ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

TÄTIGKEITSBERICHT
2026



ULD – SCHLESWIG-HOLSTEINS ZENTRUM FÜR DATENSCHUTZ UND INFORMATIONSZUGANG

Tätigkeitsbericht 2026
des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein

BERICHTSZEITRAUM: 2025

REDAKTIONSSCHLUSS: 31.12.2025

LANDTAGSDRUCKSACHE: 20/4234

(44. 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

1	**DATENSCHUTZ UND INFORMATIONSFREIHEIT**	**9**
1.1	Zehn Jahre Datenschutz-Grundverordnung – ein Zwischenfazit	10
1.2	Zahlen und Fakten	11
1.3	Weiterentwicklung von LDSG und IZG-SH in Schleswig-Holstein	13
1.4	Neue Zuständigkeiten des ULD – vom Zugang zu Produktdaten bis zur politischen Werbung	14
1.5	Die Datenschutzbeauftragten vor Ort: wichtige Stütze, Entlastung vor Ort	17
1.6	Beratung für die öffentliche Verwaltung	18
1.7	Öffentlichkeitsarbeit	19
1.7.1	Informationsmaterialien	19
1.7.2	Veranstaltungen	20
1.7.3	AK Presse-und Öffentlichkeitsarbeit	20
2	**DATENSCHUTZ UND INFORMATIONSFREIHEIT – GLOBAL UND NATIONAL**	**23**
2.1	Datenschutz zwischen Koalitionsvertrag und Modernisierungsagenda	23
2.2	Die Ergebnisse der DSK im Jahr 2025 im Überblick	25
2.3	Geschenke für den Datenschutz aus dem Cybersicherheitsrecht	27
2.4	Gamechanger Herstellerverantwortung – vielleicht schon in Sichtweite	29
2.5	Datenschutzreform in Europa: Omnibusse, Fitnesscheck und die Büchse der Pandora	31
3	**LANDTAG**	**35**
3.1	Entwicklung nach der EuGH-Entscheidung zum parlamentarischen Datenschutz	35
3.2	Datenschutzgremium	36
3.3	Service für Abgeordnete in Fragen zu Datenschutz und Informationsfreiheit	37
4	**DATENSCHUTZ IN DER VERWALTUNG**	**41**
4.1	Allgemeine Verwaltung	41
4.1.1	Interessenkonflikt bei behördlichen Datenschutzbeauftragten?	41
4.1.2	Ortsbeiräte und Seniorenbeiräte als Mandatsträger	42
4.1.3	Einhaltung der Vorgaben zur Schuleingangsuntersuchung	42
4.1.4	Löschung von Daten auf schulisch genutzten Tablets via Fernlöschung	43
4.1.5	Einbrüche in Verwaltungs- und Büroräume	45
4.1.6	Vollstreckungsankündigung ohne Umschlag im gemeinsamen Briefkasten mit dem Vermieter	45
4.1.7	Befristetes Arbeitsverhältnis: Namentliche Benennung der zu vertretenden Beschäftigten?	46
4.1.8	Mitteilung des Arztes zur Fahruntauglichkeit eines Patienten an Fahrerlaubnisbehörde?	47
4.1.9	Anfertigung von Sozialberichten	48
4.2	Polizei und Verfassungsschutz	49
4.2.1	Gesetzliche Prüfpflichten nach dem Landesverwaltungsgesetz	49
4.2.2	Gesetzentwurf der Landesregierung: Einführung von biometrischer Gesichtserkennung und Datenanalyse bei der Polizei	50

4.2.3 Einführung der elektronischen Aufenthaltsüberwachung zum Schutz von Opfern häuslicher Gewalt 50
4.2.4 Zweckänderung im OWi-Verfahren: Zulässig – aber nicht ohne dokumentierte Aktenlage 51
4.2.5 Löschanspruch trifft Fachverfahren: owi21 braucht eine nachvollziehbare Löschfunktion 52
4.2.6 Gefährderansprache am Scheibenwischer 53
4.2.7 Novellierung des Landesverfassungsschutzgesetzes 54

4.3 Justiz 54
4.3.1 Aushang eines Fotos nach Erteilung eines Hausverbots 54

4.4 Soziales 55
4.4.1 Befreiung vom Bankgeheimnis – eine Blankovollmacht wird nicht benötigt 55
4.4.2 Sozialdaten zum Mitlesen – unverschlüsselter Versand 56

4.5 Schutz des Patientengeheimnisses 56
4.5.1 Kein Auskunftsanspruch nach dem Tod des Patienten? 56
4.5.2 Anspruch auf Kopie der Patientenakte per Post? 57
4.5.3 Arztpraxis erteilt keine Auskunft – Anordnung der Ersatzzwangshaft? 58
4.5.4 Ärger durch Reaktion auf Ärztebewertung? 59

4.6 Datenpannen im Medizinbereich 60
4.6.1 Veröffentlichung eines Recruiting-Videos – mit Patientendaten 60
4.6.2 Herausgabe unausgefüllter Rezepte an einen Tablettendealer 61
4.6.3 Versand eines Arztbriefes an einen Hausarzt ohne Einwilligung der Patientin 61

4.7 Bildung 62
4.7.1 Informationsweitergabe an Elternvertretungen in Kindertagesstätten 62
4.7.2 Fehldruck von Willkommensbriefen 64

4.8 Datenschutz- und Medienkompetenz 65
4.8.1 Mitarbeit im AK Datenschutz- und Medienkompetenz 65
4.8.2 Mitarbeit im Netzwerk Medienkompetenz in Schleswig-Holstein 65

5 DATENSCHUTZ IN DER WIRTSCHAFT 67
5.1 Gebrauchte Festplatte mit Daten zum Verkauf 67
5.2 Hardwarereparatur und Preisgabe von Passwörtern 68
5.3 Anfertigen von Personalausweiskopien durch Elektronikhändler 68
5.4 Abfrage von Halterdaten durch Dienstleister bei Parkverstößen 69
5.5 Kennzeichenerfassung als Zutrittskontrolle auf einem Campingplatz 70
5.6 Bildveröffentlichung durch nicht sorgeberechtigten Elternteil 71
5.7 Überwachung von Müllbehältern 71
5.8 Bestandskundin oder nicht? 72
5.9 Neues Gewerbe – alte Kundendaten 73
5.10 Satellitenortung I: Erreichbarkeit von Beschäftigten und Leistungskontrolle 73
5.11 Satellitenortung II: Sicherheit auf Autobahnen 75
5.12 Informationsverknüpfung führt zu Identifizierbarkeit 76
5.13 Sportwetten im Internet – Auskunftsanspruch 77

5.14 Weitergabe von Beschäftigtendaten an das Ordnungsamt 78
5.15 Bewerbungsgespräch mit unerwarteten Folgen 78
5.16 Gezielte Videoüberwachung mit Tonaufzeichnung von Beschäftigten 80

5.17 Datenpannen in der Wirtschaft – Meldungen nach Artikel 33 DSGVO 81
5.17.1 Zugang zu Räumen mit Generalschlüsseln 81
5.17.2 Besucherfotos aus Fotobox gespeichert 82

5.18 Videoüberwachung 83
5.18.1 Allgemeine Entwicklungen 83
5.18.2 Zwischen Tomaten und Technik – Videoüberwachung in Kleingärten 84
5.18.3 Kamera an Bord – Videoüberwachung in Taxis 85
5.18.4 Privatsphäre auf dem Teller – Videoüberwachung in Restaurants 86

5.19 Geldbußen für Datenschutzverstöße 86
5.19.1 Analyse von Kundendaten zu Werbezwecken mit Smart-Data-Verfahren 86
5.19.2 Veröffentlichung von Patientendaten durch einen Arzt in einer Antwort auf eine Internetrezension 87

6 SYSTEMDATENSCHUTZ 89
6.1 Landesebene 89
6.1.1 Zusammenarbeit mit dem Zentralen IT-Management (ZIT SH) 89
6.1.2 Zusammenarbeit mit dem ITV.SH 90
6.1.3 Prüfleitfaden KI – Zusammenarbeit mit dem Landesrechnungshof 90

6.2 Deutschlandweite und internationale Zusammenarbeit der Datenschutzbeauftragten 91
6.2.1 AK Technik 91
6.2.2 Standard-Datenschutzmodell – ein Update 92
6.2.3 EDSA-Guidelines zu Pseudonymisierung und Anonymisierung – ein Update 94
6.2.4 Orientierungshilfe RAG-Systeme 95
6.2.5 Orientierungshilfe zu Maßnahmen bei Entwicklung und Betrieb von KI-Systemen 96

6.3 Ausgewählte Ergebnisse aus Prüfungen, Beratungen und Meldungen nach Artikel 33 DSGVO 97
6.3.1 Erkenntnisse aus Datenpannenmeldungen 97
6.3.2 Datenpannen in Verbünden und verteilten Systemen 98
6.3.3 KI-Fachgespräch: „Frag' für 'nen Freund" 100

7 NEUE MEDIEN 103
7.1 Änderungen zum Medienstaatsvertrag 103
7.2 Aktuelles aus dem AK Medien 104

8 MODELLPROJEKTE UND STUDIEN 107
8.1 Plattform Privatheit: Forschung für ein selbstbestimmtes Leben in der digitalen Welt 107
8.2 Projekt DatenTRAFO – Neue Datenschutz-Governance – Technik, Regulierung und Transformation 107

8.3 Projekt Unboxing.IoT.Privacy – Transparenz für Datenschutzeigenschaften von IoT-Geräten 108
8.4 Projekt TRUMAN – Der Mensch im Mittelpunkt: vertrauenswürdige KI-Anwendungen 110
8.5 Projekt AnoMed – Kompetenzcluster Anonymisierung für medizinische Anwendungen 112

9 ZERTIFIZIERUNG UND AKKREDITIERUNG 115
9.1 Stand der Akkreditierung und Zertifizierung in Deutschland und der EU 115
9.2 Themen des AK Zertifizierung in Deutschland 116
9.3 Themen auf europäischer Ebene in der Expert Subgroup 116
9.4 Überarbeitung des Prüfkriterienpapiers 117

10 AUS DEM IT-LABOR 121
10.1 Fingerabdrücke im Web – wie funktioniert Browser-Fingerprinting? 121
10.2 Sicherheit von Webbrowsern durch Filtermechanismen – neue Entwicklungen 122
10.3 KI-Systeme und die Privatsphäre 123

11 EUROPA UND INTERNATIONALES 127
11.1 Anwendungshinweise der DSK zur Datenübermittlung in Drittländer zu medizinischen Zwecken 127
11.2 Wiedergänger Chatkontrolle – Risiko für die gesamte digitale Infrastruktur 128

12 INFORMATIONSFREIHEIT 131
12.1 Beanstandungen 131
12.2 Neue Kostenverordnung zum IZG-SH 132
12.3 Top 5 der Themen in Schleswig-Holstein 133
12.4 Besondere Fälle und Fragen 135
12.5 Beschlüsse der IFK 136

13 DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN 139
13.1 Fortbildungsveranstaltungen im Programm der DATENSCHUTZAKADEMIE 139
13.2 Sommerakademie – jährliche Datenschutzkonferenz in Kiel 139

Index 141

01

KERNPUNKTE

Zehn Jahre Datenschutz-Grundverordnung

Zahlen und Fakten

Neue Zuständigkeiten des ULD

Beratung für die öffentliche Verwaltung

1 Datenschutz und Informationsfreiheit

Alles ist im Fluss – diese Erkenntnis ist nicht neu. Aber was wir seit einigen Jahren immer stärker sehen, ist keine allmähliche Veränderung mehr, sondern eine **abrupte und disruptive Abkehr von der bekannten und erprobten Welt**, in der wir es uns zuvor eingerichtet haben. Da sind nicht nur die Vorboten der gigantischen Naturkatastrophen, die der Klimawandel mit sich bringt. Oder die Angriffswellen auf die Computer und die kritische Infrastruktur, die das Rückgrat der Digitalisierung darstellen. Geopolitische Spannungen, Zeitenwende, eine Weltordnung, die aus den Fugen gerät. Und der Datenschutz mittendrin.

Denn Daten sind Macht. Nicht von ungefähr setzt die **US-Behörde ICE (Immigration and Customs Enforcement)** Smart Glasses und Bodycams mit biometrischer Gesichtserkennungssoftware ein, um Gesichter zu scannen und mit Datenbanken abzugleichen. Das **US-amerikanische Department of Government Efficiency (DOGE)** hat nicht nur auf Daten zum Regierungshandeln zugegriffen, wie es sich aus seiner Aufgabe einer Effizienzprüfung erklären ließe, sondern sich auch Zugang zu sensiblen Daten von Millionen von Bürgerinnen und Bürgern verschafft und diese kopiert. Gerichte haben im Nachhinein versucht, dem Einhalt zu gebieten, der Supreme Court hat derartige Zugriffe wiederum erlaubt. Zweckbindung? Fehlanzeige.

In der globalisierten Welt können politische Entwicklungen in anderen Ländern auf einen selbst durchschlagen. Beispielsweise wenn dort ansässige Anbieter von Produkten oder Anwendungen die eigenen personenbezogenen Daten speichern und dortige Behörden darauf zugreifen. Oder wenn eine Firma, eine Nichtregierungsorganisation oder eine Privatperson auf einer schwarzen Liste landet und befürchten muss, auf einmal von Bank- oder E-Mail-Konten ausgeschlossen zu werden.

Man kann nicht sagen, dass es angesichts dieser unguten Abhängigkeiten an Warnungen gefehlt hätte. Wirklich verstanden wurden diese Warnungen leider nicht, wie man an der gegenwärtigen Situation leicht ablesen kann. „Ausspähen unter Freunden, das geht gar nicht“, sagte die damalige Bundeskanzlerin Angela Merkel im Oktober 2013, als kurz zuvor die Snowden-Dokumente bekannt geworden waren. Später wurde als noch unerreichtes Ziel im Koalitionsvertrag festgelegt, Deutschland solle „Verschlüsselungsstandort Nummer eins“ werden. Verschlüsselung muss dringend ausgebaut werden, das stimmt – aber Verschlüsseln allein hilft auch nicht über die Abhängigkeiten hinweg, die sich nicht nur auf das digitale Leben der Menschen negativ auswirken können.

Die Lösung: **digitale Souveränität**. Die schleswig-holsteinische Regierung ist weit voran auf dem Weg, sich aus den Abhängigkeiten von Anbietern herauszulösen, die nicht verlässlich die europäischen Werte verfolgen. Die Open-Source-Strategie wird seit Jahren vorangetrieben. Schleswig-Holstein zeigt Schritt für Schritt, dass digitale Souveränität möglich ist. Dabei geht es auch um Datenschutz. Und um den Schutz der eigenen Infrastruktur. Das Gute: Wenn sich erst mal einige Pioniere auf den Weg gemacht haben, um digital souverän zu werden, ist es für nachfolgende Akteure einfacher. Sie können die Wege der Pioniere als Blaupausen nutzen.

Das Titelbild dieses Berichts zeigt symbolisch, wie eine Brücke auf- und umgebaut wird: mit den blauen Bausteinen der Europäischen Union, die allmählich die anderen Komponenten ersetzen. **Weniger Abhängigkeiten, mehr Verlässlichkeit und Transparenz, mehr Garantien für europäische Werte – und dazu gehört auch der Datenschutz.**

In diesem Bericht habe ich einiges zu den großen Themen unserer (Datenschutz-)Zeit und viele kleine Beispiele aus unserer täglichen Arbeit zusammengestellt. Eines ist klar: Datenschutz im Wandel wird uns auch künftig begleiten – das ist so sicher wie der Wandel selbst. Ich wünsche Ihnen viel Spaß beim Lesen!

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

1.1 Zehn Jahre Datenschutz-Grundverordnung – ein Zwischenfazit

Die meisten Personen, die an die Anfänge der Datenschutz-Grundverordnung denken, werden wahrscheinlich das Jahr 2018 im Kopf haben: Zum 25.05.2018 wurde die DSGVO wirksam, ab dann mussten die Verantwortlichen und Auftragsverarbeiter die darin beschriebenen Pflichten erfüllen. Einige Expertinnen oder Experten werden weiter zurückdenken, z. B. an den 25.01.2012, als die Europäische Kommission ihren Gesetzentwurf vorstellte, der anschließend durch das Parlament und den Rat noch verändert wurde.

In Kraft trat die **DSGVO** im Mai 2016, also etwa zehn Jahre vor Erscheinen dieses Berichts. Zu diesem Zeitpunkt konnten alle Verantwortlichen und Auftragsverarbeiter den Gesetzestext lesen und die zweijährige Umsetzungsfrist bis zum Wirksamwerden der DSGVO nutzen. Ebenso wie die anderen Aufsichtsbehörden boten wir Beratung an. Da sich die Anforderungen der DSGVO gar nicht so sehr von den vorherigen Regelungen in den Bundes- und Landesdatenschutzgesetzen unterschieden, konzentrierten wir uns damals in unseren Vorträgen und Beratungen darauf, wie Verantwortliche und Auftragsverarbeiter ausgehend von der bisherigen Rechtslage nur wenig ändern oder ergänzen mussten, um zum 25.05.2018 weiterhin die neuen datenschutzrechtlichen Anforderungen zu erfüllen.

Im Nachhinein war dieser Ansatz zu optimistisch gewesen, denn offenbar hatten sich nicht alle Firmen vor 2018 um ihren Datenschutz gekümmert. Wer bereits einen **Datenschutzbeauftragten** benannt hatte, war besser aufgestellt (Tz. 1.5). Aber erst als die Storys über mögliche Geldbußen oder Abmahnrisiken durch die Medien rauschten – möglicherweise lanciert oder angeheizt von Berufsgruppen, die sich dann unmittelbar als Lösung anboten –, war Datenschutz in aller Munde. Dieses Image, in dem Datenschutz als Schreckgespenst dargestellt wird, hallt immer noch nach.

Der europäische Gesetzgeber hat mit der DSGVO einen Instrumentenkasten zur Verfügung gestellt, der **viel Bewährtes und einiges Neues** enthielt. Wahrscheinlich hätte sich aber keiner träumen lassen, dass für die Vorbereitung und Einführung des Instruments der Zertifizierung so viele Jahre ins Land gehen würden (Tz. 9.1), wobei die Produkte, die bei der Verarbeitung personenbezogener Daten zum Einsatz kommen, selbst gar nicht nach der DSGVO zertifizierbar sind. Aber auch heute noch ist eine **Zertifizierung nach der DSGVO** bisher die Ausnahme.

Das Instrument der Verhaltensregeln (Codes of Conducts) wurde von den Branchenverbänden bisher nur in homöopathischem Ausmaß genutzt. Dabei läge es doch nahe, diesen Ansatz mit den branchenspezifischen Anforderungen an die Gestaltung (**Datenschutz by Design & by Default**) zu kombinieren und damit die Verarbeitungen innerhalb der Branche schon aus Eigeninteresse ein Stück weit **standardisieren** zu können. Und nicht nur die **Verarbeitungen**, sondern auch die **Informationspflichten** und die **Prozesse zur Umsetzung der Betroffenenrechte** sowie die **Dokumentation zur Umsetzung der Rechenschaftspflicht**.

Hoffnung lag (und liegt immer noch) auch auf den „**standardisierten Bildsymbolen**" nach Art. 12 Abs. 8 DSGVO. Dabei handelt es sich um Piktogramme, die es den betroffenen Personen erleichtern sollen, die vom Verantwortlichen nach Artikel 13 und 14 DSGVO bereitgestellten Informationen zu verstehen und – gegebenenfalls mithilfe von Assistenz-Tools – automatisiert auszuwerten. Der Ball liegt seit zehn Jahren bei der **Europäischen Kommission**, denn sie hat die Befugnis, delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole zu erlassen. Mit der **Standardisierung der Bildsymbole und im digitalen Bereich auch der elektronischen Repräsentanz und maschinenlesbaren Darstellung** (siehe Art. 12 Abs. 7 DSGVO) wäre auch ein großer Schritt dafür getan, dass die Informationspflichten insgesamt leichter für die Verantwortlichen umsetzbar wären. Es ist unklar, wann die Europäische Kommission eigene Vorschläge vorlegen wird – oder ob sie überhaupt zu diesem Thema aktiv werden möchte. Wenn nein, dann

sollte überlegt werden, diese Aufgabe dem Europäischen Datenschutzausschuss zuzuweisen.

Auf der Habenseite zu verbuchen sind die Entscheidungen des **Europäischen Gerichtshofs (EuGH)**: Für alle, die Datenschutzrecht verstehen wollen oder müssen, hat der EuGH über die letzten Jahre einen großen Schatz an Urteilen und Auslegungsvorgaben geschaffen. Es ist nicht so, dass man ohne den EuGH die DSGVO nicht verstehen könnte – tatsächlich hat der EuGH vielfach genau das wiederholt, was bereits im Gesetzestext steht. Für die einheitliche Auslegung in allen Mitgliedstaaten mit verschiedenen Rechts- und Verwaltungstraditionen sind die Entscheidungen des EuGH jedoch ein Segen.

Zehn Jahre Datenschutz-Grundverordnung – ist nun das meiste geschafft? Kann man sich auf dem Erreichten ausruhen und die Hände in den Schoß legen? Nein, das geht generell nicht in der heutigen Welt, in der die verschiedenen Risiken – hier: für **Datenschutz und Cybersicherheit** – beherrschbar bleiben müssen. Der technische Fortschritt (Stichwort KI) und der Wandel in den Anforderungen der Umgebung, nicht zuletzt durch geopolitische Herausforderungen und Souveränitätsnotwendigkeiten, erfordern ein ständiges (Re-)Agieren. Gerade in Bezug auf die weiteren Rechtsakte der Europäischen Union beispielsweise zu KI, Datennutzung oder Cybersicherheit **muss das Wechselspiel mit dem Datenschutzrecht austariert werden**.

Vielleicht passt die Analogie zu einem Chor mit dem Einsingen oder einem Sportteam mit dem Aufwärmen: Jede Vorbereitungsphase kostet Zeit, sie ist aber auch nötig, damit die Qualität der darauffolgenden Performance stimmt und möglichst keine Pannen passieren. Dazu dient eigentlich die Übergangszeit, die der europäische Gesetzgeber einräumt. Bei der DSGVO war diese Übergangszeit von zwei Jahren unmittelbar vor dem 25.05.2018 nicht perfekt genutzt worden. Dies hängt auch mit der **Herstellerlücke der DSGVO** (Tz. 2.4) zusammen, denn die Hersteller sind nicht Verpflichtete nach dem Datenschutzrecht, sondern sollen nur „ermutigt" werden (Erwägungsgrund 78 Satz 4 der DSGVO). Wäre es durch Unterstützung der Hersteller und durch mehr Standardisierung in der Gestaltung und Dokumentation von Anfang an einfach gewesen, die datenschutzrechtlichen Anforderungen zu erfüllen, hätten die Verantwortlichen nicht den Eindruck gehabt, dass jeder für sich das Rad neu hätte erfinden müssen.

Nun stehen **Reformen im europäischen Datenrecht** – einschließlich des Datenschutzrechts – an (Tz. 2.3). Dieses Mal gilt es, die Übergangszeiten effektiv zur Vorbereitung zu nutzen. Die Leitschnur sollte sein: **Rechtskonformität muss leichtfallen** – wer Recht und Gesetz erfüllen will, soll es einfach haben. Dazu gehört es, dass insbesondere Aufsichtsbehörden, Branchenverbände, Kammern, die Regierungen und die Standardisierungsgremien aufzeigen, wie man das europäische Recht in der Praxis umsetzen kann. Im Endeffekt geht es darum, die europäischen Werte, die in der Europäischen Grundrechte-Charta niedergelegt sind, in den technischen und organisatorischen Systemen zu implementieren.

1.2 Zahlen und Fakten

Immer mehr Beschwerden, immer mehr Datenpannen – das Jahr 2025 wartet mit Spitzenwerten auf.

Vor dem Jahr 2018, als die Datenschutz-Grundverordnung wirksam wurde (Tz. 1.1), wussten viele Menschen nicht über ihre Datenschutzrechte Bescheid und wären wahrscheinlich auch nicht auf die Idee gekommen, eine Beschwerde an die Datenschutzaufsichtsbehörde zu senden. Dies hat sich mittlerweile geändert: **Das Datenschutzbewusstsein ist in der Bevölkerung weit verbreitet.** Wer von möglichen Datenschutzverstößen betroffen ist, entwickelt oft eine hohe Sensibilität. Auch wissen viele betroffene Personen, wie sie ihre Rechte geltend machen können. Ein Teil der Beschwerdeführenden lässt sich anscheinend von KI-Systemen beraten, wie sie in Internetsuchmaschinen integriert sind. Wer möchte, kann ein KI-Sprachmodell anweisen, seine Beschwerde fertig auszuformulieren.

In dieser Situation – größeres Datenschutzbewusstsein, Wissen über Aufsichtsbehörden und Beschwerdemöglichkeiten sowie etwaige KI-Unterstützung – hat sich bei uns und anderen Aufsichtsbehörden die Zahl der bearbeiteten Beschwerden deutlich erhöht. Den Trend konnten wir schon im Vorjahr ausmachen, als die Beschwerdezahlen 2024 gegenüber dem Jahr 2023 um 21 Prozent gestiegen waren. Im Jahr 2025 gibt es **mit 2.276 Eingängen einen neuen Spitzenwert** (zum Vergleich: 2021: 1.464, 2022: 1.334, 2023: 1.344, 2024: 1.628). Dies ist eine **Steigerung um knapp 40 Prozent**.

Auch die Zahl der gemeldeten Verletzungen des Schutzes personenbezogener Daten (sogenannte Datenpannen) ist gestiegen: Im Jahr 2025 sind **775 Meldungen** bei uns eingegangen – ein neuer Spitzenwert für die schleswig-holsteinische Datenschutzaufsicht. Im Vergleich zum Vorjahr mit 602 Meldungen handelt es sich um eine Zunahme von 29 Prozent.

