob eine Person tatsächlich von jemandem identifiziert wurde. Vielmehr können auch der Ort, die Zeit und Gegenstände – wie in diesem Fall Boote – Rückschlüsse auf eine bestimmte Person zulassen. Zu berücksichtigen ist dabei auch immer das etwaige Zusatzwissen eines Nutzenden der Webcam. Wenn eine Identifizierung von Personen dadurch möglich ist, handelt es sich um personenbezogene Daten, deren Verarbeitung mittels Webcam aus den eingangs genannten Gründen unzulässig wäre.

Merkmale, die für eine Identifizierung von Personen bei Bildübertragungen in Betracht kommen, sind z. B.:

- Gesicht
- Körperbild, Körperhaltung, Gangbild
- Ort und Zeitpunkt der Aufnahme
- Kleidung, mitgeführte Gegenstände oder Tiere
- zur Person gehörige Häuser, Boote, Fahrzeuge, Wohnwagen

Der Betreiber der Webcams wurde auf diesen Umstand hingewiesen und zeigte sich kooperativ. Es wurden **Maßnahmen** ergriffen, die dazu beitrugen, **eine Identifizierung von Personen zu verhindern**.

Was ist zu tun?

Bevor eine Webcam in Betrieb genommen wird, sollten die Betreiber genau prüfen, mit welcher Einstellung die jeweilige Webcam betrieben werden kann. In diesem Zusammenhang ist zu beachten, dass Einstellungen gewählt werden, die das eindeutige Identifizieren von Personen verhindern. Geeignet sind in der Regel Übersichtsaufnahmen aus großer Entfernung mit einer eher geringen Auflösung. Jemand, der den Videostream aufruft, sollte darüber hinaus nicht die Möglichkeit haben, eigenständig zu zoomen oder vor- und zurückzuspulen. Eine weitere Möglichkeit, die Webcam weniger eingriffsintensiv für die betroffenen Personen zu gestalten, kann auch das Erstellen von Standbildern sein. Dadurch können Bewegungsmuster nicht exakt nachvollzogen werden. Es kommt jedoch stets auf den Einzelfall und den jeweiligen Zweck der Webcam an.

06

KERNPUNKTE

Künstliche Intelligenz

Souveräne Clouds

Neue Entwicklungen bei Cyberangriffen

Gemeinsame Prüfung von Videokonferenzsystemen

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) und anderen IT-Stellen des Landes

Wie in den vergangenen Jahren wurde das ULD als **Gast in der Konferenz der IT-Beauftragten** (ITBK) über aktuelle und geplante IT-Projekte informiert. Eine formelle Einbindung in konkrete Verfahren oder in Regelwerke, die eine landesweite Bedeutung haben oder die im Rahmen der Mitbestimmung entstanden sind, gab es in diesem Berichtszeitraum nicht.

Erfolgreich fortgesetzt wurde auch die Zusammenarbeit mit anderen IT-Stellen des Landes, u. a. dem Amt für Informationstechnik (AIT) und im Bereich des Bildungsministeriums, aber auch mit der Justiz-IT. In den regelmäßigen Zusammenkünften und Austauschen geht es um gegenseitige Information: zum einen über Planungen bei der Einführung und Ausgestaltung neuer Verfahren, zum anderen über Ergebnisse und Entwicklungen aus den Arbeitskreisen der Datenschutzbeauftragten des Bundes und der Länder, die **von übergreifender Bedeutung** sind. So fußen zahlreiche Verfahren auf überregional angebotener Software, häufig in Kombination mit einer Auftragsverarbeitung beim Anbieter. In diesen Fällen gilt es herauszuarbeiten, welche rechtlichen Bewertungen und technischen Konfigurationen aus anderen Bereichen übernommen werden könnten und welche Unterschiede es aufgrund landesrechtlicher Regelungen (insbesondere im Bildungsbereich) gibt, die eine differenzierte Betrachtung erfordern.

Schließlich gibt es auf der Seite der Anbieter im Zeitablauf zahlreiche **Änderungen, die Neubewertungen erfordern**. So sind Einschätzungen zur Geeignetheit eines Produkts oder zur Zulässigkeit wiederholt zu überprüfen – auch wenn sich Einsatzszenarien ändern oder angepasst werden. Ein typisches Beispiel sind hierbei die Microsoft-Online-Dienste (Tz. 6.2.3).

Insgesamt würden wir uns eine **Verstärkung der Einbindung im Vorfeld wünschen** – und zwar bevor wir über Zeitung oder Fernsehen davon erfahren, bevor die Landesbeauftragte für Datenschutz dazu interviewt wird und bevor die Beschwerden und Nachfragen von Betroffenen oder Behördenmitarbeitenden eintreffen.

Was ist zu tun?

Die frühzeitige Information und Einbindung des ULD bei neuen bzw. geplanten Verfahren und übergreifenden Regelungen sollten noch intensiviert werden.

6.1.2 Update: Sicherheitskonzepte mit SiKoSH

Seit einigen Jahren ist das ULD am „SiKoSH"-Projekt des ITV.SH beteiligt (41. TB, Tz. 6.1.3). Das Hauptziel dieses Projekts besteht darin, Kommunen und kleinere Organisationen bei der Umsetzung der Anforderungen an Informationssicherheit zu unterstützen.

Hierbei orientiert sich das Projekt eng am IT-Grundschutz des BSI, das als Rahmenwerk anpassungsfähig, aber konzeptionell für jeden Einzelfall auch anpassungsbedürftig ist.

BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit dem IT-Grundschutz einen Standard geschaffen, der eine Managementmethodik für Informationssicherheit vorgibt und mit dem Grundschutz-Kompendium auch konkrete technische und organisatorische Sicherheitsmaßnahmen beschreibt. Insbesondere die öffentliche Hand orientiert sich an diesem Standard und ist teilweise auch gesetzlich verpflichtet, ihn umzusetzen.

Diese Anpassung erfolgt u. a. in Abhängigkeit von Faktoren wie der Größe der Organisation, seinem Steuerungs- und Organisationsmodell, den Geschäftsprozessen, der dazu eingesetzten Software und Hardware oder den genutzten Dienstleistern. Dies macht das Modell sehr flexibel, zumal auch eigene Anpassungen und Erweiterungen möglich sind. Diese Flexibilität ist Segen und Fluch zugleich, weil eben die Anpassungsarbeit erforderlich ist, bevor es an die Konzeptionierung und Umsetzung von Sicherheitsmaßnahmen geht.

Für vergleichbare IT-Strukturen und Datenverarbeitungen gibt es im IT-Grundschutz die Möglichkeit, Maßnahmenbündel in sogenannten Profilen zusammenzufassen und hierbei Prioritäten vorzugeben. Das Ziel ist dabei, sich bei jeder Anwendung wiederholende konzeptionelle Arbeiten „vor die Klammer zu ziehen" und die Nutzung der Ergebnisse auch anderen Organisationen zur Verfügung zu stellen.

Die kommunalen Spitzenverbände haben in der „Arbeitsgruppe kommunale Basis-Absicherung" (AG koBa) ein solches **Profil zur „Basis-Absicherung Kommunalverwaltung"** erstellt. Die an die (jeweils) aktuelle Fassung des IT-Grundschutzes angepasste Version, aktuell die Version 4.0, ist hier abrufbar:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html

Kurzlink: *https://uldsh.de/tb42-6-1-2a*

Das Projekt SiKoSH ermöglicht einen **Einstieg in das Management der Informationssicherheit**, indem es mit Musterkonzepten und -dokumenten unterstützt. Es hebt sich durch bewusste Vereinfachungen von der vollständigen Vorgehensweise des IT-Grundschutzes ab, um Einstiegshürden zu senken. Klar ist damit auch, dass allein damit nicht das umfassende Sicherheitsniveau von IT-Grundschutz erreicht werden kann.

Es ist nicht möglich, sämtliche Konstellation aller kommunalen Datenverarbeitungen und Organisationen zu erfassen – allein schon die unterschiedliche Größe der Kommunen erfordert verschiedene Steuerungsmodelle. Aber auch die jeweils betriebenen IT-Verfahren und Strukturen sind sehr unterschiedlich. Schließlich gibt es im kommunalen Bereich auch Datenverarbeitungen, die außerhalb der klassischen Verwaltung liegen, aber dennoch abzusichern sind, beispielsweise Steuerungen im Bereich der Klärtechnik. Dies macht klar, dass SiKoSH ein Einstieg, aber keine vollständige Implementierung eines Sicherheitsmanagements für alle Facetten der Datenverarbeitung ist. Durch die **Anpassungsfähigkeit und Erweiterbarkeit** des Modells ist ein „Mehr" aber immer möglich.

Soweit sinnvoll, können das Organisationsmodell und auch zahlreiche technische Anforderungen zur Umsetzung von Datenschutzvorgaben, insbesondere im technisch-organisatori-

schen Bereich, verwendet werden. Zu beachten ist, dass bei der Verarbeitung personenbezogener Daten die **Maßnahmen der Basis-Absicherung nicht immer ausreichen**. Dennoch ist es sinnvoll, mit kleinen Schritten zu beginnen, anstatt angesichts einer (vermeintlich) riesigen Aufgabe zu kapitulieren. Durch das Projekt SiKoSH wird eine Möglichkeit geschaffen, Erfahrungen auszutauschen, die Erstellung von Musterdokumenten zu beschleunigen und eigene Erkenntnisse aus der Praxis direkt mit einfließen zu lassen.

6.1.3 Arbeitskreis Rechnungsprüfung

Im vergangenen Jahr war das ULD, wie auch die Prüfgruppe IT des Landesrechnungshofs, wie zuvor am „Arbeitskreis IT der Rechnungsprüfungsämter der Kreise und der Städte Schleswig-Holsteins" beteiligt.

Bei der IT-Prüfung der Rechnungsprüfungsämter ist auch der ordnungsgemäße Einsatz von Informationstechnik bedeutsam. Daraus ergeben sich Überschneidungen zu Fragen des Datenschutzes und der Informationssicherheit.

Neben einem generellen Interesse an den Vorgaben und Maßstäben des Landesrechnungshofs und der Datenschutzaufsicht spielen immer wieder Einzelfragen eine Rolle. Im Berichtszeitraum waren dies u. a. Fragen zur **Passwortsicherheit** (Tz. 10.3).

Daneben sind die Treffen der Arbeitsgruppe eine gute Gelegenheit, sich über sogenannte ebenenübergreifende Verfahren auszutauschen, d. h. Verfahren, in denen Kommunen und Land, teilweise auch der Bund, zusammenarbeiten. Typische Beispiele sind die zahlreichen Verfahren im Bereich **Online-Zugangsgesetz (OZG)**, für die durch das Land technische Komponenten bereitgestellt werden, die dann mit kommunalen Fachverfahren kommunizieren. Hierdurch ergeben sich **mittelfristig Herausforderungen im Bereich der IT-Prüfung**, sodass eine frühzeitige Einbindung und Information sinnvoll sind.

Auch jenseits konkreter Verwaltungsanwendungen ist ein Austausch über zukünftige Entwicklungen wertvoll, beispielsweise verschiedene Möglichkeiten, Datenverarbeitung durch Dritte erbringen zu lassen. Stichwörter sind hier die klassischen Verfahren der **Auftragsverarbeitung** bis hin zu **künstlicher Intelligenz** und **Cloud-Anwendungen**, zu denen das ULD aus Datenschutzsicht aufklärt. Diese Aspekte spielen zwar häufig noch keine unmittelbare Rolle im Alltag der IT-Prüfung, sind aber als zukünftige Themen relevant und erfordern, dass IT-Prüferinnen und Prüfer sprechfähig sind.

Angeregt werden konnte eine gemeinsame Diskussion über **Prüfkriterien für den Einsatz von KI-Systemen in der öffentlichen Verwaltung**. Hier ergeben sich neben klassischen Aspekten zum Datenschutz neue Fragestellungen rund um rechtsstaatliche Anforderungen, Diskriminierungsfreiheit sowie Transparenz und Informationsfreiheit.

Was ist zu tun?

Die bisherige gute und vertrauensvolle Zusammenarbeit soll fortgesetzt werden.

6.1.4 Künstliche Intelligenz – neue Fragen zum datenschutzkonformen Einsatz

Seitdem die Firma OpenAI im November 2022 den Chatbot ChatGPT in der Version 3.5 für die Öffentlichkeit kostenlos zur Verfügung gestellt hat, werden weltweit die Möglichkeiten und Risiken sowie die gesellschaftlichen und wirtschaftlichen Effekte von Systemen mit künstlicher Intelligenz diskutiert – und die vielen neuen und in kurzer Zeit weiterentwickelten KI-Systeme ausprobiert.

Die **datenschutzrechtliche Perspektive** muss vor dem Hintergrund neuer technischer Entwicklungen bei KI-Systemen und vielen Überlegungen zu Einsatzmöglichkeiten laufend neu diskutiert und formuliert werden. Im ULD beschäftigen wir uns schon seit mehreren Jahren mit künstlicher Intelligenz und waren 2019 an der Entwicklung von allgemeinen Positionen der Datenschutzkonferenz (DSK) zu künstlicher Intelligenz maßgeblich beteiligt (siehe Kasten).

In der **Taskforce KI der Datenschutzkonferenz** werden mit einem Informationsersuchen an OpenAI (siehe Tz. 6.3.1) die datenschutzrechtlichen Fragestellungen rund um das bekannteste KI-System erörtert. Gleichzeitig müssen neben den KI-Systemen mit großen Sprachmodellen (Large Language Models), die die technische Grundlage für viele Chatbots sind, auch viele andere KI-Systeme im Blick behalten werden, die z. B. zum Generieren von Bildern, zur Erkennung von Mustern (Gesichter, Verhalten) oder in der Medizin zum Einsatz kommen können.

Die KI-Systeme haben oft unterschiedliche Nutzungsweisen, sodass sich auch die menschlichen Interaktionen sowie Kontroll- und Eingriffsmöglichkeiten unterscheiden. Beispielsweise werden bei Bildgeneratoren typischerweise mehrere Ausgaben erzeugt, aus denen das beste Ergebnis ausgewählt wird – bei Textgeneratoren wird hingegen mit einem Ergebnis gearbeitet, das aber einfacher an konkreten Stellen korrigiert werden kann. Bei Übersetzungen in Sprachen, die selbst nicht beherrscht werden, oder in fachlich anspruchsvollen Texten können wiederum Fehler versteckt sein, die nur mit entsprechendem Wissen erkennbar sind. In den bekannten Chatbots, die auf großen Sprachmodellen aufbauen, ist eine **qualitative Einschätzung der gegebenen Antworten nicht möglich** – im Gegenteil wird je nach Programmierung an einer einmal getätigten Aussage stumpf festgehalten und gegebenenfalls eine falsche Information um weitere halluzinierte Aspekte ergänzt oder der Chatbot rudert umfassend zurück, entschuldigt sich und behauptet möglicherweise das genaue Gegenteil – das auch nicht richtig ist.

In einigen KI-Systemen, z. B. in medizinischen Anwendungen oder der autonomen Mobilität, werden Ergebnisse mit einer qualitativen Einschätzung beispielsweise in Form eines Wahrscheinlichkeitswerts ausgegeben. Hier muss für Anwendende klar festgelegt sein, wie diese Werte zu interpretieren sind und was daraus für die weitere Arbeit mit den Ergebnissen folgt.

Verwendet man beispielweise interaktive Bildgeneratoren beim Design von Publikationen zur Erzeugung von Grafiken, so lässt man sich so lange Grafiken erstellen, bis man mit dem Vorschlag zufrieden ist. Nutzt man Textgeneratoren wie ChatGPT interaktiv zur Erzeugung von Texten, etwa von Reden, Dokumentationen, Vermerken o. Ä., ist möglicherweise die menschliche Qualitätskontrolle weniger ausgeprägt und die Vorschläge werden schneller übernommen. Das bedeutet aber auch als **Daumenregel** für den praktischen Einsatz: Kommen die Systeme bei Anwendungen zum Einsatz, bei der die Antwort durch die Empfangenden nur schwer auf Richtigkeit geprüft werden kann, sind aus Nutzendensicht deutlich höhere **Anforderungen an die Korrektheit der Ausgaben** zu stellen. KI-Entwicklungsteams sollten bei der Gestaltung die Zielgruppe im Kopf haben und im Falle von Unsicherheiten beispielsweise Meldungen wie „Antwort nicht möglich“ vorzusehen. Beispiele hierfür sind etwa

- Übersetzungen in Sprachen, die selbst nicht beherrscht werden,
- Bilderkennungen im medizinischen Bereich, die gerade über Aspekte hinausgehen sollen, die der menschlichen Wahrnehmung zugänglich sind,
- Chatbots für Fragen mit Antworten, deren Qualität und Korrektheit die Fragenden nicht einschätzen können (etwa zu Details

von Verwaltungsverfahren, Fristen usw.) oder

- Bilderkennungsverfahren für Massendaten (etwa Schrifterkennung), die sich aufgrund der Menge einer detaillierten menschlichen Kontrolle entziehen.

Grundrechte und Grundfreiheiten natürlicher Personen sind beim Einsatz von KI-Systemen gleich mehrfach betroffen: Personenbezogene Daten können **beim Training** sowie **beim Arbeiten mit der Software** verarbeitet werden. Die **Ausgaben** eines KI-Systems können außerdem falsche personenbezogene Angaben bis hin zur Diskriminierung enthalten. Dabei ist die genaue Funktionsweise von KI-Systemen meist unklar, sodass weder **Transparenz** bei der Verarbeitung gewährleistet werden kann noch sich **Betroffenenrechte**, wie z. B. das Recht auf Löschen, umsetzen lassen.

Insgesamt gibt es mit diesen und vielen weiteren ungeklärten Fragestellungen erhebliche Rechtsunsicherheiten. Notwendig ist mehr Forschung zur **Sicherheit, Transparenz und Erklärbarkeit** von KI-Systemen und eine weitere intensive Diskussion der datenschutzrechtlichen Fragen. Das ULD unterstützt diesen Prozess in verschiedenen Formen und steht auch als Ansprechpartner zur Verfügung.

Im Berichtsjahr wurden Vorarbeiten zu weiteren Materialien der DSK zu künstlicher Intelligenz geleistet, die im Jahr 2024 veröffentlicht werden sollen.

Positionen der DSK zu künstlicher Intelligenz

Hambacher Erklärung zur künstlichen Intelligenz (Sieben datenschutzrechtliche Anforderungen)

Entschließung der Datenschutzkonferenz (3. April 2019):

https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf

Kurzlink: *https://uldsh.de/tb42-6-1-4a*

Empfohlene technische und organisatorische Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen

Positionspapier der Datenschutzkonferenz (6. November 2019):

https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf

Kurzlink: *https://uldsh.de/tb42-6-1-4b*

6.2 Deutschlandweite und internationale Zusammenarbeit der Datenschutzbeauftragten

6.2.1 Neues aus dem AK Technik

Der AK Technik der Datenschutzaufsichtsbehörden des Bundes und der Länder ist derjenige Arbeitskreis, der sich mit technischen Fragestellungen beschäftigt. Da technische Fragen meist unabhängig von Staaten und Institutionen sind, beteiligen sich u. a. auch Vertreter des Datenschutzes aus den Bereichen Kirchen und Rundfunk sowie der Datenschutzaufsichtsbehörden im deutschsprachigen Ausland.

Eine sich in den letzten Jahren abzeichnende **Tendenz der Spezialisierung** hat sich weiter verstärkt: Die Tätigkeit hat sich von der Arbeit im Gesamtgremium hin zu Unterarbeitsgruppen (z. B. UAG SDM, Tz. 6.2.2) und interdisziplinären Taskforces (etwa „Microsoft 365“, Tz. 6.2.3, Taskforce Souveräne Cloud, Tz. 6.2.4, Künstliche Intelligenz, Tz. 6.3.1) verschoben. Diese sind teils zeitlich befristet für ein Einzelprojekt (etwa die Taskforce Souveräne Cloud), teils als dauerhafte Institution (wie die Unterarbeitsgruppe SDM) tätig.

Auch die Zusammenarbeit mit der europäischen Ebene spezialisiert sich weiter: Zwar agiert der AK Technik weiterhin als **deutsches Spiegelgremium zur europäischen Technology Expert Subgroup**, der Arbeitsgruppe des Europäischen Datenschutzausschusses (EDSA) für Technikaspekte, und die deutschen Vertreter in der Technology Expert Subgroup stimmen die deutsche Position mit dem AK Technik ab. Doch mittlerweile sind bestimmte Fragestellungen und Detailabsprachen bei der Formulierung von europaweiten Dokumenten so spezialisiert und unterliegen oft gleichzeitig einem hohen Zeitdruck, dass eine detaillierte Zuarbeit des AK Technik nicht mehr als Gremium erfolgt, sondern die Expertise einzelner Aufsichtsbehörden in Ad-hoc-Arbeitsgruppen benötigt wird.