Im Folgenden sind die genauen Zahlen dargestellt: Im Jahr 2025 erreichten uns 2.276 schriftliche **Beschwerden** (Vorjahr: 1.628), von denen 437 (Vorjahr: 301) 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 1.839 (Vorjahr: 1.327) Beschwerden bearbeitet, davon richteten sich **mehr als 80 Prozent der Beschwerden gegen Unternehmen** und andere nichtöffentliche Stellen (1.498; Vorjahr: 1.087), der Rest gegen Behörden (341; Vorjahr: 240). Unsere Beratungsleistung gegenüber Verantwortlichen, Auftragsverarbeitern und betroffenen Personen im öffentlichen und nichtöffentlichen Bereich wurde in 576 Fällen (Vorjahr: 443) in Anspruch genommen.

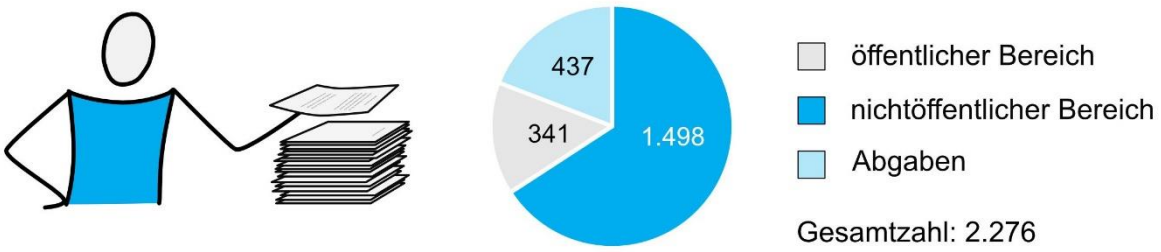


Abb. 1: Zahl der bearbeiteten Beschwerden 2025

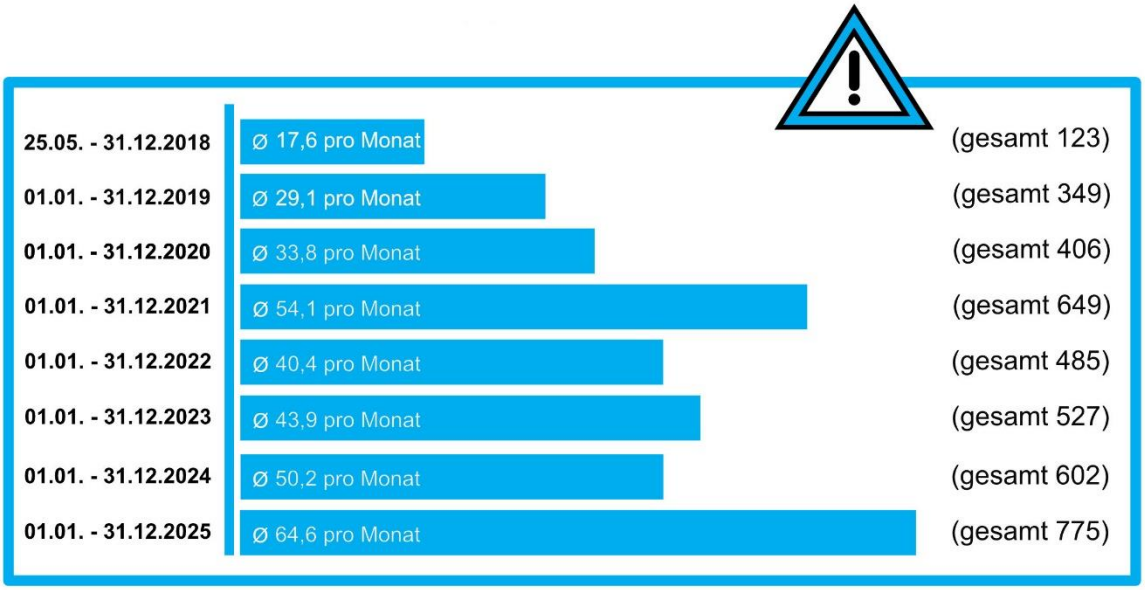


Abb. 2: Zahl der bearbeiteten Meldungen nach Artikel 33 DSGVO 2025

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

Die Zahl von 775 (Vorjahr: 602) **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 signifikant gestiegen. Viele Verantwortliche kennen mittlerweile die Pflicht zur Meldung von Datenpannen, jedoch stellen wir immer wieder in unseren Prüfungen fest, dass die ordnungsgemäßen Meldungen unterblieben sind. Wir gehen von einer hohen Dunkelziffer von Fällen aus, in denen die Verantwortlichen der Meldepflicht nicht nachgekommen sind. Die Gründe dafür sind vielfältig: Unkenntnis, Fehleinschätzungen, eine entgegenstehende Fehlerkultur in der Organisation oder auch nur der Glaube daran, dass das Malheur wohl nicht herauskäme.

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

- 35 Warnungen (Vorjahr: 29),
- 9 Verwarnungen (Vorjahr: 7),
- keine Anordnung zur Änderung oder Einschränkung der Verarbeitung (Vorjahr: 2),
- 5 Geldbußen (Vorjahr: 3) in einer Gesamthöhe von mehr als 280.000 Euro.

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 25 (Vorjahr: 18) neuen Gesetzgebungsvorhaben; einige Themen aus Gesetzgebungsvorhaben des Vorjahres wurden auch im Berichtsjahr weiterverfolgt.

1.3 Weiterentwicklung von LDSG und IZG-SH in Schleswig-Holstein

So oft ändert man Gesetze nicht, jedenfalls nicht, wenn sie im Großen und Ganzen funktionieren: „Never touch a running system". Daher war es auch gar nicht erstaunlich, dass im Berichtsjahr weder ein novelliertes Landesdatenschutzgesetz (LDSG) noch ein novelliertes Informationszugangsgesetz (IZG-SH) beschlossen wurden, obwohl die Anpassungsbedarfe, die aus Sicht meiner Dienststelle bestehen, bereits mitgeteilt wurden (43. TB, Tz. 1.4).

Im Bereich der **Informationsfreiheit** hat das Deutsche Forschungsinstitut für öffentliche Verwaltung Ende 2025 die Evaluation abgeschlossen und einen Bericht vorgelegt, zu dem wir im Jahr 2026 eine Stellungnahme abgeben werden. Unsere wichtigsten Wünsche haben wir bereits im Vorjahr kommuniziert (43. TB, Tz. 12.5):

- **Ausweitung des Geltungsbereichs auf juristische Personen des Privatrechts**, die im Besitz von öffentlichen Stellen sind (z. B. Stadtwerke),
- **Präzisierung** der Vorgaben, unter welchen Bedingungen Anfragen „zu umfangreich" sind,
- Klarstellung, dass **keine pauschale Pflicht zur Identifizierung der Antragsteller** besteht,
- Anregung zu einer **freiwilligen Benennung für die Position von Transparenzbeauftragten**.

Anders als im Informationsfreiheitsrecht bestehen im Bereich des Datenschutzes mit der DSGVO und weiteren Rechtsnormen detaillierte europäische Vorgaben. Die zentralen Begriffe und Instrumente werden auf EU-Ebene definiert, sodass der Landesgesetzgeber im Datenschutzrecht stärker gebunden ist.

Wir hatten vor dem vorzeitigen Koalitionsende auf Bundesebene Ende 2024 auf eine zügige **BDSG-Novellierung** gehofft, die man bei der **LDSG-Novellierung** hätte berücksichtigen kön-

nen, doch durch den Regierungswechsel auf Bundesebene im Februar 2025 hat sich dies verzögert. Nach den Informationen aus der **Föderalen Modernisierungsagenda** (Tz. 2.1) sollen einige Änderungen Ende 2026, andere Ende 2027 umgesetzt sein (Modernisierungsagenda, Seite 31):

https://bmds.bund.de/themen/staatsmodernisierung/modernisierungsagenda-foederal

Kurzlink: *https://uldsh.de/tb44-1-3a*

Wenn der Schleswig-Holsteinische Landtag die LDSG-Novelle noch in dieser Legislaturperiode beschließen möchte, die im Frühjahr 2027 endet, wäre es zu spät, erst nach Verabschiedung der BDSG-Änderungen damit anzufangen. Natürlich ist es aber sinnvoll, die geplanten Änderungen auf Bundesebene schon frühzeitig in Erfahrung zu bringen und – soweit Anpassungen auf Landesebene nötig oder sinnvoll sind – diese zu berücksichtigen.

In einem Punkt ist aber doch Eile geboten: Zum Ende meiner Amtszeit im September 2026 wäre es vorteilhaft, wenn zumindest die erkannten **Mängel im Errichtungsgesetz ULD schon beseitigt wären**. Das betrifft insbesondere die Situation, wenn nach dem Ablauf der Amtszeit der oder des Landesbeauftragten für Datenschutz keine unmittelbare Nachfolge zur Verfügung steht: Nach Ende der vorgesehenen Übergangszeit von sechs Monaten wären nach der jetzigen Regelung weder der oder die bisherige Landesbeauftragte (§ 6 Abs. 2 Satz 4 Errichtungsgesetz ULD) noch die Stellvertretung (§ 9 Abs. 2 Satz 3 Errichtungsgesetz ULD) berechtigt, die Geschäfte des ULD zu führen. Diese Situation sollte vermieden werden, um die Funktionsfähigkeit der Datenschutzaufsicht zu erhalten.

Der Vollständigkeit halber sei hier außerdem auf zwei Bereiche verwiesen, in denen **Handlungsbedarf** bestehen könnte: zum einen im **parlamentarischen Datenschutz** (siehe ausführlicher in Tz. 3.1) und zum anderen in der **Datenschutzaufsicht im Bereich justizieller Tätigkeiten** (43. TB, Tz. 4.3.2), die nicht von uns wahrgenommen werden kann, sondern von justizeigenen Kontrollstellen übernommen werden sollte (Erwägungsgrund 20 der DSGVO). Solche Kontrollstellen sind jedoch noch nicht eingerichtet worden.

Im vorherigen Berichtsjahr spielte dies in einem Gerichtsverfahren gegen das ULD eine Rolle: Ein Beschwerdeführer hatte Klage erhoben und gefordert, dass das ULD in einem Fall justizieller Tätigkeit den Sachverhalt prüfen und bewerten sollte. Das Schleswig-Holsteinische Verwaltungsgericht stellte am 8. Juni 2024 – 8 A 89/22 fest: „Es ist […] Aufgabe des Gesetzgebers, eine datenschutzrechtliche Kontrolle für den Bereich der justiziellen Tätigkeit zu schaffen." (43. TB, Tz. 4.3.2) Darauf, dass Datenschutzbeschwerden über justizielle Tätigkeiten ins Leere gehen, hatten wir schon unmittelbar nach Wirksamwerden der DSGVO verwiesen (39. TB, Tz. 4.3.5).

Was ist zu tun?

Bei den anstehenden Novellierungen bieten wir unsere Expertise und vor allem die praktischen Erfahrungen als Kontrollbehörde in den Bereichen Datenschutz und Informationszugang an.

1.4 Neue Zuständigkeiten des ULD – vom Zugang zu Produktdaten bis zur politischen Werbung

Seit dem 12. September 2025 gilt die **europäische Datenverordnung**, bekannt unter dem Titel **„Data Act"**. Die Vorschriften regeln die Verarbeitung personenbezogener und nicht personenbezogener **Produktdaten**, welche über vernetzte Produkte erlangt, generiert oder erhoben wurden. Die vernetzten Produkte können etwa Umgebungsinformationen über Sensoren erfas-

sen, Nutzungsinformationen bereitstellen oder Angaben zum Verbrauch und Verschleiß des Produktes erstellen. Die verarbeiteten Produktdaten ermöglichen gegebenenfalls eine verbesserte Fehlerkontrolle oder Fehlernachverfolgung, tragen zur Optimierung bei der Ursachenforschung in Bezug auf die Haltbarkeit und Verwendbarkeit von Verkaufs-, Miet- oder Leasinggegenständen bei und reduzieren durch eine effizientere Schwachstellenanalyse den Aufwand der Fehlerbehebung. Die Palette der vernetzten Produkte reicht von Alltagsgegenständen, wie z. B. einer elektrischen Zahnbürste, bis zum Einsatz von Maschinen in industriellen Herstellungsverfahren. Vernetzte Produkte sind durch eine **technische Schnittstelle** gekennzeichnet, über welche die Produktdaten abrufbar sind, wofür ein elektronischer Kommunikationsdienst bzw. eine Internetverbindung, ein physischer Kontakt oder ein geräteinterner Zugang in Betracht kommen.

Bei den Produktdaten kann es sich um aggregierte bzw. statistische Angaben handeln, wodurch im Falle einer Verarbeitung keine datenschutzrechtlichen Fragestellungen entstehen. Ein Personenbezog ist hingegen denkbar, wenn etwa spezifische Gebrauchs- und Verbrauchsinformationen zu Produkten im Fokus stehen, die auf eine natürliche Person rückführbar sind. Im letzteren Fall wird für die Überwachung und Kontrolle der Datenverarbeitung eine **Zuständigkeit der Datenschutzaufsichtsbehörden** begründet, was der Verordnungsgeber im Data Act zum Ausdruck bringt. Dafür bedarf es keiner nationalen Zuweisung. Die Zuständigkeit der Datenschutzaufsichtsbehörden ergibt sich direkt aus Artikel 37 des Data Acts.

Art. 37 Abs. 3 Data Act

Die für die Überwachung der Anwendung der Verordnung (EU) 2016/679 zuständigen Aufsichtsbehörden sind bezüglich des Schutzes personenbezogener Daten auch für die Überwachung der Anwendung der vorliegenden Verordnung zuständig. Die Kapitel VI und VII der Verordnung (EU) 2016/679 finden sinngemäß Anwendung.

Kontrollzuständigkeiten des ULD können sich im Zusammenhang mit der **Verarbeitung personenbezogener Produktdaten** etwa in folgenden Themengebieten ergeben:

- Rechte und Pflichten von Nutzern und Dateninhabern in Bezug auf den Zugang, die Nutzung und Bereitstellung von Produktdaten,
- Weitergabe von Produktdaten an Dritte und Pflichten der Datenempfänger,
- Verträge zwischen Dateninhabern und Datenempfängern,
- technische Schutzmaßnahmen über die unbefugte Nutzung oder Offenlegung von Daten.

Das ULD hat Informationen zu den neuen aufsichtsbehördlichen Zuständigkeiten im Zusammenhang mit dem Data Act in Form einer Pressemitteilung veröffentlicht:

https://www.datenschutzzentrum.de/artikel/1516-Geltung-des-Data-Act-mit-neuen-Rechten-der-Nutzenden-ULD-erhaelt-weitere-Zustaendigkeit.html

Kurzlink: *https://uldsh.de/tb44-1-4a*

Das **Beschwerdeformular** des ULD, welches auch für Beschwerden nach dem Data Act verwendet werden kann, ist unter diesem Link abrufbar:

https://www.datenschutzzentrum.de/meldungen

Kurzlink: *https://uldsh.de/tb44-1-4b*

Seit dem 10. Oktober 2025 gilt die **Verordnung über die Transparenz und das Targeting politischer Werbung (TTPW-VO)**. Der europäische Verordnungsgeber verfolgt mit der Verordnung das Ziel, Vorgaben

- einschließlich Transparenz- und Sorgfaltspflichten für die Erbringung politischer Werbung und damit verbundener Dienstleistungen sowie gegebenenfalls für Sponsoren über die Erhebung, Speicherung, Offenlegung und Veröffentlichung von Informationen, die mit der Erbringung

solcher Dienstleistungen im Binnenmarkt in Zusammenhang stehen,

- für den Einsatz von Targeting- und Anzeigenschaltungsverfahren, welche die Verarbeitung personenbezogener Daten im Zusammenhang mit der Erbringung politischer Onlinewerbung umfassen,
- über die Überwachung und Durchsetzung dieser Verordnung einschließlich der Zusammenarbeit und Koordinierung der zuständigen Behörden

zu schaffen. Dabei möchte der Verordnungsgeber Risiken mindern, die sich bei der Nutzung von Onlineplattformen und sozialen Netzwerken durch politische Akteure ergeben können, welche **Wahlwerbemaßnahmen** gezielt auf bestimmte Personengruppen abstimmen möchten.

Kontrollzuständigkeiten des ULD können sich etwa in folgenden Bereichen ergeben (Artikel 18 und 19 TTPW-VO):

- spezielle Anforderungen in Bezug auf das Targeting und die Anzeigenschaltung im Zusammenhang mit politischer Werbung im Internet, z. B. Direkterhebungsgebot bei der betroffenen Person, Vorgaben für die Einwilligung zur Datenverarbeitung, Verbot der Wahlwerbung bei Unterschreitung des Wahlalters,
- Transparenzpflichten hinsichtlich des Einsatzes und der Funktionsweise von Targeting- und Anzeigenschaltungsverfahren einschließlich Angaben zu Parametern zur Bestimmung der zu bewerbenden Personenkreise, der verwendeten Datenkategorien, gegebenenfalls zur Verwendung von KI und der Anzahl betroffener Personen.

Die Zuständigkeit des ULD ergibt sich wiederum direkt aus der EU-Verordnung, sodass es keiner nationalen Zuweisung bedarf:

Art. 22 Abs. 1 TTPW-VO

Die Aufsichtsbehörden nach Artikel 51 der Verordnung (EU) 2016/679 oder der Europäische Datenschutzbeauftragte nach Artikel 52 der Verordnung (EU) 2018/1725 sind in ihrem jeweiligen Zuständigkeitsbereich für die Überwachung der Anwendung der Artikel 18 und 19 der vorliegenden Verordnung verantwortlich. Artikel 58 der Verordnung (EU) 2016/679 und Artikel 58 der Verordnung (EU) 2018/1725 gelten sinngemäß. Kapitel VII der Verordnung (EU) 2016/679 findet Anwendung auf Maßnahmen nach den Artikeln 18 und 19 der vorliegenden Verordnung.

Das oben verlinkte Beschwerdeformular kann auch für Beschwerden in Bezug auf Verletzungen der Artikel 18 und 19 TTPW-VO verwendet werden.

Noch nicht gesetzlich festgelegt ist übrigens die **Zuständigkeit der Marktüberwachungsbehörde nach der KI-Verordnung für KI-Systeme** in den Bundesländern. Ob diese Rolle den Landesbeauftragten für Datenschutz zugewiesen wird, soll im Jahr 2026 geklärt sein. Unabhängig davon wird die Zuständigkeit der Landesbeauftragten für Datenschutz für die Überwachung der Verarbeitung von personenbezogenen Daten nach der DSGVO auch in Bezug auf den KI-Einsatz im Land bestehen.

Was ist zu tun?

Mit den neuen Zuständigkeiten für die Kontrolle von Vorgaben nach dem Data Act und der TTPW-VO im Kontext der Verarbeitung personenbezogener Daten erhält das ULD zusätzliche Aufgaben, die mit dem zur Verfügung stehenden Personal erledigt werden müssen. Derzeit ist noch nicht absehbar, ob der Aufgabenzuwachs zu einem nennenswerten zusätzlichen Zeit- und Arbeitsaufwand führt. Das ULD wird den Umfang eingehender Anfragen evaluieren und anschließend darüber berichten.

1.5 Die Datenschutzbeauftragten vor Ort: wichtige Stütze, Entlastung vor Ort

In Deutschland sind sie seit 1977, als sie im BDSG verankert wurden, eine Erfolgsstory: die **betrieblichen und behördlichen Datenschutzbeauftragten**, die vor Ort überall dort unterstützen, wo Datenschutzkenntnisse gefragt sind. Mit der Datenschutz-Grundverordnung wurde die Rolle der Datenschutzbeauftragten geschärft – sie setzen nicht selbst operativ die Datenschutzanforderungen um, sondern prüfen und beraten.

Aus Sicht der Datenschutzaufsichtsbehörde sind die Datenschutzbeauftragten wichtige Ansprechpartner. Wenn ihre Expertise in die Gestaltung der Verarbeitung eingeflossen ist, wirkt dies etwaigen datenschutzrechtlichen Verstößen und Datenschutzverletzungen entgegen. Passiert doch etwas, wissen die Datenschutzbeauftragten, was zu tun ist, z. B. in Bezug auf die Melde- und Benachrichtigungspflichten. Und ist die Situation unklar, können sie sich an die Datenschutzaufsichtsbehörden wenden und sich beraten lassen.

Aber auch für die Verantwortlichen, die – wie die Bezeichnung im Deutschen schon nahelegt – ihre Verantwortung für die Erfüllung der DSGVO nicht delegieren können, sind die betrieblichen und behördlichen Datenschutzbeauftragten wertvoll. Denn die Leitung hat selten Zeit, sich persönlich im Detail darum zu kümmern, dass alle Rechtsvorschriften – übrigens nicht nur im Datenschutz – eingehalten werden. Hier ist die Unterstützung durch die Datenschutzbeauftragten wesentlich. Sie erkennen **die Risiken für die Rechte und Freiheiten natürlicher Personen** und können einschätzen, inwieweit diese Risiken **durch Umsetzung geeigneter technischer und organisatorischer Schutzmaßnahmen eingedämmt werden können**. Und sie sind Ansprechpartner für betroffene Personen und für Mitarbeitende, die Datenschutzfragen haben. Nach unserer Erfahrung tragen Datenschutzbeauftragte dazu bei, dass bei etwaigen Datenschutzproblemen unangenehme und vor allem ressourcenaufwendige Eskalationssituationen vermieden werden.

Aus diesen Gründen sehen wir mit Sorge, dass sich Bund und Länder in der Föderalen Modernisierungsagenda (Tz. 2.1) vorgenommen haben, die Zusatzregeln im BDSG zu Datenschutzbeauftragten, die sich nach unserer Ansicht schon in den Vorgängerregelungen über viele Jahrzehnte bewährt haben, zurückzunehmen:

> **Föderale Modernisierungsagenda, Nr. 160**
>
> **2.2 Beschränkung der Pflicht zur Bestellung von Datenschutzbeauftragten**
>
> Der Bund wird bis zum 31.12.2026 eine Aufhebung des § 38 Abs. 1 BDSG einbringen und damit die Pflicht zur Bestellung von Datenschutzbeauftragten im nichtöffentlichen Bereich auf die Regelung in Artikel 37 DSGVO beschränken.

Wird § 38 Abs. 1 BDSG abgeschafft, gelten jedoch immer noch die Regeln des Artikels 37 DSGVO, nach dem die Benennung einer oder eines Datenschutzbeauftragten verpflichtend ist, wenn es sich um eine öffentliche Stelle handelt oder wenn die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, die mit einem höheren Risiko verbunden ist, beispielsweise bei einer umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 DSGVO.

> **§ 38 Abs. 1 Satz 1 BDSG Datenschutzbeauftragte nichtöffentlicher Stellen**
>
> (1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. […]

Jedenfalls muss allen Verantwortlichen bewusst sein, dass sie ohne eine Datenschutzbeauftragte und ohne einen Datenschutzbeauftragten dieselben datenschutzrechtlichen Anforderungen

erfüllen müssen. Nur stellt sich die Frage, ob dies mit oder ohne kundigen Berater oder kundige Beraterin umgesetzt wird und wer im Falle des Falles – bei Datenpannen, Beratungserfordernissen der Beschäftigten oder für Beschwerden – Ansprechstelle ist.

1.6 Beratung für die öffentliche Verwaltung

Der EU-Verordnungsgeber weist den Datenschutzaufsichtsbehörden vordergründig die Aufgabe zu, die **Anwendung der Datenschutz-Grundverordnung zu überwachen und durchzusetzen**. In diesem Kontext führt das ULD Prüfverfahren durch und muss anhand des anwendbaren Verfahrensrechts entscheiden, welche präventiven oder repressiven Maßnahmen zu ergreifen sind.

Die Aufgabenwahrnehmung erschöpft sich jedoch nicht im **Verhängen von Zwangs- und Bußgeldern**. Vielmehr obliegt dem ULD auch die Aufgabe, im Einklang mit dem Recht des Mitgliedstaats das nationale Parlament, die Regierung und andere Einrichtungen und Gremien **über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen** in Bezug auf die Verarbeitung **zu beraten** (Art. 57 Abs. 1 Buchst. c DSGVO). **Legislative Maßnahmen** beziehen sich in diesem Zusammenhang auf den Erlass von Gesetzen und Rechtsverordnungen. Als **administrative Maßnahmen** kommen etwa Weisungen der Ministerien an untergeordnete Dienststellen in Ausübung ihrer Fach- und Rechtsaufsicht in Betracht, wenn eine bestimmte Maßgabe zum Umgang mit personenbezogenen Daten oder zur Gewährleistung der Sicherheit in der Datenverarbeitung erteilt werden soll. Erfasst sind z. B. auch Rechtsverordnungen oder Erlasse. Da die maßgebliche Vorschrift in der DSGVO neben dem nationalen Parlament und der Regierung auch andere Gremien und Einrichtungen erwähnt, zählen im Grundsatz die Träger der öffentlichen Verwaltung in Schleswig-Holstein hinzu, namentlich das Land, die Gemeinden, die Kreise und die Ämter einschließlich die der Aufsicht des Landes unterstehenden Körperschaften des öffentlichen Rechts ohne Gebietshoheit und rechtsfähige Anstalten und Stiftungen des öffentlichen Rechts. Eingeschlossen sind letztlich auch die Landesbehörden.

Die Beratung kann sich auch auf die **Ausgestaltung der Verwaltungsabläufe** beziehen, z. B. im Rahmen der Verfolgung politischer Zielsetzungen bezüglich der Digitalisierung der Verwaltung.

Die Vorteile einer Beratung liegen auf der Hand: Im Rahmen der Konzeptionierung neuer Datenverarbeitungsverfahren, der Schaffung neuer Rechtsvorschriften, von Fragen zu vertraglichen Vereinbarungen und der damit verbundenen Anforderungen z. B. zu Rechtsgrundlagen, zur Einhaltung von Informationspflichten, der Gestaltung von Formularen und zur Gewährleistung der Datensicherheit kann das ULD einerseits die **Rahmenvorgaben** erläutern und andererseits nach Möglichkeit **praktische Tipps und Empfehlungen** wie etwa Formulierungshilfen sowie Hinweise zur Vereinfachung und rechtskonformen, transparenten Gestaltung von Verarbeitungsverfahren geben. In den Fällen eingehender Beschwerden zu bereits umgesetzten Verarbeitungsverfahren, die sich im Einzelfall als nicht datenschutzkonform erweisen, kann das ULD hingegen nur noch eingeschränkt oder überhaupt nicht beraten, sondern wird von Amts wegen nur die vom EU-Verordnungsgeber zugewiesene Aufgabe der Überwachung und Durchsetzung wahrnehmen können. Die Beratung kann auch dazu dienen, **Datenpannen und die damit oft verbundenen Reputationsverluste zu vermeiden.**

Die Beratungskonzeption umfasst folgende Punkte:

- Ziel der Beratung ist es, Entscheidungsträger bei der Planung und Umsetzung datenschutzrechtlicher Vorgaben zu unterstützen.
- Zur Zielgruppe zählen die Träger öffentlicher Verwaltung bzw. deren Landesbehörden.

- Zu den Formaten der Beratung gehören z. B. die Teilnahme an Gesprächsrunden, die Beteiligung im Vorfeld von Gesetzes- und Verordnungsvorhaben, die Abgabe von Stellungnahmen und Einschätzungen zu Einzelfragen, das Angebot von Vorträgen und Seminaren, die Erweiterung des Informationsangebots sowie die Teilnahme an Arbeitskreisen. Das ULD hat zu den erwähnten Formaten bereits sehr positive Erfahrungen gesammelt.
- Zu den Beratungsstandards zählen eine unabhängige Beratung, die Sicherstellung der Fachlichkeit und Qualifikation von Beratungspersonen, die Verfolgung lösungsorientierter Ansätze im Rahmen der rechtlichen Rahmenvorgaben sowie eine offene und konstruktive Beratungsatmosphäre.

Was ist zu tun?

Das ULD wird sein Beratungsangebot für die Träger der öffentlichen Verwaltung auf Grundlage der bestehenden Konzeption im Rahmen der personellen und zeitlichen Möglichkeiten weiter ausbauen.

1.7 Öffentlichkeitsarbeit

Im Berichtszeitraum wurde im Rahmen der Öffentlichkeitsarbeit durch verschiedene Maßnahmen die Kommunikation mit Bürgerinnen und Bürgern, öffentlichen Stellen des Landes und Unternehmen gepflegt. Ziel ist es, die Öffentlichkeit für die Risiken, Vorschriften und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären.

1.7.1 Informationsmaterialien

Das ULD stellt eine Vielzahl von Informationsmaterialien in digitaler und gedruckter Form zur Verfügung. Dies sind u. a.:

- Themenhefte Praxis-Reihe:
  Datenschutzbestimmungen praktisch umsetzen für öffentliche Stellen und Unternehmen
  Nr. 1: Datenschutz bei Vereinen
  Nr. 2: Datenschutzbeauftragte
  Nr. 3: Mustervereinbarung für einen Vertrag zur Auftragsverarbeitung
  Nr. 4: Informationspflichten
  Nr. 5: Videoüberwachung
  Nr. 6: Fotos und Webcams
  Nr. 7: Informationszugangsgesetz für das Land Schleswig-Holstein (IZG-SH)
- Broschüre „Datenschutz und Sozialarbeit in Schulen“
- Faltblatt „Datenschutz im Melderecht“
- Gesetzestext „Datenschutz-Grundverordnung (DSGVO)“
- Gesetzestext „Landesdatenschutzgesetz (LDSG)“ und „Bundesdatenschutzgesetz (BDSG)“

Die Informationsmaterialien können als gedruckte Broschüre beim ULD bestellt oder online auf der Website abgerufen werden:

https://www.datenschutzzentrum.de/informationsmaterial/

Kurzlink: *https://uldsh.de/tb44-1-7-1a*

1.7.2 Veranstaltungen

Das ULD hat eine Reihe von Veranstaltungen durchgeführt und sich an Veranstaltungen beteiligt. Dies waren u. a.:

- Fünf Einzelveranstaltungen im Rahmen der Digitalen Woche (13. bis 16. Mai 2025) im ULD
- Tag der offenen Tür im Schleswig-Holsteinischen Landtag mit einem Informationsstand, 13. Juli 2025
- Datenschutzkonferenz 2025 „Im Alarmmodus: Sicherheit und Datenschutz?“ am 8. September 2025 in Kiel (Tz. 13.2)
- Medienkompetenz-Festival mit einem Informationsstand, 10. und 11. Oktober 2025 in Kiel
- Fachveranstaltung: Austausch rund um KI und Datenschutz „Frag‘ für n‘ Freund“ an vier Terminen 2025 im ULD (Tz. 6.3.3)
- Schulveranstaltungen „Entscheide DU, sonst tun es andere für Dich!“ für Schülerinnen und Schüler ab Klassenstufe 5 vor Ort in der Schule (Tz. 13.1)
- Vielzahl an Fortbildungsveranstaltungen für Datenschutz (Tz. 13.1)

1.7.3 AK Presse-und Öffentlichkeitsarbeit

Die Datenschutzbehörden der Länder und des Bundes organisieren ihre Zusammenarbeit in regelmäßig tagenden Arbeitskreisen (AK). Im Bereich der Außenkommunikation ist dies der AK Presse- und Öffentlichkeitsarbeit.

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

Im Berichtszeitraum waren die wichtigsten Themen des Arbeitskreises u. a. ein **Austausch zu einer Kommunikationsstrategie für die Datenschutzkonferenz (DSK)** und Diskussion zu der Presse- und Öffentlichkeitsarbeit in den einzelnen Häusern. Weiterer Punkt war u. a. **gemeinsame Präsenz auf zentralen Messeveranstaltungen** zu unterschiedlichen Themenbereichen des Datenschutzes.

Das ULD beteiligt sich aktiv an der Arbeit und den Treffen des AK Presse- und Öffentlichkeitsarbeit.

02

KERNPUNKTE

Koalitionsvertrag und Modernisierungsagenda

Geschenke aus dem Cybersicherheitsrecht

Herstellerverantwortung

Datenschutzreform und die Büchse der Pandora

2 Datenschutz und Informationsfreiheit – global und national

Datenschutz in Schleswig-Holstein ist nicht zu trennen von den Entwicklungen auf Bundesebene, in Europa und schließlich auch international. Dies gilt jedenfalls für Rechtsänderungen oder Technikentwicklungen. Das ULD ist über die **Konferenz der unabhängigen Datenschutzaufsichtsbehörden (DSK)** auf nationaler Ebene und über den **Europäischen Datenschutzausschuss** auf europäischer Ebene in die Abstimmung zwischen den Datenschutzbehörden eingebunden. Alles ist im Wandel – das zeigt sich besonders in diesem Kapitel, das auf die Weiterentwicklung des Datenschutzes in Deutschland (Tz. 2.1), die Positionen der Datenschutzkonferenz (Tz. 2.2), die Entwicklungen des Cybersicherheitsrechts (Tz. 2.3), den vielleicht schon in greifbare Nähe gerückten Punkt der Herstellerverantwortung (Tz. 2.4) und die anstehende Datenschutzreform auf europäischer Ebene (Tz. 2.5) eingeht.

2.1 Datenschutz zwischen Koalitionsvertrag und Modernisierungsagenda

Der Koalitionsvertrag des Bundes ist für die Bundesangelegenheiten maßgeblich – und das betrifft vor allem **Novellierungsbedarfe im Bundesdatenschutzgesetz (BDSG)**. Nachdem im Koalitionsvertrag der vorherigen Regierung bereits geplant war, die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu institutionalisieren, jedoch das Projekt keine großen Fortschritte gemacht hatte, waren wir gespannt, was die neue Koalition zum Datenschutz vereinbaren würde. Die Zusammenarbeit in der Datenschutzkonferenz ist wesentlich, damit wir uns optimal abstimmen und auch arbeitsteilig ressourcensparend arbeiten können.

Über die Datenschutzkonferenz

Die Datenschutzkonferenz besteht aus den unabhängigen Datenschutzbehörden des Bundes und der Länder. Sie 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. […]

Nach unseren Vorstellungen ist dringend geboten, die Arbeit der Datenschutzkonferenz weiter zu professionalisieren, insbesondere durch eine **Geschäftsstelle** (43. TB, Tz. 1.5). Insoweit ist begrüßenswert, dass die Verankerung der Datenschutzkonferenz auch im Koalitionsvertrag 2025 vorgesehen ist. Auch das dort genannte Ziel, „gemeinsame Standards zu erarbeiten", passt zu der Arbeitsweise der Datenschutzkonferenz und zu ihren Plänen.

Koalitionsvertrag 2025, Zeilen 2248–2252

Reform des Datenschutzes

Wir reformieren die Datenschutzaufsicht. Die Datenschutzkonferenz (DSK) verankern wir im Bundesdatenschutzgesetz (BDSG), um gemeinsame Standards zu erarbeiten. Wir nutzen alle vorhandenen Spielräume der DSGVO, um beim Datenschutz für Kohärenz, einheitliche Auslegungen und Vereinfachungen für kleine und mittlere Unternehmen, Beschäftigte und das Ehrenamt zu sorgen.

Eine andere Stelle im Koalitionsvertrag ließ jedoch aufhorchen: Auf Bundesebene werde „im Interesse der Wirtschaft" die **Bündelung der Zuständigkeiten und Kompetenzen bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)** angestrebt. Die

Formulierungen eröffnen einen großen Interpretationsspielraum: Sollen die zigtausenden Beschwerden, die im nichtöffentlichen Bereich bei den Landesbeauftragten eingereicht werden, künftig durch die BfDI bearbeitet werden? Ist dies überhaupt im Interesse der Wirtschaft? Und welche „Wirtschaft" ist überhaupt gemeint: die großen Konzerne oder auch die kleinen und mittleren Unternehmen (KMU), die für die Firmenkultur in Deutschland prägend sind?

Koalitionsvertrag 2025, Zeilen 2253–2255

Im Interesse der Wirtschaft streben wir eine Bündelung der Zuständigkeiten und Kompetenzen bei der Bundesdatenschutzbeauftragten an. Sie soll dann Bundesbeauftragte für Datennutzung, Datenschutz und Informationsfreiheit sein.

Nach unseren Erfahrungen profitieren KMU von der Erreichbarkeit und Nähe vor Ort, beispielsweise wenn es um Teilnahme an unseren Veranstaltungen wie der Sommerakademie (Tz. 13.2) oder den niedrigschwelligen Veranstaltungen wie „Frag´ für ´nen Freund (Tz. 6.3.3) geht. Der Weg nach Bonn, wo die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ihren Sitz hat, ist weit.

Die Idee der Bündelung kann aber auch ganz anders verstanden werden, z. B. wenn die recht seltenen Fälle, in denen mehrere Datenschutzaufsichtsbehörden zuständig sind, oder die häufigeren Fälle, in denen Sachverhalte der Verarbeitung personenbezogener Daten in vielen oder allen Ländern ähnlich ablaufen, jeweils von einer federführenden Aufsichtsbehörde übernommen und bearbeitet werden. Das Prinzip EfA („Einer für alle") kann unter den Datenschützern zu „Epfa – Einer prüft für alle" werden. Behörden suchen sich allerdings ihre Zuständigkeiten nicht selbst aus, sondern diese müssen vom Gesetzgeber zugewiesen werden.

Dies erscheint durchaus realistisch, weil der Koalitionsvertrag im Herbst 2025 durch die **Föderale Modernisierungsagenda** ergänzt wurde, die konkrete Handlungspunkte enthält. So liest man beim Punkt 158:

Föderale Modernisierungsagenda, Nr. 158

1. Reform der Datenschutzaufsicht

Der Bund wird in Abstimmung mit den Ländern die Datenschutzaufsicht für den nichtöffentlichen Bereich bis spätestens 31.12.2027 reformieren und dabei gegebenenfalls auch die Aufgabenverteilung im Föderalstaat neu justieren. Ziel ist die Sicherstellung der **einheitlichen Rechtsauslegung und -anwendung sowie Erhöhung der Effizienz** im Zusammenspiel der Aufsichtsbehörden. Hierzu können insbesondere die **Bündelung von Kompetenzen bei der BfDI oder Aufsichtsbehörden der Länder** (z. B. durch Zuständigkeitskonzentration und/oder One-Stop-Shop-Regelungen), eine bessere Einbindung der DSK und/oder die Einführung eines Kohärenzverfahrens unter Nutzung der Möglichkeiten des Art. 87 Abs. 3 GG auf Bundesebene oder im Wege von Staatsverträgen zwischen den Ländern gehören. […]

Zum Zusammenspiel der Aufsichtsbehörden bieten wir dem Bundesgesetzgeber gern an, unsere Erfahrungen in die Diskussion einzubringen. Dies betrifft übrigens nicht nur die Zusammenarbeit in der Datenschutzkonferenz, sondern auch den Dialog mit anderen Aufsichtsbehörden im Datenschutz und zu Themen mit Überschneidungen zu unseren Kompetenzen, beispielsweise mit der Bundesnetzagentur, dem Bundeskartellamt oder der Medienaufsicht.

Den Link zum Koalitionsvertrag finden Sie unter:

https://www.koalitionsvertrag2025.de/

Kurzlink: *https://uldsh.de/tb44-2-1a*

Der Link zur Föderalen Modernisierungsagenda ist hier verfügbar:

https://bmds.bund.de/themen/staatsmodernisierung/modernisierungsagenda-foederal

Kurzlink: *https://uldsh.de/tb44-2-1b*

2.2 Die Ergebnisse der DSK im Jahr 2025 im Überblick

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat vielfältige Themen diskutiert und Festlegungen zu Positionierungen oder Orientierungshilfen abgestimmt. Im Folgenden werden die Veröffentlichungen der Datenschutzkonferenz aus dem Jahr 2025 aufgelistet:

- 26.03.2025: Entschließung „Eckpunkte für eine freiheitliche und grundrechtsorientierte digitale Zukunft"

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

  Kurzlink: *https://uldsh.de/tb44-2-2a*

- 28.05.2025: Beschluss „Meldung von Mieter:innendaten an Grundversorger"

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

  Kurzlink: *https://uldsh.de/tb44-2-2b*

- 16.06.2025: Entschließung „Ohne Sicherheit keine Freiheit – Ohne Freiheit keine Sicherheit"

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

  Kurzlink: *https://uldsh.de/tb44-2-2c*

- 16.06.2025: Entschließung „Confidential Cloud Computing"

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

  Kurzlink: *https://uldsh.de/tb44-2-2d*

- 16.06.2025: „Datenschutz bei der Terminverwaltung durch Heilberufspraxen – Positionspapier zum datenschutzkonformen Einsatz von Dienstleistern für Onlineterminbuchungen und das Terminmanagement"

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

  Kurzlink: *https://uldsh.de/tb44-2-2e*

- Juni 2025: Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen, Version 1.0

  https://www.datenschutzkonferenz-online.de/media/oh/DSK-OH_KI-Systeme.pdf

  Kurzlink: *https://uldsh.de/tb44-2-2f*

- 17.09.2025: Entschließung „Automatisierte Datenanalyse durch Polizeibehörden verfassungskonform gestalten!"

  https://www.datenschutzkonferenz-online.de/media/en/2025-09-17_DSK-Entschliessung_Automatisierte-Datenanalyse.pdf

  Kurzlink: *https://uldsh.de/tb44-2-2g*

- September 2025: Beschluss „Anwendungshinweise zu den Anforderungen an Datenübermittlungen an Drittländer im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken"

  https://www.datenschutzkonferenz-online.de/media/oh/20250917_DSK_OH_Datenuebermittlungen.pdf

  Kurzlink: *https://uldsh.de/tb44-2-2h*

- September 2025: Beschluss „Empfehlungen für Informationspflichten bei Datenübermittlungen an Drittländer im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken (Anlage zu Orientierungshilfe zu Anwendungshinweisen)“

  https://www.datenschutzkonferenz-online.de/media/oh/20250917_DSK_OH_Datenuebermittlungen_Anlage.pdf

  Kurzlink: *https://uldsh.de/tb44-2-2i*

- Oktober 2025: Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode, Version 1.0

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

  Kurzlink: *https://uldsh.de/tb44-2-2j*

- 17.11.2025: Anforderungen an datenschutzrechtliche Zertifizierungsprogramme – Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6), Version 3.0 (17.11.2025), siehe auch Tz. 9.4

  https://www.datenschutzkonferenz-online.de/media/ah/DSK_Zertifizierungskriterien_Version_3_0.pdf

  Kurzlink: *https://uldsh.de/tb44-2-2k*

- 20.11.2025: Entschließung „Verbesserung des Datenschutzes von Kindern in der Datenschutz-Grundverordnung“

  https://www.datenschutzkonferenz-online.de/media/en/Entschliessung_Datenschutz-von-Kindern.pdf

  Kurzlink: *https://uldsh.de/tb44-2-2l*

- 12.12.2025: Entschließung „DSGVO-Reform: Rechtssicherheit und Innovation gehen Hand in Hand – Anpassungen für KI erforderlich“

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

  Kurzlink: *https://uldsh.de/tb44-2-2m*

- 12.12.2025: Entschließung „DSGVO-Reform: IT-Hersteller in die Verantwortung nehmen!“

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

  Kurzlink: *https://uldsh.de/tb44-2-2n*

- Dezember 2025: Beschluss „Standardisierter Prüfprozess zu datenschutzrechtlichen Anforderungen bei EfA-Onlinediensten nach Onlinezugangsgesetz (OZG)“

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

  Kurzlink: *https://uldsh.de/tb44-2-2o*

- Dezember 2025: Orientierungshilfe zu ausgewählten Fragestellungen des neuen Onlinezugangsgesetzes (OZG) – Anwendungshilfe für Stellen, die (länderübergreifende) Onlinedienste nach OZG betreiben oder nutzen, Version 1.1

  https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_OZG_Version_1_1.pdf

  Kurzlink: *https://uldsh.de/tb44-2-2p*

- Dezember 2025: Orientierungshilfe zur Zusammenarbeit mehrerer Aufsichtsbehörden im Rahmen von § 5 GDNG, Version 1.0

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

  Kurzlink: *https://uldsh.de/tb44-2-2q*

2.3 Geschenke für den Datenschutz aus dem Cybersicherheitsrecht

Die DSGVO gilt zwar nicht nur für die automatisierte Verarbeitung von personenbezogenen Daten, aber mit der zunehmenden Digitalisierung aller Lebensbereiche findet ein Großteil der Verarbeitung auf vernetzten (oder vernetzbaren) Computern statt. Unabhängig davon, ob personenbezogene Daten betroffen sind oder nicht, sollte eine angemessene Sicherheit der Verarbeitung eine Selbstverständlichkeit sein.

Die DSGVO nimmt dies im Datenschutzgrundsatz Art. 5 Abs. 1 Buchst. f DSGVO auf: „Integrität und Vertraulichkeit" müssen gewährleistet sein. Artikel 32 DSGVO beschäftigt sich im Detail mit der Sicherheit. Artikel 25 DSGVO fordert die Gestaltung der Verarbeitung gemäß allen Datenschutzgrundsätzen; die Sicherheit spielt hier also auch hinein. Und auch bei Auftragsverarbeitern gehört **Sicherheit der Verarbeitung** zu den rechtlichen Standardanforderungen.

Cybersicherheit by Design war lange Zeit für den Großteil der Hard- und Softwareentwicklungen graue Theorie. Angesichts der Bedrohungslage durch Cyberangriffe aus vielfältiger Motivation und der riesigen Zahl bekannt gewordener Schwachstellen gewinnt die **Cybersicherheitsstrategie** der EU an Bedeutung.

Für kritische Infrastrukturen fordert die Umsetzung der **NIS-2-Richtlinie** mit technischen und organisatorischen Maßnahmen das angemessene Sicherheitsniveau ein. Noch interessanter ist aber die **Cyberresilienz-Verordnung (Cyber Resilience Act, CRA)**, die für alle vernetzbaren Produkte (sogenannte „Produkte mit digitalen Elementen") gilt. Zum einen wird damit ein Schwachstellenmanagement mit Updates für einen definierten Zeitraum (mindestens fünf Jahre), zum anderen Cybersicherheit by Design verlangt:

Anhang I des CRA (Grundlegende Cybersicherheitsanforderungen), Teil 1

(1) Produkte mit digitalen Elementen werden so konzipiert, entwickelt und hergestellt, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten.

Als Daumenregel im CRA gilt: **Je risikoreicher die Produkte, desto mehr müssen die Hersteller nachweisen, dass sie die Cybersicherheitsanforderungen erfüllen.** Bei geringem Risiko können Selbstbestätigungen ausreichen, doch bei einem höheren Risiko kann es erforderlich sein, dass Dritte, gegebenenfalls im Rahmen einer Zertifizierung, die Compliance mit den Anforderungen der Cyberresilienz-Verordnung bestätigen.

Für den Datenschutzbereich ist praktisch, dass Vertraulichkeit, Integrität und Verfügbarkeit aus Cybersicherheitssicht zu den Designzielen gehören (Anhang I, Teil I Abs. 2 CRA). Der Schulterschluss geht aber sogar darüber hinaus: Interessanterweise kennt das Cybersicherheitsrecht ebenfalls die Anforderung der **Datenminimierung**.

Anhang I, Teil I, Abs. 2 Buchst. g CRA

(2) Auf der Grundlage der Bewertung der Cyber-sicherheitsrisiken gemäß Artikel 13 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend,

[…]

g) die Verarbeitung personenbezogener oder sonstiger Daten auf solche, die angemessen und von Bedeutung sind, und auf das für die Zweckbestimmung des Produkts mit digitalen Elementen erforderliche Maß beschränken („Datenminimierung"), […]

Dies erklärt sich daraus, dass ein Zuviel an Daten bzw. an Datenverarbeitung ein Sicherheitsrisiko darstellen kann.

Natürlich muss der Hersteller auch nachweisen können, dass die Sicherheitsziele umgesetzt wurden. Dies wird in der sogenannten technischen Dokumentation niedergelegt (zum Umfang siehe Anhang VII des CRA). Darin müssen auch die Konzeption, Entwicklung und Herstellung des Produkts mit digitalen Elementen und der Verfahren zur Behandlung von Schwach-

stellen beschrieben und das Produkt in Bezug auf Cybersicherheitsrisiken bewertet werden. Die Datenschutzfragen, welche Daten wo wie verarbeitet werden und wie lange sie gespeichert bleiben, spielen dort selbstverständlich hinein. Wo heutzutage den Verantwortlichen oft Informationen über die Verarbeitungssysteme fehlen und sie damit Probleme haben, die Rechenschaftspflicht nach Art. 5 Abs. 2 und Art. 24 Abs. 1 DSGVO zu erfüllen, müssen beim Hersteller künftig gewisse Informationen dazu vorliegen. Hier gilt es, die aus Datenschutzsicht relevanten Informationen abzufragen oder sich, z. B. im Falle einer Ausschreibung zur Beschaffung, vorlegen zu lassen.

Ebenfalls wertvoll sind die **Informationen und Anleitungen für den Nutzer**, die in Anhang II des CRA definiert werden:

Anhang II CRA

Dem Produkt mit digitalen Elementen muss mindestens Folgendes beigefügt sein:

[…]

4. die Zweckbestimmung des Produkts mit digitalen Elementen, einschließlich des vom Hersteller bereitgestellten Sicherheitsumfelds, sowie die Hauptfunktionen des Produkts und Informationen über die Sicherheitseigenschaften;

5. alle bekannten oder vorhersehbaren Umstände im Zusammenhang mit der Zweckbestimmung des Produkts mit digitalen Elementen oder dessen vernünftigerweise vorhersehbaren Fehlanwendung, die zu erheblichen Cybersicherheitsrisiken führen können;

[…]

7. die Art der vom Hersteller angebotenen technischen Sicherheitsunterstützung und das Enddatum des Unterstützungszeitraums, in dem die Nutzer die Behebung von Schwachstellen und den Erhalt von Sicherheitsaktualisierungen erwarten können;

8. ausführliche Anleitungen oder eine Internetadresse, unter der auf solche ausführlichen Anleitungen und Informationen verwiesen wird, dazu,

a) welche Maßnahmen bei der ersten Inbetriebnahme und während der gesamten Lebensdauer des Produkts mit digitalen Elementen getroffen werden müssen, um dessen sichere Verwendung sicherzustellen,

b) wie sich Änderungen am Produkt mit digitalen Elementen auf die Datensicherheit auswirken können,

c) wie sicherheitsrelevante Aktualisierungen installiert werden können,

d) wie eine sichere Außerbetriebnahme des Produkts mit digitalen Elementen erfolgt und wie Nutzerdaten sicher entfernt werden können;

[…]

9. für den Fall, dass der Hersteller dem Nutzer die Softwarestückliste zur Verfügung stellt, wo auf die Softwarestückliste zugegriffen werden kann.

Besonders die Informationen über die Sicherheitseigenschaften sowie darüber, wie eine sichere Inbetriebnahme und Außerbetriebnahme erfolgen können, werden in der Praxis hilfreich sein.

Die **Cyberresilienz-Verordnung** gilt vollständig ab dem 11.12.2027. Nach unserer Einschätzung wird sie wertvoll für Verantwortliche und Auftragsverarbeiter sein, weil das reale Cybersicherheitsniveau deutlich steigen und die Systeme weniger verwundbar sein dürften. Insbesondere werden die Informationen über die Sicherheitseigenschaften, die der Hersteller über die Produkte in den verschiedenen Phasen der Konzeption, der Entwicklung, der Herstellung und der Verwendung zu dokumentieren hat, den Verantwortlichen in seiner datenschutzrechtlichen Rechenschaftspflicht unterstützen. Alles in allem

sind dies Geschenke für den Datenschutz, die das Cybersicherheitsrecht schaffen wird.

Aber Achtung: Auch bei Geschenken muss der Verantwortliche genau hinschauen, ob sie kompatibel mit den Anforderungen der DSGVO sind (Stichworte Rechtsgrundlagen, Informationspflichten, Betroffenenrechte). Nicht jede Sicherheitsmaßnahme ist in jeder Konfiguration auch datenschutzkonform, beispielsweise wenn damit Eingriffe in die Rechte und Freiheiten von Kundinnen und Kunden oder Beschäftigten verbunden sind.

Hier finden Sie den Link zur Cyberresilienz-Verordnung – konsolidierte Fassung:

https://eur-lex.europa.eu/eli/reg/2024/2847/2024-11-20

Kurzlink: *https://uldsh.de/tb44-2-3a*

Was ist zu tun?

Die Hersteller müssen sich spätestens jetzt darauf vorbereiten, ihre Pflichten nach der Cyberresilienz-Verordnung rechtzeitig zu erfüllen.