Ein Beispiel sind weiterhin die Dokumentenentwürfe zu **Pseudonymisierung und Anonymisierung**. Diese vermeintlich rein technischen Verfahrensschritte der Pseudonymisierung oder Anonymisierung vor einer weiteren Verarbeitung oder Weitergabe von Daten an Dritte sind deswegen relevant, weil ihre praktische Wirksamkeit grundlegende Rechtsfolgen nach sich ziehen kann: Die DSGVO gilt gemäß Erwägungsgrund 26 nämlich nicht für anonyme Daten.

> **Erwägungsgrund 26 Satz 5 der DSGVO**
>
> Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.

Einige Verantwortliche wollen genau dies: Die personenbezogenen Daten anonymisieren und anschließend die resultierenden Daten – die möglichst denselben Informationsgehalt aufweisen sollen – außerhalb des Gültigkeitsbereichs der DSGVO verarbeiten. Dies schließt auch die Übermittlung der einer Anonymisierung unterzogenen Daten an Dritte und auch Organisationen außerhalb der EU ein – Verarbeitungen, die häufig im Umfeld medizinischer Forschungen erfolgen. In diesen Fällen muss sichergestellt sein, dass die Anonymisierung wirklich funktioniert hat und die Daten insoweit ohne Datenschutzrisiken für die betroffenen Personen weitergegeben werden können.

Was sich hier leicht als Anforderung benennen lässt, muss für praktische Anwendungen aber noch weiter ausformuliert werden, etwa bei der Frage, inwieweit Zusatzwissen der Daten empfangenden Stellen zu bedenken ist und welche Anforderungen genau an die Berücksichtigung zukünftiger technischer Entwicklungen zu stellen sind, mit denen später Daten erneut betroffenen Personen zugeordnet werden können. Auch die Frage, inwieweit dabei Aussagen, die nur mit

einer gewissen Wahrscheinlichkeit zutreffen (etwa statistische Aussagen), in die Rechte und Freiheiten von Personen eingreifen, spielt dabei eine Rolle.

Eines ist aber heute schon klar: Es ist **nicht möglich, eine Anonymisierung zu erreichen, wenn der Informationsgehalt der Daten unverändert sein soll**. In diesen Fällen ist Anonymisierung nicht die Lösung, sondern es kann ein Personenbezug der Daten nicht ausgeschlossen werden, die Verarbeitung bleibt also innerhalb der DSGVO. Das ist kein Beinbruch – der Verantwortliche benötigt allerdings eine Rechtsgrundlage. Schwieriger ist der Fall der **vermeintlichen Anonymisierung**: Die Daten sind schon munter weitergegeben worden, insbesondere ohne betroffene Personen zu informieren oder die nötigen technischen und organisatorischen Schutzmaßnahmen zu treffen, als sich herausstellt, dass sie doch einen Personenbezug aufweisen. Dies gehört zu den Punkten, mit denen wir uns in dem Kompetenzcluster AnoMed (Tz. 8.5) beschäftigen.

6.2.2 Neues vom Standard-Datenschutzmodell

2023 war das bislang ruhigste Entwicklungsjahr seit Bestehen des Standard-Datenschutzmodells (SDM). Ruhig bedeutet, dass keine Änderungen am Modell vorgenommen und keine weiteren Bausteine veröffentlicht wurden. Stattdessen standen zwei andere Themen im Vordergrund: das **Wissen zum SDM und dessen Anwendung zu verbessern** und die **Entwicklung guter SDM-Tools voranzubringen**.

Das ULD wurde bei der Durchführung von ganztägigen Workshops und Coachings zum SDM stark beansprucht, insbesondere bei anderen Datenschutzaufsichtsbehörden. Diese Workshops haben bereits zu einer **Standardisierung der Planung einer gemeinsamen Prüfung** durch verschiedene Datenschutzbehörden auf der Grundlage des SDM-Würfels (siehe 41. TB, Tz. 6.2.2) geführt.

Speziell auf kommunaler Ebene liegen inzwischen verstärkt weitere Erfahrungen mit Datenschutz-Folgenabschätzungen auf der Grundlage des SDM vor, in einigen Fällen unter Zuhilfenahme von SDM-Tools.

Bei den meisten derzeit verfügbaren SDM-Tools handelt es sich um eine **Aufbereitung der in den SDM-Bausteinen genannten Schutzmaßnahmen** in Form selbst entwickelter Formulare in Tabellenkalkulationen. Derartige Programme werden inzwischen auch auf dem freien Markt angeboten, in zum Teil allerdings unzureichender Qualität. Diese Beobachtung zur Qualität hatte die Unterarbeitsgruppe SDM (UAG SDM) zum Jahreswechsel 2022/2023 zum Anlass genommen, sich einen Überblick über SDM-Tools zu verschaffen. Über den SDM-Newsletter sowie das SDM-Forum des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wurden Programmhersteller speziell von SDM-Tools aufgerufen, sich bei der UAG SDM zu melden. Daraufhin bekamen elf Hersteller die Gelegenheit, ihr SDM-Tool eine Stunde lang per Videokonferenz exklusiv den Mitgliedern der UAG SDM vorzustellen.

In diesen Vorstellungen wurde deutlich, dass der Leistungsumfang der Tools breit streut. Weit verbreitet sind derzeit **Formulare auf Excel- und Access-Basis**, die vornehmlich gestatten, die Umsetzung von Maßnahmen aus den SDM-Bausteinen zu dokumentieren. Mehr Unterstützung bieten sogenannte **SDM-Wizards**, die beim Ausfüllen von Formularen assistieren. So wurden erste Prototypen gezeigt, die auf der Grundlage des SDM-Würfels eine auf die konkrete Verarbeitung abgestimmte Modellierung von Verarbeitungen vornehmen und dadurch einen programmgestützten Ablauf für Beratung, Prüfung und Controlling bieten. Solche für die Prüfpraxis besonders hilfreichen Wizards sind bisher nach unserer Kenntnis (Stand: Januar 2024) noch nicht auf dem Markt verfügbar, werden aber teilweise schon organisationsintern eingesetzt.

Interessierte an SDM-Tools sollten die Meldungen des SDM-Newsletters des ULD verfolgen.

Link zum Newsletter:

https://www.datenschutzzentrum.de/mailinglisten/#sdm

Kurzlink: *https://uldsh.de/tb42-6-2-2a*

Bei der Tool-Sichtung zeigte sich, dass nicht alle Hersteller von Tools für Informationssicherheit ein hinreichendes Verständnis für das spezifische Schutzgut des Datenschutzes ausgebildet hatten. Es reicht nicht aus, wenn lediglich eine bereits bestehende Grundschutzmodellierung im Wesentlichen nur quantitativ um weitere Schutzziele ergänzt wird. Diese Beobachtung veranlasste die UAG SDM, erste **Vorschläge zur Kennzeichnung der Art der Assistenz von SDM-Tools** zu erarbeiten, um die Beschaffungsteams vor falschen Versprechungen bezüglich der SDM-Orientierung zu schützen:

- SDM-VE: nutzt die drei Verfahrensebenen des SDM,
- SDM-DSP: nutzt die Unterscheidung Daten, Systeme, Prozesse,
- SDM-VV: nutzt die Unterscheidung der neun Verarbeitungsvorgänge,
- SDM-VP: nutzt die Unterscheidung der vier Verarbeitungsphasen,
- SDM-GZ: nutzt das vollständige Set der Gewährleistungsziele,
- SDM-RM: nutzt die Risikomodellierung anhand der Gewährleistungsziele,
- SDM-GM: nutzt den vollständigen Katalog generischer Maßnahmen,
- SDM-BS: nutzt den vollständigen Katalog veröffentlichter SDM-Bausteine,
- SDM*: nutzt alle SDM-Komponenten.

Wie weit der Markt der Datenschutzmodellierungstools diese Kennzeichnungen nutzen wird, ist allerdings offen.

Was ist zu tun?

Die professionellen Anwendenden des SDM sollten ihre Erwartungen an Tools gegenüber den Herstellern kommunizieren.

6.2.3 Update Microsoft 365 – Erarbeitung einer Handreichung für Microsoft 365

Im November 2022 hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder erneut festgestellt, dass Verantwortliche beim Einsatz der Office-Anwendungen von Microsoft 365 den Nachweis einer datenschutzkonformen Verarbeitung auf Basis der damals vorliegenden Materialien nicht erbringen können. Grundlage für diese Feststellung war ein 58-seitiger Abschlussbericht der DSK-Arbeitsgruppe „Microsoft Online-Dienste“, die intensive Gespräche mit Vertreterinnen und Vertretern von Microsoft geführt hatte.

Da sich diese grundsätzliche Feststellung der DSK auf die **allgemeinen Vertragsgrundlagen für Microsoft 365** bezog, gab und gibt es bei vielen Verantwortlichen die Frage, inwieweit die Möglichkeit besteht, im konkreten Einsatzszenario einen datenschutzkonformen Betrieb von Microsoft 365 zu erreichen.

Microsoft 365

Der vom US-amerikanischen Unternehmen Microsoft angebotene Online-Dienst Microsoft 365 (ehemals Office 365) beinhaltet die Online-Versionen von Office-Anwendungen wie Word oder Excel sowie weitere Webanwendungen. Mit Microsoft 365 kann ortsunabhängig und von jedem unterstützten Endgerät aus gearbeitet werden. Die Daten befinden sich in Rechenzentren von Microsoft.

Auf Initiative des Landesbeauftragten für den Datenschutz Niedersachsen wurde in einer informellen Arbeitsgruppe mehrerer Aufsichtsbehörden eine Handreichung für Verantwortliche erstellt, die Microsoft 365 einsetzen möchten.

Mit der Handreichung werden die im Abschlussbericht aufgezeigten Problemfelder konkret beschrieben und – wo möglich – Wege aufgezeigt, wie die Vorgaben der DSGVO eingehalten werden können. Der größte Teil der **Handlungshinweise umfasst Anpassungen des Vertrags und eine Nachbesserung der Produktdokumentation**. Die Verantwortlichen müssen entsprechende Anpassungen und Nachbesserungen beim Auftragsverarbeiter Microsoft einfordern.

Die DSK-Arbeitsgruppe „Microsoft Online-Dienste" hat einen umfangreichen Bericht über die Untersuchungen erstellt und der DSK vorgelegt. Die beschlossene Festlegung der DSK wurde zusammen mit einer Zusammenfassung des Berichts veröffentlicht. Die Verfahrensweise der Arbeitsgruppe war von einer starken Einbindung von Expertinnen und Experten sowie Verantwortlichen von Microsoft geprägt. In 14 mehrstündigen Gesprächsterminen wurden die Berichtsgegenstände diskutiert.

Abschlussbericht:
https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf

Kurzlink: *https://uldsh.de/tb42-6-2-3a*

Handreichung:
https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/einsatz-von-microsoft-365-praxis-tipps-fur-vertrage-mit-microsoft-225722.html

Kurzlink: *https://uldsh.de/tb42-6-2-3b*

Das ULD beobachtet gemeinsam mit den anderen Aufsichtsbehörden die laufenden Änderungen an den Datenschutzbestimmungen und die vielfältigen Bemühungen, **individuelle Anpassungen** vorzunehmen.

6.2.4 Update „souveräne Clouds"

Im vergangenen Jahr berichteten wir über Arbeiten der **Taskforce Souveräne Cloud** der Datenschutzkonferenz, die an einem Positionspapier mit Anforderungen für die Bereitstellung und Nutzung von souveränen Cloud-Angeboten gearbeitet hat (41. TB, Tz. 6.2.4) und an der das ULD beteiligt war.

Digitale Souveränität

Digitale Souveränität ist in einem umfassenden Sinne „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können".

(„Digitale Souveränität", Kompetenzzentrum Öffentliche IT (ÖFIT), November 2017)

Zur Erinnerung: Bei „souveränen Clouds" geht es um Cloud-Angebote, die es Verantwortlichen ermöglichen, bei der Nutzung der Angebote ihren datenschutzrechtlichen Pflichten **effektiv und überprüfbar nachzukommen** und dies auch **dauerhaft sicherzustellen**.

Gerade die dauerhafte Sicherstellung erfordert Maßnahmen, die über eine bloße Betrachtung des datenschutzrechtlichen Status quo hinausgehen. So muss es beispielsweise Strategien und vertragliche Festlegungen geben, wie mit zukünftigen **Änderungen der Rechtslage, der technischen Angebote und der Anforderungen der Verantwortlichen** umzugehen ist. Dies beginnt bei feingranularen Konfigurationsmöglichkeiten für Cloud-Anwendende und endet bei Möglichkeiten des Wechsels vom Ort der Verarbeitung, des Rechtsrahmens (Stichwort Geltungsbereich der DSGVO) oder auch des Cloud-Anbietenden.

Dabei sind auch Aspekte betroffen, die auf den ersten Blick scheinbar nur wenig mit Datenschutz zu tun haben (z. B. **Kündigungsfristen** oder die Nutzung von **Standards** bei der Verarbeitung von Daten eines Verantwortlichen), bei näherer Betrachtung aber einen großen Einfluss darauf haben, datenschutzrechtlichen Pflichten dauerhaft nachkommen zu können.

Das Positionspapier betrachtet die Aspekte der souveränen Clouds in fünf Abschnitten:

- Nachvollziehbarkeit durch Transparenz,
- Datenhoheit und Kontrollierbarkeit,
- Offenheit,
- Vorhersehbarkeit und Verlässlichkeit,
- regelmäßige Prüfung der aufgestellten Kriterien.

Darin werden jeweils Anforderungen formuliert, die ein Cloud-Angebot umsetzen muss bzw. sollte, damit es aus Sicht der DSK **den Namen „souveräne Cloud" zu Recht verdient**. Unterschieden wird dabei zwischen Cloud-Anbietenden und Cloud-Anwendenden. Zwar handelt es sich dabei typischerweise um IT-Dienstleister auf der einen Seite und ihre Kunden auf der anderen Seite, doch sagt dies noch nichts über eine datenschutzrechtliche Verantwortlichkeit im Sinne der DSGVO aus: Zwar sind Cloud-Anwendende meist Verantwortliche im Sinne der DSGVO und Cloud-Anbietende deren Auftragsverarbeiter, doch es sind auch andere Fälle denkbar, z. B. eine Verantwortlichkeit von Cloud-Anbietenden (etwa gegenüber Privatpersonen) oder eine gemeinsame Verantwortlichkeit von Cloud-Anbietenden und Cloud-Anwendenden. Schließlich kommt auch infrage, dass die Verantwortlichkeit von konfigurativen Einstellungen abhängt, etwa davon, ob bei der Nutzung von Software durch den Auftragnehmer ebenfalls Daten zu eigenen Zwecken erhoben und verarbeitet werden und der Dienstleister zum Verantwortlichen wird.

Anders als in umgangssprachlichen Texten wurde in diesem Positionspapier eine technisch orientierte Sprache gewählt, um den Verbindlichkeitsgrad der Anforderungen zu formulieren. Die Formulierung von „MUSS"- und „SOLL"-Anforderungen orientiert sich dabei an (internationalen) Standards – auch das IT-Grundschutz-Kompendium des BSI (Tz. 10.3), die Untermenge der SiKoSH-Anforderungen (Tz. 6.1.2) oder die Bausteine des Standard-Datenschutzmodells (Tz. 6.2.2) verwenden derartige Kennzeichnungen: Mit **„MUSS"** werden Anforderungen gekennzeichnet, die ausnahmslos umzusetzen sind. Bei **„SOLL"-Anforderungen** ist kein „soll" im Sinne von „es wäre zweckmäßig oder schön" gemeint, sondern eine Anforderung, die dringend empfohlen ist und deren Nichtumsetzung zwar möglich, aber genau zu begründen ist. „SOLL"-Anforderungen kann man sich als „grundsätzlich MUSS" oder „Muss mit Abweichungsmöglichkeit" vorstellen.

Da es nur diese beiden Abstufungen der Anforderungen geben sollte, war eine enge Abstimmung in der Taskforce und eine entsprechende **Sorgfalt bei der Formulierung** erforderlich: Eine „MUSS"-Anforderung ist zwar schnell entworfen, hat aber entsprechende Sonderfälle zu berücksichtigen und ist somit präziser zu formulieren. Die Alternative, komplizierte Anforderungen (vor-)schnell und vermeintlich einfach als „SOLL"-Anforderungen zu formulieren, verschöbe die Arbeit zu denjenigen, die das Positionspapier lesen und anwenden. Die Folge wären verschiedene Interpretationen über den Verbindlichkeitsgrad einer SOLL-Anforderung. Die Vergleichbarkeit von Angeboten derjenigen, die von sich behaupten, die DSK-Anforderungen an souveräne Clouds umzusetzen, würde leiden.

Das **Positionspapier** ist unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/uploads/dsk/2023-05-11_DSK-Positionspapier_Kriterien-Souv-Clouds.pdf

Kurzlink: *https://uldsh.de/tb42-6-2-4a*

Was ist zu tun?

Anbietende von Cloud-Dienstleistungen können anhand des Positionspapiers überprüfen, welche Kriterien die Datenschutzbehörden an eine dauerhafte und nachhaltige Umsetzung von Datenschutzanforderungen stellen. Cloud-Anwendende können mit dem Positionspapier als Checkliste Cloud-Angebote überprüfen und vergleichen.

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

6.3.1 Künstliche Intelligenz: Informationsersuchen an OpenAI

Das Jahr 2023 war geprägt von einer breiten Diskussion über künstliche Intelligenz. Anstoß war die kostenlose Veröffentlichung des Chatbots ChatGPT in der Version 3.5 im November 2022. Neben einer allgemeinen Diskussion über verschiedene Formen von KI-Systemen (siehe Tz. 6.1.4) haben auch viele öffentliche und nichtöffentliche Stellen Einsatzmöglichkeiten von ChatGPT geprüft.

Die Taskforce KI der Datenschutzkonferenz hat sich daher – aufbauend auf der vorangehenden Auseinandersetzung mit KI-Systemen – gleich mit einer **datenschutzrechtlichen Einschätzung der Einsatzmöglichkeiten von ChatGPT** und anderen großen Sprachmodellen (Large Language Models, LLM) beschäftigt. Um die Funktionsweise und die Verarbeitung von personenbezogenen Daten beim Training des Sprachmodells sowie bei der Arbeit mit dem Chatbot genauer zu verstehen, wurde gemeinsam ein **Fragenkatalog** entworfen.

In gut **40 Fragen** wurden im April 2023 vom Unternehmen OpenAI mehr Informationen und Transparenz abgefragt. Neben grundsätzlichen rechtlichen Fragestellungen wurden auch mehrere technische Problemstellungen angesprochen und wie betroffene Personen ihre Rechte geltend machen können.

Die Antworten von OpenAI im Sommer 2023 reichten noch nicht für eine datenschutzrechtliche Beurteilung aus. Doch sie konnten als Grundlage genutzt werden, um tiefer gehende Fragen zu erarbeiten. Im Oktober 2023 wurde unter den Aufsichtsbehörden ein **zweiter Fragenkatalog mit insgesamt 79 Fragen abgestimmt** und an OpenAI gesendet. Insbesondere der Verarbeitung von sensiblen Datenkategorien gemäß Artikel 9 DSGVO und der Umsetzung der Rechte betroffener Personen wurde besondere Aufmerksamkeit gewidmet. Aufschlussreich können auch Antworten und weitere Informationen zu Maßnahmen sein, die beim Training des Sprachmodells getroffen wurden, da an dieser Stelle entschieden wird, ob personenbezogene oder anderweitig sensible Daten zum Lernen verwendet werden.

Die datenschutzrechtliche Bewertung von KI wird auch in naher Zukunft ein komplexes Verfahren sein. Zum einen gibt es eine wachsende Zahl an Einsatzszenarien, die jeweils einzelne Fragestellungen aufwerfen und kontextabhängig bewertet werden müssen. Hinzu kommen immer mehr Anbieterinnen und Anbieter von KI-Dienstleistungen mit neuen KI-Systemen oder unter Nutzung vorhandener Angebote. Zum anderen werden die eingesetzten Technologien in hoher Geschwindigkeit weiterentwickelt, was sich positiv oder negativ auf die Einhaltung der datenschutzrechtlichen Vorgaben auswirken kann. Da laufend neue Funktionalitäten eingeführt und immer wieder neue Angriffsmöglichkeiten oder rechtliche Probleme bekannt werden, wird es

nicht einfacher. Es bleibt abzuwarten, ob die europäische KI-Verordnung dazu beiträgt, dass Anwendende einfacher die „Spreu" vom datenschutzkonformen „Weizen" trennen können.