Verantwortliche sollten diese „Sicherheitsgeschenke" aus der Dokumentation und den Anleitungen auf Datenschutzkonformität prüfen und im Betrieb geeignete und wirksame technische und organisatorische Maßnahmen treffen, um alle Datenschutzgrundsätze zu erfüllen.

2.4 Gamechanger Herstellerverantwortung – vielleicht schon in Sichtweite

Artikel 25 DSGVO verlangt vom Verantwortlichen, das Prinzip **„Datenschutz by Design"** umzusetzen. Das bedeutet, die Anforderungen der DSGVO von Anfang an in die Verarbeitungen personenbezogener Daten zu implementieren. Die Macht von „by Design" sollte nicht unterschätzt werden: Die Systeme sollen so gestaltet sein, dass den Verantwortlichen die Umsetzung der Anforderungen der DSGVO leichtfällt, weil die Datenschutzgrundsätze umgesetzt wurden, die Voreinstellungen datenschutzfreundlich gewählt sind, das Risiko für die Rechte und Freiheiten natürlicher Personen stets beherrscht wird und etwaige Fehler und Pannen nach Möglichkeit vermieden werden. Jedoch ist die Realität eine andere.

Der Webfehler der DSGVO ist das Ausschließen der Hersteller von Produkten, Diensten und Anwendungen. Sie sind **nicht Verpflichtete** nach dem Datenschutzrecht (es sei denn, sie geraten in die Rolle als Auftragsverarbeiter oder Verantwortlicher). Artikel 25 DSGVO verpflichtet den Verantwortlichen zu **Datenschutz by Design und by Default**.

Erwägungsgrund 78 der DSGVO

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

Doch entscheidet über einen Großteil der Gestaltung der Verarbeitung nicht der Verantwortliche allein, denn er bedient sich typischerweise der Produkte, Dienste und Anwendungen von Herstellern.

Die Situation für die Verantwortlichen wäre deutlich besser, wenn auf dem europäischen Markt für die Verarbeitung personenbezogener Daten nur Produkte, Dienste und Anwendungen angeboten würden, die ohne größere Verrenkungen datenschutzkonform einsetzbar sind. Am besten wäre es, wenn die Produkte und Dienste, die zur Verarbeitung personenbezogener Daten dienen, bereits unter Berücksichtigung der europäischen Datenschutzanforderungen entwickelt worden wären und unmittelbar darüber informieren würden, wie die Verantwortlichen sie datenschutzkonform verwenden und die Einhaltung des Datenschutzrechts nachweisen können.

Bei der DSGVO handelt es sich **nicht um Produktsicherheitsrecht**. Daher hat sich die Hoffnung des Gesetzgebers nicht erfüllt, dass die Marktakteure von allein auf ein ausreichendes Datenschutzniveau der angebotenen Produkte, Dienste und Anwendungen hinwirken. Es ist sogar so, dass die Verantwortlichen, die bei Herstellern und Anbietern genau nachfragen, heutzutage Schwierigkeiten haben, alle Informationen zu erhalten, die für ihre eigene datenschutzrechtliche Rechenschaftspflicht sowie für die Beherrschung des Risikos relevant sind.

Dabei ist es durchaus möglich, **Hersteller und Anbieter mehr in die Pflicht zu nehmen**: Neben der Cyberresilienz-Verordnung (Tz. 2.3) kennt beispielsweise auch die KI-Verordnung Designpflichten, die sich an die Anbieter richten. Wie bei der Systementwicklung die rechtlichen Anforderungen umgesetzt wurden, ist Bestandteil der verpflichtenden technischen Dokumentation, die Hersteller und Anbieter erstellen und bereithalten müssen.

Diese Ansätze ließen sich zu einem guten Stück auf das Datenschutzrecht übertragen, um die bisherige Herstellerlücke der DSGVO zu schließen. Verantwortliche könnten dann darauf vertrauen, dass die Produkte, Dienste und Anwendungen auf dem Markt datenschutzkonform einsetzbar wären. Ein Großteil der Informationen für die Dokumentation im Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 DSGVO, zur Schwellenwertanalyse des Risikos und gegebenenfalls zur Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO könnte ihnen in standardisierter Form zur Verfügung gestellt werden. Der Aufwand für die Verantwortlichen wäre deutlich reduziert, und vor allem könnten sie leichter ihre Rechenschaftspflicht erfüllen.

Rückenwind für die jahrealten Forderungen der Datenschutzkonferenz gibt es durch die Festlegung von Bund und Ländern in der Föderalen Modernisierungsagenda:

> **Föderale Modernisierungsagenda, Nr. 166**
>
> 7. EU-Datenrecht
>
> Bund und Länder werden auf europäischer Ebene […]
>
> 4. [sich] dafür [einsetzen], dass nach Vorbild des Cyber-Resilience-Acts und der KI-VO auch die DSGVO die Hersteller und Anbieter von Standardlösungen künftig in die Verantwortung nimmt, damit die Anwender unkompliziert und rechtssicher Standardlösungen nutzen können.

Die **Forderung nach Herstellerverantwortung** liegt damit auf dem Tisch. Nach unserer Auffassung fällt für die Hersteller, die ohnehin die Cyberresilienz-Verordnung umsetzen müssen, kein großer zusätzlicher Aufwand in der Dokumentation an. Wichtig ist aber, dass tatsächlich Datenschutz by Design und by Default von Anfang an in die Produktentwicklung und in den Betrieb Eingang finden. Das wäre wirklich der Gamechanger für einen praxistauglichen und effektiven Datenschutz ohne großen Aufwand.

Was ist zu tun?

Bund und Länder sollten zusammen mit der Datenschutzkonferenz ihre Vorschläge zur Herstellerverantwortung in den europäischen Prozess der Datenschutzreform einbringen.

2.5 Datenschutzreform in Europa: Omnibusse, Fitnesscheck und die Büchse der Pandora

Bereits die Entstehung der DSGVO war von einem massiven Lobbying begleitet – aus allen Richtungen wurden Unzulänglichkeiten des noch nicht einmal in Kraft getretenen Gesetzestextes beklagt und Alternativvorschläge vorgelegt. Die beiden Evaluationen der EU-Kommission, die nach Art. 97 Abs. 1 DSGVO alle vier Jahre durchzuführen sind, hatten keine fundamentalen Bedarfe an Änderungen ergeben, jedoch sah die EU-Kommission stellenweise Optimierungspotenzial. Insgesamt hatte man den Eindruck, dass die DSGVO wie die sprichwörtliche Büchse der Pandora nicht geöffnet werden sollte. Wer dies täte, würde eine noch viel größere Lobbyschlacht auslösen.

Im Jahr 2025 war von dieser Zurückhaltung nichts mehr zu verspüren: Im Eilverfahren hat die EU-Kommission zwei Omnibus-Verfahren zur Änderung der DSGVO und anderer Digitalrechtsakte wie der KI-Verordnung vorgelegt. Besonders der „digitale Omnibus" könnte sich stark auf die DSGVO auswirken:

https://eur-lex.europa.eu/procedure/DE/2025_360

Kurzlink: *https://uldsh.de/tb44-2-5a*

Mehrere Punkte sehen wir zusammen mit den anderen Datenschutzaufsichtsbehörden im Europäischen Datenschutzausschuss kritisch. Fundamentale Auswirkungen hätte die vorgeschlagene Änderung der Definition der personenbezogenen Daten, in der vor allem der Personenbezug von pseudonymisierten Daten geregelt werden soll. Möglicherweise sollte die Formulierung nur klarstellenden Charakter haben, indem EuGH-Feststellungen referenziert wurden. Dann ist dieser Versuch jedoch gesetzestechnisch verunglückt – die Definition stimmt nämlich nicht mit den EuGH-Aussagen überein. Würde an diesem Grundpfeiler des Personenbezugs gerüttelt, könnte dies dazu führen, dass die Klarstellungen des EuGH auf der bisherigen Rechtslage künftig keine Bedeutung mehr hätten; der Fundus an EuGH-Entscheidungen müsste teilweise erst wieder neu aufgebaut werden.

Die Kritik des EDSA findet sich unter diesem Link:

https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22026-proposal_de

Kurzlink: https://uldsh.de/tb44-2-5b

Das Bild der Büchse der Pandora ist vielleicht nicht so passend: Jetzt gilt es, in die Schatzkiste der guten Ideen, die sich aus den Erfahrungen der letzten zehn Jahre speist, zu schauen, um die DSGVO und das Digitalrecht insgesamt zu verbessern. Diese Ideen mit ihren Wirkungen und Nebenwirkungen müssen unter verschiedenen Perspektiven diskutiert werden. Ein solcher Diskurs ist nicht in den bereits „fahrenden Omnibussen" vorgesehen, wohl aber kann dies in einem anderen Instrument der EU-Kommission möglich sein: dem digitalen Fitnesscheck.

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/15554-Eignungsprufung-der-Digitalvorschriften-Uberprufung-der-kumulativen-Auswirkungen-der-EU-Digitalvorschriften_de

Kurzlink: *https://uldsh.de/tb44-2-5c*

Digitaler Fitnesscheck

Die Eignungsprüfung der Digitalvorschriften ist die zweite Phase des Plans der Kommission zur Vereinfachung der EU-Digitalvorschriften nach den Anpassungen im Zuge der Omnibus-Verordnung für den Digitalbereich.

Um sicherzustellen, dass die EU-Digitalvorschriften wirksam, verhältnismäßig und zukunftsfähig sind, werden im Rahmen der Eignungsprüfung der Digitalvorschriften das Zusammenspiel der verschiedenen Vorschriften sowie ihre kumulativen Auswirkungen auf Unternehmen, ihre Wirksamkeit für die Wettbewerbsfähigkeit und ihre Wirkung auf die Werte und die Grundrechte der EU analysiert.

In diesen Diskurs werden wir unsere Ideen insbesondere zu den größeren Themenbereichen einbringen, in denen wir Verbesserungspotenzial im aktuellen Datenschutzrecht sehen: der **Herstellerverantwortung** (Tz. 2.4) und dem **Kinderdatenschutz**.

Fragen des Kinderdatenschutzes hatten wir bereits vor mehreren Jahren zusammen mit wissenschaftlichen Partnern in der Plattform Privatheit (Tz. 8.1) aufgegriffen. Auf Basis dieser Vorarbeiten haben wir in der Datenschutzkonferenz die wichtigsten Forderungen zusammengestellt, die unter diesem Link veröffentlicht sind:

https://www.datenschutzzentrum.de/artikel/1525-Safer-Internet-Day-und-die-Kinderrechte-Reformvorschlaege-zur-Verbesserung-des-gesetzlichen-Datenschutzes-von-Kindern.html

Kurzlink: *https://uldsh.de/tb44-2-5d*

https://www.datenschutzkonferenz-online.de/media/en/Entschliessung_Datenschutz-von-Kindern.pdf

Kurzlink: *https://uldsh.de/tb44-2-5e*

03

KERNPUNKTE

Parlamentarischer Datenschutz

Datenschutzgremium

Beratungsangebot für Abgeordnete

3 Landtag

Der **parlamentarische Datenschutz** lag früher außerhalb der Zuständigkeit der Landesbeauftragten für Datenschutz – doch ein Urteil des Europäischen Gerichtshofs (EuGH) aus dem Jahr 2024 hat zu Änderungen geführt (Tz. 3.1). Wie bisher war die Landesbeauftragte für Datenschutz Gast bei den Sitzungen des **Datenschutzgremiums** des Schleswig-Holsteinischen Landtages (Tz. 3.2). Nützlich für Abgeordnete ist außerdem unser Angebot, dass sie sich von uns zu konkreten Fragen und Einzelfällen oder aber auch zu allgemeineren Themen beraten lassen können (Tz. 3.3).

3.1 Entwicklung nach der EuGH-Entscheidung zum parlamentarischen Datenschutz

In den früheren Tätigkeitsberichten (z. B. 41. TB, Tz. 3.1; 42. TB, Tz. 3.1) hatten wir stets die parlamentarische Sonderrolle im Datenschutz betont. So ging auch die Datenschutzkonferenz – also alle unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – davon aus, dass **Parlamente** wegen ihrer **verfassungsrechtlich geschützten Autonomie** der Aufsicht der Datenschutzaufsichtsbehörden grundsätzlich nicht unterlägen.

So ist es auch noch in der geltenden Fassung des Landesdatenschutzgesetzes geregelt: Die Verarbeitung personenbezogener Daten in **Wahrnehmung parlamentarischer Aufgaben** wird im LDSG ausgenommen.

§ 2 Abs. 3 LDSG

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

Wie im letzten Tätigkeitsbericht bereits ausgeführt, gibt es mittlerweile mehrere Entscheidungen des EuGH zu Fragen des parlamentarischen Datenschutzes (43. TB, Tz. 3.1). In seiner Entscheidung vom 16.01.2024 – C-33/22 – stellt der EuGH fest, dass die DSGVO auch für die Verarbeitung personenbezogener Daten im parlamentarischen Kontext gilt. Das betrifft alle **datenschutzrechtlichen Anforderungen an die Verarbeitung selbst**; darüber hinaus ist die Frage zu klären, wer die **Datenschutzaufsicht** wahrnehmen kann oder soll. Die vermeintlich einfache Lösung, dass die bestehende Datenschutzaufsicht für den öffentlichen und nichtöffentlichen Bereich auch für den parlamentarischen Bereich zuständig wird, würde dazu führen, dass **eine Behörde der Exekutive die Legislative beaufsichtigt**. Das stünde nicht im Einklang mit der im Grundgesetz verankerten **Gewaltenteilung**.

Die Geltung der DSGVO bedeutet aber nicht automatisch, dass dieselbe Aufsichtsstruktur gilt. Stattdessen sieht Art. 51 Abs. 1 DSGVO vor, dass **jeder Mitgliedstaat weitere Aufsichtsbehörden einrichten** kann, wenn dies insbesondere aufgrund der verfassungsmäßigen Struktur erforderlich ist. Die Aufgabe besteht dann darin, zum einen passende Datenschutzregelungen für den parlamentarischen Betrieb zu treffen und zum anderen die Aufsicht auszugestalten.

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

Jedoch ist damit noch nicht automatisch die **Aufsicht zur Umsetzung und Überwachung**

der spezifischen parlamentarischen Datenschutzregelungen geregelt. Die Rückfallposition – so auch vom EuGH entschieden – ist die Wahrnehmung der Aufsicht durch die bereits etablierte Datenschutzaufsichtsbehörde, nämlich die **Landesbeauftragte für Datenschutz**. Allerdings überwacht damit die eine Stelle der Exekutive die Legislative – das bewerten wir als kritisch.

In dieser Situation kann der Landtag aber **eine eigene Datenschutzaufsicht** einrichten, z. B. indem gesetzlich festgelegt wird, dass das Datenschutzgremium dazu herangezogen wird. Eine solche Aufsicht muss den Anforderungen der DSGVO genügen. Es gibt in Deutschland bereits spezifische Aufsichtsstellen in den Bereichen des Rundfunks oder der Religionsgemeinschaften. In ähnlicher Form ließe sich auch eine Aufsichtsstelle für den parlamentarischen Bereich einrichten – das könnte eine Person oder ein Kollegialorgan sein.

Ein bedenkenswertes Beispiel für eine Lösung der Datenschutzaufsicht im Parlament hat das Land Baden-Württemberg vorgelegt: Im Sommer 2025 wurde im dort geltenden **Landesdatenschutzgesetz ein neuer Abschnitt 5** für den Bereich des Landtages eingeführt und eine **Datenschutzaufsichtsordnung** bekannt gemacht. Demnach gibt es als Aufsichtsstelle ein Gremium, dessen Mitglieder vom Landtag aus seiner Mitte gewählt werden und bei dessen Besetzung das Verhältnis zwischen Regierungsfraktionen und Oppositionsfraktionen berücksichtigt wird. Die nötige Sachkunde soll dadurch gewährleistet sein, dass mindestens ein Mitglied des Gremiums die Befähigung zum Richteramt besitzt.

Den Link zur Bekanntmachung über die Datenschutzaufsichtsordnung für den Landtag von Baden-Württemberg vom 24. Juli 2025 finden Sie unter:

https://www.landesrecht-bw.de/bsbw/document/jlr-LTDSAufsOBWrahmen

Kurzlink: *https://uldsh.de/tb44-3-1a*

Datenschutzaufsichtsordnung für den Landtag von Baden-Württemberg vom 24.07.2025

1. Der Landtag setzt zur Aufsicht über die Datenverarbeitung durch den Landtag gemäß § 19a Absatz 1 des Landesdatenschutzgesetzes ein Datenschutzaufsichtsgremium ein.

2. Die Mitglieder des Gremiums werden vom Landtag aus seiner Mitte für die Dauer der Wahlperiode gewählt. Die Anzahl der Mitglieder wird vom Landtag festgelegt. Bei der Besetzung muss das Verhältnis zwischen Regierungsfraktionen und Oppositionsfraktionen berücksichtigt werden.

[…]

In der Datenschutzaufsichtsordnung werden in den weiteren Ziffern 3 bis 12 Regelungen zu Amtszeit, Unabhängigkeit, Sachkunde, Aufgaben, Befugnissen, Organisation, Beschlussfähigkeit, Beratungen, Unterrichtungen und Tätigkeitsberichten getroffen. Meines Erachtens verdient dieser Ansatz Beachtung.

Es gibt **mehrere Möglichkeiten**, eine eigene Aufsicht über die Verarbeitung personenbezogener Daten in Wahrnehmung parlamentarischer Aufgaben zu regeln. Diese Aufgabe könnte – zusammen mit der ohnehin geplanten Novellierung der Regelungen zum Datenschutzgremium (Tz. 3.2) – noch in dieser Legislaturperiode angegangen werden.

3.2 Datenschutzgremium

Seit vielen Jahren bewährt: das **Datenschutzgremium** des Schleswig-Holsteinischen Landtages. Mehrfach im Jahr tagt das Datenschutzgremium, um Datenschutzthemen im parlamentarischen Bereich zu diskutieren, etwaige Beschwerden zu bearbeiten und sich mit neuen Entwicklungen zu beschäftigen. 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/tb44-3-2a*

Basis für die Arbeit des Datenschutzgremiums ist die Datenschutzordnung:

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

Kurzlink: *https://uldsh.de/tb44-3-2b*

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

3.3 Service für Abgeordnete in Fragen zu Datenschutz und Informationsfreiheit

Einige Abgeordnete nutzen es immer mal wieder, andere kennen vielleicht noch gar nicht unser Angebot: Zusammen mit ihrem Team bietet die Landesbeauftragte für Datenschutz an, dass sich **jede und jeder Abgeordnete vertrauensvoll an das ULD wenden** kann, um Beratung oder Hilfestellung in Fragen des Datenschutzes oder der Informationsfreiheit zu erhalten.

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

Die heutigen Zeiten sind gekennzeichnet von Unsicherheit und ständiger Veränderung. Gerade in dieser Situation ist die Kommunikation miteinander und das **Einbeziehen der vielfältigen verschiedenen Perspektiven** notwendig, um die Herausforderungen zu meistern, die sich für unsere Gesellschaft stellen. Dies gilt genauso für die regionalen und landesspezifischen Aktivitäten wie auch für die Politik im Großen auf Bundesebene oder in Europa.

§ 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; [...]

Unser Interesse ist es, im Austausch mit den Abgeordneten Chancen und Risiken verschiedener Handlungsoptionen zu verstehen und kon-

struktiv zu praxistauglichen Lösungen für die diskutierten Sachverhalte beizutragen. So werden wir weiterhin alle Fragen der Abgeordneten zu Datenschutz und Informationsfreiheit mit **unserer juristischen und auch informations-technischen Expertise** sowie auf Basis unserer Erfahrung in der Anwendung der Rechtsnormen beantworten und dem Beratungsbedarf nachkommen.

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

Anfertigung von Sozialberichten

Elektronische Aufenthaltsüberwachung

Löschanspruch an Fachverfahren owi21

Sozialdaten zum Mitlesen

Datenpannen im Medizinbereich

Datenschutz- und Medienkompetenz

4 Datenschutz in der Verwaltung

4.1 Allgemeine Verwaltung

4.1.1 Interessenkonflikt bei behördlichen Datenschutzbeauftragten?

Zu prüfen war die Frage, ob die Tätigkeit in einem Rechnungsprüfungsamt mit der parallelen Wahrnehmung von Aufgaben als behördlicher Datenschutzbeauftragter zu einem Interessenkonflikt führen kann. Der Landesgesetzgeber hat hierzu bereits eine Regelung getroffen:

§ 115 Abs. 4 der Gemeindeordnung

Die Leiterin oder der Leiter und die Prüferinnen und Prüfer des Rechnungsprüfungsamtes können nicht zu gleicher Zeit eine andere Stellung in der Gemeindeverwaltung innehaben; dies gilt nicht für die Stellung einer oder eines Beauftragten für den Datenschutz.

Maßgebend ist darüber hinaus Art. 38 Abs. 6 Satz 2 DSGVO. Demnach stellt insbesondere der Verantwortliche sicher, dass in Abgrenzung zum Aufgabenkatalog in Artikel 39 DSGVO die Wahrnehmung anderer Aufgaben und Pflichten nicht zu einem Interessenkonflikt führt. Nähere Ausführungen dazu, wie und durch welche Maßnahmen der Verantwortliche eine Interessenkollision vermeidet, enthält die DSGVO nicht. Insoweit besteht ein Ermessen des Dienstherrn.

Allerdings ist vor allem zu gewährleisten, dass die oder der Datenschutzbeauftragte seine Aufgaben weisungsfrei erledigen kann. Ihre bzw. seine insoweit unabhängige Stellung setzt andererseits voraus, dass ein unbefangenes Tätigwerden möglich bleibt und ferner die Fähigkeit zu wertneutralen Entscheidungen in datenschutzrechtlichen Fragestellungen besteht, die nicht infolge der Wahrnehmung anderer Aufgaben beeinflusst wird. Betrifft eine solche Fragestellung die Praxis der Verarbeitung personenbezogener Daten im Bereich des Rechnungsprüfungsamtes, so kann im Einzelfall ein solcher Interessenkonflikt entstehen. § 115 Abs. 4 GO ist daher europarechtskonform auszulegen.

Das VG Stuttgart hat in einem vergleichbaren Fall einige Erwägungen zur Thematik angestellt. Das Gericht kommt zum Ergebnis, dass zwar ein Interessenkonflikt entstehen könne. Allerdings sei ein solcher Konflikt „unkompliziert durch die Benennung eines Stellvertreters aus einer anderen Dienststelle" vermeidbar, welcher „im Konfliktfall unbefangen einen Vorgang anstelle des Datenschutzbeauftragten übernimmt". Ein solches Vorgehen erscheint auch aus unserer Sicht denkbar (VG Stuttgart, Beschluss vom 29.03.2021, 11 K 484/21).

Was ist zu tun?

Die kommunalrechtlichen Vorgaben werden durch die europarechtlichen Vorgaben eingeschränkt. Ist gerade die Verarbeitung personenbezogener Daten Gegenstand einer Beurteilung der oder des behördlichen Datenschutzbeauftragten, so kann diese Person in jenem Fall keine unabhängige Prüfung vornehmen, wenn sie im Rechnungsprüfungsamt eine Leitungsposition wahrnimmt. Der bloße Wortlaut von § 115 Abs. 4 der Gemeindeordnung hilft da nicht weiter. Folglich muss für diesen Fall eine andere unabhängige Prüfperson tätig werden, welche die hinreichende Qualifikation und Datenschutzpraxis besitzt.

4.1.2 Ortsbeiräte und Seniorenbeiräte als Mandatsträger

Nach der Gemeindeordnung kann die Gemeinde durch Beschluss der Gemeindevertretung Ortsteile bilden und deren Namen bestimmen. Die Gemeindevertretung kann die Bezeichnung Ortsteil durch die Bezeichnung „Dorfschaft" oder eine andere Bezeichnung ersetzen. Die Gemeinde kann durch die Hauptsatzung für einen Ortsteil einen Ortsbeirat bilden. Die Hauptsatzung kann für den Ortsbeirat eine andere Bezeichnung vorsehen. Einige Kommunen haben davon Gebrauch gemacht und in ihren Satzungen anstelle der Formulierung „Ortsbeirat" die Bezeichnung „Dorfvorsteher" gewählt.

Der **Ortsbeirat** ist über alle wichtigen Angelegenheiten, die den Ortsteil betreffen, zu unterrichten. Die Geschäftsordnung bestimmt die Art der Unterrichtung. Der Ortsbeirat kann in Angelegenheiten, die den Ortsteil betreffen, Anträge an die Gemeindevertretung stellen. Ferner kann die Gemeindevertretung durch die Hauptsatzung bestimmte Entscheidungen auf den Ortsbeirat übertragen.

Weiterhin kann die Gemeinde durch Satzung die Bildung von Beiräten für gesellschaftlich bedeutsame Gruppen und Belange vorsehen. Zu nennen sind in diesem Kontext insbesondere **Seniorenbeiräte**, die als Interessenvertretung Beteiligungsrechte erhalten können.

Ortsbeiräte und Seniorenbeiräte benötigen zur Erfüllung ihrer Aufgaben gegebenenfalls Daten der Einwohnerschaft aus dem Melderegister. Maßgeblich ist hierfür das Bundesmeldegesetz.

§ 50 Abs. 2 Bundesmeldegesetz (BMG)

Verlangen Mandatsträger, Presse oder Rundfunk Auskunft aus dem Melderegister über Alters- oder Ehejubiläen von Einwohnern, darf die Meldebehörde Auskunft erteilen über

1. Familienname,
2. Vornamen,
3. Doktorgrad,
4. Anschrift sowie
5. Datum und Art des Jubiläums.

Altersjubiläen im Sinne des Satzes 1 sind der 70. Geburtstag, jeder fünfte weitere Geburtstag und ab dem 100. Geburtstag jeder folgende Geburtstag; Ehejubiläen sind das 50. und jedes folgende Ehejubiläum.

Die genannten Beiräte können nach Auffassung des ULD als Mandatsträger im Sinne von § 50 Abs. 2 des BMG gelten und im Rahmen ihrer Aufgaben die entsprechenden Daten erhalten.

Was ist zu tun?