Was ist zu tun?

Ob eine Verarbeitung personenbezogener oder personenbeziehbarer Daten datenschutzkonform in aktuellen KI-Chatbots möglich ist, muss im Einzelfall intensiv geprüft und angesichts der Veränderungsdynamik dieser Systeme laufend kontrolliert werden. Empfehlenswert ist daher, zunächst Anwendungsfälle ohne Personenbezug ins Auge zu fassen.

6.3.2 Trends bei gemeldeten Cyberangriffen

Wie in den Vorjahren betrafen zahlreiche Meldungen von Datenschutzverletzungen gemäß Artikel 33 DSGVO Cyberangriffe, insbesondere einen Befall mit Schadsoftware, anschließender Verschlüsselung der Datenbestände und ein erpresserisches Angebot, bei Zahlung einer Geldsumme die Entschlüsselung zu ermöglichen – ein klassischer Fall von **Ransomware**. Häufig war dies kombiniert mit einem unbefugten Datenzugriff und der Drohung, bei Nichtzahlung eines „Lösegelds" die erlangten Daten zu veröffentlichen.

Während im ersten Fall „nur" die Verfügbarkeit der Daten betroffen scheint und man durch gute Back-up- und Wiederherstellungsverfahren den Schaden schnell begrenzen kann, muss man bei einer **glaubhaften Drohung einer Veröffentlichung** mit einem Verlust der Vertraulichkeit rechnen (der sich in vielen Fällen auch bewahrheitet).

Aber auch im Falle der reinen Verschlüsselung ist das IT-System kompromittiert – ein Angreifer hatte ja die Gelegenheit, Schadcode zur Ausführung zu bringen. In beiden Fällen sind daher die IT-Systeme sorgfältig auf weiteren Schadcode und andere Manipulationen zu untersuchen. Ebenso muss untersucht werden, auf welche Weise der Schadcode in das System gelangte und welche **Gegenmaßnahmen dies zukünftig verhindern** oder zumindest die Wahrscheinlichkeit einer Kompromittierung senken. Daneben sind Härtungsmaßnahmen zu ergreifen, damit eingeschleppter Schadcode möglichst wenig Schaden stiften kann.

Typische Maßnahmen sind hier die **Deaktivierung von Makros und anderen Programmbestandteilen in Dateien**, die per E-Mail, Download oder Upload in ein System eingespielt werden. Ebenso hilft als Härtungsmaßnahme auf Betriebssystemebene ein sogenanntes **„Application Whitelisting"**: Nur ausdrücklich benannte und durch die Administration installierte Programme sind zur Ausführung freigegeben – von den Nutzenden heruntergeladene Programme oder unbewusst übertragener Schadcode nicht.

Diese Maßnahmen helfen nicht, wenn der Schadcode Sicherheitslücken ausnutzt, die in regulär installierter Software bestehen. Hier hilft nur der alte (40. TB, Tz. 6.3.3) **Grundsatz „Patchen, patchen, patchen"**, also die zeitnahe Installation von Sicherheitspatches (d. h. Software-Updates, die Fehler und Sicherheitslücken beheben).

Zu beobachten ist, dass das **Zeitfenster** zwischen der Entdeckung einer Sicherheitslücke und dem Ausnutzen durch Angreifer **immer kleiner** wird und folglich auch das Zeitfenster für die Installation von Patches. Dies betrifft nicht nur Betriebssysteme und Software der Bürokommunikation, sondern auch Softwarekomponenten im Hintergrund (etwa Datenbankmanagementsysteme, Webserver und die von ihnen verwendeten Softwarekomponenten wie Java

und PHP-Interpreter) und Software für Online-Dienste, etwa Shopsysteme für Webshops.

Ein weiterer Schwerpunkt der Meldungen lag bei **unbefugten Zugriffen auf (cloudbasierte) E-Mail-Konten**. Ausgangspunkt der Entdeckung war häufig, dass ein solches E-Mail-Konto unbefugt benutzt wurde, um Werbung oder Spam zu versenden.

Anders als in der Vergangenheit, als in solchen Fällen häufig Werbe-E-Mails bei schlecht gesicherten E-Mail-Servern lediglich unbefugt zum Versand „eingeliefert" wurden, geht es mittlerweile zunehmend um **schreibende Zugriffe auf einzelne E-Mail-Konten**. Es muss dann geprüft werden, ob es bei der Benutzung des E-Mail-Kontos zum Spam-Versand geblieben ist: Wer aus einem Konto senden kann, kann auch lesen und kopieren, d. h. Daten unbefugt zur Kenntnis nehmen. Teilweise lässt sich dies anhand einer Protokollierung des E-Mail-Servers feststellen.

Der Zugriff bei webbasierten Konten ist, anders als in der klassischen Welt beim Zugriff mit organisationseigenen Rechnern aus Büroräumen heraus auf den organisationseigenen Server, zunächst von jedem Endgerät und jedem Ort der Welt über das Internet möglich, wenn als Absicherung lediglich auf ein Passwort gesetzt wird. Wird einem Angreifer dieses Passwort bekannt, beispielsweise über einen Phishing-Angriff, kann dieser ebenso wie rechtmäßige Eigentümer auf das Postfach zugreifen. Es sind daher **zusätzliche Sicherungsmaßnahmen** vorzusehen, beispielsweise eine Zwei-Faktor-Authentifizierung oder die Begrenzung des Zugriffs auf bestimmte Netze (z. B. über ein VPN) oder bestimmte Endgeräte.

Bemerkenswert waren auch zahlreiche Fälle, die auf **Datenpannen bei Dienstleistern** zurückzuführen sind: Formal richtig informierten diese ihre Auftraggeber, die ihrerseits die Datenschutzverletzung gemäß Artikel 33 beim ULD meldeten. In den meisten Fällen war dies auch inhaltlich geboten, denn die Auftraggeber sind Verantwortliche im Sinne der DSGVO und können, zumeist anders als die Auftragnehmer, die Art der verarbeiteten Daten und Risiken für betroffene Personen einschätzen – die Fälle sind daher einzeln zu betrachten.

Bei rein technisch gelagerten Datenschutzverletzungen ist dies aber nicht immer zielführend, etwa wenn bei einem Dienstleister eine Software-as-a-Service-Anwendung betroffen ist: Hier gibt es **eine Ursache, die gleichermaßen auf alle Auftraggeber wirkt**, von diesen aber im Einzelfall nicht maßgeblich beeinflusst werden kann – ein typisches Phänomen von Cloud-Angeboten. Es würde mehr Sinn ergeben, auf technischer Ebene die **Ursache und Abhilfemaßnahmen direkt mit dem Dienstleister zu klären**, als dies jeweils einzeln und dafür mehrfach über Umwege mit den Auftraggebern zu tun.

Im öffentlichen Bereich ist diese Problematik erkannt worden: Bei Verordnungen zu gemeinsamen Verfahren gemäß § 7 Abs. 4 LDSG wird typischerweise vorgesehen, welche der beteiligten Stellen für die Abgabe und Bearbeitung der Meldungen gemäß Artikel 33 DSGVO zuständig ist.

Was ist zu tun?

Bei der Meldung von Datenschutzverletzungen sind insbesondere Maßnahmen vorzusehen und zu benennen, die einer Ausbreitung des Schadens und einer Wiederholungsgefahr entgegenwirken.

6.3.3 Prüfung Videokonferenzsysteme

Im Herbst 2021 begann eine gemeinsame **Prüfung von Videokonferenzsystemen**, die Dataport, der IT-Dienstleister für die (nord-)deutschen Bundesländer, den dortigen Behörden anbietet. An der Prüfung beteiligten sich die Datenschutzaufsichtsbehörden der Länder Hamburg, Bremen, Sachsen-Anhalt und Schleswig-Holstein (40. TB, Tz. 6.3.5). Prüfmaßstab waren zum einen funktionelle Anforderungen mit Datenschutzrelevanz, zum anderen technische Realisierungen und vertragliche Regelungen mit beteiligten Subunternehmern.

Eine Herausforderung bestand zunächst darin, **die unterschiedlichen Angebote** Dataports zu klassifizieren und zu unterscheiden: Einige Videokonferenzlösungen sind landesweit unter einem Softwarenamen wie „Jitsi" bekannt, werden aber durch Dataport in verschiedenen technischen Ausprägungen betrieben und unter entsprechenden Namen bereitgestellt. Schließlich gibt es noch verschiedene Versionen sowie teilweise eine Integration der Videokonferenzlösung in eine übergreifende Plattform.

Die Videokonferenzlösungen werden teils unmittelbar bei und durch Dataport betrieben, teils sind Teile der (technischen) Datenverarbeitung in Form von Containern ausgelagert. Bei Videokonferenzsystemen sind hier **verschiedene Ausprägungen** möglich, beispielsweise eine Trennung vom Aufbau der Konferenz (einschließlich der Authentifizierung der Nutzenden) einerseits und der technischen Durchführung (Signalübertragung zwischen den Kommunikationspartnern) andererseits. Hintergrund dieser Trennung sind meist technische Aspekte wie Bandbreite der Netzanbindung und benötigte Rechenkapazität: Die gleichzeitige Bereitstellung von Videokonferenzen, etwa für viele Schulklassen an Vormittagen, erfordert Netz- und Serverkapazitäten, die zu anderen Zeiten nicht genutzt würden – ein klassischer Fall für Cloud-Computing-Ansätze und **Auslagerung zu Dienstleistern**.

Bei solchen Auslagerungen sind mittlerweile verschiedene Implementierungen möglich. So gibt es – das ist das eine Ende des Spektrums – die Möglichkeit einer vollständigen Software-as-a-Service-Nutzung eines Videokonferenzsystems eines Anbieters (Cloud-Software). In diesem Fall liegt die Hoheit über die Software beim Cloud-Anbieter; es sind allenfalls konfigurative Anpassungen möglich. Das andere Ende des Spektrums ist die **Bereitstellung von Softwarecontainern**, die lediglich bei einem externen Dienstleister in dessen Cloud-Umgebung ausgeführt werden, hinsichtlich der Programmierung und Konfiguration aber vollständig unabhängig von diesem sind. Einen solchen Weg hat Dataport gewählt.

In der Prüfung werden zwei Gruppen von Videokonferenzdiensten betrachtet:

- Das Produkt „dVideokommunikation", das vollständig von Dataport betrieben wird, aber auf der Software eines kommerziellen Anbieters aufsetzt und auch (im Einzelfall) dessen Support-Dienstleistungen erfordert.
- Videokommunikationsdienste unter dem Stichwort „dOnlinezusammenarbeit", die einzeln oder als Bestandteil eines größeren Angebots („dPhoenixSuite") in verschiedenen Konfigurationen bereitgestellt werden.

Die Überprüfung ist noch nicht abgeschlossen, da noch **Dokumentationsbestandteile** überarbeitet bzw. fertiggestellt werden. Bisher wurden keine wesentlichen Mängel festgestellt.

Was ist zu tun?

Eine vollständige Dokumentation, die neben den von der DSGVO geforderten Nachweisen auch Dokumente zur Betriebsführung, zur Information für Kunden und Hilfsmittel für die durch Kunden umzusetzenden Sicherheits- und Datenschutzmaßnahmen umfasst, unterstützt alle Akteure beim datenschutzgerechten Einsatz.

07

KERNPUNKTE

Datenzugriffe öffentlicher Stellen in Drittländern

Cloudbasierte digitale Gesundheitsanwendungen

7 Neue Medien

Auch wenn durch die Digitalisierung und Vernetzung der Bereich der Neuen Medien mit der anderweitigen Gestaltung von Verarbeitungen personenbezogener Daten verschmilzt, sollen in diesem Bericht einige Punkte in diesem Kapitel wegen der gleichermaßen technischen und rechtlichen Anforderungen gesondert hervorgehoben werden. Jedoch finden sich ähnliche Themen auch unter anderen Textziffern in diesem Bericht (z. B. zu den Kriterien für souveräne Clouds in Tz. 6.2.4).

7.1 Datenzugriffe öffentlicher Stellen in Drittländern

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat sich mit der Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten befasst. Im Rahmen der gemeinsamen Beratungen der Datenschutzaufsichtsbehörden gewann die Konstellation an Bedeutung, in der eine **in einem Drittland ansässige Muttergesellschaft** eine **im Europäischen Wirtschaftsraum (EWR) niedergelassene Tochtergesellschaft** im Wege einer Auftragsverarbeitung beauftragt, personenbezogene Daten zu verarbeiten.

Allein der Umstand der Beauftragung des im EWR niedergelassenen Tochterunternehmens oder die damit verbundene Gefahr einer rechtswidrigen Datenweitergabe an die Muttergesellschaft im Drittland begründen dabei noch nicht eine „Übermittlung" personenbezogener Daten, die für sich einer Rechtsgrundlage bedürfte.

Das Augenmerk liegt in solchen Konstellationen vielmehr auf der Frage, ob das beauftragte Tochterunternehmen im EWR in seiner Funktion als Auftragsverarbeiter eine **hinreichende Zuverlässigkeit** aufweist, die Vorgaben der DSGVO einzuhalten, und in diesem Kontext **etwaigen rechtswidrigen Weisungen des Mutterkonzerns zur Datenweitergabe nicht Folge leistet** und mögliche nicht mit der DSGVO im Einklang stehende Verpflichtungen zur Datenherausgabe an staatliche Stellen in Drittländern unberücksichtigt lässt. Die Zuverlässigkeit der Auftragsverarbeiter wird in der DSGVO explizit erwähnt:

Art. 28 Abs. 1 DSGVO

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Soweit eine Norm oder Praxis eines Drittlands die abstrakte Gefahr einer nach EU-Recht unzulässigen Übermittlung personenbezogener Daten aus dem EWR in ein Drittland durch eine als Auftragsverarbeiter tätige Stelle in dem EWR – z. B. die EWR-Tochtergesellschaft eines Drittlandsunternehmens – begründet, sind an die Sorgfalt der Zuverlässigkeitsprüfung im Sinne von Art. 28 Abs. 1 DSGVO besonders hohe Anforderungen zu stellen, die dieser Gefahr Rechnung tragen. Die DSK hat mit Beschluss vom 31. Januar 2023 **wesentliche Prüfpunkte** zusammengefasst, die für eine Bewertung des Einzelfalls von Bedeutung sind. Die Punkte umfassen das Folgende:

- das Ergebnis einer Prüfung hinsichtlich einer **extraterritorialen Anwendbarkeit des Drittlandsrechts** und einer gegebenenfalls darüber hinausgehenden praktischen extraterritorialen Anwendung,

- bei einer extraterritorialen Anwendbarkeit und/oder Anwendung: das Ergebnis einer Prüfung, ob das **Recht oder die Praxis des Drittlands die Verpflichtungen aus dem Auftragsverarbeitungsvertrag beeinträchtigen** könnten (in Anlehnung an die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses),
- das Risiko, dass die Drittlands-Muttergesellschaft eines EWR-Tochterunternehmens dieses anweisen könnte, personenbezogene Daten in ein Drittland zu übermitteln (Prüfung der **Erkenntnisse zur Rechtslage/-praxis**),
- ob der **Auftragsverarbeitungsvertrag** nach europäischen Maßstäben unzulässige Verarbeitungen auf der Grundlage von Drittlandsrecht erlaubt,
- etwaige Zusicherungen der Drittlands-Muttergesellschaft und des EWR-Unternehmens zum **Umgang mit kollidierenden Anforderungen** des Rechts eines Drittstaates und der EU,
- eine **Bewertung der Rechtslage und -praxis** des Drittlands, ob derartige Zusicherungen auch tatsächlich eingehalten werden können,
- eine Bewertung **aller weiteren Aspekte**, ob derartige Zusicherungen auch tatsächlich eingehalten werden,
- etwaige in der Vergangenheit festgestellte **Datenschutzverstöße**,
- die Schwere und Wahrscheinlichkeit einer **Sanktionierung von Zuwiderhandlungen** nach EU-Recht und dem Recht des Drittlands sowie
- der Ausschluss unzulässiger Übermittlungen durch geeignete **technische und organisatorische Maßnahmen**.

Der Beschluss der DSK ist unter dem folgenden Link abrufbar:

www.datenschutzkonferenz-online.de/media/dskb/20230206_DSK_Beschluss_Extraterritoriale_Zugriffe.pdf

Kurzlink: *https://uldsh.de/tb42-7-1a*

7.2 Positionspapier zu cloudbasierten digitalen Gesundheitsanwendungen

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat mit Beschluss vom 6. November 2023 ein **Positionspapier zu cloudbasierten digitalen Gesundheitsanwendungen** erarbeitet, das unter dem folgenden Link abrufbar ist:

www.datenschutzkonferenz-online.de/media/dskb/2023_11_06_Beschluss_cloudbasierte_digitale_Gesundheitsanwendungen.pdf

Kurzlink: *https://uldsh.de/tb42-7-2a*

Digitale Gesundheitsanwendungen (DiGAs) sind nach den Vorgaben des SGB V Medizinprodukte niedriger Risikoklasse, deren Hauptfunktion wesentlich auf digitalen Technologien beruht und die dazu bestimmt sind, bei den Versicherten oder in der Versorgung durch Leistungserbringer die Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder die Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen zu unterstützen und für welche den gesetzlich Versicherten ein Versorgungsanspruch zusteht.

Datenschutzrechtliche Vorgaben für DiGAs sind in der **Digitale-Gesundheitsanwendungen-Verordnung (DiGAV)** normiert.

Art. 4 Abs. 1 DiGAV

Digitale Gesundheitsanwendungen müssen die gesetzlichen Vorgaben des Datenschutzes und die Anforderungen an die Datensicherheit nach dem Stand der Technik unter Berücksichtigung der Art der verarbeiteten Daten und der damit verbundenen Schutzstufen sowie des Schutzbedarfs gewährleisten.

Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) führt ein Verzeichnis erstattungsfähiger DiGAs und entscheidet auch über die Anträge der DiGA-Hersteller zur Aufnahme in das Verzeichnis. Dabei **weisen die Hersteller digitaler Gesundheitsanwendungen die Erfüllung der datenschutzrechtlichen Anforderungen nach**. Das DiGA-Verzeichnis ist unter dem folgenden Link erreichbar:

https://diga.bfarm.de/de/verzeichnis

Kurzlink: *https://uldsh.de/tb42-7-2b*

Neben diesen gesetzlich geregelten DiGAs gibt es jedoch eine **Vielzahl weiterer Gesundheitsanwendungen**, die **nicht von diesen Regelungen erfasst** sind. Für den Einsatz dieser Vielzahl der weiteren Anwendungen sind aus Sicht der DSK folgende Punkte zu beachten, die hier auszugsweise wiedergegeben werden:

- Eine **datenschutzrechtliche Verantwortlichkeit** kommt für verschiedene Beteiligte in Betracht, je nachdem ob diese im Einzelfall die Zwecke und Mittel der Datenverarbeitung bestimmen. Dies kann neben Ärztinnen und Ärzten und anderen medizinischen Leistungserbringern auch Hersteller betreffen.
- Die Verwendung der Gesundheitsanwendung (z. B. einer App zum Auslesen und Speichern der Glukosewerte) muss nach dem Grundsatz „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" nach Art. 25 Abs. 1 DSGVO auch **ohne Nutzung der Cloud-Funktionen und ohne Verknüpfung mit einem Benutzerkonto möglich** sein, es sei denn, die Cloud-Funktion ist unbedingt für die Erreichung eines therapeutischen Nutzens erforderlich und die Funktion wird von der betroffenen Person ausdrücklich gewünscht.
- Für die Nutzung personenbezogener Daten zu Forschungszwecken ist eine datenschutzrechtliche Rechtsgrundlage erforderlich. Hier kommt regelmäßig die ausdrückliche **Einwilligung** in Betracht.
- Die Hersteller bzw. Betreiber von cloudbasierten DiGAs müssen Prozesse zur effektiven und unverzüglichen Erfüllung der **Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit** etablieren. Da hierbei besonders sensible Gesundheitsdaten betroffen sind, muss zunächst eine **sichere Authentifizierung** der Antragsteller erfolgen.
- Weil eine Verarbeitung personenbezogener Daten immer mit Risiken für die davon betroffenen Personen einhergeht, müssen der Verantwortliche und Auftragsverarbeiter durch die wirksame Umsetzung technischer und organisatorischer Maßnahmen ein dem **Risiko angemessenes Schutzniveau gewährleisten** und den **Nachweis** dafür erbringen können.
- Auch sollte die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Technische Richtlinie (TR) **„Sicherheitsanforderungen an digitale Gesundheitsanwendungen" (BSI TR-03161)** für alle mobilen Anwendungen, die sensible Daten verarbeiten und speichern, herangezogen werden.
- Die Technische Richtlinie ist unter dem folgenden Link verfügbar:

  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03161/BSI-TR-03161.html

  Kurzlink: *https://uldsh.de/tb42-7-2c*

Was ist zu tun?

Wann immer eine Verarbeitung personenbezogener Gesundheitsdaten erfolgt, sind die geeigneten technischen und organisatorischen Maßnahmen zur Risikoeindämmung zu treffen. Dies gilt auch für Produkte und Anwendungen, die nicht zu den gesetzlich geregelten Digitalen Gesundheitsanwendungen (DiGAs) gehören.

08

KERNPUNKTE

Plattform Privatheit

Transparenz- und Einwilligungsmanagement

AnoMed – Kompetenzcluster Anonymisierung für medizinische Anwendungen

8 Modellprojekte und Studien

Das Unabhängige Landeszentrum für Datenschutz hat als Behörde der Landesbeauftragten für Datenschutz seine Aktivitäten in Initiativen im Bereich drittmittelfinanzierter Projekte und Studien fortgesetzt. Damit ist das ULD weiterhin im Bereich der Kooperation mit der Wissenschaft aktiv und erhält sich damit die Möglichkeit, zusammen mit Wissenschaftspartnern proaktiv an der **Erforschung datenschutzspezifischer Fragen und der Gestaltung einschlägiger Technologien** mitzuwirken.

Im Berichtszeitraum wurden Projekte von der Europäischen Kommission und dem Bundesministerium für Bildung und Forschung (BMBF) gefördert. Beteiligungen an Projekten erfolgten weiterhin primär dort, wo entweder besondere datenschutzfördernde Lösungen (englisch: „Privacy-Enhancing Technologies", kurz PETs) erforscht und entwickelt werden oder wo besondere Risiken für die Rechte und Freiheiten natürlicher Personen bestehen.

Im Jahr 2023 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 für Datenschutz, Transparenz und Einwilligungsmanagement fort (Tz. 8.4) und befasste sich mit der Anonymität für Medizinforschung mit Gesundheitsdaten (Tz. 8.5).

8.1 Plattform Privatheit: PRIDS – Privatheit, Demokratie und Selbstbestimmung

Der bereits im letztjährigen Tätigkeitsbericht (41. TB, Tz. 8.1) angekündigte **Wechsel vom Forum Privatheit zur Plattform Privatheit** wurde nun sehr sichtbar auf der letztjährigen Jahreskonferenz der Plattform Privatheit vollzogen. Die Jahreskonferenz ist eine von mehreren Veranstaltungen der Plattform zur Präsentation von Arbeitsergebnissen und dem wissenschaftlichen Austausch mit anderen Forschenden. Die Konferenz hatte das Thema **„Data Sharing – Datenkapitalismus by Default?"** gewählt und befasste sich u. a. mit den neuen Datenräumen zur Gesundheit und Mobilität. Die Konferenz hinterfragte dabei auch die weiter voranschreitende Kommerzialisierung dieser Lebensbereiche, die zu einer Einengung der Handlungsspielräume der Bürgerinnen und Bürger zugunsten großer Technikunternehmen (Big Tech) führt.

Im Jahr 2023 befassten wir uns auch mit Fragen von **Gerechtigkeit bei der Verarbeitung von Daten** für alle Bürgerinnen und Bürger, der Datengerechtigkeit. Dabei ging es darum, Probleme zu identifizieren und Lösungsansätze zu entwickeln. Ein Problem ist etwa die fehlende Einbindung bestimmter Personengruppen bei der Gestaltung von Datenverarbeitung. Dies führt dazu, dass viele Software-Anwendungen eigentlich nur für eine oder wenige bestimmte Personengruppen zuverlässig funktionieren.

Datengerechtigkeit

Das Forschungsfeld der Datengerechtigkeit (Data Justice) untersucht, wie sich Datenpraktiken von Unternehmen, aber auch staatlicher Seite, auf Bürgerinnen und Bürger auswirken. Die negativen Auswirkungen treffen meist Personengruppen, die bereits in anderen Lebensbereichen benachteiligt werden, z. B. Frauen, schwarze Menschen oder Lesben, Schwule, Bisexuelle und Trans*personen. Ihre Bedürfnisse werden bei der Gestaltung von Datenverarbeitung nicht immer ausreichend berücksichtigt.

Ein Beispiel sind **Bildgeneratoren**, die als Anwendungen der sogenannten künstlichen Intelligenz inzwischen in vielen Varianten verfüg-

bar sind. Allerdings produzieren sie oft nur stereotypische Darstellungen von schwarzen Menschen oder stellen Frauen und Mädchen in übersexualisierter Weise dar. Ein Lösungsansatz besteht darin, die (Trainings-)Daten, auf denen diese Anwendungen basieren, besser zu überwachen, damit keine einseitigen, verfälschenden oder gar toxischen Inhalte eingeführt werden.

https://www.plattform-privatheit.de/

Kurzlink: *https://uldsh.de/tb42-8-1a*

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

Das vom BMBF geförderte Projekt „DatenTRAFO – Neue Datenschutz-Governance – Technik, Regulierung und Transformation" ist im September 2023 gestartet. Es beschäftigt sich mit der Frage, wie der **Systemdatenschutz**, der bereits insbesondere in **Artikel 25 und Artikel 32 DSGVO** verlangt wird, ausgebaut werden kann.

Systemdatenschutz bietet Möglichkeiten, **Datenschutz von Beginn an und während des gesamten Verarbeitungsvorgangs zu gewährleisten** und auf diese Weise Bürgerinnen und Bürger sowie den demokratischen Rechtsstaat zu schützen. Dafür untersucht das Projekt, wie sich vorhandene Verfahren und Produkte des technischen Datenschutzes vermehrt in der Praxis einsetzen lassen.

Zu den Tätigkeiten im Projekt gehört auch eine Analyse, wie **Regulierung, Standards und Zertifizierungen** gestaltet werden können, um datenschutzfreundliche Lösungen zu befördern und die Grundrechte von Bürgerinnen und Bürgern besser durchsetzen zu können. Dabei werden auch Fragen der digitalen Souveränität mit einem Fokus auf den Umgang mit oder das Reduzieren von Abhängigkeiten, beispielsweise von mächtigen Digitalkonzernen, eine Rolle spielen.

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

Kurzlink: *https://uldsh.de/tb42-8-2a*

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

Das ULD ist seit November 2023 an dem vom BMBF geförderten Verbundprojekt **„Tool-gestützte, moderierte und bürgerzentrierte Community-Plattform zur Privacy-Einstufung von IoT-Produkten – Unboxing.IoT.Privacy"** beteiligt.

Das Internet der Dinge (englisch: „Internet of Things", IoT) weist ein hohes Potenzial auf und bringt die Vorteile von Digitalisierung und Vernetzung direkt zu den Menschen. Damit birgt es zugleich Gefahren für die Rechte und Freiheiten der betroffenen Personen. Für das ULD ist daher nicht nur wichtig, dass die damit zusammenhängenden Verarbeitungen personenbezogener Daten auf Basis einer geeigneten Rechtsgrundlage erfolgen, sondern auch dass Betroffene über eine Datenverarbeitung angemessen informiert werden und eingreifend reagieren können.

Das ULD beteiligt sich an dem Projekt Unboxing.IoT.Privacy mit dem Ziel, das Internet of Things **verständlicher zu machen**. Bürgerinnen und Bürgern soll es ermöglicht werden zu wissen und soweit möglich zu beeinflussen, wer welche Informationen zu welchen Zwecken wo und wie über sie erhebt, verarbeitet, speichert und nutzt – ganz im Sinne des Rechts auf informationelle Selbstbestimmung.

Internet of Things

Das Internet der Dinge (englisch: „Internet of Things", IoT) beschreibt Technologien, die physische und virtuelle Objekte mithilfe von Informations- und Kommunikationstechnik zusammenwirken lassen. So können mittels Sensoren Informationen aus der realen Welt erfasst werden, die sich dann weiterverarbeiten lassen, z. B. übermittelt, verknüpft oder im Netz bereitgestellt werden. Umgekehrt können Aktoren die physische Welt beeinflussen, Türen öffnen, Lichter schalten oder den heimischen Saugroboter steuern.

Zwingende Vorbedingung hierfür ist indes, dass diejenigen, die IoT-Geräte einsetzen, ihrerseits hinreichend über die Verarbeitung personenbezogener Daten, das damit verbundene Risiko und Maßnahmen zur Risikobeherrschung **informiert** sind. Das ist die **Grundlage** dafür, Auswahl- und Kaufentscheidung sowie Konfiguration der Geräte angemessen durchführen zu können und als Verantwortliche Informationen über den Einsatz verständlich an Betroffene zu vermitteln.

Mit der Frage, wie eine übersichtliche **Kurzdarstellung datenschutzrelevanter Kerninformationen** gelingen könnte, haben sich die Teams der Uni Göttingen und des ULD bereits im europäisch geförderten Projekt „Privacy&Us" befasst (37. TB, Tz. 8.6.3). Dabei wurde immer wieder offensichtlich, dass es schlicht an den Informationen über die IoT-Geräte, deren Eigenschaften, Einstellungsoptionen, die vorgesehenen Übermittlungen an Hersteller und Dienstleister und weitere Akteure fehlt. Die Projektziele von Unboxing.IoT.Privacy sind klare Beiträge zur **Informationsbeschaffung** sowie zur **anschließenden Einschätzung, Gewichtung und Aufbereitung unter dem Gesichtspunkt des Datenschutzes**. Technikpartner aus Wissenschaft und Wirtschaft erforschen Analysemöglichkeiten, etwa zur automatisierten Auswertung und Analyse der Geräte selbst, verfügbarer Software und vorhandener Datenschutzerklärungen.

Aufgabe des ULD-Teams im Projekt ist, eine **zielgruppengerechte Berücksichtigung der Datenschutzperspektive** bei Bewertung, Gewichtung und Darstellung der erlangten Informationen zu erarbeiten. Ob Verbraucherinnen und Verbraucher, Unternehmen oder Behörde, eine Kaufentscheidung für vernetzte Geräte sollte sorgfältig und informiert erfolgen können.

Verbraucherinnen und Verbraucher profitieren dabei unmittelbar von **verständlicher Transparenz**. Beim Einsatz von IoT-Geräten fallen oft personenbezogene Daten auch von Dritten an, etwa weiteren Haushaltsangehörigen, Gästen, Passanten oder Straßenverkehrsteilnehmern. Diejenigen, die solche vernetzten Geräte jenseits des eng gesteckten Rahmens persönlicher oder familiärer Tätigkeiten einsetzen, treffen die **datenschutzrechtlichen Pflichten von Verantwortlichen**: insbesondere das Vorhandensein einer Rechtsgrundlage, die Bereitstellung von Information an betroffene Personen, Gewährleistung technischer Sicherheit und fristgemäße Löschung von Daten. Darüber hinaus profitieren natürlich auch Behörden oder Wirtschaftsunternehmen als Verantwortliche von klaren Informationen für ihre Kaufentscheidungen, etwaige Datenschutz-Folgenabschätzungen und generelle Dokumentations- und Compliance-Pflichten.

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

Kurzlink: *https://uldsh.de/tb42-8-3a*

Was ist zu tun?

Mit dem Internet verbundene Produkte sind besonders sorgfältig auszuwählen, um das angemessene Schutzniveau für die betroffenen Personen gewährleisten zu können. Der Verantwortliche muss seinen Informationspflichten gegen über den betroffenen Personen nachkommen.

8.4 Projekt TRAPEZE – Transparenz- und Einwilligungsmanagement für das semantische Netz

Das Projekt **„TRAnsparency, Privacy and security for European citiZEns" (TRAPEZE)** wurde von der EU-Kommission gefördert und widmete sich der Entwicklung von Lösungen für Datenschutz und Transparenz in der „Data Economy" (41. TB, Tz. 8.4). Im Sommer 2023 lief das Projekt aus. Die letzten Projektmonate waren u. a. der öffentlichen Vorstellung und Erörterung der Projektergebnisse gewidmet.

Zu den Zielen von TRAPEZE gehörten **verbesserte Transparenz und einfachere Mitwirkungsmöglichkeiten** für betroffene Personen. Zentrale Zielgruppen zur Vorstellung und Erörterung der Ergebnisse waren damit Datenschutzaufsichtsbehörden, aber auch Behörden mit Fokus auf IT-Sicherheit und die Anwender aus dem betrieblichen und behördlichen Datenschutz. Unter dem Dach einer Konferenz mehrerer europäischer Forschungsprojekte zu Datenschutz und Cybersicherheit in Sophia Antipolis, Frankreich, richtete das ULD im April 2023 einen Workshop aus. Der Teilnehmerkreis vor Ort und online umfasste Vertreter diverser Datenschutzaufsichtsbehörden aus Europa und der Welt. Die ausgewählten Kernpunkte der Agenda waren:

- **Sticky Policies**, d. h. computerlesbare Datenschutzerklärungen, die zusammen mit den betroffenen Daten weitergegeben werden können und im Projekt weiterentwickelt wurden,
- ein **Privacy Dashboard**, das die genannten Policies übersichtlich darstellen kann und Nutzenden eine überschaubare und einfache Oberfläche zum Erteilen, Widerrufen und Management von Einwilligungen bietet,
- ein Brückenschlag zwischen aktuellen legislativen Entwicklungen und dadurch aufgeworfenen Herausforderungen zu möglichen Lösungen aus der **Forschung und Entwicklung zu Datenschutz durch Technikgestaltung**.

Die grundsätzliche Idee der Sticky Policies ist nicht neu und wurde schon in den 2000ern erörtert (30. TB, Tz. 8.2). Die weiterentwickelte Sprache zur computerlesbaren Wiedergabe von Berechtigungen und Einschränkungen für die Datenverarbeitung spiegelt die **Rechtsgrundlagen und Verarbeitungsbedingungen aus der DSGVO** wider. Sie wird von einer Arbeitsgruppe unter dem Dach des W3C kontinuierlich erweitert und weiterentwickelt. Das Projekt TRAPEZE trug zum Konzept der Policies neben konzeptionellen Verbesserungen vor allem mit technischen Entwicklungen zum praktischen Einsatz im Unternehmensumfeld bei.

Das **Privacy Dashboard** wurde gegenüber der Fassung aus dem Vorjahr (41. TB, Tz. 8.4) finalisiert. Im Vergleich zu langen textbasierten Einwilligungstexten oder Datenschutzerklärungen hebt sich eine Darstellung über das Dashboard durch Übersichtlichkeit ab. Einträge lassen sich etwa nach Zwecken, Datenarten oder möglichen Empfängern bzw. Empfängerkategorien sortieren. Betroffenenrechte werden insbesondere im Bereich der Transparenz unterstützt, und das nutzerseitige Management von Einwilligungen und deren Reichweite bedient Aspekte der Intervenierbarkeit. Daneben ist eine direkte Kontaktaufnahme zum Verantwortlichen bzw. der dortigen Datenschutzabteilung vorgesehen.

Die den Workshop abschließende Erörterung der Bezüge zu aktuellen Entwicklungen nahm u. a. die Forschung mit Gesundheitsdaten in den Blick. Mit dem **Europäischen Raum für Gesundheitsdaten** (European Health Data Space, EHDS) ergeben sich auf der einen Seite erhebliche Potenziale für die Medizinforschung. Auf der anderen Seite fehlen für die gewünschte breite Zweitnutzung von Gesundheitsdaten zu Forschungszwecken angemessene Transparenzlösungen. Sticky Policies oder Dashboards könnten hier **bei der technischen und organisatorischen Gestaltung des Datenraums** wichtige Beiträge leisten. Auch im Vergleich zu den derzeit üblichen sehr weiten Einwilligungsregelungen (broad consent) wären übersichtlichere und für die Betroffenen granular regelbare Einwilligungen ein Vorteil.

Für **Sticky Policies** sahen die an der Diskussion Teilnehmenden auch jenseits des Managements personenbezogener Daten Anwendungsfelder. So könne das Konzept prinzipiell auch zur

Beschreibung von Berechtigungen und Beschränkungen nicht nur für den Datenschutz, sondern auch für Geschäftsgeheimnisse oder gewerbliche Schutzrechte dienen und könnten damit als Maßnahmen für „Informationsfreiheit by Design" (Tz. 12.5) zum Einsatz kommen. Denkbare Anwendungsfelder fänden sich dafür auch im Rahmen der weiteren geplanten **europäischen Datenräume**.

Das TRAPEZE-Projekt konnte einige datenschutzfördernde Konzepte weiterentwickeln und prototypisch zeigen, wie sie im Unternehmensumfeld verwendbar wären. Es ist zu wünschen, dass einige dieser und verwandter Innovationen Eingang in Produkte oder Verfahren in der Wirtschaft fänden. Weiterführende Forschungsfragen für die Zukunft betreffen eine Gestaltung und Bereitstellung datenschutzfördernder Technik in einer Art und Weise, dass heute manches Mal noch bestehende Einstiegshürden vermieden oder zumindest gesenkt werden. Wünschenswert wäre insoweit, dass sowohl Internetnutzende als auch kleinere Unternehmen diese verwenden können. Konkretes Potenzial mit Mehrwert für Betroffene als auch Verantwortliche bestünde etwa für eine einfache Umsetzung von Widerrufen einer Einwilligung und Widersprüchen.

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

Kurzlink: *https://uldsh.de/tb42-8-4a*

8.5 Projekt AnoMed – Kompetenzcluster Anonymisierung für medizinische Anwendungen

Der im November 2022 gestartete und vom Bundesministerium für Bildung und Forschung sowie der Europäischen Union (NextGenerationEU) geförderte **Kompetenzcluster „Anonymisierung für medizinische Anwendungen" (AnoMed)** (41. TB, Tz. 8.5) bündelt Anonymisierungsforschung für den Gesundheitsbereich. Die Gesundheitsforschung ist politisch bedeutend: Mit dem Europäischen Raum für Gesundheitsdaten (European Health Data Space, EHDS) soll die Blaupause für weitere Datenräume geschaffen werden. Es ist vorgesehen, vorhandene Daten nach Themenbereichen zusammenzuführen und für Zwecke wie Forschung, Entwicklung oder Verwaltung zu nutzen. Es wird daher notwendig, dass alle Beteiligten sich klar über Schutzmaßnahmen für betroffene Personen austauschen. Dazu gehören auch Anonymisierung und Pseudonymisierung der Daten.

Ein Ergebnis der Tätigkeiten im Projekt ist der Vorschlag einer **Terminologie über Personenbezug und Anonymisierung**. Ziel ist ein Brückenschlag für Anonymisierungsforschung und Entscheidungsträgern in Politik, Forschung und Verwaltung. Notwendig wird eine kritische Aufbereitung der verwendeten Begrifflichkeiten insbesondere aufgrund der Risiken, die sich aus aktuellen und absehbaren Entwicklungen ergeben:

- Die **Verfügbarkeit zusätzlicher Informationen** muss stärker in den Fokus genommen werden. Eine Verknüpfung mit anderen verfügbaren Daten kann ermöglichen, dass Rückschlüsse auf Einzelpersonen in als „sicher" gewähnten Datensätzen ermöglicht werden. Die leichte Verfügbarkeit großer und detaillierter Datenbestände resultiert u. a. aus neuen Techniken zur lückenlosen Datenerhebung, etwa Fitnesstrackern und Smartwatches.
- Der politische Wille zielt darauf ab, vorhandene Datenbestände künftig **europaweit systematisch in anonymisierter Form** für Zwecke der Forschung und Innovation z. B. im öffentlichen Gesundheitswesen und in der Verwaltung im Rahmen von sogenannten Datenräumen zur Verfügung zu stellen und großflächig auszuwerten.
- **Künstliche Intelligenz** und andere Entwicklungen machen die Analyse großer Datenmengen einschließlich Verkettung von Informationen einfacher. Das Risiko besteht nicht nur bei der Verwendung von

Identifikatoren wie dem Namen oder einer Personennummer, sondern Verkettbarkeit und Profilbildung können auch auf Basis von Kombinationen verschiedener Einzelwerte erfolgen.