§ 50 Abs. 2 BMG beinhaltet eine Rechtsgrundlage für Ortsbeiräte und Seniorenbeiräte, Meldedaten zur eigenen Aufgabenerfüllung zu erhalten. Gemäß § 50 Abs. 5 BMG haben betroffene Personen aus der Einwohnerschaft das Recht, der Übermittlung ihrer Daten an Mandatsträger zu widersprechen. Auf das Widerspruchsrecht ist bei der Anmeldung im Rahmen des Bezugs einer Wohnung sowie einmal jährlich durch ortsübliche Bekanntmachung hinzuweisen.

4.1.3 Einhaltung der Vorgaben zur Schuleingangsuntersuchung

Bereits für den Berichtszeitraum im Jahr 2023 wurden die Inhalte des standardisierten Verfahrens für Schuleingangsuntersuchungen erläutert (42. TB, Tz. 4.1.4). Demnach erhalten die Eltern vor allem einen Fragebogen, bei welchem die mit einem Sternchen (*) gekennzeichneten Angaben verpflichtend zu beantworten

sind. Die Fragen beziehen sich vor allem auf den Gesundheitszustand des Kindes. Hierfür 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.

§ 27 Abs. 3 Satz 1 und 2 des Schulgesetzes

Zur Durchführung der Untersuchungen nach Absatz 1 dürfen bei der untersuchenden Stelle diejenigen Anamnese- und Befunddaten als personenbezogene Daten verarbeitet werden, die für den Untersuchungszweck notwendig sind. Kinder, Jugendliche, Schülerinnen, Schüler und Eltern haben die erforderlichen Angaben zu machen.

Besorgte Eltern wandten sich bezüglich des Fragebogens mit den Gesundheitsfragen an das ULD und baten um Prüfung, ob es sich dabei um jene Fragen handelt, die verpflichtend zu beantworten sind. Nach Durchsicht des Fragebogens konnte das ULD dies bejahen und im Ergebnis keinen datenschutzrechtlichen Verstoß feststellen. So zählen zu den **Pflichtangaben** z. B. folgende Punkte:

- Angaben zu chronischen Erkrankungen,
- Auskünfte zu möglichen Allergien wie etwa bezüglich Nahrungsmitteln, Pollen, Hausstaubmilben, Medikamenten,
- durchlebte Infektionskrankheiten wie etwa Masern, Röteln, Mumps, Scharlach,
- Krankenhausaufenthalte oder Operationen,
- entwicklungsfördernde Therapien oder Maßnahmen wie Physiotherapie, Ergotherapie, Sprachförderung, Logopädie, Frühförderung,
- Angaben zur Schwangerschaftswoche, in welcher das Kind geboren wurde,
- Besonderheiten beim Schwangerschafts- und Geburtsverlauf.

Von Bedeutung ist auch, dass die Angaben der ärztlichen **Schweigepflicht** unterliegen, nur der Wahrnehmung des schulärztlichen Dienstes dienen und nicht an die Schule weitergeleitet werden. Entsprechende Hinweise ergeben sich auch direkt aus dem Fragebogen. Weiterhin sind auch aus den standardisierten Pflichtangaben nach Artikel 13 DSGVO nähere Erläuterungen zu entnehmen, welche Fragen auf welcher gesetzlichen Grundlage zu beantworten sind und bei welchen Fragenkomplexen es sich um freiwillige Angaben handelt.

Im Ergebnis hatte sich der maßgebliche Kreis bei der Durchführung der Schuleingangsuntersuchung korrekt verhalten und alle datenschutzrechtlichen Vorgaben erfüllt. Maßgebend waren vor allem die Inhalte einer Beratung des ULD zur damaligen Entwicklung standardisierter Fragebögen und der datenschutzrechtlichen Pflichtangaben für die Eltern. Der damalige Entwicklungsprozess zur Schaffung einheitlicher Unterlagen für Schleswig-Holstein wurde von Vertretern des Ministeriums für Gesundheit und Justiz sowie von einigen Schulärztinnen und Schulärzten der Kreise und kreisfreien Städte sehr konstruktiv begleitet.

4.1.4 Löschung von Daten auf schulisch genutzten Tablets via Fernlöschung

Das ULD erhielt eine Beschwerde, dass unberechtigt personenbezogene Daten auf einem schulisch genutzten Tablet gelöscht wurden.

Unter anderem auf dem privaten Tablet des Kindes der Beschwerdeführer wurden versehentlich personenbezogene Daten ohne Zustimmung der Eltern oder des Kindes durch die verantwortliche Stelle gelöscht. Die verantwortliche Stelle informierte die betroffenen Schüler und Eltern umgehend, dass es aufgrund einer Fernlöschung zu dem Vorfall gekommen war. Es waren nicht nur schulische Dokumente, sondern auch private Fotos, Kontakte, Chatverläufe usw. betroffen.

Daraufhin beschwerten sich die Eltern beim ULD: Sie führten aus, dass sie nicht ausreichend informiert gewesen seien und von dem Umstand der Möglichkeit einer Fernlöschung keine Kenntnis hatten. Die Eltern waren zudem sehr besorgt, dass so auch eine komplette Einsichtnahme durch dritte Personen auf die Daten des Sohnes nicht ausgeschlossen werden konnten.

Im Rahmen eines Anhörungsverfahrens hat das ULD bei der verantwortlichen Stelle um Erläuterungen zu dem konkreten Vorfall gebeten. Daraufhin wurde ausgeführt, dass es sich bei dem Tablet um das Eigentum der Schüler bzw. Eltern handelte. Die Datensicherung obliegt den Eigentümern. Eine automatische Sicherung privater Daten durch die verantwortliche Stelle kann und darf nicht erfolgen, denn die Einsichtnahme in private Daten auf den Geräten war und ist durch die verantwortliche Stelle nicht möglich.

Die Schule wurde über die geplanten Maßnahmen – der Wechsel des Mobile Device Managements – der IT informiert und kommunizierte die geplante Zurücksetzung auch im Voraus an die Schülerschaft. Seitens der Schul-IT wurden über die Schule Anleitungen übermittelt, wie Datensicherungen erfolgen könnten, damit mit Sicherheit brauchbare Back-ups bestehen.

MDM – Mobile Device Management

Mit einem MDM können mobile Geräte wie Tablets, Smartphones und Notebooks zentral verwaltet werden. Wichtige Funktionen sind die Installation und Deinstallation von Apps, die Konfiguration und die Sperrung oder Löschung verlorener Geräte.

Es hätte gruppenweise ein Entfernen der Geräte aus dem alten MDM und anschließend die Installation und Registrierung im neuen MDM stattfinden sollen. Aufgrund des Fehlers eines Mitarbeiters der Schul-IT kam es jedoch zu einer versehentlichen Löschung von Daten auf mehreren hundert Schülergeräten im Rahmen dieser Umstellung des MDM. Durch eine fehlerhafte Ausführung wurde eine zentrale Funktion aktiviert, die dazu führte, dass betroffene Geräte vollständig zurückgesetzt wurden. Dabei wurden auch alle lokal gespeicherten Daten gelöscht.

Nach Feststellen des Fehlers wurde der Auftrag umgehend gestoppt. Der Elternschaft wurde im Rahmen eines auch an das ULD übermittelten Schreibens erläutert, dass ein MDM ein wichtiger Bestandteil des digitalen Schulbetriebs ist, welches aber auch gewisse Risiken mit sich bringt, die sich im vorliegenden Fall leider verwirklicht haben.

Die verantwortliche Stelle entschuldigte sich bei den betroffenen Personen und versuchte – soweit technisch möglich – die Daten auf den verschiedenen Geräten wiederherzustellen. Intern wurden Maßnahmen ergriffen, um einen ähnlichen Vorfall in Zukunft zu verhindern.

Da es sich um einen unglücklichen menschlichen Individualfehler handelte, hat das ULD das Verfahren mit einigen Hinweisen abgeschlossen: Künftig soll die verantwortliche Stelle vermehrt und insbesondere in Zeiträumen von technischen Umstellungen darauf hinweisen, dass wichtige Daten regelmäßig gesichert werden. Die verantwortliche Stelle sollte zudem sicherstellen, dass eine **Kommunikationsweitergabe an die Schüler und Eltern** erfolgt. Eine Überprüfung seitens der verantwortlichen Stelle, ob gleichartige Fehler technisch verringert oder gar vermieden werden können, wird ebenfalls von der verantwortlichen Stelle erwartet.

Letztlich handelt es sich auch bei diesem Vorfall um einen nach Artikel 33 DSGVO **meldepflichtigen Datenschutzverstoß**. Die verantwortliche Stelle wurde dazu aufgefordert, zukünftige vergleichbare Fälle eigenständig innerhalb der 72-Stunden-Frist an das ULD zu melden.

Was ist zu tun?

Datensicherungen sollten regelmäßig vorgenommen werden. Dies gilt nicht nur für Privatpersonen, sondern auch für verantwortliche Stellen, soweit es um die Verarbeitung personenbezogener Daten geht, auf die diese Einfluss und Zugriff haben. Wenn zur Datensicherung Handlungen der Nutzerinnen und Nutzer notwendig sind, sollte dies klar und regelmäßig kommuniziert werden.

4.1.5 Einbrüche in Verwaltungs- und Büroräume

Das ULD erhielt mehrere Datenpannenmeldungen aufgrund von Einbrüchen in Verwaltungsräume bzw. in Büroräumlichkeiten, in denen auch Dokumente mit personenbezogenen Daten gelagert wurden. Es wurden Fenster eingeschlagen oder gewaltsam aufgebrochen, Türen aufgehebelt, verschlossene Schränke aufgebrochen und Büros verwüstet.

In fast allen Fällen konnte ein Entwenden von Akten oder Dokumenten mit personenbezogenen Daten ausgeschlossen werden, da Ziel der Einbrüche Bargeld oder Wertgegenstände waren. Es bestand jedoch die Möglichkeit, dass Einsicht in personenbezogene Daten genommen wurde.

Für einen Einbruch kann eine verantwortliche Stelle nichts, wenn Fenster und Türen ordnungsgemäß verschlossen waren. Problematisch aus Sicht des ULD waren jedoch die Fälle, in denen Papierakten mit personenbezogenen Daten unverschlossen auf Schreibtischen gelagert wurden.

Hierzu kam es aufgrund von Überarbeitung und Unaufmerksamkeit der Mitarbeitenden. Einige verantwortliche Stellen führten ergänzend aus, dass ein Aktenschrankschloss einen Täter, der bereits Fenster eingeschlagen hat, nicht daran hindere, auch diese Schlösser zu öffnen. Das mag bis zu einem gewissen Grad richtig sein, jedoch stellt auch das Aktenschrankschloss ein weiteres Hindernis für einen Einbrecher dar und ist zumindest eine technisch-organisatorische Maßnahme, die seitens der verantwortlichen Stelle getroffen werden kann, um personenbezogene Daten auch für den Fall eines Einbruchs zu schützen.

Nach Feststellen der jeweiligen Einbrüche folgten durch die verantwortlichen Stellen **Sensibilisierungen der Mitarbeitenden**, Papierakten entsprechend den Vorgaben in verschlossenen Schränken zu lagern, Montagen von zusätzlichen Fenstersicherungsbeschlägen, die Installation von zusätzlichen Lichtquellen mit Bewegungsmeldern und zum Teil die Einrichtung von Kameraüberwachungen bzw. Bestreifungen durch Sicherheitsdienstmitarbeitende. Selbstverständlich wurden auch jeweils Anzeigen bei der Polizei gestellt.

Seitens des ULD erfolgte noch der ergänzende Hinweis, dass bei Veranlassung von Kameraüberwachungen der Einrichtungen ebenfalls datenschutzrechtliche Vorgaben bezüglich Videoüberwachungen Berücksichtigung zu finden haben.

Was ist zu tun?

Türen und Fenster sind bei Verlassen von Büros zu verschließen. Papierakten sollten bei längerem bzw. für den Arbeitstag endgültigem Verlassen des Büros in abgeschlossenen Aktenschränken gelagert werden. Technische Geräte sind bei Verlassen des Gebäudes für den Feierabend immer zu sperren und sollten festplattenverschlüsselt sein. Hierfür sollten Verantwortliche (schriftliche) Vorgaben für ihre Mitarbeitenden festlegen. Eine „Clean Desk"-Richtlinie sollte durchgesetzt werden.

4.1.6 Vollstreckungsankündigung ohne Umschlag im gemeinsamen Briefkasten mit dem Vermieter

Das ULD erhielt eine Datenpannenmeldung nach Artikel 33 DSGVO und einen Tag später auch eine Beschwerde zu den Handlungen eines Vollstreckungsbeamten eines Amtes. Dieser hatte eine Vollstreckungsankündigung mit einem Termin für einen weiteren Besuch vor Ort ohne Umschlag in den Briefkasten des Schuldners eingeworfen. Der Briefkasten war allerdings deutlich mit zwei Namen beschriftet – dem des Schuldners und dem des Vermieters. Da der Vermieter als Erster den Briefkasten öffnete, konnte er ohne Probleme die offen einsehbare Vollstreckungsankündigung gegen seinen Mieter lesen.

In der Meldung nach Artikel 33 DSGVO führte das Amt aus, dass der Vollstreckungsbeamte angewiesen worden sei, künftige Terminankündigungen **nur mit Umschlag** zu hinterlegen. Da das Amt auf das Fehlverhalten des Vollstreckungsbeamten aufgrund einer auch dort eingegangenen Beschwerde des Schuldners aufmerksam wurde, war eine Benachrichtigung nach Artikel 34 DSGVO obsolet.

Das ULD hat das Amt ergänzend darauf hingewiesen, dass sämtliche Mitarbeitenden dahin gehend sensibilisiert werden sollten, dass zukünftig alle Schreiben, die personenbezogene Daten aufweisen, auch bei persönlicher Überbringung in einem Umschlag übermittelt werden sollten, um die Daten vor der unmittelbaren Einsehbarkeit durch Dritte zu schützen. Dies gilt auch, wenn Briefkästen nur einen Namen auszeichnen, da auch in diesem Fall selbstverständlich dennoch mehrere Personen auf schützenswerte personenbezogene Daten Zugriff haben könnten.

Was ist zu tun?

Personenbezogene Daten müssen in jeglicher Übermittlungsform vor Zugriffen und Einsichtsmöglichkeiten Dritter geschützt werden. Hierfür können z. B. Verschlüsselungen bei elektronischer Übermittlung und Briefumschläge bei postalischer Übermittlung geeignete Maßnahmen sein. Mitarbeitende sollten diesbezüglich sensibilisiert sein und über entsprechende technische Möglichkeiten und Ressourcen verfügen.

4.1.7 Befristetes Arbeitsverhältnis: Namentliche Benennung der zu vertretenden Beschäftigten?

Sind Beschäftigte für einen bestimmten Zeitraum abwesend, kommt deren Vertretung durch andere Beschäftigte in Betracht, indem mit Letzteren ein befristeter Arbeitsvertrag geschlossen wird. Maßgeblich ist dann § 14 Abs. 1 Nr. 3 des Teilzeit- und Befristungsgesetzes:

> **§ 14 Abs. 1 Nr. 3 des Teilzeit- und Befristungsgesetzes**
>
> Die Befristung eines Arbeitsvertrages ist zulässig, wenn sie durch einen sachlichen Grund gerechtfertigt ist. Ein sachlicher Grund liegt insbesondere vor, wenn der Arbeitnehmer zur Vertretung eines anderen Arbeitnehmers beschäftigt wird.

Der maßgebliche Sachgrund muss bei Abschluss des befristeten Arbeitsvertrags vorliegen. In Betracht kommen z. B. vorübergehende Beschäftigungsverbote, etwa wegen Mutterschutz, die Wahrnehmung von Elternzeit oder die längere Erkrankung eines Beschäftigten. Fraglich ist, ob Arbeitgeber in einem befristeten Vertrag die zu vertretende Person namentlich bezeichnen müssen.

Soweit ersichtlich gibt es für die Fragestellung noch keine vertiefte Rechtsprechung. In einer Entscheidung hat das Arbeitsgericht München ausdrücklich offengelassen, ob die Benennung der vertretenen Person im befristeten Vertrag einen Datenschutzverstoß darstellen würde (ArbG München, Endurteil vom 09.09.2020 – 8 Ca 10000/18 – Rz. 25).

Aus der Rechtsprechung der Arbeitsgerichte oder aus der Literatur ist – soweit ersichtlich – bisher nicht zu entnehmen, dass die Aufnahme des Namens der vertretenen Person obligatorisch ist. Der Arbeitgeber wird im Streitfall aber belegen müssen, dass die Vorgaben des § 14 Abs. 1 Nr. 3 TzBfG erfüllt sind und hierfür die Umstände der vertretenen Beschäftigten dokumentieren.

Offen bleibt, weshalb die Benennung des sachlichen Befristungsgrundes (z. B. Befristung auf Grundlage einer Vertretung in der Elternzeit einer Beschäftigten; Befristung aufgrund der Krankheitsabwesenheit einer Person; Befristung aufgrund der Abordnung eines Beschäftigten) nicht ausreichen soll, um eine höhere Transparenz sicherzustellen. Dies mag derzeit dafür sprechen, dass eine namentliche Benennung der vertretenen Person im befristeten Arbeitsvertrag nicht

erforderlich ist. Allerdings kann die mehr arbeitsrechtliche Fragestellung durch das ULD kompetenzhalber nicht abschließend beantwortet werden. Es ist zu empfehlen, auf mögliche künftige Konkretisierungen durch die Rechtsprechung zu achten.

4.1.8 Mitteilung des Arztes zur Fahruntauglichkeit eines Patienten an Fahrerlaubnisbehörde?

Das ULD war mit der Frage befasst, inwieweit Ärztinnen und Ärzte Angaben zur Fahruntauglichkeit einer Patientin oder eines Patienten, die während der Untersuchung festgestellt wurden, an eine Fahrerlaubnisbehörde weiterleiten dürfen. Im Grundsatz besteht nach den verkehrsrechtlichen Vorschriften eine Befugnis zur Datenweitergabe nur für die Polizeibehörden:

> **§ 2 Abs. 12 Satz 1 Straßenverkehrsgesetz (StVG)**
>
> Die Polizei hat Informationen über Tatsachen, die auf nicht nur vorübergehende Mängel hinsichtlich der Eignung oder auf Mängel hinsichtlich der Befähigung einer Person zum Führen von Kraftfahrzeugen schließen lassen, den Fahrerlaubnisbehörden zu übermitteln, soweit dies für die Überprüfung der Eignung oder Befähigung aus der Sicht der übermittelnden Stelle erforderlich ist.

Insbesondere hinsichtlich der Ergebnisse einer gesundheitlichen Untersuchung sind Ärztinnen und Ärzte an die berufliche **Verschwiegenheitspflicht** gebunden. Mit der Weitergabe von **Patientendaten** an eine Fahrerlaubnisbehörde würden Ärztinnen und Ärzte auch den Verarbeitungszweck ändern, da die ärztliche Untersuchung den ursprünglichen Erhebungszweck kennzeichnet. Zweckänderungen bedürfen wiederum einer rechtlichen Grundlage, wobei die engen Vorgaben im Landesdatenschutzgesetz nicht weiterhelfen. Da besondere Rechtsvorschriften fehlen, welche eine Datenübermittlung an die Fahrerlaubnisbehörden legitimieren, kommt es auf eine Schweigepflichtentbindung der Patientin oder des Patienten bzw. auf deren/dessen **Einwilligung** bezüglich der Datenweitergabe an.

Die Rechtsprechung hat allerdings in den vergangenen Jahren eine Datenweitergabe durch die Ärztin oder den Arzt im Einzelfall als befugt erachtet, soweit dies durch einen **Notstand** (§ 34 Strafgesetzbuch – StGB) gerechtfertigt ist:

- Nach Auffassung des Verwaltungsgerichts Oldenburg kommt ein solcher Notstand gegebenenfalls in Betracht, wenn ein Patient Heroin konsumiert, er sich nunmehr in einer Substitutionstherapie befindet und von ihm erhebliche Gefahren für das Leben und die Gesundheit unbeteiligter Personen ausgehen, falls er weiterhin im öffentlichen Straßenverkehr Kraftfahrzeuge führt (VG Oldenburg, Beschluss vom 21.08.2019, 7 B 2289/19).
- Das Oberlandesgericht Düsseldorf verdeutlicht unter Berufung auf den Bundesgerichtshof, dass bei der Prüfung, ob eine Gefahr noch anders abwendbar war, aufgrund des Vertrauensverhältnisses zum Patienten grundsätzlich zu verlangen ist, dass der Arzt bei Zweifeln an der Kraftfahrtauglichkeit vor einer Information an die Fahrerlaubnisbehörde die gesundheitlichen Einschränkungen erläutert und auf die Gefahren im Falle einer Teilnahme am Straßenverkehr hinweist. Anderes mag dabei gelten, wenn der Patient aufgrund der Art seiner Erkrankung oder aufgrund seiner Uneinsichtigkeit nicht ansprechbar ist (OLG Düsseldorf, Beschluss vom 04.05.2015, III-2 Ws 101/15; BGH, Urteil vom 08.10.1968, VI ZR 168/67).

Eine pauschale Befugnis zur Weitergabe von Informationen zur Fahruntauglichkeit an eine Fahrerlaubnisbehörde besteht hingegen nicht. In jedem Einzelfall muss unter strafrechtlichen Gesichtspunkten geprüft werden, ob eine Notstandssituation besteht. Das Oberlandesgericht Düsseldorf führt aus, dass selbst bei einer ausnahmsweise befugten Durchbrechung der ärztlichen Verschwiegenheitspflicht die Datenweitergabe an die Fahrerlaubnisbehörde auf das Notwendige zu beschränken ist. Demnach reiche für den Ausnahmefall die Bezeichnung der Diagnose nebst der Mitteilung aus, dass Zweifel an der Fahruntauglichkeit bestehen. Die Fahrerlaubnisbehörde hätte dann die Möglichkeit, auf dieser Basis eine Anordnung **zur Überprüfung der Eignung zum Führen von Kraftfahrzeugen** nach § 11 Abs. 2 der Fahrerlaubnis-Verordnung zu treffen. Die zusätzliche Mitteilung einer ausführlichen Diagnose sowie Angaben zu

stationären Aufenthalten und Therapieempfehlungen zählen nach Auffassung des Oberlandesgerichts Düsseldorf nicht zum zulässigen Informationsumfang der Ärztin oder des Arztes.

Was ist zu tun?

Ärztinnen und Ärzte dürfen aufgrund ihrer Eigenschaft als Berufsgeheimnisträger die Angaben aus der ärztlichen Untersuchung einer Patientin oder eines Patienten nicht unbefugt offenbaren. Zur befugten Weitergabe von Angaben zur Fahruntauglichkeit an die Fahrerlaubnisbehörde bedarf es grundsätzlich einer Einwilligungs- und Schweigepflichtentbindungserklärung der Patientin oder des Patienten. Nur im Ausnahmefall dürfen Einzelangaben von der Ärztin oder vom Arzt an die Fahrerlaubnisbehörde ohne eine solche Erklärung weitergegeben werden, wenn die Voraussetzungen eines Notstandes nach § 34 StGB vorliegen.

4.1.9 Anfertigung von Sozialberichten

Das ULD war mit Fragen zur Erstellung von Sozialberichten befasst. Entsprechende Berichte sollen eine Übersicht zur **sozialräumlichen Entwicklung einer Kommune** geben, etwa in den Bereichen der Leistungen zur Sozialhilfe, der Erziehungs- und Jugendhilfe, der Kindertagesförderung und der Wohnraumversorgung. Der Sozialbericht enthält statistische Angaben, z. B. Daten zur Bevölkerungsentwicklung, zum Alter der Bevölkerung, zu Haushaltsstrukturen, zu Gebäudestrukturen und Standorten besonderer Einrichtungen, zum Mietpreisniveau, zur Arbeitslosenquote und den Standorten von Kindertagesstätten.

Eine transparente Darstellung in einem Sozialbericht erfordert die **Darstellung der Datengrundlagen**. Zum Vergleich: Der vom Ministerium für Soziales, Jugend, Familie, Senioren, Integration und Gleichstellung veröffentlichte Bericht zur sozialen Situation von Kindern und Jugendlichen in Schleswig-Holstein 2023, der teils andere inhaltliche Schwerpunkte als kommunale Sozialberichte enthält, weist klare Ausführungen zu den Datenquellen auf.

Zu beachten ist, dass zur Erstellung kommunaler Sozialberichte die Kommune erläutern können muss, woher die statistischen Angaben stammen. Sollte hierfür eine Verarbeitung personenbezogener Daten in einzelnen Fachbereichen erfolgen, so muss hierfür eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO vorhanden sein.

Auszug aus dem Bericht zur sozialen Situation von Kindern und Jugendlichen in Schleswig-Holstein 2023

Der Kinderarmutsbericht greift ausschließlich auf Daten der amtlichen Statistik zurück, überwiegend auf den Mikrozensus und die Bevölkerungsstatistik (Fortschreibung des Bevölkerungsstandes).

Den aktuellen Rand der Analysen bildet dabei das Jahr 2022, im Falle der Bevölkerungsfortschreibung zum Stichtag 31.12.2022. Aus dem Mikrozensus (MZ) waren für diesen Bericht ausschließlich Erstergebnisse verfügbar. Daher können vergleichbare Analysen zu einem späteren Zeitpunkt unter Verwendung der MZ-Endergebnisse des Jahres 2022 zu abweichenden Ergebnissen gelangen.

Die **Anonymisierung personenbezogener Daten** stellt dabei eine Verarbeitung nach Art. 4 Nr. 2 DSGVO dar, für welche eine solche Rechtsgrundlage bestehen muss. Der EU-Verordnungsgeber hat in der genannten Vorschrift den Verarbeitungsbegriff sehr weit gefasst und keine abschließende Aufzählung von Verarbeitungsformen vorgenommen.

Als Rechtsgrundlage wäre vor allem zu prüfen, ob gegebenenfalls landesrechtliche Vorschriften eine Anonymisierung für konkrete statistische Zwecke autorisieren.

Handelt es sich bei der Erstellung des Sozialberichts um eine Kommunalstatistik, so müssen die Vorgaben nach dem Landesstatistikgesetz erfüllt werden:

Auszug aus § 7 Landesstatistikgesetz

(1) Die Gemeinden, Kreise und Ämter können zur Wahrnehmung ihrer Selbstverwaltungsaufgaben eigene Statistiken mit oder ohne Auskunftspflicht durchführen, soweit das Statistische Amt für Hamburg und Schleswig-Holstein Einzelangaben in dem erforderlichen Umfang nicht zur Verfügung stellen kann.