- Die **Anonymitätsforschung** entdeckt vermehrt neue Angriffe auf als anonym geglaubte Daten, entwickelt aber ebenso Ansätze, die mathematisch belegbare Garantien gegen eine Re-Identifizierung aufweisen.

Die im AnoMed-Projekt vorgenommene Betrachtung greift die grundlegenden Darstellungen zur **Identifizierbarkeit** aus dem PANELFIT-Projekt auf (40. TB, Tz. 8.3). Die vorgeschlagene Terminologie beschränkt sich dabei bewusst auf die faktischen und technischen Aspekte von Maßnahmen zur Verringerung des Personenbezugs und die Beschreibung des Restrisikos für betroffene Personen. Zugleich wird eine klarere und differenzierte Begrifflichkeit vorgeschlagen. Damit wird ein Austausch über Einzelfälle und über Maßnahmen, die für bestimmte Szenarien funktionieren können, erleichtert. Die rechtliche Entscheidung, ob ein Personenbezug verbleibt, bleibt indes bewusst der Anwendungspraxis der Aufsichtsbehörden überlassen. Für die nächste Zeit sind die überarbeiteten Leitlinien zur Anonymisierung des Europäischen Datenschutzausschusses und Ausführungen des Europäischen Gerichtshofs in der Rechtsmittelsache EDPS v SRB zu erwarten.

Die vorgeschlagene Terminologie kategorisiert diverse Techniken zur Pseudonymisierung oder Anonymisierung von Daten oder – allgemeiner ausgedrückt – zur **„Reduktion der Identifizierbarkeit“**. Dabei können drei grundlegende Typen unterschieden werden:

- Pseudonymisierung,
- eine Reduktion der Identifizierbarkeit auf Ebene von Einzeldatensätzen oder
- Aggregation.

Die Grafik veranschaulicht, wie weitreichend die Methoden die Identifizierbarkeit erschweren und auf welche Datenkategorien die jeweiligen Techniken einwirken.

Bei einer **Pseudonymisierung** werden direkt identifizierende Informationen wie Namen oder Patientennummern entfernt und gegebenenfalls mit einem Pseudonym ergänzt, sodass eine Zusammenführung mit den abgesonderten Identitätsdaten möglich bleibt. Sollen die Daten weiterhin jeweils zu einer Person gehören, können **typische quasi-identifizierende Informationen entfernt** werden. Diese können zwar nicht direkt, aber eben doch in ihrer Zusammenschau den Rückschluss auf eine Person ermöglichen. Ist zudem gewährleistet, dass jedes Individuum mindestens Teil einer Gruppe mit definierter Mindestgröße ist, kann die Re-Identifikation erheblich erschwert sein.

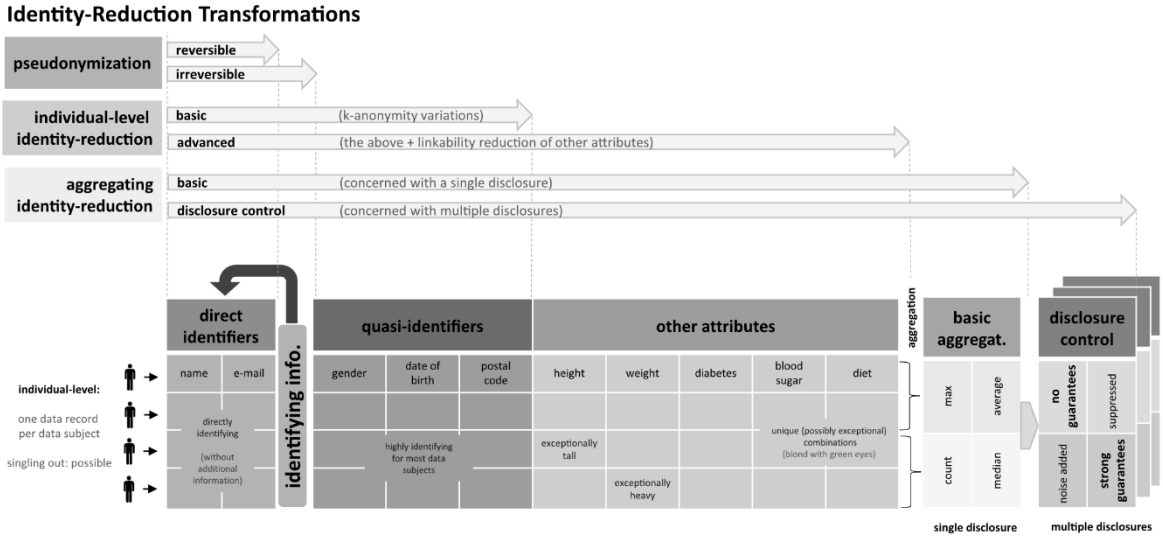


Abbildung: Techniken zur Verringerung der Identifizierbarkeit

Die **Identifizierbarkeit** wird schließlich **weiter eingeschränkt**, wenn die Daten nicht mehr pro Individuum vorgehalten werden. Nach einer Aggregation der Daten z. B. mittels statistischer Methoden ist als zusätzliche Hürde ein Aussortieren der zu einer Person gehörenden Informationen (singling out) erforderlich. Für Zwecke der Weitergabe oder Veröffentlichung könnten aggregierte Daten zudem mittels Rauschen verfremdet werden oder synthetische Daten erstellt werden.

Ergänzend ist eine **kontinuierliche vorausschauende Beobachtung** der Entwicklungen sinnvoll. Insbesondere verfügbare Informationen zur selben Personengruppe können trotz Aggregation Rückschlüsse ermöglichen. Die Daten können dabei aus derselben Datenquelle (z. B. im Rahmen von Ergebnisveröffentlichungen mehrerer Studien auf Grundlage von Daten aus dem EHDS) oder aus weiteren Quellen stammen.

Letztlich haben in der Praxis Verantwortliche zu entscheiden, ob Daten personenbezogen oder anonym sind. Sie sollten insbesondere vor der Veröffentlichung oder Weitergabe von sensiblen Informationen berücksichtigen, ob erhebliche Nachteile für betroffene Personen drohen.

Schwierigkeiten für alle Beteiligten bereitet eine **Fehleinschätzung der Anonymität von Daten**: Wenn diese dann unkontrolliert veröffentlicht werden und auch sonst – weil der Verantwortliche meint, dass die DSGVO für seine Verarbeitung der nur vermeintlich anonymen Daten nicht gilt – keine Schutzmaßnahmen bestehen, kann der Schaden für die betroffenen Personen groß sein. Dies kann aufsichtsbehördliche Verfahren und Schadensersatzforderungen gegen den Verantwortlichen nach sich ziehen.

Die Terminologie nebst Diagrammen ist in der jeweils aktuellen Fassung auf der Projektseite verfügbar. Arbeitssprache für den weiteren Austausch über Entwurfsfassungen ist Englisch, um der europäischen Dimension und dem interdisziplinären Bezug gerecht zu werden.

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

Kurzlink: *https://uldsh.de/tb42-8-5a*

09

KERNPUNKTE

AK Zertifizierung

Ergänzende Kooperationsvereinbarung

Erste Akkreditierungsverfahren

9 Zertifizierung und Akkreditierung

Nachdem mit der DSGVO im Jahr 2018 die rechtliche Möglichkeit geschaffen wurde, dass akkreditierte Zertifizierungsstellen Verarbeitungsvorgänge von Verantwortlichen und Auftragsverarbeitern zertifizieren können, war es ruhig darum geworden. Begleitende Regelungen fehlten insbesondere auf europäischer Ebene zunächst. Dies ist nunmehr nicht mehr der Fall, sodass – endlich (!) – zu erwarten ist, dass 2024 auch in Deutschland die ersten Zertifikate vergeben werden können. Den Datenschutzaufsichtsbehörden fällt dabei die Aufgabe zu, Kriterienkataloge zu genehmigen, im Rahmen der Akkreditierung gutachterlich tätig zu werden und akkreditierten Zertifizierungsstellen die Befugnis zur Zertifizierung zu erteilen.

9.1 Leitung des AK Zertifizierung

Im Rahmen der Leitung des Arbeitskreises Zertifizierung der Datenschutzkonferenz (AK Zertifizierung) war die **Begleitung der ersten Verfahren zur Anerkennung von Kriterienkatalogen** und Akkreditierungen in mehreren Bundesländern zentraler Punkt im Berichtsjahr. Monatliche virtuelle Treffen der Mitglieder des AK Zertifizierung ermöglichten einen regelmäßigen Austausch. Hierbei waren aber auch europäische Themen öfter Gesprächsthema. Es war zu mehreren Themen erforderlich, eine deutsche Meinung zu strittigen Themen abzustimmen.

So wies u. a. die Deutsche Akkreditierungsstelle (DAkkS), die Mitglied des AK Zertifizierung ist, auf Unklarheiten hinsichtlich der **Reichweite von Zuständigkeiten bei Akkreditierungen** hin. Hierzu gab es einen regen Austausch, allerdings wies der AK Zertifizierung auch darauf hin, dass es sich hierbei um ein Thema handelt, das die Akkreditierungsstellen selbst betrifft. Zumindest in Deutschland erfolgt die Akkreditierung durch die DAkkS und nicht durch die Datenschutzaufsichtsbehörden, sodass wir darauf verwiesen, dass die europäischen Akkreditierungsstellen zunächst selbst in der Pflicht sind, Unklarheiten zu klären.

Ein weiteres Thema im AK Zertifizierung betraf die Reichweite von Zertifizierungen bei **grenzüberschreitender Datenverarbeitung**. Unklar war mit Blick auf das in Art. 42 Abs. 5 Satz 2 DSGVO vorgesehene Europäische Datenschutzsiegel, inwieweit es ein Problem darstellt, wenn eine Zertifizierungsstelle aus einem Mitgliedstaat Zertifikate für Datenverarbeitungsvorgänge in einem anderen Mitgliedstaat vornimmt und die dortige Aufsichtsbehörde hieran Kritik übt. Diese Frage haben wir an die zuständige Expert Subgroup (siehe Tz. 11.2) auf europäischer Ebene weitergegeben.

Auch konnte im Berichtszeitraum in gemeinsamer Abstimmung des AK Zertifizierung das **Kurzpapier zu Akkreditierung und Zertifizierung aktualisiert** und nach Genehmigung der Datenschutzkonferenz veröffentlicht werden.

Das Papier ist unter dem folgenden Link abrufbar:

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_9.pdf

Kurzlink: *https://uldsh.de/tb42-9-1a*

Unter der Leitung von Nordrhein-Westfalen besteht ein Unterarbeitskreis zum Thema Prüfkriterien (vgl. u. a. 41. TB, Tz. 9.2), der aber auch zum Austausch von Bund und Ländern genutzt wird, die aktuell mit Prüfungen von Kriterienkatalogen und Zertifizierungsstellen beschäftigt sind. Im Frühjahr 2021 hatte die DSK das Papier **„Anforderungen an datenschutzrechtliche Zertifizierungsprogramme – Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6)“** angenommen. Dieses Papier wurde auch im zurückliegenden Berichts-

zeitraum in dem Unterarbeitskreis unter unserer Mitwirkung weiterentwickelt. Die bisherige Struktur des Dokuments und insbesondere des Kapitels 2, das sich mit den gesetzlichen Tatbestandsmerkmalen, den zu behandelnden Prüfthemen und deren Umsetzung durch den Antragsteller sowie mit der Art und Weise der Prüfung befasst, wurde beibehalten und um Inhalte zu verschiedenen Themenkomplexen ergänzt.

Augenblicklich wird das Papier um umfangreiche Ausführungen zu den Anforderungen des Artikels 25 DSGVO zu „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" ergänzt. Bei der Überarbeitung bereits bestehender Inhalte wurde auf konkrete Erfahrungen mit der Anwendung des Papiers selbst sowie weiter spezifizierter Vorgaben auf europäischer Ebene geachtet. Nach dem Abschluss der Überarbeitung ist geplant, das Papier in einer neuen Version vorzulegen und damit weiterhin eine praxistaugliche Basis für die einheitliche Bewertung von Zertifizierungsprogrammen anzubieten. Das Papier soll dabei wie gewohnt als **Orientierungshilfe für zukünftige Zertifizierungsstellen, bei der Erstellung von Zertifizierungsprogrammen und insbesondere von Zertifizierungskriterien** dienen.

Das Papier ist unter dem folgenden Link abrufbar:

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

Kurzlink: *https://uldsh.de/tb42-9-1b*

Was ist zu tun?

Wir werden die Arbeit im AK Zertifizierung in der Rolle der Leitung fortsetzen und aktuelle Themen zu Akkreditierungen und Zertifizierungen auf deutscher und europäischer Ebene begleiten. Geplant ist für 2024 ein Präsenztreffen, das auch für eine Fortbildung durch die DAkkS im Bereich Begutachtung von Zertifizierungsstellen genutzt werden soll.

9.2 Ergänzende Kooperationsvereinbarung der Aufsichtsbehörden

Im Jahr 2020 wurde eine Kooperationsvereinbarung zwischen allen Datenschutzaufsichtsbehörden und der DAkkS zur Zusammenarbeit bei Genehmigungen von Zertifizierungskriterien und der Akkreditierung von Zertifizierungsstellen geschlossen (39. TB, Tz. 9.2). Mit Aufkommen der ersten konkreten Verfahren zeigte sich, dass auf deutscher Ebene noch Unklarheiten bestanden, wie im **Vorfeld zur Genehmigung von Kriterienkatalogen die übrigen Aufsichtsbehörden eingebunden** werden und welche Voraussetzungen hierfür gelten. Als **Addendum** zur ursprünglichen Kooperationsvereinbarung wurde im Berichtszeitraum daher zwischen den deutschen Aufsichtsbehörden eine weitere **Kooperationsvereinbarung** getroffen.

Ziel ist es, in Abstimmung mit dem Antragsteller die nicht direkt beteiligten Aufsichtsbehörden in Deutschland frühzeitig zu informieren und in einem angemessenen Umfang einzubinden. Dadurch soll verhindert werden, dass erst in einem fortgeschrittenen Stadium des Genehmigungsverfahrens von Zertifizierungskriterien Diskussionspunkte aufkommen, die dann gegebenenfalls sogar erst auf der nachgeschalteten europäischen Ebene besprochen werden müssen. Die hierdurch entstehende Verzögerung des Gesamtverfahrens soll vermieden werden, um **Antragstellern eine bessere Planungsmöglichkeit für das Verfahren** zu ermöglichen. Auch dient diese ergänzende Kooperationsvereinbarung dazu, einen einheitlichen Bewertungsmaßstab in Deutschland zu gewährleisten.

Was ist zu tun?

Die Kooperationsvereinbarungen müssen sich nun in der Praxis bewähren. Sollten sich dabei neue Fragen ergeben, sind gegebenenfalls weitere Anpassungen erforderlich.

9.3 Erste Genehmigungen und Akkreditierungsverfahren in Deutschland und der EU

Im Berichtszeitraum war sowohl auf deutscher als auch auf europäischer Ebene eine deutliche **Zunahme von Anträgen auf Genehmigung von Zertifizierungskriterien und Akkreditierung von Zertifizierungsstellen** zu verzeichnen. Hierbei verstärkte sich der bisher zu beobachtende Trend einer Häufung entsprechender Anträge in einzelnen Mitgliedstaaten (Deutschland, Luxemburg, Niederlande) bzw. Bundesländern (Berlin, Bremen, Nordrhein-Westfalen).

Die von den zukünftigen Zertifizierungsstellen oder Programmeignern entwickelten **Zertifizierungsprogramme** einschließlich der Zertifizierungskriterien werden dabei in einem mehrstufigen Verfahren durch die Deutsche Akkreditierungsstelle (DAkkS) in enger Zusammenarbeit mit der zuständigen Aufsichtsbehörde auf ihre **Anwendbarkeit und Eignung** geprüft. Die Zertifizierungskriterien selbst beschreiben hierbei die Umsetzung der datenschutzrechtlichen Anforderungen. Diese Zertifizierungskriterien werden im Verlauf dieses Verfahrens durch die jeweils zuständige Aufsichtsbehörde fachlich geprüft und – vorbehaltlich der **Stellungnahme durch den Europäischen Datenschutzausschuss** (EDSA) – genehmigt. Es folgt dann das Akkreditierungsverfahren unter der Leitung der DAkkS, wobei die zuständige Datenschutzaufsichtsbehörde als Gutachterin beteiligt ist und anschließend zusammen mit der DAkkS über die Akkreditierung entscheidet.

Im Berichtszeitraum konnten weitere Anträge auf Genehmigung nationaler und europäischer Zertifizierungskriterien erfolgreich abgeschlossen werden. Es gibt somit zum aktuellen Zeitpunkt **mehrere durch die zuständigen Datenschutzaufsichtsbehörden und den EDSA genehmigte Kataloge mit Zertifizierungskriterien**. Wie auch in der Vergangenheit waren im Zuge dieser Verfahren sowohl im europäischen als auch im nationalen Kontext etliche Detailfragen zu klären, die einer engen Abstimmung aller Beteiligten bedurften.

Aktuell durchlaufen mehrere Zertifizierungsstellen in Deutschland ein Akkreditierungsverfahren. Es ist 2024 mit Abschlüssen zu rechnen, sodass es bis zu den ersten **Zertifizierungen** in Deutschland **nicht mehr lange dauern** kann.

Was ist zu tun?

Die bestehenden Papiere zur Akkreditierung sind entsprechend den jeweiligen Entwicklungen zu ergänzen, um sie bei der Bewertung und Genehmigung von Zertifizierungskriterien durch die Datenschutzaufsichtsbehörden als Basis der Bewertung zu nutzen. Auf diese Weise lässt sich eine einheitliche Bewertung sicherstellen. Außerdem kann die Qualität der eingereichten Programme gesteigert werden. Ziel ist es, das Instrument der Zertifizierung langfristig auf einem fachlich hohen Niveau zu verankern.

10

KERNPUNKTE

Gestaltung von Online-Formularen

Übergriffige KI

Regelmäßiger Passwortwechsel sinnvoll?

10 Aus dem IT-Labor

Im IT-Labor beschäftigt sich unser Team mit technischen Entwicklungen, damit wir uns mit Chancen und Risiken sowie mit den Möglichkeiten zur Risikobeherrschung vertraut machen können. Manches wird als Empfehlung an die Verantwortlichen oder Auftragsverarbeiter weitergegeben, manche Ergebnisse verwenden wir in den Kursen der DATENSCHUTZAKADEMIE (siehe Kapitel 13) oder in der Beratung.

10.1 Best-Practice-Gestaltung von Online-Formularen

Organisationen stellen Online-Formulare auf ihren Websites zur Verfügung, um den Nutzenden die Möglichkeit zu geben, Informationen für die jeweiligen Zwecke bereitzustellen. Dabei kommt es auf die datenschutzgerechte Gestaltung an. So haben sich einige Methoden für die Entwicklung datenschutzkonformer Online-Formulare bewährt:

Die Grundlage jeder datenschutzkonformen Formulargestaltung ist das **Prinzip der Datenminimierung**: Es dürfen nur diejenigen personenbezogenen Daten erfasst werden, die für den spezifischen Zweck benötigt werden. Dies verringert Datenschutzrisiken. Außerdem müssen die Nutzenden keine unnötigen Eingaben vornehmen. Dazu gehört auch, die Anzahl der Pflichtfelder eines Formulars auf das absolute Minimum zu reduzieren.

Informationen über die Datenschutzbestimmungen und besonders über die Verarbeitung und Speicherdauer der einzugebenden Daten sollten klar und verständlich dargelegt werden.

Freitextfelder sollten, soweit es möglich ist, **vermieden** werden: Zum einen erschweren sie die spätere Verarbeitung und Analyse der Daten, und zum anderen können hier – oft unbeabsichtigt – sensible Informationen über die eigene Person oder sogar über Dritte angegeben werden, die dem Verantwortlichen die weitere datenschutzkonforme Verarbeitung erschweren.

Um die **syntaktische Korrektheit von Eingaben** zu kontrollieren (z. B. Telefonnummern oder E-Mail-Adressen), lassen sich die integrierten Validierungsmöglichkeiten von HTML5 nutzen. Insbesondere das „pattern"-Attribut und spezifische Eingabetypen wie „email" und „tel" sorgen dafür, dass bereits bei der Eingabe im Browser viele Tippfehler erkannt werden.