(2) Statistiken nach Absatz 1 sind durch Satzung anzuordnen. [...]

Was ist zu tun?

Die Kommunen müssen vor der Erstellung von Sozialberichten prüfen, ob Angaben aus anderen Statistiken verwendet werden oder ob bestimmte Angaben nur auf Basis einer Anonymisierung personenbezogener Daten ermittelbar wären. Für die Anonymisierung müssen wiederum konkrete Rechtsgrundlagen bestehen. Fehlen diese, darf die Anonymisierung nicht erfolgen.

4.2 Polizei und Verfassungsschutz

4.2.1 Gesetzliche Prüfpflichten nach dem Landesverwaltungsgesetz

Gegenstand der Prüfung	Prüfturnus
a) Bundesgesetzliche Prüfpflichten	
Antiterrordatei (ATD)	alle 2 Jahre
Rechtsextremismusdatei (RED)	alle 2 Jahre
b) EU-Rechtsinstrumente	
Schengener Informationssystem (SIS II)	N.SIS II: alle 4 Jahre im Übrigen: regelmäßig
Visa-Informationssystem (VIS)	N-VIS: alle 4 Jahre Abfragen alle 4 Jahre im Übrigen: regelmäßig
European Dactyloscopy-System (Eurodac)	jährlich
Einreise-/ Ausreisesystem (Entry-/Exit-System – EES)	alle 3 Jahre im Übrigen: regelmäßig
Interoperabilität zw. EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration)	Überprüfung der CIR-Zugangsprotokolle: alle 6 Monate Datenverarbeitungsvorgänge der nationalen Behörden: alle 4 Jahre
c) Landesrechtliche Prüfpflichten (SH)	
Verdeckte Maßnahmen (LVwG) nach: § 180a Abs. 2 § 180a Abs. 4 § 185 (mehrere Maßnahmen) § 185a § 185b § 185c § 195a	mindestens alle 2 Jahre stichprobenartige Überprüfungen
Übermittlungen an Drittstaaten nach: § 193 LVwG §§ 54 bis 57 LDSG	mindestens alle 2 Jahre stichprobenartige Überprüfungen

Mit der letzten größeren Novellierung des Polizeirechts sind auch Prüfpflichten für das ULD in das Gesetz aufgenommen worden (40. TB, Tz. 4.2.1). Danach müssen bestimmte Maßnahmen alle zwei Jahre durch uns **stichprobenartig** überprüft werden.

Dies betrifft die besonders eingriffsintensiven, in der Regel verdeckten, **präventiven polizeilichen Maßnahmen**. Dazu gehören etwa Telekommunikationsüberwachung, Auskunft über Telekommunikationsbestandsdaten, Observationen oder der Einsatz von Vertrauenspersonen. Über diese Maßnahmen muss die Polizei außerdem den Landtag unterrichten.

Im Berichtszeitraum hat die Polizei die Überarbeitung ihrer Prozesse an die Erfordernisse der Pflichtprüfungen abgeschlossen. Dabei ging es u. a. um die Art und den Umfang der Protokollierung der Maßnahmen bei der Polizei sowie die damit verbundenen polizeiinternen Prozesse. Außerdem stellte sie uns eine Übersicht der im Jahr 2023 durchgeführten Maßnahmen zur Verfügung. Wir haben auf dieser Grundlage eine Stichprobe ausgewählt, die im Jahr 2026 geprüft werden wird. Davon betroffen sind alle Polizeidirektionen, die verdeckte Maßnahmen durchgeführt haben, sowie das Landeskriminalamt.

Neben der Prüfung der Stichprobe wird es auch um die Frage gehen, ob und inwieweit die bestehende Protokollierung der verdeckten Maßnahmen im Hinblick auf eine effektive Überprüfung verbessert werden kann.

4.2.2 Gesetzentwurf der Landesregierung: Einführung von biometrischer Gesichtserkennung und Datenanalyse bei der Polizei

Das Innenministerium hat im Berichtszeitraum einen Gesetzentwurf erarbeitet, mit dem die Landespolizei neue Befugnisse erhalten soll. Darunter befinden sich Maßnahmen mit erheblichem Eingriffsgewicht, z. B.:

- Fernidentifizierung durch biometrische Gesichtserkennung im öffentlichen Raum,
- nachträgliche biometrische Gesichtserkennung mit Daten aus dem Internet,
- automatisierte Datenanalyse.

Gleichzeitig sollen die Voraussetzungen für den Einsatz von **Videoüberwachung** durch die Polizei oder durch Ordnungsbehörden im öffentlichen Raum abgesenkt werden. Damit wäre ein Einsatz polizeilicher Videoüberwachung im öffentlichen Raum künftig in weiterem Umfang möglich, als es bislang der Fall ist.

Die vorgeschlagenen Regelungen ermächtigen die Polizei zu erheblichen Grundrechtseingriffen. Besonders schwerwiegend sind sie deshalb, weil von ihnen regelmäßig eine große Menge von Personen betroffen ist, von denen die meisten keinen Anlass für die Maßnahme gegeben haben und nur durch Zufall darin einbezogen werden.

Das Innenministerium hat das ULD zu dem geplanten Gesetzentwurf angehört. In unserer Stellungnahme haben wir in genereller Hinsicht die Frage nach der Verhältnismäßigkeit der neuen Eingriffsbefugnisse gestellt. Denn die Erläuterungen im Referentenentwurf erscheinen uns nicht dazu geeignet, die **fachliche Erforderlichkeit** der weitreichenden Eingriffsbefugnisse zu begründen. Zu den konkreten Regelungsvorschlägen haben wir ebenfalls Änderungen vorgeschlagen. Der Gesetzentwurf wird voraussichtlich 2026 in den Landtag eingebracht.

4.2.3 Einführung der elektronischen Aufenthaltsüberwachung zum Schutz von Opfern häuslicher Gewalt

Im Berichtszeitraum hat der Schleswig-Holsteinische Landtag eine Änderung des Landesverwaltungsgesetzes beschlossen, mit der die elektronische Aufenthaltsüberwachung auch zum Schutz von Opfern häuslicher Gewalt eingeführt worden ist. Gefährder können seitdem auch bei drohender häuslicher Gewalt zum Tragen einer **elektronischen Fußfessel** verpflichtet werden, mit der ihr Aufenthaltsort überwacht werden kann. Mit der Gesetzesänderung wurde in Schleswig-Holstein das sogenannte spanische Modell eingeführt. Dies bedeutet, dass auf freiwilliger Basis das Opfer ebenfalls ein Ortungsgerät erhalten kann. In der Überwachungsstelle werden die Aufenthaltsdaten von Gefährder und Opfer abgeglichen und das Opfer

erhält über das Gerät eine Warnung, wenn sich die gefährdende Person in seiner Nähe befindet.

Das ULD ist im Gesetzgebungsverfahren beteiligt worden und hat gegenüber dem Innen- und Rechtsausschuss des Schleswig-Holsteinischen Landtags schriftlich und im Rahmen einer Anhörung im Ausschuss mündlich Stellung genommen. Im Gesetzgebungsverfahren konnten wir einige **Verbesserungen** erreichen.

So ist die Schwelle für Maßnahmen auf *bestimmte* Tatsachen für die Annahme einer Gefahr heraufgesetzt worden. Außerdem wurde auf unseren Hinweis hin ergänzt, dass für die Zustimmung des Opfers zum Tragen eines eigenen Ortungsgeräts dieselben Transparenzanforderungen und Widerrufsmöglichkeiten gelten wie für eine datenschutzrechtliche Einwilligung. Die Zustimmung ist damit jederzeit mit Wirkung für die Zukunft widerrufbar. Zudem konnten wir erreichen, dass eine Weiterverarbeitung der mittels des Geräts erlangten Standortdaten für die Verfolgung auch anderer Straftaten nur für die Standortdaten der gefährdenden Person, nicht aber für die Standortdaten des Opfers zugelassen wurde.

4.2.4 Zweckänderung im OWi-Verfahren: Zulässig – aber nicht ohne dokumentierte Aktenlage

Ein Petent wandte sich an das ULD, weil Informationen aus einem Ordnungswidrigkeitenverfahren innerhalb der Polizei an seine Dienststelle und an seinen unmittelbaren Vorgesetzten weitergegeben worden waren. Der Betroffene war zum Zeitpunkt des Vorfalls privat unterwegs und hatte sich vor Ort nicht als Polizeibeamter zu erkennen gegeben, wurde jedoch als solcher erkannt. Aus Sicht des Petenten war die interne Weitergabe ein unzulässiger Dienstweg aus einem privaten Vorfall – und damit eine Verletzung seiner Rechte.

Im Verfahren stellte sich zunächst die Grundfrage: Darf eine Stelle Daten aus einem Ordnungswidrigkeitenverfahren überhaupt für einen anderen Zweck nutzen – hier zur Prüfung möglicher beamtenrechtlicher Pflichtverletzungen oder zur Bewertung von Eignung, Zuverlässigkeit oder Befähigung?

Materiell-rechtlich – also inhaltlich – war die Zweckänderung hier vertretbar. Für eine Übermittlung zur dienstlichen Eignungsprüfung reicht es jedoch nicht, dass jemand „irgendwie auffällt". Es müssen Tatsachen vorliegen, die zumindest begründete Zweifel an Eignung, Zuverlässigkeit oder Befähigung auslösen können. Im geprüften Fall wurden hierfür mehrere Gesichtspunkte angeführt (u. a. das Verhalten im Zusammenhang mit der Ordnungswidrigkeit sowie Umstände, die im Gesamtbild eine Relevanz für dienstliche Pflichten nahelegen können). Zudem verlangen die gesetzlichen Grundlagen „besondere Umstände des Einzelfalls" sowie eine Interessenabwägung. Auch die schutzwürdigen Interessen der betroffenen Person müssen in die Abwägung einfließen. In der Gesamtschau konnte die Übermittlung in diesem Einzelfall als rechtmäßig eingeordnet werden.

Damit war das Verfahren aber nicht erledigt. Denn Datenschutzrecht erschöpft sich nicht in der Frage „Dürfen wir das?", sondern verlangt auch: „Können wir später nachvollziehbar zeigen, warum wir es durften?" Genau daran fehlte es hier. Für zweckändernde Nutzungen – erst recht wenn Vorgänge als sensibel gekennzeichnet sind – braucht es eine **dokumentierte Prüfung der gesetzlichen Voraussetzungen und der Abwägung**. Die Dokumentation ist kein Selbstzweck: Sie ist Voraussetzung dafür, dass Rechtsaufsicht, Gerichte und Aufsichtsbehörden Entscheidungen überprüfen können. Sie schützt am Ende auch die handelnden Behörden selbst, weil sie belegt, dass nicht „aus dem Bauch heraus", sondern regelgebunden entschieden wurde.

Im konkreten Fall ließ sich aus der Aktenlage nicht nachvollziehen, ob und wie die Zweckänderung vor der Übermittlung tatsächlich geprüft und abgewogen wurde. Eine solche Prüfung ist gerade dann erforderlich, wenn mehrere gesetzliche Voraussetzungen erfüllt sein müssen und der Vorgang zudem als sensibel eingestuft wird. Dass die rechtliche Einordnung im Laufe des Verfahrens durch die Polizeidirektion erst nachträglich geschärft werden musste, unterstreicht das Problem: Ohne eine kurze, saubere und aktenkundige Begründung bleibt offen, welche Erwägungen zum Zeitpunkt der Entscheidung maßgeblich waren. Deshalb haben wir gegenüber der Polizeidirektion einen Verstoß gegen die Dokumentationspflichten festgestellt und eine Verwarnung ausgesprochen.

Was ist zu tun?

Behörden sollten bei zweckändernden Nutzungen eine kurze, aber nachvollziehbare Prüfdokumentation in der Akte führen: Rechtsgrundlagen, besondere Umstände des Einzelfalls, Abwägung der betroffenen Interessen und Ergebnis. Dies reduziert Risiken, erleichtert interne Qualitätssicherung und schafft die nötige Transparenz für Kontrolle und Rechtsschutz.

4.2.5 Löschanspruch trifft Fachverfahren: owi21 braucht eine nachvollziehbare Löschfunktion

Im Rahmen einer konkreten Beschwerde hat das ULD geprüft, ob das Fachverfahren owi21 die gesetzlichen Anforderungen an die Löschung personenbezogener Daten erfüllt. Im vorliegenden Fall ging es konkret um die Bearbeitung von Verkehrsordnungswidrigkeiten in owi21. Ergebnis: In der derzeit genutzten Programmversion ist eine manuelle Löschung weder von ganzen Vorgängen noch von einzelnen personenbezogenen Daten innerhalb eines Vorgangs möglich. Die Löschung erfolgt stattdessen ausschließlich automatisiert – nach Abschluss des Verfahrens und einer anschließenden Aufbewahrung zu Dokumentationszwecken von sechs Monaten.

Diese pauschale Dauer der Aufbewahrung orientiert sich an einem Erlass zur Aufbewahrung von Bußgeldakten aus dem Jahr 1998. Grundsätzlich ist eine solche allgemeine Aufbewahrungsfrist nicht zu beanstanden: Behörden müssen ihr Handeln dokumentieren, damit es später überprüfbar bleibt – dies dient auch dem Schutz der Rechte betroffener Personen. Entscheidend ist aber: **Eine allgemeine Speicherfrist ersetzt keine Einzelfallprüfung, wenn eine betroffene Person die Löschung verlangt.**

Die Rechtslage hat sich seit 1998 erheblich weiterentwickelt. Unabhängig davon, ob im Bußgeldkontext § 58 BDSG oder die einschlägigen Regelungen des Landesdatenschutzrechts herangezogen werden, **kann im Einzelfall ein Anspruch auf unverzügliche Löschung bestehen** – etwa wenn Daten unzulässig verarbeitet wurden, für die Aufgabenerfüllung nicht mehr erforderlich sind oder aufgrund einer rechtlichen Verpflichtung zu löschen sind. Dies betrifft nicht nur den ganzen Vorgang, sondern kann auch einzelne, unrechtmäßig erhobene Daten betreffen (z. B. bei einem offensichtlichen Erfassungs- oder Ablesefehler).

Besonders wichtig: Ein Löschanspruch darf nicht allein mit dem Hinweis abgelehnt werden, die eingesetzte Software könne das technisch nicht. Die gesetzlichen Ausnahmen, die eine Löschung trotz Anspruch im Einzelfall zulassen können, sind eng auszulegen. Erwartet wird vielmehr, dass **die IT-Infrastruktur so ausgestaltet ist, dass Löschpflichten technisch auch tatsächlich erfüllt werden können**.

Datenschutz durch Technikgestaltung

Die JI-Richtlinie (EU 2016/680) sieht gemäß Artikel 20 vor, dass bereits bei der Planung von IT-Systemen sichergestellt werden muss, dass sie dafür ausgelegt sind, Datenschutzgrundsätze wirksam umzusetzen. Im nationalen Recht wurde dieser Grundsatz in § 71 Bundesdatenschutzgesetz (BDSG) und § 47 Landesdatenschutzgesetz (LDSG) verankert.

Wo eine Löschung vorzunehmen ist, endet die Pflicht nicht mit dem „Wegklicken" von Daten. Die Löschung muss **nachvollziehbar dokumentiert** werden: mindestens **wer wann was gelöscht hat und warum** (z. B. durch den Löschantrag). Diese Dokumentation ist so lange aufzubewahren, wie die ursprünglichen Daten ohne Löschung aufzubewahren gewesen wären.

Da owi21 in Schleswig-Holstein von einer Vielzahl an Behörden eingesetzt wird, ist davon auszugehen, dass das Problem über den konkreten Fall hinausgehend auch andere Behörden betrifft. Weitere Behörden, von denen bekannt war, dass sie owi21 einsetzen, wurden über das Ergebnis der Prüfung informiert.

Was ist zu tun?

Behörden, die owi21 einsetzen, sollten kurzfristig klären, wie Löschanträge derzeit rechtssicher bearbeitet werden können (inklusive Einzelfallprüfung und Begründung). Soweit dies noch nicht funktionieren sollte, muss owi21 zeitnah dahin gehend verändert werden, dass (1) ganze Vorgänge und (2) unrechtmäßig erhobene Daten auf Antrag nachvollziehbar gelöscht werden können – inklusive einer Protokollierung der Löschung (wer/wann/warum) und Aufbewahrung dieser Dokumentation für die Dauer der ursprünglichen Speicherfrist. Eine Software, die eine rechtskonforme Bearbeitung von Löschanträgen durch die Behörden verhindert, dürfte nicht zum Einsatz kommen.

4.2.6 Gefährderansprache am Scheibenwischer

Ein Bürger wandte sich mit einer Beschwerde an das ULD, weil er nach einer körperlichen Auseinandersetzung mit einer anderen Person im öffentlichen Raum an seinem regelmäßig genutzten Parkplatz in der Nähe eines Bahnhofs einen Brief der Polizei unter dem Scheibenwischer vorfand. Auf dem Umschlag standen sein Name und seine private Anschrift. Die Polizei hatte den Umschlag nach eigenen Angaben so platziert, dass das Adressfeld nach innen zeigte, um es möglichst zu verdecken. Trotzdem blieb das Grundproblem bestehen: Jede Person auf dem Parkplatz hätte den Brief mit einem Handgriff drehen und die Daten lesen können.

Der Fall ist nicht nur eine Frage korrekter Zustellung, sondern berührt unmittelbar die Vertraulichkeit personenbezogener Daten – und damit auch das Sicherheitsgefühl der betroffenen Person. Denn der Petent schilderte, dass sein Konfliktpartner das von ihm genutzte Fahrzeug sehr genau kannte und sich regelmäßig im Umfeld aufhielt. Nach der Zustellung am Scheibenwischer habe sein Konfliktpartner ihn zudem plötzlich mit seinem Namen angesprochen. Ob der Name tatsächlich über den Umschlag bekannt wurde, lässt sich im Nachhinein nicht sicher beweisen – entscheidend ist aber: Die Möglichkeit einer unbefugten Kenntnisnahme bestand und war angesichts der Umstände besonders naheliegend.

Nach § 22 Abs. 1 Nr. 6 LDSG müssen personenbezogene Daten so verarbeitet werden, dass eine angemessene Sicherheit gewährleistet ist. Dazu gehört gerade auch der Schutz vor unbefugter Kenntnisnahme. Im öffentlichen Raum – und insbesondere an Orten mit Publikumsverkehr – reicht es nicht, Daten „irgendwie" zu verdecken, wenn sich die getroffene Schutzmaßnahme mit geringem Aufwand umgehen lässt. **Wenn Name und Anschrift sichtbar gemacht werden können, liegt ein Sicherheitsrisiko auf der Hand.**

Die Polizei begründete ihr Vorgehen mit zeitlicher Dringlichkeit: Mit dem Schreiben habe sie eine Gefährderansprache durchgeführt. Diese sei kurzfristig erforderlich gewesen, eine Postzustellung dauere zu lange. Dieses Anliegen ist nachvollziehbar. Gerade bei potenziellen Eskalationslagen müssen Behörden handlungsfähig sein und schnell reagieren können. Geschwindigkeit entbindet aber nicht von der Pflicht, den Schutz personenbezogener Daten mitzudenken – zumal es hier nicht um irgendeine Verwaltungsinformation ging, sondern um Daten, die in der konkreten Konfliktlage zusätzliche Risiken auslösen können.

In der Prüfung zeigte sich, dass es **mildere, gleich geeignete Alternativen** gegeben hätte. Dazu gehört etwa eine **persönliche Übergabe** oder eine **kurzfristige Zustellung an der Wohnanschrift**. Auch ein neutraler Hinweis ohne personenbezogene Daten – mit der Bitte um umgehende Kontaktaufnahme zur Dienststelle – wäre möglich gewesen. Die für jedermann sichtbare Zustellung am Fahrzeug war daher in der gewählten Form nicht erforderlich. Dabei ist zu berücksichtigen, dass die Konfliktpartei sich regelmäßig in der Nähe aufhielt und das Fahrzeug des Betroffenen gut kannte. Das Risiko, dass gerade diese Person oder auch unbeteiligte Dritte die Daten zur Kenntnis nehmen, war nicht nur theoretisch, sondern real.

Im Ergebnis wurde ein Verstoß gegen § 22 Abs. 1 Nr. 6 LDSG festgestellt. Der Fall macht deutlich, dass ein vermeintlich praktikables Vorgehen im Einsatzalltag schnell zu einem Datenschutzproblem werden kann, wenn damit personenbezogene Daten unnötig dem Zugriff Dritter ausgesetzt werden – und dass diese Risiken gerade in konfliktbelasteten Situationen besonders ernst zu nehmen sind.

Was ist zu tun?

Behörden müssen bei Zustellungen mit personenbezogenen Daten auch unter Zeitdruck ausreichend datenminimierende und sichere Zustellwege wählen. Wo eine unmittelbare Kontaktaufnahme erforderlich erscheint, kommen insbesondere persönliche Übergaben oder neutrale Kontaktzettel ohne weiteren Personenbezug in Betracht. In konfliktbelasteten Situationen ist das Risiko unbefugter Kenntnisnahme in die Abwägung einzubeziehen und durch geeignete organisatorische Maßnahmen einzudämmen.

4.2.7 Novellierung des Landesverfassungsschutzgesetzes

Die Landesregierung hat im Berichtszeitraum eine **Novelle des Landesverfassungsschutzgesetzes** vorgelegt. Zu dem Gesetzentwurf haben wir gegenüber der Landesregierung Stellung genommen. Mit dem Gesetzentwurf soll das Verfassungsschutzgesetz vollständig reformiert und an **verfassungsrechtliche Vorgaben** der neueren Rechtsprechung des Bundesverfassungsgerichts sowie an veränderte fachliche Erfordernisse angepasst werden. Gleichzeitig werden die Regelungen zum Datenschutz aktualisiert, was wir für unbedingt erforderlich halten und in der Zielrichtung uneingeschränkt begrüßen.

Die derzeitige Regelung des Datenschutzrechts für die Verfassungsschutzbehörde ist **unübersichtlich und enthält Lücken**. Durch die EU-Datenschutzreform und deren Umsetzung im Landesrecht im Jahr 2018 sind bisher geltende allgemeine Datenschutzregelungen im Landesdatenschutzgesetz (LDSG) weggefallen. Sie sind durch Verweisungen in § 2 Abs. 7 LDSG auf einzelne Vorschriften des Landesdatenschutzgesetzes und einzelne Vorschriften des Bundesdatenschutzgesetzes ersetzt worden. Dies ist nicht nur für die Rechtsanwendenden unübersichtlich, sondern hat auch zu Regelungslücken geführt. Aufgaben und Befugnisse der Datenschutzaufsichtsbehörde und das Recht für betroffene Personen, die Datenschutzaufsichtsbehörde anzurufen, sind von den Verweisungen in § 2 Abs. 7 LDSG nur unzureichend erfasst. Auf unsere Kontrollpraxis hat sich dies nicht negativ ausgewirkt, aber eine **klare gesetzliche Regelung ist erforderlich**.

Durch unsere Stellungnahme konnten wir einige Verbesserungen in dem Gesetzentwurf erreichen. Dennoch bleiben wichtige Fragen offen, beispielsweise zur vorgesehenen Einführung der **automatisierten Datenanalyse unter Nutzung von künstlicher Intelligenz**. Wir werden diese Fragen in das nun anstehende parlamentarische Verfahren einbringen.

4.3 Justiz

4.3.1 Aushang eines Fotos nach Erteilung eines Hausverbots

Meine Dienststelle erhielt im Berichtszeitraum eine Beschwerde von einer Person, gegenüber der ein Hausverbot für ein Gerichtsgebäude ausgesprochen worden war. Zur Umsetzung dieses Hausverbots im Bereich der Gerichtshilfe war in deren Räumen ein Foto der betroffenen Person ausgehängt worden. Auf

dem Bild war auch das Geburtsdatum dieser Person enthalten. Es war zudem so angebracht, dass jeder, der das Gericht aufsuchte, den Aushang zur Kenntnis nehmen konnte. Die betroffene Person hat Kenntnis von der Existenz des Aushangs erlangt und dies telefonisch dem Gericht mitgeteilt, woraufhin der Aushang unverzüglich entfernt wurde. Die betroffene Person reichte aufgrund des datenschutzrechtlichen Verstoßes eine Beschwerde bei der Landesbeauftragten für Datenschutz ein. Gleichzeitig meldete die Staatsanwaltschaft, der die Gerichtshilfe zugeordnet ist, uns den Vorfall als Datenpanne.

Das öffentliche Aushängen des Lichtbilds der betroffenen Person war nicht durch eine gesetzliche Grundlage gerechtfertigt. Der Umstand, dass sich der Aushang für einen Zeitraum von mehreren Jahren öffentlich im Gerichtsgebäude befand und somit für Beschäftigte und Besucher einsehbar war, hat zu einer erheblichen Verletzung der Grundrechte und Grundfreiheiten der betroffenen Person geführt. Aufgrund des festgestellten datenschutzrechtlichen Verstoßes wurde die Staatsanwaltschaft für dieses Vorgehen gemäß Art. 58 Abs. 2 Buchst. b DSGVO verwarnt.

4.4 Soziales

4.4.1 Befreiung vom Bankgeheimnis – eine Blankovollmacht wird nicht benötigt

Immer wieder berichten Antragstellerinnen und Antragsteller von Sozialleistungen, dass sie aufgefordert wurden, ihre Kreditinstitute vom Bankgeheimnis zu befreien. Mit einer vorgefertigten Erklärung sollen sich die Betroffenen damit einverstanden erklären, dass die Kreditinstitute der Sozialleistungsbehörde jederzeit und ohne Einschränkung Auskunft über den Kontostand und über Kontobewegungen geben.

Diese pauschale Befugnis zur Datenerhebung ist jedoch weder gesetzlich vorgesehen noch unterliegt es der Mitwirkungspflicht der betroffenen Personen, diese Erklärung zu unterschreiben.

Sozialleistungsträger, die diese Erklärungen (noch) verwenden, scheinen zudem ihre eigenen gesetzlich vorgesehenen Befugnisse nicht zu kennen.