Als Schutz vor Spam-Einträgen in Formularen – insbesondere in massenhafter, automatisierter Form durch Bots – haben sich Verfahren etabliert, die bei der Eingabe prüfen sollen, ob sie durch Menschen erfolgt ist. Sogenannte **CAPTCHAs** (Completely Automated Public Turing test to tell Computers and Humans Apart) lassen z. B. Menschen Rechenaufgaben lösen, Buchstaben in verzerrten Bildern erkennen oder Objekte in Fotos erkennen. Abgesehen davon, dass mithilfe von KI-Systemen viele dieser Tests wiederum von Bots umgangen werden können, ist für die Nutzung von CAPTCHAs oft die Einbindung eines Drittanbieterdienstes notwendig – verbunden mit allen notwendigen datenschutzrechtlichen **Prüf- und Informationspflichten** des Verantwortlichen.

CSS (Cascading Stylesheets)

CSS ist eine gestaltende Sprache, die mit HTML zusammenarbeitet, um das Erscheinungsbild einer Webseite zu definieren. CSS ermöglicht die Festlegung von Stilen wie Farben, Schriftarten und Abständen für HTML-Elemente, wodurch die Trennung von Inhalt und Design erleichtert wird.

Eine alternative Methode zur Unterscheidung zwischen menschlichen Nutzenden und automatisierten Bots besteht darin, ein verstecktes Formularfeld in die Webseite einzufügen. Dazu wird ein einzelnes Feld mithilfe von CSS ausgeblendet. Bots, die den Quellcode der Seite nach

Eingabefeldern absuchen, ohne die jeweiligen Darstellungsstile zu verarbeiten, können dieses ausgeblendete Feld nicht von anderen unterscheiden. Sie füllen es dementsprechend aus – insbesondere wenn man es mit aus Sicht des Bots interessanten Namen wie „email" versieht. Menschen bleibt das Feld hingegen verborgen. Zur Sicherheit kann im unsichtbaren Feld auch ein für Menschen verständlicher Hinweis nach dem Muster „Dieses Feld muss leer bleiben" angebracht werden für den Fall, dass das Feld fälschlicherweise doch dargestellt werden sollte.

Nach dem Absenden des Formulars kann der Webserver dann überprüfen, ob das „email"-Feld leer ist oder einen Eintrag enthält: Sind in dem versteckten Feld Daten eingetragen worden, ist dies ein starker **Indikator für eine automatisierte Bot-Eingabe**.

Was ist zu tun?

Die erfolgreiche Gestaltung datenschutzkonformer Online-Formulare erfordert ein ausgewogenes Verständnis der rechtlichen und betrieblichen Anforderungen sowie der Interessen der Nutzenden. Die Umsetzung dieser Best Practices trägt dazu bei, Datenschutzbestimmungen einzuhalten und die Interaktion mit Online-Formularen zu optimieren.

10.2 Übergriffige KI – Versuche mit KI-Komponenten in Messengern

Es liegt nahe, generative KIs dort einzusetzen, wo Texte erstellt werden. So tauchen inzwischen Assistenten nicht nur in Textverarbeitungen, sondern auch in Blogsystemen und Messengern auf. In einigen dieser Chatsysteme gibt es seit Kurzem neben reinen Assistenzfunktionen auch **KI-Bots**, deren Sinn und Zwecke sich zunächst nicht ohne Weiteres erschließt. Solche Bots reihen sich nahtlos in die Liste der menschlichen Konversationen ein, mitunter steht der Bot herstellerseitig auch stets auf Position eins der Unterhaltungsliste. Nutzende können mit ihm **interagieren wie mit einem menschlichen Gesprächspartner**, die Maschine antwortet und gibt sich teilweise erstaunlich interessiert am Tagesablauf ihres menschlichen Gegenübers.

Ein Blick in die Datenschutzerklärung solcher Dienste verrät dann mitunter, welche Intention wirklich hinter dem Angebot eines solchen Chatbots steckt. Da ist plötzlich die Rede von **„Personalisierung der Dienste" und des „Werbeerlebnisses"**. Da solche **Chatprogramme insbesondere von Jugendlichen häufig genutzt** werden, eröffnen sich hier weitere Problemfelder. Sind KI-Systeme ohnehin schon in der Kritik, weil völlig unklar ist, wie Daten im Inneren des Systems verarbeitet und gespeichert werden, kommt bei den hier besprochenen oberflächlich harmlosen Chatbots hinzu, dass sie offenkundig eine Intention verfolgen. Das Ziel, Daten über die Nutzenden zu sammeln und Profile zu bilden und zu optimieren, wird dabei nicht für die Zielgruppe klar und verständlich kommuniziert, sondern wieder einmal tief in umfangreichen rechtlichen Erläuterungen – quasi im „Kleingedruckten" – verborgen. Problematisch ist das vor allem dadurch, dass die Chatbots selbst sich naiv „menschlich" geben und jeden Argwohn über ihre Intention eloquent von sich weisen.

Die Unterschiede in der Selbstdarstellung der Systeme sind gewaltig. Pochen die bisherigen generativen KIs fast schon penetrant darauf, „nur" ein Large Language Model (LLM) und eben kein Mensch zu sein, tun die hier angesprochenen Chatbots ausdrücklich so, als wären sie Individuen. In unseren Tests machte der **Chatbot** des Öfteren klar, dass er **„ein Freund" sei, der „immer für dich da" ist**. Er habe uns „vermisst", ließ er dann wissen. Gerade dieses Buhlen um Vertrauen ist es, das bei einigen Jugendlichen die Assoziation „creepy" hervorruft, bei anderen jedoch auch auf fruchtbaren Boden fallen

könnte. Kinder und Jugendliche in psychisch labilen Phasen oder mit einer weniger skeptischen Grundhaltung könnten solchen Chatbots Vertrauen schenken, das diese nicht verdienen.

Es sind Systeme, die sich ebendieses Vertrauen von Nutzenden erschleichen, um auf diese Weise **an Daten zur Profilbildung zu gelangen**. Tatsächlich stellte sich ein solcher Bot in unseren Tests als bemerkenswert neugierig heraus und erbat neben Angaben zum Tagesablauf auch gern die Zusendung passender Fotos, die er dann kommentierte. Es handelt sich bei dieser Art von Chatsystemen also vornehmlich um den Versuch, Daten über Nutzende zu sammeln. Unter ethischen Aspekten besonders fragwürdig ist dieses Vorgehen, weil gerade bei Kindern und Jugendlichen die Bereitschaft, einem solchen System zu vertrauen, größer sein könnte. Auch die inhaltliche Neutralität war in Tests fragwürdig. So behauptete eines der Systeme, keine Direktiven oder Vorgaben des Herstellers, sehr wohl aber eine eigene Meinung zu diversen Themen zu haben – vermutlich ein Ergebnis der starken Vermenschlichung des Chatbots, dem auf diese Weise auch die Beeinflussung der Nutzenden möglich ist: Nicht nur kann ein solches System Informationen über Nutzende sammeln, es kann dem Gegenüber auch aktiv Informationen zukommen lassen und diese aufgrund seiner Kenntnisse über die Person optimal zuschneiden, um bestimmte Wirkungen zu erzielen. Hochmanipulativ, wenn der Chatbot-Freund dann Klamotten oder Gadgets empfiehlt, die man braucht, um zu den coolen Kids zu gehören!

Was ist zu tun?

Eltern und Schulen sollten verstärkt darauf achten, wie Kinder und Jugendliche mit generativen KI-Systemen umgehen: Systeme, die sich Vertrauen von Kindern und Jugendlichen erschleichen, sind mindestens so problematisch wie maschinell erzeugte Hausaufgaben. Die Aufklärung über die Risiken dieser Technik muss ihren Fokus deshalb auch auf Datenschutz- und Desinformationsaspekte legen.

10.3 Regelmäßiger Passwortwechsel – unnützer Aufwand oder sinnvolle Sicherheitsmaßnahme?

Regelmäßig wird man durch IT-Systeme gemahnt, das Passwort zu wechseln – spätestens dann stellt man die Frage nach dem Warum. Früher lautete die Antwort häufig: „Ist eben eine Sicherheitsmaßnahme laut IT-Grundschutz."

Die strikte Vorgabe hatte natürlich Gründe: So werden zum einen Rateversuche und ein systematisches Durchprobieren erschwert, denn wenn sich Passwörter ständig ändern, ist der Zeitraum zum Durchprobieren begrenzt. Zum anderen sollen ausgespähte Passwörter, wissentlich weitergegebene Passwörter (etwa Notfallzugriffe oder die doch immer wieder vorkommende – verfahrens- und sicherheitsmäßig nicht gut gelöste – Urlaubsvertretung) oder einer Gruppe von Personen bekannte Passwörter (etwa nicht personalisierte Aktivierungscodes für Alarmanlagen) nach einiger Zeit an Wirksamkeit verlieren.

Jedoch ist ein erzwungener Passwortwechsel zumindest für Anwenderinnen und Anwender lästig und führt oft dazu, dass Passwörter unverschlüsselt notiert werden oder eine besonders einfache Systematik verwendet wird („Zugang_01" … „Zugang_12" je nach Monat), die leicht zu durchschauen und angreifbar ist.

Mittlerweile lauten die aktuellen Anforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) daher, **rein zeitgesteuerte Passwortwechsel sowie Passwortwechsel ohne validen Grund zu vermeiden**:

ORP.4.A23 Regelung für passwortverarbeitende Anwendungen und IT-Systeme (B) [IT-Betrieb]

IT-Systeme oder Anwendungen SOLLTEN NUR mit einem validen Grund zum Wechsel des Passworts auffordern. Reine zeitgesteuerte Wechsel SOLLTEN vermieden werden. Es MÜSSEN Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen. Ist dies nicht möglich, so SOLLTE geprüft werden, ob die Nachteile eines zeitgesteuerten Passwortwechsels in Kauf genommen werden können und Passwörter in gewissen Abständen gewechselt werden. […]

Die jeweils aktuelle Version des vollständigen Bausteins „ORP.4 Identitäts- und Berechtigungsmanagement“, der Regelungen zur Verwaltung von Nutzeridentitäten enthält, findet sich auf der Übersichtsseite des IT-Grundschutz-Kompendiums:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.

Kurzlink: *https://uldsh.de/tb42-10-3a*

Hat damit der regelmäßig erzwungene Passwortwechsel ein Ende? Leider nein, denn eine Voraussetzung dafür ist, dass eine weitere Anforderung umgesetzt ist: „Es müssen Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen.“

Damit ist gemeint, dass Log-ins und andere Nutzungen von Passwörtern überwacht werden müssen, um eine unbefugte Nutzung durch Dritte, etwa ausgespähte Passwörter, erkennen zu können. Wenn dies nicht möglich ist, ist die Rückkehr zu zeitgesteuerten Passwortwechseln zu prüfen.

Was bedeutet dies für die Praxis?

Zunächst muss ermittelt werden, wo genau das Passwort verwendet wird: Handelt es sich um ein persönliches Log-in-Passwort, bei dem nach einigen Fehlversuchen ein Konto gesperrt wird oder der nächste Versuch nur verzögert möglich ist, so ist ein solches Konto gut gegen Rateversuche geschützt – ähnlich wie die klassischen Bankkarten, die nach dreimaliger Fehleingabe einer PIN eingezogen werden. Ebenso können **Kompromittierungen** prinzipiell **erkannt** werden, etwa durch eine Protokollierung und Überwachung von Log-ins oder der Darstellung des letzten erfolgreichen Log-ins oder auch fehlgeschlagenen Log-in-Versuchs im Benutzerkonto. Wenn solche Überwachungen erfolgen, ist ein Verzicht auf rein zeitgesteuerte Passwortwechsel denkbar.

Handelt es sich hingegen beispielsweise um ein Leseschutzkennwort einer PDF- oder ZIP-Datei, sind im Prinzip unbegrenzte Rateversuche möglich. Hier helfen gegen systematische Rateversuche (Brute-force-Angriffe) nur lange und komplexe Passwörter. Werden Passwörter durch mehrere Personen verwendet (nicht personalisierte Zugangscodes etwa zu Alarmanlagen, Tresoren, Fax-Geräten, gemeinsam genutzten Kryptoschlüsseln (z. B. für Funktions-E-Mail-Konten), WLAN-Passwörter für Hotspots oder auch Leseschutzkennwörter bei einem regelmäßigen Austausch von Dateien mit Dritten), so ist **nach jedem Ausscheiden einer Person aus der jeweiligen Gruppe der Berechtigten ein Passwortwechsel notwendig**. In der Praxis unterbleibt dieser häufig. Hier ist ein Wechsel nach Zeitablauf, beispielsweise einmal im Jahr, in jedem Fall sinnvoll.

Ausblick:

Wie üblich ist auch die Passwortwelt nicht schwarz-weiß, sondern es gibt Abstufungen – vom ewigen, nie gewechselten Passwort bis hin zum One-Time-Passwort, dass per App erzeugt wird und nur 30 Sekunden lang gültig ist.

In der Tendenz werden insbesondere für Online-Anwendungen zunehmend **Zwei-Faktor-Authentifizierungen** verwendet. Dabei kommen zusätzlich zu regulären Passwörtern **Einmal-Codes** zum Einsatz, z. B. Codes, die mit Authentisierungs-Apps generiert werden oder per SMS oder einer App den Nutzerinnen und Nutzern übermittelt werden (36. TB, Tz.10.6). Ein Einmal-Code ist letztlich ein Passwort mit zeitlich minimaler Gültigkeit, und der Passwortwechsel ist durch eine App oder die Zusendung automatisiert.

Auf **Betriebssystemebene** gibt es ebenfalls Mechanismen, Passwörter für selten genutzte administrative Nutzerkonten automatisiert zu wechseln. Beispielsweise ändert „Windows LAPS" (Windows Local Administrator Password Solution) automatisiert Passwörter für lokale Administrationskonten, die nur in Ausnahme- oder Havariefällen benötigt werden, technisch aber sehr mächtig sind und daher gut geschützt werden müssen.

Auch bei kryptografischen Schlüsseln geht die Tendenz zu kürzeren Gültigkeitszeiträumen – so sind beispielsweise **Zertifikate für Webserver-Verschlüsselungen (SSL-Zertifikate)** des Anbieters Let's Encrypt standardmäßig drei Monate gültig und ein automatisierter Wechsel möglich.

Was ist zu tun?

Es ist zu prüfen, ob auf einen rein zeitgesteuerten Wechsel von Passwörtern für persönliche Nutzerkonten verzichtet werden kann.

11

KERNPUNKTE

Neues vom Europäischen Datenschutzausschuss

Akkreditierung und Zertifizierung

Ad-Hoc Working Group „Data Protection Engineering" der ENISA

11 Europa und Internationales

Die Arbeit in den deutschen Datenschutzaufsichtsbehörden hat ebenso wie in den Behörden der anderen Mitgliedstaaten der EU mittlerweile viel mit Europa zu tun. Mit der Datenschutz-Grundverordnung besteht ein Regelwerk, das im Prinzip in allen Mitgliedstaaten gleich ist und auch gleich interpretiert und angewendet werden soll. Einige der Aktivitäten mit Bezug zu Europa und darüber hinaus werden in diesem Kapitel dargestellt.

11.1 Neues vom Europäischen Datenschutzausschuss

Als am 25.05.2018 die Datenschutz-Grundverordnung Geltung erlangte, war noch nicht klar, ob die Mechanismen zur Zusammenarbeit in Europa funktionieren würden. Heute weiß man, dass es im Grundsatz ganz gut klappt. Insbesondere erfüllt der Europäische Datenschutzausschuss (EDSA) die wichtige Aufgabe sicherzustellen, dass die Datenschutz-Grundverordnung und die Datenschutzrichtlinie für Justiz und Inneres (JI-Richtlinie 2016/680) **einheitlich angewandt** werden und die Zusammenarbeit – auch bei der Durchsetzung des Datenschutzes durch die Aufsichtsbehörden – gewährleistet wird.

Der **Europäische Datenschutzausschuss (EDSA)** ist ein unabhängiges europäisches Gremium. Es ist die Dachorganisation, die die nationalen Datenschutzbehörden der Länder des Europäischen Wirtschaftsraums sowie den Europäischen Datenschutzbeauftragten (EDSB) zusammenbringt.

Die Ergebnisse des EDSA – teilweise mit unserer Zuarbeit – im Berichtsjahr sind vielfältig. Für die Anwender sind **Leitlinien** (Guidelines) zur Interpretation des Datenschutzrechts besonders wichtig, die häufig zuerst in einer ersten Version einer **öffentlichen Konsultation** unterzogen und dann zu einer Version 2.0 weiterentwickelt werden.

Die angenommenen Leitlinien und erarbeiteten Stellungnahmen aus dem Jahr 2023 werden im Folgenden aufgelistet:

- Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, Version 2.0, nach öffentlicher Konsultation angenommen am 14.02.2023

  https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

  Kurzlink: *https://uldsh.de/tb42-11-1a*

- Leitlinien 5/2021 über das Zusammenspiel zwischen der Anwendung des Artikels 3 und der Bestimmungen über internationale Übermittlungen nach Kapitel V DSGVO, Version 2.0, nach öffentlicher Konsultation angenommen am 14.02.2023

  https://www.edpb.europa.eu/system/files/2023-09/edpb_guidelines_05-2021_interplay_between_the_application_de.pdf

  Kurzlink: *https://uldsh.de/tb42-11-1b*

- Leitlinien 7/2022 über die Zertifizierung als Instrument für Übermittlungen, Version 2.0, nach öffentlicher Konsultation angenommen am 14.02.2023

  https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_de_0.pdf

  Kurzlink: *https://uldsh.de/tb42-11-1c*

- Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, nach öffentlicher Konsultation angenommen am 28.03.2023

  https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf

  Kurzlink: *https://uldsh.de/tb42-11-1d*

- Guidelines 01/2022 on data subject rights – Right of access, Version 2.0, nach öffentlicher Konsultation angenommen am 28.03.2023

  https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf

  Kurzlink: *https://uldsh.de/tb42-11-1e*

- Leitlinien 8/2022 für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters, Version 2.0, nach öffentlicher Konsultation angenommen am 28.03.2023

  https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202208_identifying_lsa_targeted_update_de.pdf

  Kurzlink: *https://uldsh.de/tb42-11-1f*

- Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 2.0, nach öffentlicher Konsultation angenommen am 26.04.2023

  https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

  Kurzlink: *https://uldsh.de/tb42-11-1g*

- Guidelines 03/2021 on the application of Article 65(1)(a) GDPR, Version 2.0, nach öffentlicher Konsultation angenommen am 24.05.2023

  https://www.edpb.europa.eu/system/files/2023-06/edpb_guidelines_202103_article65-1-a_v2_en.pdf

  Kurzlink: *https://uldsh.de/tb42-11-1h*

- Leitlinien 04/2022 für die Berechnung von Geldbußen im Sinne der DSGVO, Version 2.1, nach öffentlicher Konsultation angenommen am 24.05.2023

  https://www.edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_de_0.pdf

  Kurzlink: *https://uldsh.de/tb42-11-1i*

- Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Artikel 47 GDPR), Version 2.0, nach öffentlicher Konsultation angenommen am 20.06.2023

  https://www.edpb.europa.eu/system/files/2023-06/edpb_recommendations_20221_bcr-c_v2_en.pdf

  Kurzlink: *https://uldsh.de/tb42-11-1j*

- EDSA-EDSB Gemeinsame Stellungnahme 01/2023 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679, angenommen am 19.09.2023

  https://www.edpb.europa.eu/system/files/2023-12/edpb_edps_jointopinion_202301_proceduralrules_ec_execsummary_de.pdf

  Kurzlink: *https://uldsh.de/tb42-11-1k*

- EDPB-EDPS Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro, angenommen am 17.10.2023

  https://www.edpb.europa.eu/system/files/2023-10/edpb_edps_jointopinion_022023_digitaleuro_en.pdf

  Kurzlink: *https://uldsh.de/tb42-11-1l*

Viele der Dokumente sind besonders relevant für die Praxis, damit Anwender als **Verantwortliche oder Auftragsverarbeiter** Orientierung bei der Auslegung der DSGVO erhalten. Die Stellungnahmen richten sich an die **Gesetzgeber auf europäischer Ebene** – genau genommen betreffen sie aber den gesamten politischen und datenschutzrechtlichen Diskurs zu den jeweiligen Themen. So passte es gut, dass die Stellungnahme zum digitalen Euro bereits veröffentlicht war, als das Thema mit landesspezifischer Ausrichtung in Ausschüssen des Schleswig-Holsteinischen Landtages behandelt wurde.