So sieht sowohl das SGB II als auch das SGB XII vor, dass **Kreditinstitute unabhängig von einer Einwilligung der Betroffenen den Sozialleistungsbehörden auf Verlangen über Einkommen und Vermögen Auskunft zu erteilen haben**, soweit dies zur Durchführung der Leistungen im Einzelfall erforderlich ist.

Das Auskunftsersuchen der Sozialleistungsbehörde muss also unter Berücksichtigung der Besonderheiten des Einzelfalles zur Aufgabenerfüllung erforderlich sein. Ein pauschales, unbegründetes und somit nicht erforderliches Auskunftsverlangen wird durch die gesetzlichen Regelungen nicht gedeckt.

§ 60 Abs. 2 Satz 1 SGB II – Bürgergeld, Grundsicherung für Arbeitsuchende – Auskunftspflicht

Wer jemandem, der eine Leistung nach diesem Buch beantragt hat oder bezieht, zu Leistungen verpflichtet ist, die geeignet sind, Leistungen nach diesem Buch auszuschließen oder zu mindern, oder wer für ihn Guthaben führt oder Vermögensgegenstände verwahrt, hat der Agentur für Arbeit auf Verlangen hierüber sowie über damit im Zusammenhang stehendes Einkommen oder Vermögen Auskunft zu erteilen, soweit es zur Durchführung der Aufgaben nach diesem Buch erforderlich ist.

§ 117 Abs. 3 Satz 1 SGB XII – Sozialhilfe – Auskunftspflicht

Wer jemandem, der Leistungen nach diesem Buch beantragt hat oder bezieht, zu Leistungen verpflichtet ist oder war, die geeignet sind oder waren, Leistungen auszuschließen oder zu mindern, oder für ihn Guthaben führt oder Vermögensgegenstände verwahrt, hat dem Träger der Sozialhilfe auf Verlangen hierüber sowie über damit im Zusammenhang stehendes Einkommen oder Vermögen Auskunft zu erteilen, soweit es zur Durchführung der Leistungen nach diesem Buch im Einzelfall erforderlich ist.

Was ist zu tun?

Sozialleistungsbehörden müssen ihre Vordrucke regelmäßig überprüfen und bei Bedarf an die aktuelle Gesetzeslage anpassen.

4.4.2 Sozialdaten zum Mitlesen – unverschlüsselter Versand

Die Arbeit in den Jugendämtern, Wohngeldstellen oder Grundsicherungsbehörden kann stressig sein. Nachfragen bei Antragstellenden, fehlende Unterlagen anfordern oder sich mit den Kolleginnen und Kollegen austauschen. Alles muss schnell gehen. Einfach und schnell kann man per E-Mail kommunizieren. Aber was ist dabei zu beachten?

Die personenbezogenen Daten der Antragstellenden und Leistungsempfangenden unterliegen als Sozialdaten den hohen Anforderungen des Sozialdatenschutzes. Die Sozialleistungsträger sind in der Pflicht, auch bei der Übermittlung von Sozialdaten durch technische und organisatorische Maßnahmen sicherzustellen, dass Unbefugte von diesen keine Kenntnis erlangen können.

Eine unverschlüsselte E-Mail via Internet wird diesen gesetzlichen Anforderungen nicht gerecht und ist regelhaft als Datenschutzverletzung zu bewerten.

2017 wiesen wir in unserem Informationsbeitrag „Sozialdaten dürfen nicht per unverschlüsselter E-Mail via Internet übermittelt werden!“ auf die Gefahren dieser unsicheren Kommunikation und die möglichen Alternativen hin. Die Anforderungen haben sich durch die DSGVO noch einmal konkretisiert (36. TB, Tz. 4.5.1).

Übrigens, auch mit Kenntnis oder der Einwilligung der Betroffenen ist die Nutzung eines unsicheren Übermittlungsweges grundsätzlich unzulässig (Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 24.11.2021).

Was ist zu tun?

Sozialleistungsträger müssen gewährleisten, dass Sozialdaten nur auf sicheren Wegen übermittelt werden. Sollen Sozialdaten per E-Mail via Internet übermittelt werden, müssen angemessene Sicherheitsvorkehrungen getroffen werden (z. B. Möglichkeit der Verschlüsselung). Die Beschäftigten sind regelmäßig zu schulen.

4.5 Schutz des Patientengeheimnisses

4.5.1 Kein Auskunftsanspruch nach dem Tod des Patienten?

Wenn ein Angehöriger stirbt, haben Hinterbliebene häufig Fragen und hoffen Antworten in der Patientenakte des Verstorbenen zu finden. Eine Klinik weigerte sich, den Angehörigen die Auskunft zu erteilen, und verwies darauf, dass die Vorschriften der DSGVO für die Verarbeitung der personenbezogenen Daten von Verstorbenen keine Anwendung finden würden. Die Angehörigen könnten daher ihr Auskunftsersuchen nicht auf die DSGVO stützen. Die Angehörigen baten um Unterstützung.

Die Einschätzung der Klinik ist zutreffend. Maßgeblich ist insoweit der Erwägungsgrund 27 der DSGVO. Die Vorschriften der DSGVO gelten nicht für die Verarbeitung von personenbezogenen Daten von Verstorbenen.

Aber das ist nur die halbe Wahrheit.

So findet sich im § 630g Abs. 3 Bürgerliches Gesetzbuch (BGB) der zivilrechtliche Anspruch, dass im Fall des Todes eines Patienten den Erben zur Wahrnehmung vermögensrechtlicher Interessen das Recht zur Einsichtnahme in die Patientenakte zusteht. Gleiches gilt für die nächsten Angehörigen des Patienten, soweit diese immaterielle Interessen geltend machen. Diese Rechte der Angehörigen sind nur dann ausgeschlossen, soweit der Einsichtnahme der ausdrückliche oder mutmaßliche Wille des verstorbenen Patienten entgegensteht. Zur Durchsetzung dieses Anspruches können Angehörige den zivilrechtlichen Rechtsweg beschreiten.

§ 630g BGB

(1) Dem Patienten ist auf Verlangen unverzüglich Einsicht in die vollständige, ihn betreffende Behandlungsakte zu gewähren. § 811 ist entsprechend anzuwenden. Der Patient kann auch Abschriften von der Behandlungsakte, einschließlich elektronischer Abschriften, verlangen. Die erste Abschrift wird unentgeltlich zur Verfügung gestellt.

(2) Das Recht nach Absatz 1 besteht nicht, soweit erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Die Ablehnung der Einsichtnahme ist zu begründen.

(3) Im Fall des Todes des Patienten stehen die Rechte nach Absatz 1 zur Wahrnehmung der vermögensrechtlichen Interessen seinen Erben mit der Maßgabe zu, dass die Erben die entstandenen Kosten zu erstatten haben. Gleiches gilt für die nächsten Angehörigen des Patienten, soweit sie immaterielle Interessen geltend machen. Die Rechte sind ausgeschlossen, soweit der Einsichtnahme der ausdrückliche oder mutmaßliche Wille des Patienten entgegensteht.

(4) Datenschutzrechtliche Rechte des Betroffenen bleiben von den Absätzen 1 bis 3 unberührt, soweit in diesem Absatz nichts anderes geregelt ist. Soweit datenschutzrechtliche Auskunftsansprüche und Informationspflichten unentgeltlich zu erfüllen sind, steht dies Entgelten für Einsichtnahmen nach Absatz 1 entgegen. Der Ausschluss des Einsichtsrechts nach Absatz 2 steht im Verhältnis zwischen Behandelndem und Patienten auch datenschutzrechtlichen Auskunftsansprüchen und Informationspflichten entgegen.

4.5.2 Anspruch auf Kopie der Patientenakte per Post?

Im letzten Jahr wurde uns von Beschwerdeführern geschildert, dass Arztpraxen sich weigern würden, ihnen Kopien der **Patientenunterlagen** per Post zu schicken. Man sei aufgefordert worden, persönlich in der Praxis die Unterlagen abzuholen. Zur Begründung hätten die Praxen darauf hingewiesen, dass die Versichertenkarte eingelesen werden müsste oder die Ärztin bzw. der Arzt zunächst ein persönliches Gespräch führen wolle. Allerdings hatten die betroffenen Personen gute Gründe, warum sie nicht in der Praxis vorstellig werden wollten.

Besteht ein Anspruch darauf, dass die Arztpraxis die angeforderten Kopien per Post übersendet?

Artikel 15 DSGVO sieht vor, dass betroffene Personen von dem Verantwortlichen eine Bestätigung darüber verlangen können, ob sie betreffende personenbezogene Daten verarbeitet werden und – wenn ja – ein Recht auf Auskunft über diese personenbezogenen Daten haben. Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, dem Betroffenen zur Verfügung. Die erste Kopie der Patientenunterlagen ist kostenfrei (42. TB, Tz. 4.5.3).

Diese Vorschriften sehen nicht vor, dass Patientinnen und Patienten

- ihre Unterlagen persönlich in der Arztpraxis abholen müssen,
- die Versichertenkarte eingelesen werden muss oder
- ihr Auskunftsverlangen zunächst in einem Gespräch mit der Ärztin bzw. dem Arzt erklären.

Selbstverständlich muss die Arztpraxis sicherstellen, dass auch bei einer Auskunft bzw. wenn eine Kopie der Unterlagen zur Verfügung gestellt werden soll, unbefugte Personen keine Kenntnis von den Gesundheitsdaten erhalten. Patientenunterlagen dürfen nicht in falsche Hände gelangen. Die Arztpraxis muss die Identität des Auskunftssuchenden und seinen Auskunftsanspruch prüfen. Geforderte Kopien können in der Praxis ausgehändigt oder auf Wunsch des Patienten per Post an eine von dem Auskunftssuchenden angegebene und von der Arztpraxis verifizierte Postanschrift übermittelt werden (z. B. per Einschreiben).

Hat die Arztpraxis begründete Zweifel an der Identität des Auskunftssuchenden, so kann diese zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind. Dies gilt insoweit auch, wenn z. B. Zweifel an der Richtigkeit oder der Aktualität der angegebenen bzw. bislang bekannten Kontaktdaten bestehen.

Aufgepasst! Stellt die Patientin oder der Patient ihren/seinen Auskunftsantrag elektronisch, so sind die geforderten Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern die Patientin oder der Patient nichts anderes angibt (Art. 15 Abs. 3 DSGVO).

Was ist zu tun?

Arztpraxen müssen die Datenschutzrechte ihrer Patientinnen und Patienten beachten und gewährleisten. Hierzu zählt auch das Auskunftsrecht. Bei der Wahrnehmung des Auskunftsrechts sind die Patientinnen und Patienten zu unterstützen. Die unbegründete Verweigerung, eine Kopie der Patientenakte zur Verfügung zu stellen, stellt eine Datenschutzverletzung dar und kann entsprechend geahndet werden.

4.5.3 Arztpraxis erteilt keine Auskunft – Anordnung der Ersatzzwangshaft?

Eine kleine Scheuerstelle am Fuß, die Wunde entzündete sich und am Ende musste der Fuß amputiert werden. Hatten die behandelnden Ärzte alles richtig gemacht? Der Patient wollte seine Patientenakten sehen. Doch ein Arzt weigerte sich.

Die Ärztekammer wurde eingeschaltet, ein Rechtsanwalt beauftragt, es ging vors Gericht, doch der Arzt reagierte einfach nicht. Der Patient bat uns um Hilfe.

Es wurde ein Verwaltungsverfahren der Datenschutzaufsicht eingeleitet. Die Arztpraxis wurde um eine (freiwillige) Stellungnahme und um Mitteilung gebeten, warum der Patient die gewünschte Auskunft nicht erhält. Aber der Arzt reagierte auch auf unsere Anhörung nicht. Anrufversuche blieben erfolglos.

Per Verwaltungsakt wurde daraufhin unter Androhung eines Zwangsgeldes angeordnet, dass die Arztpraxis unsere Fragen beantwortet. Trotzdem antwortete der Arzt nicht. Kein Wort der Erklärung. Und weiterhin keine Auskunft an den Patienten.

Mittlerweile wurden vier Zwangsgelder gegen die Arztpraxis verhängt. Das erste Zwangsgeld bezahlte die Arztpraxis, die weiteren bisher nicht. Der Rechtsanwalt des Patienten berichtete über finanzielle Schwierigkeiten der Arztpraxis. Die Landeskasse bestätigte, dass die noch offenen Zwangsgelder nicht beglichen wurden. Was nun?

§ 240 Landesverwaltungsgesetz sieht vor, dass – wenn ein Zwangsgeld uneinbringlich ist – das Verwaltungs-

gericht auf Antrag der Vollzugsbehörde die Ersatzhaft anordnen kann, wenn bei Androhung des Zwangsgeldes hierauf hingewiesen worden ist.

Mit der letzten Auskunftsanordnung und der letzten Zwangsgeldfestsetzung wurde die Arztpraxis mit Nachdruck darauf hingewiesen, dass – wenn die Auskunft weiterhin nicht erteilt wird – in einem nächsten Schritt die Beantragung der Anordnung einer Ersatzzwangshaft beim Schleswig-Holsteinischen Verwaltungsgericht geprüft wird.

Die Ersatzzwangshaft beträgt mindestens einen Tag, höchstens zwei Wochen.

Was ist zu tun?

Verantwortliche müssen bestandskräftige Auskunftsverlangen der Aufsichtsbehörde erfüllen. Bei einer hartnäckigen Weigerung, die verlangte Auskunft zu erfüllen, kommt die Beantragung einer Ersatzzwangshaft bei Gericht in Betracht.

4.5.4 Ärger durch Reaktion auf Ärztebewertung?

Unzufrieden mit Ihrer Arztpraxis? Trotz Termin wieder zu lange gewartet? Hat sich die Ärztin bzw. der Arzt nicht genügend Zeit genommen? Nicht richtig zugehört? Dann sprechen Sie dies doch direkt an. Unabhängig davon wählen Patientinnen und Patienten oft einen anderen bzw. weiteren Weg, um ihre Verärgerung kundzutun.

Patientinnen und Patienten können und dürfen über negative Erfahrungen mit Arztpraxen berichten. Hierzu zählt auch die Veröffentlichung von Rezensionen in Bewertungsportalen im Rahmen dessen, was verfassungsrechtlich zulässig ist. Geschützt wird in diesem Kontext auch eine anonyme Bewertung.

Für die Arztpraxen können negative Bewertungen schlimme Folgen haben. Patientinnen und Patienten meiden Praxen mit einer schlechten Internetbewertung.

Nicht immer sind negative Bewertungen von Patientinnen und Patienten berechtigt. Verständlicherweise möchten sich Arztpraxen wehren und Sachverhalte aus ihrer Sicht darstellen.

Aber aufgepasst! Wenn eine Antwort der Arztpraxis bedeutet, dass personenbezogene Daten von Patientinnen und Patienten im Internet veröffentlicht werden, bedarf es hierfür einer ausreichenden Befugnis, die jedoch in den meisten Fällen nicht vorliegt. Es handelt sich um **Gesundheitsdaten**, und der Schutzbedarf von Patientendaten ist hoch.

Arztpraxen müssen regelhaft mit negativen Bewertungen leben. Werturteile von Patientinnen und Patienten sind im Allgemeinen rechtlich nicht untersagt. Anderes gilt z. B. für Werturteile, die von der Meinungsfreiheit nicht geschützt sind, wie rein diffamierende Mitteilungen oder unwahre Tatsachenbehauptungen. Gegebenenfalls besteht im Einzelfall eine zivilrechtliche Möglichkeit, sich gegen die Veröffentlichung unzulässiger Werturteile zur Wehr zu setzen.

Vorsicht ist geboten, wenn die Ärztin oder der Arzt direkt auf eine Internetrezension antwortet und diese Antwort veröffentlicht: Enthält die Antwort einer Arztpraxis auf eine Internetbewertung z. B. Angaben zur Identität einer Patientin oder eines Patienten oder zum Umstand, dass und wie diese/-r in der Praxis behandelt wurde, wird dies regelhaft als Verstoß gegen das Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten zu bewerten sein, es sei denn, die betroffene Patientin oder der betroffene Patient hat sich nachweislich mit der Veröffentlichung ihrer/seiner Daten einverstanden erklärt.

4.6 Datenpannen im Medizinbereich

4.6.1 Veröffentlichung eines Recruiting-Videos – mit Patientendaten

Der kreative Versuch einer Klinik, offene Stellen mittels eines Recruiting-Videos zu besetzen, führte letztlich zu einer Datenpannenmeldung beim ULD.

Die Klinik hatte eine Agentur mit der Erstellung des Recruiting-Videos beauftragt. Diese sollte auch Einwilligungserklärungen von Mitarbeitenden und Patientinnen und Patienten einholen. Diese Vorgaben sollten seitens einer Mitarbeiterin der Klinik sichergestellt werden.

Bei der Durchführung der Filmaufnahmen in der Klinik sollten CT-Bilder von früher behandelten Patientinnen und Patienten an den Geräten eingeblendet und abgefilmt werden. Die Agentur wurde in diesem Zusammenhang angewiesen, identifizierende Merkmale in den Aufnahmen des Rohmaterials unkenntlich zu machen, was jedoch weisungswidrig – im Anschluss auch bei der Veröffentlichung der Videos – unterlassen wurde. Verwendet wurden Aufnahmen von zwei Patienten, von denen keine entsprechende Einwilligung eingeholt wurde.

Neben den CT-Bildern waren Name, Geburtsdatum und Geschlechtskürzel erkennbar. Die Einblendung der identifizierenden Daten erfolgte nur innerhalb eines sehr kurzen Schnitts von deutlich unter einer Sekunde. Jedoch waren die Angaben bei einem Stoppen des Videos im entsprechenden Moment erkennbar. Trotz einer Kontrolle des Videos durch die Agentur und die Klinik vor einer nachfolgenden Veröffentlichung wurden die problematischen Stellen im Video nicht bemerkt und es folgten Veröffentlichungen auf verschiedenen Plattformen.

Etwa eine Woche nach der ersten Veröffentlichung des Recruiting-Videos bemerkte ein Mitarbeiter der Klinik zufällig die problematischen Stellen in dem veröffentlichten Video und meldete den Vorfall intern. Die Veröffentlichungen des Videos wurden daraufhin noch am gleichen Tag gelöscht. Die geplante Veröffentlichung des Videos auf anderen Bewerbungsplattformen wurde unterlassen. Die Agentur bestätigte nach diesbezüglicher Aufforderung durch die Klinik, sämtliche Aufnahmen mit personenbezogenen Patientendaten sofort und endgültig gelöscht zu haben.

Die verantwortliche Stelle kündigte zudem eine Social-Media-Richtlinie an, nach der jede Veröffentlichung von Patientendaten auch in anonymisierter Form auf Social Media untersagt wird. Zudem wurden spezifische Datenschutzschulungen für Mitarbeitende des PR-Bereiches angekündigt, und die verantwortliche Stelle plant den generellen Verzicht, Patientendaten für Marketing-/PR-Zwecke zu verwenden.

Die betroffenen Patienten wurden gemäß Artikel 34 DSGVO sowohl telefonisch als auch schriftlich über die Verletzung des Schutzes ihrer personenbezogenen Daten informiert.

Was ist zu tun?

Gesundheits- bzw. Patientendaten stellen Daten besonderer Kategorien im Sinne von Art. 9 Abs. 1 DSGVO dar. Insbesondere bei solchen sensiblen Daten gilt es besondere Vorsicht walten zu lassen – bereits kleinere Unaufmerksamkeiten können schwerwiegende Datenschutzverletzungen zur Folge haben.

4.6.2 Herausgabe unausgefüllter Rezepte an einen Tablettendealer

Das ULD erhielt eine Datenpannenmeldung im Medizinbereich, die das Fehlverhalten eines Mitarbeiters schilderte.

Der Mitarbeiter hatte Hilfsmittelrezepte mit echten **Patientendaten** (Name, Krankenkasse und Versichertennummer) aus dem Krankenhausinformationssystem ausgestellt, eigenhändig unterschrieben und als Blankorezepte an einen Tablettendealer, also einen unberechtigten Dritten, weitergegeben. Dieser hat die Rezepte wiederum weiter mit beliebigen Medikamenten ausgefüllt, um diese in der Apotheke erstehen zu können. Die eingetragenen Medikamente haben in keinem Zusammenhang mit Krankheiten der im Rezept genannten Patientinnen und Patienten gestanden.

Nach Feststellen dieses Fehlverhaltens wurde der Mitarbeiter befragt und er gab an, ca. 50 Rezepte unberechtigterweise ausgedruckt und unterschrieben zu haben.

Die verantwortliche Stelle handelte umgehend: Der Zugriff des Mitarbeiters auf das **Krankenhausinformationssystem** wurde gesperrt und der Mitarbeiter unverzüglich von der Arbeit freigestellt. Eine Strafanzeige wurde ebenfalls gestellt. Zudem kündigte die verantwortliche Stelle an zu prüfen, ob ein Vieraugenprinzip bei der Ausstellung von Rezepten eingeführt werden könnte, sodass zwar eine Ausstellung der Rezepte möglich wäre, die endgültige Freigabe und der Druck jedoch durch eine weitere Person ermöglicht werden müsste.

Da es sich um das bewusste Fehlverhalten eines einzelnen Mitarbeiters handelte, konnte die Meldung der verantwortlichen Stelle mit dem Hinweis abgeschlossen werden, sämtliche verbliebenen Mitarbeitenden bezüglich des Umgangs mit sensiblen personenbezogenen Daten zu sensibilisieren.

Aufgrund der bereits gestellten Strafanzeige wurde von der Einleitung eines OWi-Verfahrens gegenüber dem Mitarbeiter seitens des ULD abgesehen.

Was ist zu tun?

Um den eigenen Verpflichtungen nachzukommen, sollten Verantwortliche ihre Mitarbeitenden regelmäßig zum Umgang mit personenbezogenen Daten sensibilisieren. Datenschutzrechtliche Vorgaben der verantwortlichen Stelle sind von Mitarbeitenden einzuhalten, anderenfalls können arbeitsrechtliche und gegebenenfalls strafrechtliche Konsequenzen drohen.

4.6.3 Versand eines Arztbriefes an einen Hausarzt ohne Einwilligung der Patientin

Arztbriefe können von Kliniken an Hausärztinnen und Hausärzte übermittelt werden, wenn hierfür eine Einwilligung der Patientinnen und Patienten vorliegt. Liegt keine Einwilligung der Patientin oder des Patienten vor und wird eine Hausärztin oder ein Hausarzt dennoch Adressat/-in eines Arztbriefes, handelt es sich um einen nach Artikel 33 DSGVO meldepflichtigen Datenschutzverstoß. Eine solche Meldung erhielt das ULD von einer Klinik in Schleswig-Holstein, nachdem sich die betroffene Person bei der verantwortlichen Stelle hierüber beschwert hatte.

Das ULD eröffnete u. a. aufgrund der sehr sporadisch ausgefüllten Meldung ein Anhörungsverfahren gegenüber der verantwortlichen Stelle.

Im Laufe des Verfahrens stellte sich heraus, dass es bereits interne Vorgaben zum Versand von Arztbriefen gab, welche dennoch nicht beachtet wurden. Die internen Vorgaben legten eindeutig fest, **dass Briefe an weitere Behandler nur versendet werden dürfen, wenn eine Einwilligung hierzu vorliegt**. Entsprechende technische Voreinstellungen im System waren zwar vorhanden, diese wiesen jedoch eine

Lücke auf, sodass es trotz dieser technischen Einstellungen möglich war, Arztbriefe zu versenden, auch wenn keine Einwilligung hierfür vorlag.

Der konkrete Versand ohne Einwilligung wurde zunächst damit begründet, dass in einigen Fällen der Arzt entscheiden müsse, ob wichtige medizinische Daten den ärztlichen Kollegen in der Niederlassung erreichen müssten, um einen Informationsverlust zu verhindern. Im vorliegenden Fall sei entsprechend dem mutmaßlichen Willen der Patientin gehandelt worden.

Diese Stellungnahme widersprach eindeutig den eigenen internen Vorgaben und es mangelte auch an einer rechtlichen Grundlage im Sinne der DSGVO, die diesen Umgang mit personenbezogenen Daten rechtfertigen würde.

Auf diesbezügliche weitere Rückfragen erhielt das ULD schließlich die Rückmeldung, dass bei der verantwortlichen Stelle allgemein bekannt sei, dass eine Übermittlung von Arztbriefen an Hausärztinnen und Hausärzte und/oder nach- und mitbehandelnde Ärztinnen und Ärzte nur erfolgen darf, wenn eine eindeutige und klare Einwilligung der Patientinnen und Patienten zur Datenübermittlung vorliegt. Es habe sich um ein Fehlverhalten eines einzelnen Mitarbeiters der verantwortlichen Stelle gehandelt.

Um zu verhindern, dass aufgrund der Unachtsamkeit eines einzelnen Mitarbeiters Arztbriefe ohne Einwilligung einer Patientin oder eines Patienten verschickt werden, hat die verantwortliche Stelle weitere **Schutzmechanismen ins Krankenhausinformationssystem** eingeführt, die sicherstellen, dass auch ein versehentlicher Versand technisch nicht erfolgen kann und im Zweifelsfall eine Rückversicherung mit der Patientin oder dem Patienten erfolgen muss. Warnhinweise im System sollen weitere Vorfälle ergänzend verhindern.

Die verantwortliche Stelle erhielt vom ULD einen abschließenden Hinweis, dass eine **Sensibilisierung** sämtlicher Mitarbeitenden zeitnah erfolgen sollte. Die verantwortliche Stelle wurde zudem darauf hingewiesen, dass es sich bei dem gemeldeten Vorgehen um ein datenschutzwidriges Verhalten handelt, das bei bewusster Wiederholung unter Umständen auch Bußgeldrelevanz nach Artikel 83 DSGVO entfalten könnte, oder je nach Sachverhalt in vergleichbaren Vorfällen weitere Maßnahmen nach Artikel 58 DSGVO ergriffen werden würden.

Was ist zu tun?

Für die Verarbeitung von personenbezogenen Daten nach Art. 9 Abs. 1 DSGVO sind die Vorgaben aus Art. 9 Abs. 2 DSGVO zu berücksichtigen. Auch diesbezüglich sollten Mitarbeitende regelmäßig sensibilisiert und technische und organisatorische Maßnahmen getroffen werden, um der besonderen Sensibilität der Daten bei der Verarbeitung gerecht zu werden.