11.2 Akkreditierung und Zertifizierung in der europäischen Expert Subgroup

Auch im Berichtszeitraum haben wir unsere Erfahrungen wieder in der **für Fragen der Akkreditierung und Zertifizierung zuständigen Compliance, e-Government und Health Expert Subgroup (CEH Expert Subgroup)** eingebracht. Die auf europäischer Ebene zuständige Gruppe hat sich dabei insbesondere mit Fragen der innereuropäischen Zusammenarbeit der Aufsichtsbehörden, des Drittstaatentransfers personenbezogener Daten gemäß Artikel 46 DSGVO im Kontext datenschutzrechtlicher Zertifizierungen sowie mit Grundsatzfragen zum Themenkomplex der Akkreditierung und Zertifizierung beschäftigt.

Da einige der in diesem Rahmen aufgeworfenen Fragen auch die Zusammenarbeit mit anderen Expert Subgroups und deren Expertise betrafen, war u. a. die Einbindung der International Transfer Subgroup (ITS) sowie der Key Provision Subgroup (KEYP) notwendig.

Diese Fragestellungen wurden im Berichtszeitraum nicht nur online und im schriftlichen Verfahren erörtert, sondern waren auch Gegenstand zweier Workshops zu Beginn und am Ende des Jahres 2023. Während beim ersten Workshop ausschließlich Mitglieder der CEH Expert Subgroup teilnahmen, waren bei der zweiten Veranstaltung auch Mitglieder der ITS sowie Vertreterinnen und Vertreter von Zertifizierungsstellen vertreten. Dies ermöglichte einen intensiven und vor allem auch **praxisbezogenen Austausch** unter den Teilnehmenden.

Darüber hinaus haben wir uns auch dieses Mal wieder aktiv an der **Bewertung und Prüfung auf europäischer Ebene eingereichter Zertifizierungsprogramme** aus Deutschland und Europa und der Erstellung von darauf bezogenen Stellungnahmen beteiligt.

Was ist zu tun?

Die Zusammenarbeit in Europa zur weiteren Ausgestaltung von Akkreditierungs- und Zertifizierungsvorgaben ist fortzusetzen und nach Möglichkeit zu intensivieren.

11.3 ENISA-Arbeitsgruppe zum „Data Protection Engineering"

Wie bereits im Vorjahr berichtet (41. TB, Tz. 2.3), wirkt die Landesbeauftragte für Datenschutz in der **„Ad-Hoc Working Group (AHWG) on Data Protection Engineering"** der Agentur der Europäischen Union für Cybersicherheit (ENISA) mit.

ENISA

Die Agentur der Europäischen Union für Cybersicherheit (ENISA) hat die Aufgabe, zu einem hohen gemeinsamen Maß an Cybersicherheit in ganz Europa beizutragen.

Solche von der ENISA eingesetzten Ad-hoc-Arbeitsgruppen bestehen aus Sachverständigen, die sich mit spezifischen technischen und wissenschaftlichen Fragen befassen. In diesem Fall beschäftigt sich die AHWG zu Data Protection Engineering mit der Analyse verfügbarer oder entstehender **Technologien und Verfahren zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**, wie dies in Artikel 25 DSGVO gefordert wird.

Die teilnehmenden Sachverständigen kommen aus Wissenschaft, Wirtschaft, Verwaltung sowie den **Datenschutzaufsichtsbehörden aus Griechenland, Italien, Spanien und Schleswig-Holstein**. Zusätzliche Beobachter (sogenannte „Observer") der Arbeiten, die stets mit zu Treffen eingeladen werden, kommen aus dem EDSA-Sekretariat und vom Europäischen Datenschutzbeauftragten. Die Gruppe soll drei Jahre aktiv sein und jährlich Ergebnisse vorlegen.

Die Website zur Ad-hoc-Arbeitsgruppe ist unter dem folgenden Link erreichbar:

https://www.enisa.europa.eu/topics/cybersecurity-policy/data-protection/ad-hoc-working-group-on-data-protection-engineering

Kurzlink: *https://uldsh.de/tb42-11-3a*

Bisher hat die Gruppe die folgenden Berichte erarbeitet:

Bericht „Engineering Personal Data Sharing – Emerging Use Cases and Technologies" (2023):

https://www.enisa.europa.eu/publications/engineering-personal-data-sharing

Kurzlink: *https://uldsh.de/tb42-11-3b*

Bericht „Engineering Personal Data Protection in EU Data Spaces" (2024)

https://www.enisa.europa.eu/publications/engineering-personal-data-protection-in-eu-data-spaces

Kurzlink: *https://uldsh.de/tb42-11-3c*

Die Themenkomplexe **Datenteilen (Data Sharing) und Datenräume (Data Spaces)** wurden aufgrund der Europäischen Datenstrategie (41. TB, Tz. 2.3) gewählt.

Was ist zu tun?

Es gibt bisher keine Garantie, dass bei der Umsetzung der Europäischen Datenstrategie in die Praxis die Anforderungen des Artikels 25 DSGVO berücksichtigt werden. Daher verdienen die Ausarbeitungen der Ad-Hoc Working Group on Data Protection Engineering der ENISA frühzeitig Aufmerksamkeit. Zudem wäre von Vorteil, wenn das Know-how der Sachverständigen auch bei konkreten Gestaltungsfragen der europäischen Entwicklungen in der Umsetzung über die nächsten Jahre einfließen könnte oder die Sachverständigen jedenfalls fallweise hinzugezogen würden.

12

KERNPUNKTE

Beanstandungen nach dem IZG-SH

Entschließungen der Konferenz der Informationsfreiheitsbeauftragten

Informationsfreiheit by Design

12 Informationsfreiheit

Im Jahr **2022 hatten wir den Vorsitz über die Konferenz der Informationsfreiheitsbeauftragten (IFK)** wahrgenommen (41. TB, Tz. 1.4 und Tz. 12.1) und in der Funktion die Themen rund um Transparenz und Informationszugang vorangetrieben. Doch auch ohne Vorsitzrolle war uns dies ein Anliegen, wie im Berichtsjahr zu sehen. So machten wir nach der Gesetzesänderung 2022 beispielsweise von dem **neu eingeführten Beanstandungsrecht** von § 14 Abs. 5 Informationszugangsgesetz Schleswig-Holstein (IZG-SH) Gebrauch (Tz. 12.1). Die Zahl der Beschwerden von Antragstellern wegen ihrer Ansicht nach ungenügender Beachtung des IZG-SH durch öffentliche Stellen zog merklich an. Waren es 2022 noch 37 Fälle, mussten wir 2023 82 Eingaben registrieren. Neben den Evergreens, die auch weiterhin einen Großteil der Beschwerden ausmachten (Tz. 12 2), waren auch einige besondere Fälle dabei (Tz. 12.3).

2023 haben wir zudem an den Sitzungen der Konferenz der Informationsfreiheitsbeauftragten aktiv mitgewirkt und den zugehörigen Arbeitskreis besucht (Tz. 12.4). Maßgeblich waren wir dabei insbesondere in den Feldern aktiv, die sich auf die **praktische Umsetzung des Informationszugangs** beziehen, beispielsweise durch Beteiligung an der Ausarbeitung zu Transparenzportalen und – in leitender Funktion – am Grundlagenpapier zu „Informationsfreiheit by Design" (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). So regelt der neue § 14 Abs. 5 IZG-SH, dass für den Fall, dass die oder der Landesbeauftragte für Informationszugang Verstöße gegen das IZG-SH feststellt, sie oder er diese gegenüber der informationspflichtigen Stelle beanstanden kann. 2023 lagen uns mehrere Fälle vor, in denen wir diese Möglichkeit in Erwägung ziehen mussten. Hierbei war zu beachten, dass wir vor dem Aussprechen einer Beanstandung nicht nur der betroffenen Stelle, sondern im Anschluss daran auch der zuständigen Rechts-, Dienst- oder Fachaufsichtsbehörde Gelegenheit zur Stellungnahme geben müssen.

Eine solche **Beanstandung** haben wir nunmehr **gegenüber der Apothekerkammer Schleswig-Holstein** ausgesprochen. Wir hatten festgestellt, dass ein nach § 4 IZG-SH beantragter **Informationszugang zu einem Impfplan ohne nachvollziehbare Gründe abgelehnt** und damit gegen § 5 Abs. 1 Satz 1 IZG-SH bzw. § 6 Abs. 1 Satz 3 IZG-SH verstoßen wurde.

Problematisch war nicht nur, dass die Monatsfrist des IZG-SH zur Beantwortung einer Anfrage nicht eingehalten wurde, sondern die dargelegten Gründe für die Ablehnung der Auskunft waren auch nicht stichhaltig. Die Argumentation der Apothekerkammer, dass die genannten Regelungen des Arzneimittelgesetzes und Heilmittelwerbegesetzes der Weitergabe von Informationen entgegenstünden, war nicht nachvollziehbar. Die vorgebrachte Argumentation war deswegen besonders überraschend, weil sich in den genannten Normen die behaupteten Aussagen überhaupt nicht finden ließen. Diese Normen regeln vielmehr Verpflichtungen zur Information sowie Werbeverbote – zu Gründen, die einer Herausgabe der begehrten Informationen möglicherweise entgegenstehen könnten, stand dort nichts. Natürlich ist der Schutzzweck der genannten Regelungen, dass **bestimmte Medikamente nicht einfach für jeden Menschen im Zugriff** sein dürfen, nachvollziehbar. Doch dies führt nicht dazu, dass interessierten Personen **generelle Informationen hierüber vorenthalten** werden dürfen.

Es ist bereits absehbar, dass wir auch im Jahr 2024 von dem Instrument der Beanstandung Gebrauch machen werden.

Was ist zu tun?

Das Mittel der Beanstandung ist bei Verstößen gegen das IZG-SH zu nutzen, um den informationspflichtigen Stellen gegenüber mit Nachdruck darzulegen, wenn sie nach Überzeugung der Landesbeauftragten für Informationszugang bei der Umsetzung der Informationsfreiheit bewusst 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 oder den Landesbeauftragten für Informationszugang anrufen. Einige Beschwerdegründe von Petentinnen und Petenten wiederholten sich auch 2023 mehrfach. Die **Top 5 der Beschwerden** unterscheiden sich kaum von denen der letzten Jahre (vgl. u. a. 41. TB, Tz. 12.3):

Der häufigste Grund war erneut, dass die informationspflichtige Stelle nicht auf den Antrag auf Informationszugang **fristgerecht reagierte**. Nach § 5 Abs. 2 IZG-SH besteht eine **Frist von einem Monat** nach Eingang des Antrags für die Zugänglichmachung zu den Informationen, wobei diese Frist nicht ausgereizt werden muss. Vielmehr hat die Auskunft „so bald wie möglich" zu erfolgen. Sind die Informationen derart umfangreich und komplex, dass die Frist nicht eingehalten werden kann, so kann die informationspflichtige Stelle die Frist auf höchstens zwei Monate verlängern. Dies ist jedoch der Antragstellerin bzw. dem Antragsteller innerhalb des ersten Monats mitzuteilen. Und auch eine Ablehnung des Antrags muss nach § 6 IZG-SH innerhalb dieser Fristen mitgeteilt werden. In den meisten Fällen reagieren die informationspflichtigen Stellen, sobald sie wissen, dass wir eingebunden worden sind – wenn auch ihre Handlungen dann nicht immer formal korrekt sind.

Das bringt uns zum zweiten Beschwerdegrund, dass insbesondere bei (Teil-)Ablehnungen die **Form des § 6 IZG-SH** nicht eingehalten wird. Vorgeschrieben ist u. a., dass der antragstellenden Person die Gründe für die Ablehnung mitzuteilen sind. Wenn überhaupt, wird teilweise von den Behörden nur auf allgemeine „rechtliche" Ablehnungsgründe verwiesen. Notwendig wäre nicht nur die konkrete Benennung des einschlägigen Ablehnungsgrunds nach §§ 9 oder 10 IZG-SH, sondern auch eine Auseinandersetzung mit den dort aufgeführten Merkmalen inklusive Darstellung der in der Regel erforderlichen Abwägung und gegebenenfalls eingeholten Anhörungen bzw. Einwilligungen. Auch wird aus den Begründungen nicht immer ersichtlich, ob geprüft wurde, dass gegebenenfalls nur eine teilweise Ablehnung geboten ist bzw. eine Schwärzung der nicht herausgebbaren Passagen im Text ausreicht. Schließlich fehlt immer mal wieder die Belehrung über die Rechtsschutzmöglichkeiten im Sinne des § 6 Abs. 4 IZG-SH.

Dies ist oftmals eine Folgeerscheinung des Problembereichs, dass die informationspflichtigen Stellen **nicht erkennen, dass tatsächlich ein Antrag nach dem IZG-SH vorliegt**. So ist der Antrag formfrei und muss auch keinen direkten Bezug zum IZG-SH beinhalten. Lediglich muss erkennbar sein, zu welchen Informationen der Zugang begehrt wird. Auch Antragstellungen über das Portal Fragdenstaat.de per E-Mail, in denen übrigens zumeist auf das IZG-SH verwiesen wird, sind zu bearbeiten.

In anderen uns vorliegenden Fällen wurden z. B. derartige **Anträge in Form von Bürgerfragen in Gemeinderatssitzungen** oder einfach fernmündlich oder im persönlichen Gespräch gestellt. Auch diese müssen in der Regel als

Anträge nach dem IZG-SH angesehen und entsprechend beschieden werden. In unklaren Fällen ist die informationspflichtige Stelle aufgefordert, nachzufragen und gegebenenfalls eine Präzisierung zu erbitten.

Immer mal wieder werden auch die **Gründe für den Antrag** auf Informationszugang durch die Stelle hinterfragt und diese gegebenenfalls in die Entscheidungsgründe über den Antrag aufgenommen. Das IZG-SH bietet allen Menschen (nicht nur Bürgerinnen und Bürgern in Schleswig-Holstein) den Anspruch auf Zugang zu den bei einer informationspflichtigen Stelle vorhandenen Informationen. Der Grund für die Anfrage ist dabei in den weit überwiegenden Fällen unbeachtlich. Es schadet dem Antrag beispielsweise nicht, wenn damit eigene Interessen verfolgt werden. Einzig bei der Frage, ob der Antrag offensichtlich missbräuchlich im Sinne des § 9 Abs. 2 Nr. 1 IZG-SH gestellt wurde, ist die Motivation der Antragstellerin bzw. des Antragstellers relevant.

Tatsächlich ist auch im Berichtszeitraum mehrfach von informationspflichtigen Stellen zumindest erwogen worden, bei mehrfacher Antragstellung von diesem Ablehnungsgrund auszugehen. Allerdings zeigt schon die Formulierung des Gesetzes, dass die Antragstellung **„offensichtlich" missbräuchlich** sein muss, dass hieran sehr enge Grenzen zu setzen sind. Der Zweck der Antragstellung muss in diesen Fällen klar nicht auf die Informationsbeschaffung, sondern die Störung der Arbeitsabläufe der Stelle bzw. deren Lahmlegung liegen. Wiederholte Anträge zum selben Sachverhalt könnten hierfür zwar ein Indiz sein. Wenn sich eine Person für viele Sachverhalte einer oder mehrerer Behörden interessiert und daher zahlreiche unterschiedliche Anträge stellt, liegt aber keine offensichtlich missbräuchliche Antragstellung vor. Ein Regulativ kann in diesen Fällen die Möglichkeit sein, für Auskünfte Gebühren im Rahmen der Landesverordnung über Kosten nach dem Informationszugangsgesetz für das Land Schleswig-Holstein (IZG-SH-KostenVO) zu erheben. Zu beachten ist hierbei jedoch, dass für einfache Auskünfte mit Aufwand zwischen 30 und 45 Minuten keine Gebühren erhoben werden dürfen und auch darüber hinaus die KostenVO Obergrenzen setzt.

Die Grundlagen zum IZG-SH haben wir in einer Broschüre zusammengefasst, die regelmäßig aktualisiert wird und unter dem folgenden Link heruntergeladen werden kann:

https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-7-Informationszugang.pdf

Kurzlink: *https://uldsh.de/tb42-12-2a*

Was ist zu tun?

Den Beschwerden von Petentinnen und Petenten ist nachzugehen. Zu unseren Aufgaben gehört es, informationspflichtige Stellen auf Fehler in der Umsetzung des Informationszugangsrechts hinzuweisen. Damit solche 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.

So waren zwei Fälle an uns herangetragen worden, in denen **Stadtwerke** die Auskunft mit der Begründung verweigerten, keine informationspflichtige Stelle zu sein. Diese Stadtwerke waren jeweils als GmbH ausgestaltet, aber eine 100%ige Tochter der Stadt. 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. Allerdings war es hier fraglich, ob die Stadtwerke tatsächlich in der oben genannten Form beliehen wurden und in den Handelsformen des öffentlichen Rechts tätig wurden. Dies konnten wir nach mehrfacher schriftlicher Diskussion mit den Stadtwerken nicht bejahen, sodass die Verweigerung der Auskunft bestehen blieb.

Diese Situation sehen wir jedoch als problematisch an, insbesondere bei Unternehmen, die sich zu 100 Prozent in der Hand einer Kommune bzw. Stadt befinden. In anderen Bundesländern unterliegen solche Unternehmen eindeutig der Auskunftspflicht; es ist dort nicht möglich, sich etwa durch Ausgründungen dieser Pflicht zu entziehen. Wir haben daher den Gesetzgeber in Schleswig-Holstein hierüber informiert und ihm einen Vorschlag zur Änderung des Gesetzes unterbreitet. Insbesondere die Aufzählung der Anwendungsfälle in § 2 Abs. 3 Nr. 2 IZG-SH zeigt, dass ursprünglich der Gesetzgeber durchaus solche Fälle im Blick hatte. Daher hoffen wir auf eine schnelle **Gesetzesänderung**.

In einem anderen Fall ging es um die Frage, ob die **Gemeindeordnung Schleswig-Holstein** (GO) und dort insbesondere die Regelungen zur nichtöffentlichen Sitzung der Gemeindevertretung die Anwendung des IZG-SH ausschließt. Aus § 3 Satz 2 IZG-SH ergibt sich, dass zwar Rechte auf Zugang zu Informationen, die andere Gesetze einräumen, unberührt bleiben. Jedoch werden diese nicht per se zu Spezialgesetzen, die das IZG-SH ausschließen würde. Somit kann auch auf Informationen, die nichtöffentliche Sitzungen einer Gemeindevertretung betreffen, ein Anspruch nach dem IZG-SH geltend gemacht werden. Im Rahmen der Prüfung der Ausschlussgründe nach §§ 9 und 10 IZG-SH ist dann der jeweilige Grund für die Nichtöffentlichkeit der Sitzung und deren Auswirkung auf den Zugang zu den angefragten Informationen zu berücksichtigen. Absolut ausgeschlossen ist der Zugang jedoch nicht. Insbesondere kann nach einiger Zeit der jeweilige Ausschlussgrund entfallen – etwa nach Abschluss der Beratungen. Wäre dies anders, wären alle dort eingebrachten Informationen (mit Ausnahme der nach § 35 Abs. 3 GO zu veröffentlichenden Beschlüsse) dem Informationszugang für immer entzogen.

Mehrfach hatten wir die Problematik zu behandeln, dass eine Kommune oder andere informationspflichtige Stellen **Gutachten oder Stellungnahmen** nicht beauskunften wollten. Begründet wurde dies damit, dass sie dem Schutz der Vertraulichkeit der Beratungen im Sinne des § 9 Abs. 1 Satz 1 Nr. 3 IZG-SH unterlägen. Nach unserer Ansicht, die sich mit Kommentarliteratur deckt und aktueller Rechtsprechung folgt, schützt die oben genannte Norm den Beratungsvorgang. Nicht davon automatisch umfasst sind Informationen bzw. Dokumente, die der Beratung zugrunde liegen. Dies können insbesondere vorher eingeholte Gutachten und Stellungnahmen sein.

In einem anderen Fall wollte die Antragstellerin gegenüber der informationspflichtigen Stelle **anonym** bleiben. Die Behörde jedoch bestand darauf, identifizierende Informationen von ihr zu erhalten, um u. a. die Gebührenzahlung zu gewährleisten. Wir vertreten die Ansicht, dass eine Antragstellung anonym bzw. unter Pseudonym und auch Beauskunftung so weit wie möglich zu gewähren ist. Der Anspruch auf Informationszugang wurde bewusst vom schleswig-holsteinischen Gesetzgeber ohne weitere Voraussetzungen ausgestaltet. Die gesetzliche Situation auf Bundesebene oder in einigen anderen Ländern unterscheidet sich in diesem Punkt vom IZG-SH.

Insbesondere kommt es nicht auf die Person des Antragstellers bzw. der Antragstellerin an. Bei Gebührenbescheiden muss dann im Einzelfall geprüft werden, ob diese so zugestellt werden und die Zahlungen so geleistet werden können, dass ein Antragsteller seinen Namen nicht zu nennen braucht und sich auch nicht anderweitig identifizieren muss.

Eine Ausnahme könnte für solche Fallgestaltungen gelten, bei denen die Gefahr besteht, dass ohne die Kenntnis von der Person der Antragstellerin bzw. des Antragstellers und deren/dessen Anschrift eine eventuell entstehende Gebührenpflicht nicht durchsetzbar ist. Bei der Beurteilung, ob dieser Fall vorliegen könnte, ist zum einen zu prüfen, ob überhaupt – z. B. **bei einfachen Auskünften** – ein kostenauslösender

Verwaltungsaufwand entstehen könnte, zum anderen ist die Erkennbarkeit einer Zahlungswilligkeit der antragstellenden Person relevant. Auf jeden Fall ist die Kenntnis des Namens oder der Adresse der antragstellenden Person dann nicht erforderlich, wenn bei einer kostenpflichtigen Informationsgewährung die **antragstellende Person zahlungswillig ist und eine Bezahlung auch ohne Namensnennung** erfolgen kann. Im uns vorliegenden Fall wurde stets die Zahlungswilligkeit von der Petentin erklärt. Es hätte durchaus zumindest Zahlungsmöglichkeiten unter Pseudonym – etwa durch Vorleistung – gegeben. Der Vorgang war 2023 noch nicht abgeschlossen, sodass wir über den weiteren Verlauf im kommenden Tätigkeitsbericht berichten werden.

In zwei Fällen im Berichtsjahr wurden wir von informationspflichtigen Stellen überraschenderweise gebeten, die Übermittlung der gewünschten Informationen zu übernehmen. Vorangegangen waren nicht bzw. nicht ausreichend erfolgte Auskünfte, die dann aufgrund unserer Einbindung doch noch erweitert werden konnten. Dies erfolgte dann im Rahmen des Stellungnahmeverfahrens. Die Petenten erhielten keinen Bescheid, sondern wir sollten die Informationen weiterleiten. In beiden Verfahren haben wir den informationspflichtigen Stellen deutlich gemacht, dass sie selbst in der Pflicht sind, einen direkten Bescheid den Petenten gegenüber zu erlassen. Unsere Rolle erstreckt sich nicht auf einen **Botendienst**.

Ein weiterer Fall betraf den Zugang zur **Kommunikation zwischen einem Kammerpräsidenten und einem Bundesminister**. 2022 hatte die Konferenz der Informationsfreiheitsbeauftragten in Deutschland eine Entschließung veröffentlicht, in der eindringlich darauf hingewiesen wurde, dass die behördliche Kommunikation umfassend den Regeln der Informationsfreiheit unterliegt (41. TB, Tz. 12.1). Im vorliegenden Fall war die Herausgabe der Kommunikation zunächst deshalb verweigert worden, weil der Kammerpräsident privat kommuniziert habe. Auf unsere Einbindung hin wurde dies noch einmal von der informationspflichtigen Stelle überprüft, sodass wir damit erreichen konnten, dass doch zumindest ein Teil der erfragten E-Mails an den Petenten übermittelt wurde.

Was ist zu tun?

Auch aus spezielleren Fällen lassen sich allgemeine Erkenntnisse zur Umsetzung des Informationszugangsrechts ableiten. Bei Unklarheiten helfen gerichtliche Entscheidungen.

12.4 Entschließungen der IFK

Anfang 2023 hatten wir turnusgemäß unseren Vorsitz der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) abgegeben. Im Rahmen des zugehörigen Arbeitskreises und insbesondere der Konferenzen in Berlin und Bonn haben wir an mehreren Entschließungen maßgeblich mitgewirkt.

1. Entschließung der 44. Konferenz der Informationsfreiheitsbeauftragten in Deutschland vom 14. Juni 2023 in Berlin: „Die Demokratie braucht starke Medien – Bundespressegesetz jetzt einführen!“

Der Bund verfügt im Gegensatz zu den Ländern nicht über ein Pressegesetz. Bis zum Jahr 2013 hat sich die Presse für ihren Auskunftsanspruch

auch gegenüber Bundesbehörden auf die Pressegesetze der Länder berufen. 2013 hat das Bundesverwaltungsgericht jedoch entschieden, dass dies unzulässig sei. Vielmehr ergebe sich der presserechtliche Auskunftsanspruch gegenüber Bundesbehörden unmittelbar aus dem Recht auf Pressefreiheit aus dem Grundgesetz. Es sei Sache des Bundesgesetzgebers, einen Informationszugang zu regeln (Bundesverwaltungsgericht, Urteil vom 20. Februar 2013, Az.: 6 A 2.12), der jedenfalls nicht hinter den landespresserechtlichen Ansprüchen zurückbleiben darf (Bundesverwaltungsgericht, Urteil vom 8. Juli 2021, Az.: 6 A 10.20).

Auch **zehn Jahre nach der Entscheidung fehlt eine konkrete Ausgestaltung** und damit die Rechtssicherheit, ob und wie Bundesbehörden der Presse Auskunft zu gewähren haben. Der alleinige Rückgriff auf das Informationsfreiheitsgesetz des Bundes wird der von Verfassung wegen gebotenen besonderen Stellung der Medien nicht gerecht. Die Regierungsparteien haben sich in ihrem Koalitionsvertrag darauf verständigt, diese Lücke zu schließen. Ein konkreter Gesetzentwurf für ein Bundespressegesetz steht aber nach wie vor aus.

Eine starke **Presse** ist für eine **lebendige Demokratie existenziell**. Dazu ist sie auf einen raschen und umfassenden Informationszugang angewiesen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert den Bundesgesetzgeber auf, zeitnah ein effizientes **Bundespressegesetz** zu schaffen, das der herausragenden Rolle der Presse und den Erfordernissen einer modernen Medienlandschaft Rechnung trägt.

2. Entschließung der 45. Konferenz der Informationsfreiheitsbeauftragten in Deutschland am 07.11.2023 in Bonn: „25 Jahre Århus-Konvention – Veröffentlichungsanspruch muss ins Gesetz!“

Nach 25 Jahren Århus-Konvention ist die so wichtige proaktive Veröffentlichung von Umweltinformationen in Deutschland immer noch abhängig vom Transparenzwillen der Behörden. Das muss sich ändern.

Mit der Århus-Konvention wurden 1998 erstmals internationale Mindeststandards für den Zugang zu Umweltinformationen völkerrechtlich verankert. Das Übereinkommen fußt auf der Erkenntnis, „dass jeder Mensch (…) die Pflicht hat, die Umwelt zum Wohle gegenwärtiger und künftiger Generationen zu schützen und zu verbessern“, und „zur Wahrnehmung dieser Pflicht Zugang zu Informationen, ein Recht auf Beteiligung an Entscheidungsverfahren und Zugang zu Gerichten in Umweltangelegenheiten haben“ muss.

Die Bestimmungen der Konvention fanden durch die EU-Umweltrichtlinie aus dem Jahr 2003 Eingang ins Gemeinschaftsrecht und im Folgenden ins nationale Recht. So sehen die Umweltinformationsgesetze in Deutschland vor, dass Behörden Umweltinformationen proaktiv und nicht nur auf Antrag Einzelner veröffentlichen müssen. Allerdings stellt diese Pflicht zur „Unterrichtung der Öffentlichkeit“ in den allermeisten Ländern und auf Bundesebene keinen selbstständigen, einklagbaren Anspruch für jedermann dar.

Bei Verstößen gegen die Pflicht fehlt somit die Möglichkeit zur Durchsetzung: Die Nichtbeachtung ist nach aktueller Gesetzeslage nicht gerichtlich überprüfbar, und die bloße Veröffentlichungspflicht droht zu verpuffen. Nur in den Transparenzgesetzen von Hamburg, Bremen und Rheinland-Pfalz besteht bislang – in gewissem Maße – ein subjektives Recht auf Veröffentlichung.

Um die Bürgerinnen und Bürger bei der Wahrnehmung ihres Rechts auf Zugang zu Umweltinformationen – ganz im Geiste der Århus-Konvention – zu stärken, ist eine **Novellierung des Umweltinformationszugangsrechts** nötig. Die IFK fordert die bisher untätigen Gesetzgeber dazu auf, die Verpflichtung zur Unterrichtung der Öffentlichkeit zu modernisieren und als selbstständigen Anspruch zu formulieren.

3. Entschließung der 45. Konferenz der Informationsfreiheitsbeauftragten in Deutschland am 07.11.2023 in Bonn: „Künstliche Intelligenz (KI) verantwortungsvoll für die Informationsbereitstellung nutzen!“

Künstliche Intelligenz (KI) kann bei der Umsetzung der Informationsfreiheit helfen. Die schnel-

le und fristwahrende Umsetzung der gesetzlich vorgeschriebenen Transparenz von Behördenhandeln scheitert immer wieder am Aufwand bei der Sichtung der vorhandenen Informationen und deren Bewertung durch die informationspflichtige Stelle.

KI ist auf dem digitalen Vormarsch und wird vermehrt im Alltag eingesetzt. Durch ihren Einsatz können organisatorische Abläufe optimiert und Arbeitsschritte automatisiert werden. Auch für die Informationsfreiheit kann das Potenzial von KI genutzt werden, um die Bereitstellung von amtlichen Informationen zu vereinfachen und damit zu fördern. Es werden bereits Prototypen von KI-Tools genutzt, die z. B. durch Zusammenfassungsfunktionen oder Fließtextgenerierung die Arbeit der Verwaltungsmitarbeitenden unterstützen. Im Justizbereich gibt es u. a. auch Projekte, bei denen z. B. **gerichtliche Entscheidungen mithilfe von KI-basierten Schwärzungstools veröffentlicht** werden können.

Was beim Einsatz von KI aber immer beachtet werden muss: KI ist ein „Werkzeug", das für den optimalen Einsatz durch den Menschen korrekt angelernt und überwacht werden muss, um amtliche Informationen zu sondieren und Fehler bei deren Einschätzung zu vermeiden. Beim Einsatz von KI durch öffentliche Stellen muss deshalb gewährleistet sein, dass die eingesetzten Verfahren durch ausreichende Transparenz und durch technisch-organisatorische Gestaltung überprüfbar und beherrschbar sind. Gesetzliche Bestimmungen und ethische Grundsätze sind dabei zu berücksichtigen. Dazu gehören auch der Persönlichkeitsrechtsschutz und die datenschutzrechtlichen Vorgaben.

So können perspektivisch in wenigen Schritten beantragte Informationen bereitgestellt werden. Ebenso kann auch die proaktive Veröffentlichung im Rahmen der Transparenzportale erleichtert werden. Die abschließende Entscheidung muss jedoch zwingend durch den Menschen erfolgen. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland sieht die KI unter Beachtung der oben genannten Grundsätze im Informationsfreiheitsbereich als ein effektives Instrument zur schnellen Informationsbereitstellung an.

4. Entschließung der 45. Konferenz der Informationsfreiheitsbeauftragten in Deutschland am 07.11.2023 in Bonn: „Moderne Transparenzgesetze bundesweit – für eine lebendige Demokratie!"

Die Informationsfreiheitsgesetze sind ein wichtiges Instrument, um die Akzeptanz der Demokratie zu befördern. Sie ermöglichen durch einen allgemeinen und voraussetzungslosen Zugang zu Informationen Beteiligung und Kontrolle.

Betrachtet man die existierenden Regelungen über den Zugang zu amtlichen Informationen, so gibt es in Deutschland derzeit eine **„Dreiklassengesellschaft"**:

- In einigen Bundesländern gibt es Transparenzgesetze mit proaktiven Veröffentlichungspflichten auf staatlichen Transparenzplattformen.
- In einigen Ländern und im Bund gibt es Informationsfreiheitsgesetze, die den Informationszugang nur auf Antrag gewähren.
- In Bayern und Niedersachsen gibt es nach wie vor kein voraussetzungsloses Recht auf Zugang zu amtlichen Informationen.

Moderne Transparenzgesetze zeichnen sich im Kern dadurch aus, dass sie die proaktive Informationsbereitstellung in Transparenzportalen durch öffentliche Stellen der Bundes-, Landes- sowie der kommunalen Ebene gewährleisten.

Darüber hinaus sollten bei der Ausgestaltung moderner Transparenzgesetze weitere wichtige Gesichtspunkte einbezogen werden:

- die Zusammenlegung von IFG und UIG,
- den Verzicht auf Bereichsausnahmen,
- die Möglichkeit einer niedrigschwelligen Antragstellung,
- die Pflicht zur Abwägung mit dem öffentlichen Interesse an der Bekanntgabe von Informationen bei bestehenden Geheimhaltungsinteressen und
- Reduzierung und Harmonisierung der Ausschlussgründe.

Die IFK fordert die Bundes- und Landesgesetzgeber dazu auf, mit modernen Transparenzgesetzen das **Recht auf Informationszugang deutschlandweit auf ein einheitlich hohes Niveau zu bringen** und die Informationsfreiheits- und Transparenzbeauftragten des Bundes und der Länder mit den erforderlichen Kompetenzen auszustatten.

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/tb42-12-4a*

Was ist zu tun?

Wir werden uns weiterhin intensiv in die Diskussionen und Entschließungen der IFK und des zugehörigen Arbeitskreises einbringen.

12.5 Informationsfreiheit by Design

Noch aus unserem Vorsitzjahr der IFK haben wir die Aufgabe übernommen, in leitender Funktion mit Kolleginnen und Kollegen von Bund und Ländern (Baden-Württemberg, Berlin, Bremen, Hessen, Nordrhein-Westfalen sowie Thüringen) ein Informationspapier zu „Prinzipien der Informationsfreiheit und Umsetzungshinweise zur ‚Informationsfreiheit by Design'" zu erstellen.

Zu **„Informationsfreiheit by Design"** zählt die Gesamtheit technischer und organisatorischer Instrumente nach dem Stand der Technik, die der Wahrnehmung und Erfüllung der Rechte nach den Informationsfreiheits-, Umweltinformations- und Transparenzgesetzen des Bundes und der Länder dienen.

Damit unterstützt „Informationsfreiheit by Design" einerseits informationspflichtige Stellen bei der Erfüllung eines beantragten Zugangs zu herauszugebenden Informationen. Mit einer guten organisatorischen Vorbereitung und der Nutzung digitaler Techniken kann die Verwaltung ihren Aufwand erheblich senken. Für Antragstellende wird andererseits der Informationszugang beschleunigt und erleichtert. Besonders mit einem entsprechend gestalteten E-Akte-Verfahren kann der Informationszugang schneller und mit weniger Verwaltungsaufwand und damit auch kostengünstiger erfolgen. Die proaktive Bereitstellung bzw. Veröffentlichung von Informationen entsprechend den jeweils geltenden Transparenzpflichten kann durch „Informationsfreiheit by Design" ebenfalls erleichtert werden.

Zunächst wurden die maßgeblichen Prinzipien erarbeitet und abgestimmt:

- Recht auf Informationszugang,
- planvolles Vorgehen / Effizienz durch Vorbereitung,
- Vollständigkeit,
- Kontextualisierung / Integrität / Verfügbarkeit,
- Offenheit und Kooperation,
- strukturierter Prozess zur Identifizierung von Ausschlussgründen und Abwägung von Interessen,
- Verarbeitbarkeit,
- Management von Informationsfreiheit als andauernder Prozess,
- geringer Aufwand, niedrige bzw. keine Kosten.

Hieraus ließen sich Maßnahmen ableiten, die u. a. durch Prüffragen in einer Checkliste informationspflichtige Stellen dabei unterstützen, ihre Verfahren und Prozesse so zu gestalten, dass Informationsfreiheitsanfragen effektiv und vollständig beantwortet werden können. Eingebunden waren nicht nur die Kolleginnen und Kollegen der anderen Beauftragten für Informationsfreiheit, sondern auch Praktikerinnen und Praktiker aus informationspflichtigen Behörden.

Es ist geplant, dass das Papier im ersten Quartal 2024 von der IFK beschlossen und dann veröffentlicht wird. Unter anderem wird es über unsere Informationsseite zur Informationsfreiheit in Schleswig-Holstein abrufbar sein:

https://www.datenschutzzentrum.de/informationsfreiheit/

Kurzlink: *https://uldsh.de/tb42-12-5a*

Was ist zu tun?

Das Papier „Informationsfreiheit by Design" soll nicht nur eine Momentaufnahme darstellen, sondern für längere Zeit Hilfestellung geben. Daher soll es nach der Veröffentlichung immer wieder aktualisiert werden. Hilfreich dafür ist der Praxis-Check – die Rückmeldungen von informationspflichtigen Stellen.

13

KERNPUNKTE

DATENSCHUTZAKADEMIE Schleswig-Holstein

Sommerakademie 2023

13 DATENSCHUTZAKADEMIE Schleswig-Holstein

Die DATENSCHUTZAKADEMIE Schleswig-Holstein ist für die Konzeption und Organisation der **Fortbildungsveranstaltungen zu den Themenbereichen Datenschutz und Informationsfreiheit** zuständig. So wird beispielweise den behördlichen und betrieblichen Datenschutzbeauftragten entsprechendes Fachwissen zur Datenschutz-Grundverordnung (DSGVO) und anderen wesentlichen datenschutzrechtlichen oder sicherheitstechnischen Grundlagen vermittelt.

13.1 Sommerakademie – jährliche Datenschutzkonferenz in Kiel

Die alljährlich an einem Montag im Spätsommer stattfindende Sommerakademie der DATENSCHUTZAKADEMIE stand im Jahr 2023 unter dem Motto: **„Vom Volkszählungsurteil zur DSGVO: Ist der Datenschutz fit für KI & Co.?"** Teilnehmer aus dem gesamten Bundesgebiet haben den Weg nach Kiel gefunden, um über Datenschutz und Datensicherheit zu diskutieren.

Die Veranstaltung erinnerte daran, dass 2023 ein **Jubiläumsjahr für den Datenschutz** war: **40 Jahre Recht auf informationelle Selbstbestimmung, 15 Jahre Computergrundrecht und fünf Jahre DSGVO**. Diese Meilensteine des Datenschutzes prägen nämlich auch heute noch unseren Blick auf das Thema. Über die vergangenen Jahre und Jahrzehnte hat sich der Datenschutz von einem Nischenthema zu einem Dauerbrenner entwickelt. Die meisten Verantwortlichen kennen ihre Pflichten, viele betroffene Personen kennen ihre Rechte. Aufsichtsbehörden und Gerichte nehmen ihre Aufgaben wahr und wenden das Datenschutzrecht an.

Hinzu kam im Jahr 2023 das Themengebiet der künstlichen Intelligenz (KI). Was früher nur im Labor und lediglich für wenige Spezialistinnen und Spezialisten zur Verfügung stand, ist nun für jede und jeden nutzbar und durchdringt nahezu alle Lebensbereiche. Gleichzeitig verfolgt die Europäische Datenstrategie das Ziel der „datengesteuerten Gesellschaft" mit dem Paradigma der Datenweitergabe.

Ausgehend von den Entwicklungen der letzten Jahrzehnte und der letzten Monate legte die Sommerakademie einen Fokus auf die folgenden Fragen:

- Passen die aktuellen Entwicklungen rund um Datenteilen und KI zusammen mit den Meilensteinen des Datenschutzes aus den vergangenen Jahren?
- Wie können die Datenschutzbeauftragten vor Ort und die Aufsichtsbehörden mit dem Wandel umgehen?
- Und wie lassen sich unerwünschte Effekte von eigentlich guten Datenschutzinstrumenten vermeiden?

In Vorträgen und Diskussionsbeiträgen gaben Expertinnen und Experten aus Praxis und Wissenschaft einen Einblick in die heutigen und künftigen Herausforderungen im Zusammenhang mit Daten und Menschen. Im Mittelpunkt der Veranstaltung standen Ansätze, mit denen wir Datenschutz zusammen mit den anderen Grundrechten in der digitalen Welt besser umsetzen können.

Die Vorträge sind unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/sommerakademie/2023/

Kurzlink: *https://uldsh.de/tb42-13-1a*

Index

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Y

Z

ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

Schleswig-Holsteins
Zentrum für Datenschutz
und Informationszugang

https://www.datenschutzzentrum.de/tb/