4.7 Bildung

4.7.1 Informationsweitergabe an Elternvertretungen in Kindertagesstätten

Darf die Einrichtungsleitung einer Kindertagesstätte Informationen über eine dort beschäftigte Person an die Elternvertretung der Kindertagesstätte weitergeben? Zur Beantwortung dieser Frage war zunächst zu prüfen, welche gesetzlichen Aufgaben eine Elternvertretung wahrnimmt. Dies ergibt sich aus dem Kindertagesförderungsgesetz.

Bei dem zugrunde liegenden Sachverhalt handelte es sich um konkrete Angaben zu unbestätigten Vorwürfen gegen die beschäftigte Person, die sich auf die unsachgemäße Erledigung von Aufgaben innerhalb der Kindertagesstätte bezogen. In einem anderen Fall hatte die Einrichtungsleitung **Gesundheitsdaten der Beschäftigten** an die Elternvertretung verteilt.

§ 32 Abs. 2 Kindertagesförderungsgesetz (KiTaG)

Die Elternvertretung vertritt die Interessen der Erziehungsberechtigten gegenüber dem Einrichtungsträger und wirkt auf eine angemessene Beteiligung von Eltern mit Migrationshintergrund und die Berücksichtigung ihrer Interessen hin. Sie ist an den wesentlichen inhaltlichen und organisatorischen Entscheidungen der Kindertageseinrichtung rechtzeitig zu beteiligen, die insbesondere die Weiterentwicklung der pädagogischen Konzeption, die Aufnahmekriterien, die Öffnungs- und Schließzeiten, die Elternbeiträge oder die Verpflegung betreffen. Der Einrichtungsträger unterstützt die Arbeit der Elternvertretung, insbesondere deren Kommunikation mit den Erziehungsberechtigten, und gibt ihr die für eine wirkungsvolle Beteiligung erforderlichen Auskünfte unter Berücksichtigung datenschutzrechtlicher Bestimmungen und der Betriebs- und Geschäftsgeheimnisse. Er gibt der Elternvertretung vor seiner Entscheidung die Gelegenheit zur schriftlichen Stellungnahme, berücksichtigt die Interessen der Eltern angemessen und wirkt auf eine einvernehmliche Lösung hin.

Die Erteilung von Auskünften gemäß § 32 Abs. 2 Satz 3 KiTaG bezieht sich auf den Aufgabenumfang nach § 32 Abs. 2 Satz 2 KiTaG. „Wesentliche organisatorische Entscheidungen" sind von individuellen Entscheidungen zu unterscheiden. Bei individuellen arbeitsrechtlichen Maßnahmen hat eine Elternvertretung zudem keine Entscheidungskompetenz. Dies deutet darauf hin, dass eine Weitergabe von Angaben zum Gesundheitszustand einer Beschäftigten und zu bestehenden arbeitsrechtlichen Vorwürfen an eine Elternvertretung ohne Rechtsgrundlage erfolgte und damit einen **datenschutzrechtlichen Verstoß** darstellt.

Eine weitere Frage bezog sich darauf, ob die Elternvertretung als datenschutzrechtlich eigenverantwortliche Stelle anzusehen ist oder ob diese als Teil der Kindertagesstätte zu betrachten ist. So wurde dem ULD die Auffassung mitgeteilt, die Weitergabe personenbezogener Daten an Elternvertretungen sei als bloße interne Verarbeitung anzusehen und könne daher nicht als Datenschutzverstoß gelten.

Es ist nicht entscheidend, ob eine Elternvertretung als „Dritter" anzusehen ist. Erfolgt eine Weitergabe personenbezogener Daten durch die KiTa-Leitung an die Elternvertretung im Rahmen der Erteilung von Auskünften, so würde im Falle einer Qualifizierung als „Dritter" eine „Offenlegung durch Übermittlung" erfolgen. Sieht man die Elternvertretung als Teil der Einrichtung und damit nicht als eigenverantwortliche Stelle, so kämen gegebenenfalls noch die Verarbeitungsformen der „Verwendung" oder der „Bereitstellung" in Betracht. Zudem sind die Verarbeitungsformen in der DSGVO nicht abschließend benannt. Eine interne Weitergabe in der Verarbeitungssphäre der Kindertagesstätte würde daher auch die Voraussetzungen einer „Verarbeitung" erfüllen. Ergebnis: Auch für eine etwaige **interne Weitergabe von Angaben zum Gesundheitsstatus einer Beschäftigten und zu bestehenden Vorwürfen an eine Elternvertretung bedarf es einer Rechtsgrundlage** nach Art. 6 Abs. 1 DSGVO.

Das KiTaG enthält, anders als § 16 Schuldatenschutzverordnung, keine explizite Aussage zur Datenverarbeitung einer Elternvertretung. Die Situation ist aber mit einer schulischen Elternvertretung vergleichbar: Auch die Elternvertretung in einer KiTa erhält von der KiTa-Leitung die Kontaktdaten der Eltern zwecks Weiterleitung von Informationen und der Wahrnehmung der Interessenvertretung. Die in diesem Zusammenhang erfolgende Datenverarbeitung nimmt die Elternvertretung eigenverantwortlich wahr. Es ist kein Grund erkennbar, Elternvertretungen von Schulen und KiTas unterschiedlich zu behandeln. Die Elternvertretung einer KiTa kann daher nach gegenwärtigem Beurteilungsstand als Verantwortliche betrachtet werden.

Was ist zu tun?

Im Rahmen des eingeleiteten Prüfverfahrens wurden durch die Kindertagesstätte unter Einbeziehung des zuständigen Datenschutzbeauftragten zahlreiche Präventivmaßnahmen umgesetzt, um für die Zukunft vergleichbare Datenschutzverstöße zu vermeiden. Hierzu zählen vor allem Schulungen des Personals mit einer Erweiterung der Schulungsinhalte, die vertiefte Beteiligung des Datenschutzbeauftragten, die Entwicklung einer Broschüre sowie die Prüfung von Verschwiegenheitserklärungen, Dienstanweisungen und Regelwerken zum Datenschutz.

4.7.2 Fehldruck von Willkommensbriefen

Der Versand von Willkommensbriefen für neue Studierende u. a. mit Zugangsdaten, Adressdaten und Matrikelnummern endete für eine Hochschule aus Schleswig-Holstein in einer Datenpannenmeldung nach Artikel 33 DSGVO an das ULD.

Besagte Willkommensbriefe wurden versehentlich doppelseitig bedruckt, in der Folge gefaltet und händisch in Umschläge verpackt. Die doppelseitige Bedruckung ist hierbei unbemerkt geblieben, sodass die Empfängerinnen und Empfänger der Briefe den eigenen Willkommensbrief mit eigenen Zugangsdaten sowie auf der Rückseite die Daten weiterer Studierender erhielten.

Sämtliche etablierten technischen und organisatorischen Maßnahmen wie z. B. Verschlüsselungen, Berechtigungskonzepte, gesicherte Druckverfahren über interne Systeme und Anweisungen an die Mitarbeitenden, Dokumente vor dem Versand zu prüfen, konnten in diesem Fall die erfolgte Verletzung des Schutzes personenbezogener Daten nicht verhindern, da die Ursache des Fehlers in der Unachtsamkeit eines Beschäftigten lag.

Die verantwortliche Stelle reagierte nach Bemerken des Fehlversandes umgehend, sperrte sofort die betroffenen Zugangsdaten, informierte die betroffenen Studierenden über den Vorfall und dass die übermittelten Daten nicht zu verwenden und zu vernichten seien. Zudem wurden neue, veränderte Ersatzzugangsdaten an die Studierenden versendet. Die Mitarbeitenden wurden erneut zum Umgang mit personenbezogenen Daten und erforderlicher Sorgsamkeit beim Versand dieser Daten sensibilisiert.

Aufgrund dieser von der verantwortlichen Stelle bereits ergriffenen Abhilfemaßnahmen konnte das ULD die Meldung abschließen.

Was ist zu tun?

Unachtsamkeiten sind menschliche Fehler, die oft an das ULD gemeldet werden. Verantwortliche sollten ihre Mitarbeitenden regelmäßig zum Umgang mit personenbezogenen Daten sensibilisieren. Die verantwortliche Stelle sollte zudem regelmäßig überprüfen, ob Prozesse dahin gehend überarbeitet werden können, dass menschliche Individualfehler reduziert werden können. Zum Beispiel kann die Einführung vom Vieraugenprinzip in bestimmten Fällen Abhilfe schaffen.

4.8 Datenschutz- und Medienkompetenz

Datenschutzkompetenz ist ein zentraler Teil der Medienkompetenz und beschäftigt sich damit, das Wissen, dass 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 im AK Datenschutz- und Medienkompetenz

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

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

Im Jahr 2025 waren die wichtigsten Themen des Arbeitskreises u. a. die **Weiterentwicklung und Pflege des Internetauftritts des Jugendportals zum Thema Datenschutz und Informationsfreiheit** der Datenschutzkonferenz. Das Jugendportal mit dem Namen **„YoungData“** richtet sich mit dem Thema Datenschutz an Kinder und Jugendliche. Weitere Punkte waren u. a. der Austausch über die unterschiedlichen Angebote und Konzepte in den einzelnen Bundesländern zur Vermittlung und **Stärkung der Datenschutzkompetenz bei den unterschiedlichen Altersgruppen**. Zudem wird eine umfassende Sammlung und Darstellung der verschiedenen Materialien und Dokumente geplant.

4.8.2 Mitarbeit im Netzwerk Medienkompetenz in 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. Im Jahr 2025 wurde eine Überarbeitung der Webseite des Netzwerkes diskutiert, um die Sichtbarkeit zu stärken. Zudem wurde zwischen den Netzwerkmitgliedern diskutiert, wie sich das Netzwerk weiterentwickeln kann, um den Anforderungen der Medienkompetenzstrategie gerecht zu werden. Verschiedene Möglichkeiten wurden hier zwischen den Netzwerkmitgliedern intensiv diskutiert.

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

05

KERNPUNKTE

Satellitenortung

Sportwetten im Internet – Auskunftsanspruch

Datenpannen in der Wirtschaft

Videoüberwachung

Geldbußen für Datenschutzverstöße

5 Datenschutz in der Wirtschaft

5.1 Gebrauchte Festplatte mit Daten zum Verkauf

Ein Petent informierte uns, dass ihm ein Elektronikfachmarkt zwei Festplatten als vermeintliche Neuware verkauft hatte, die jedoch offenkundig bereits verwendet worden waren. Beim Versuch, ein Betriebssystem auf einer der Festplatten zu installieren, bemerkte der Petent, dass diese bereits partitioniert war. Beim schreibgeschützten Einbinden in ein bestehendes IT-System stellte der Petent schließlich fest, dass eine der beiden Festplatten bereits zuvor rege benutzt worden war. Da auch personenbezogene Daten enthalten waren, brach der Petent die weiteren Nachforschungen sofort ab und meldete uns den Vorfall.

Auf Basis dieser Informationen leiteten wir ein aufsichtsbehördliches Verfahren ein. Im Rahmen der Anhörung teilte uns das Unternehmen mit, dass die Umstände, die zu dieser Datenschutzverletzung geführt hatten, nicht mehr vollständig reproduzierbar waren. Es erhärtete sich der Verdacht, dass wegen eines Flüchtigkeitsfehlers die betroffene Festplatte in der Eile des Weihnachtsgeschäfts aufgrund geringer Bestände auf der Verkaufsfläche aus der Werkstatt des Ladens in den Verkauf genommen worden war und nicht erkannt wurde, dass diese zuvor von einem anderen Mitarbeiter als Back-up-Medium verwendet worden war. So wurde die benutzte Festplatte in der Annahme, sie sei neu, an den Petenten verkauft.

Wir konzentrierten uns gemeinsam mit dem Unternehmen auf die zu treffenden Maßnahmen, um ähnlich gelagerte Fälle in Zukunft verhindern zu können. Das Unternehmen erarbeitete einen **verbesserten Löschprozess**, der neben dem Einsatz nachhaltiger und professioneller Datenlöschsoftware auch auf eine klarere Strukturierung organisatorischer Abläufe setzte. So werden die einzelnen Schritte des Löschprozesses vollständig protokolliert. Um Fehlern aufgrund von unzureichenden Abstimmungen unter mehreren Mitarbeitenden entgegenzuwirken, wurde mit dem Prozess des Löschens von Festplatten lediglich ein Mitarbeiter betreut, der den Löschprozess von Beginn bis Abschluss allein durchführt. Festplatten, die als Back-up-Medium verwendet werden oder anderweitig bereits in Benutzung waren, werden eindeutig markiert, sodass ein unerwünschter Verkauf verhindert werden kann. Die professionell gelöschten Festplatten werden schließlich nach Absprache mit den Kundinnen und Kunden entweder zurückgegeben oder dem Recycling zugeführt.

Mit den verbesserten Prozessen und damit verbundenen umgesetzten technischen und organisatorischen Maßnahmen konnten wir das Verfahren abschließen. Der Petent wurde nach Abschluss des Verfahrens aufgefordert, die auf der Festplatte befindlichen Daten zu löschen.

Was ist zu tun?

Insbesondere bei gebrauchten Festplatten oder anderen Speichermedien ist aus datenschutzrechtlicher Sicht besondere Vorsicht geboten. Nur mit einer durch sichere Verfahren durchgeführten Löschung oder fachgerechter Vernichtung lassen sich die zuvor gespeicherten Daten sicher entfernen. Festgelegte Prozesse und dokumentierte Verarbeitungsschritte machen die Löschung dabei auch vor dem Hintergrund der Rechenschaftspflicht klar nachvollziehbar.

5.2 Hardwarereparatur und Preisgabe von Passwörtern

Das ULD erreichte eine Beschwerde hinsichtlich der Übermittlung von Passwörtern bei der Hardwarereparatur. Ein Hersteller von Elektronikartikeln verlangte im Rahmen der Einsendung des Geräts in einem Begleitschreiben das Gerätepasswort. Dieses Vorgehen ist zwar nicht unüblich, weniger üblich war hier jedoch, dass dieses Schreiben, auf dem das Passwort angegeben war, **gemeinsam mit dem Gerät** versendet werden sollte. Im Falle eines Abhandenkommens des Paketes durch Verlust oder Diebstahl hätten Dritte so vollen Zugriff auf das Gerät gehabt.

§ 5 Abs. 1 Buchst. f DSGVO

(1) Personenbezogene Daten müssen

[…]

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit"); […]

Art. 5 Abs. 1 Buchst. f DSGVO verlangt von den Verantwortlichen eine angemessene Sicherheit der personenbezogenen Daten. Weiterhin muss nach Art. 24 Abs. 1 DSGVO der Verantwortliche 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 implementieren, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.

Die verantwortliche Stelle wurde durch das ULD im Rahmen eines aufsichtsbehördlichen Verfahrens zum Sachverhalt angehört. Diese zeigte sich einsichtig und räumte ein, dass die Übermittlung der Passwörter in der gewählten Form kein ausreichendes Maß an Sicherheit bieten würde. Es wurde jedoch auch mitgeteilt, dass die direkte Übermittlung von Passwörtern nur noch einen sehr geringen Anteil ausmachen würde, da eine Einsendung der Hardware größtenteils über die Fachhändler erfolgt und hier eine Übermittlung von Passwörtern nicht erforderlich wäre.

Das Begleitschreiben wurde dahin gehend geändert, dass in diesem keine Passwörter mehr angefordert werden. Sollte eine Übermittlung eines Passworts im Einzelfall erforderlich sein, wird zukünftig eine Kontaktaufnahme mit den Kundinnen und Kunden erfolgen, um das Passwort abzufragen. Ein gemeinsames Versenden der Hardware mit dem Passwort soll demnach nicht mehr erfolgen.

Das aufsichtsbehördliche Verfahren wurde mit Erteilen eines Hinweises nach Art. 58 Abs. 1 Buchst. d DSGVO eingestellt.

5.3 Anfertigen von Personalausweiskopien durch Elektronikhändler

Beim ULD gingen mehrere Beschwerden hinsichtlich des Anfertigens von Personalausweiskopien durch private Unternehmen ein. In einem Fall wurde eine Kopie des Ausweises beim Ankauf eines Laptops durch einen Elektronikhändler angefertigt.

Hinsichtlich des Anfertigens von Personalausweiskopien gelten die Vorschriften des Personalausweisgesetzes (PAuswG). Demnach dürfen Ausweise nur vom Ausweisinhaber oder von anderen Personen mit **Zustimmung des Ausweisinhabers** so abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist (§ 20 Abs. 2 PAuswG). Es bedarf hier demnach einer Einwilligung nach Art. 6 Abs. 1 Buchst. a in Verbindung mit Artikel 7 DSGVO.

§ 20 Abs. 2 PAuswG

(2) Der Ausweis darf nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. [...]

Ausnahmen können sich z. B. aus dem Geldwäschegesetz (GWG) ergeben, sofern es sich um Verpflichtete im Sinne des § 2 Abs. 1 GWG handelt. In diesem Fall ist die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt. Die Verarbeitung der personenbezogenen Daten erfolgt demnach auf Grundlage des Art. 6 Abs. 1 Buchst. c DSGVO. In dem vorliegenden Fall wurde seitens des ULD eine solche Verpflichtung zur Anfertigung einer Personalausweiskopie jedoch nicht gesehen.

Der Verantwortliche wurde daher im Rahmen eines aufsichtsbehördlichen Verfahrens zum Sachverhalt angehört. Dieser gab in seiner Stellungnahme an, dass er sich mit der Kopie gegen einen möglichen späteren Vorwurf der Hehlerei absichern wollte, da der Verkäufer des Laptops keinen Kaufbeleg für das Gerät vorweisen konnte. Er berief sich hier auf sein berechtigtes Interesse nach Art. 6 Abs.1 Buchst. f DSGVO.

Dieses berechtigte Interesse konnte seitens des ULD nicht nachvollzogen werden. Das Anfertigen der Kopie war für den angestrebten Zweck, nämlich gegenüber den Strafverfolgungsbehörden einen möglichen Verdacht der Hehlerei zu entkräften, weder geeignet noch erforderlich, da durch die bloße Vorlage einer Ausweiskopie gegenüber den Strafverfolgungsbehörden keine Aussagen hinsichtlich des Umstands getroffen werden können, ob es sich bei der angekauften Ware um Diebesgut handelt.

Der Verantwortliche sagte dem ULD zu, zukünftig auf das Kopieren von Personalausweisen zu verzichten und die angefertigten Kopien umgehend zu vernichten. Als Alternative wurde ein **Kaufvertrag** etabliert, in dem die erforderlichen Daten des Verkäufers sowie die Zusicherung, dass es sich nicht um Diebesgut handelt, eingetragen werden können.

Dem Verantwortlichen wurde abschließend ein Hinweis nach Art. 58 Abs. 1 Buchst. d DSGVO erteilt.

5.4 Abfrage von Halterdaten durch Dienstleister bei Parkverstößen

Beim ULD gingen mehrere Beschwerden und Anfragen ein, die sich auf die Verarbeitung von Halterdaten durch private Dienstleister bei Parkverstößen bezogen. In den vorliegenden Fällen wurden die beschwerdeführenden Personen von den Dienstleistern kontaktiert und zur Zahlung aufgefordert. Ursächlich hierfür war zum einen die Begleichung der entstandenen Kosten bei **Abschleppvorgängen**, ausgelöst durch unerlaubtes Parken auf Privatflächen oder Blockieren von Ein- und Ausfahrten. Weiterhin erfolgte eine Bezugnahme auf Parkverstöße, z. B. auf einem Supermarktparkplatz. In den dem ULD vorliegenden Beschwerden wurde die Rechtmäßigkeit der Abfrage der Halterdaten durch die Dienstleister angezweifelt.

Zu § 33 Straßenverkehrsgesetz

Der Gesetzgeber unterscheidet zwischen dem örtlichen und dem Zentralen Fahrzeugregister. Diese Register beinhalten z. B. Kontaktdaten zum Halter und Fahrzeugdaten, einschließlich Angaben zur Haftpflichtversicherung, die Kraftfahrzeugbesteuerung des Fahrzeugs und die Verwertung oder Nichtentsorgung des Fahrzeugs als Abfall im Inland.

Nach § 39 Straßenverkehrsgesetz sind bestimmte im Fahrzeugregister gespeicherte Angaben zu Fahrzeug und Halter, u. a. Name und Anschrift des Halters, durch die Zulassungsbehörde oder durch das Kraftfahrt-Bundesamt (KBA) zu übermitteln, wenn der Empfänger unter Angabe des betreffenden Kennzeichens oder der betreffenden Fahrzeug-Identifizierungsnummer darlegt, dass er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt. Hierbei handelt es sich um die sogenannte **einfache Registerauskunft**. Eine Überprüfung, ob eine solche Abfrage berechtigt ist, erfolgt durch die Stelle, die die einfache Registerauskunft erteilt.

In den vorliegenden Fällen sollten seitens der Parkplatzbetreiber oder durch die betroffenen Personen, etwa durch die beauftragten Dienstleister, Ansprüche hinsichtlich begangener Parkverstöße geltend gemacht werden. Hierfür war es erforderlich, die jeweiligen Halter anzuschreiben. Die Voraussetzungen für die Übermittlung der Halterdaten waren somit erfüllt.

Ein häufiger Einwand in den Beschwerden war, dass die Abfrage durch „private" Unternehmen und nicht durch das Ordnungsamt erfolgte. Das StVG differenziert hier jedoch nicht nach der Rechtsform der abfragenden Stelle, sondern verweist lediglich auf den „Empfänger", sodass die Abfrage auch durch Privatpersonen oder beauftragte Dienstleister erfolgen kann.

5.5 Kennzeichenerfassung als Zutrittskontrolle auf einem Campingplatz

Das ULD erreichte eine Beschwerde in Bezug auf die Kennzeichenerfassung bei der Einfahrt auf einen Campingplatz. Der Beschwerdeführer monierte, dass neben den Kennzeichen auch öffentlicher Grund aufgenommen werden würde. Zusätzlich wurde beanstandet, dass der Verantwortliche seinen Informationspflichten nicht nachkommen würde.

Artikel 13 DSGVO

Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten die in Artikel 13 DSGVO genannten Informationen mit.

Die verantwortliche Stelle wurde im Rahmen eines aufsichtsbehördlichen Verfahrens zum Sachverhalt angehört. Hierdurch sollten insbesondere Informationen zum Zweck und Umfang der Erfassung sowie der Umsetzung der Informationspflichten erlangt werden.

Seitens des Verantwortlichen wurde dem ULD eine umfangreiche Stellungnahme übermittelt. Als Rechtsgrundlage für die Erfassung wurde Art. 6 Abs. 1 Buchst. f DSGVO angegeben. Das berechtigte Interesse wurde mit dem **Schutz des Eigentums und der Sicherheit auf dem Campingplatz** sowie der **Gewährleistung eines ordnungsgemäßen Campingbetriebs** begründet. Durch die Erfassung soll gewährleistet werden, dass nur berechtigte Personen, im Einzelnen Betreiber und Gäste, auf den Campingplatz fahren dürfen. Weiterhin soll durch die automatische Steuerung der Verkehrsfluss an An- und Abreisetagen gelenkt und so eine geordnete Zu- und Abfahrt gewährleistet werden.

Dem ULD wurde zudem mitgeteilt, dass das verwendete System datenschutzfreundlich ausgestaltet sei. Die Kamera sei gezielt so ausgerichtet und konfiguriert, dass ausschließlich Kennzeichen im Nahbereich (Short Range) erfasst werden. Eine Aufnahme bzw. Erfassung von Personen, die sich in den Fahrzeugen oder in dem Bereich dahinter befinden, würde nicht erfolgen.

Hinsichtlich der **Transparenz** und **Informationspflichten** wurde angegeben, dass diesen umfassend nachgekommen werde. Die Information erfolge durch Symbole und Schilder, die sowohl im Vorfeld als auch direkt an der Schrankenanlage angebracht wurden. Ergänzend hierzu werde durch einen Aushang an der Rezeption informiert.

Seitens des ULD konnten die vorgebrachten Argumente und Informationen nachvollzogen werden. Die Kennzeichenerfassung wurde als rechtmäßig angesehen, sodass das aufsichtsbehördliche Verfahren eingestellt werden konnte.

5.6 Bildveröffentlichung durch nicht sorgeberechtigten Elternteil

Gegenstand der Prüfung war die Beschwerde einer Mutter, die sich auf die Verwendung von Bildern ihres Sohnes auf **Facebook** bezog. Ihr Ex-Mann hatte regelmäßig Fotos von Aktivitäten mit dem gemeinsamen Sohn auf Facebook hochgeladen. Da das Facebook-Profil des Ex-Mannes auf „öffentlich" eingestellt war, konnten auch Personen ohne Facebook-Account die Fotos des Sohnes sehen.

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. Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da diese sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Die DSGVO sieht vor, dass für Kinder, die das 16. Lebensjahr noch nicht vollendet haben, in Bezug auf Dienste der Informationsgesellschaft eine **Einwilligung des gesetzlichen Vertreters** zur Verarbeitung der personenbezogenen Daten des Kindes vorliegen muss. Eine Einwilligung des Kindes allein ist nicht ausreichend. Das Alter des Sohnes betrug zum Zeitpunkt der Beschwerde fünf Jahre. Demnach war zur Verarbeitung seiner personenbezogenen Daten die Einwilligung des gesetzlichen Vertreters notwendig. Da das alleinige Sorgerecht der Mutter zugesprochen wurde, war hier für die Veröffentlichung der Bilder auf dem Facebook-Profil des Vaters ihre Einwilligung erforderlich. Diese lag jedoch nicht vor.

Der Vater wurde seitens des ULD angeschrieben und zur Löschung aller Bilder, auf denen der Sohn zu sehen war, aufgefordert. Dieser zeigte sich jedoch nicht sehr kooperativ und reagierte nicht auf das Schreiben des ULD. Als nach wiederholter Aufforderung keine Löschung der Bilder von dem Facebook-Profil erfolgte, wurde die Löschung der Bilder unter Androhung eines Zwangsgelds angeordnet.

Die Bilder wurden daraufhin umgehend von dem Facebook-Profil gelöscht. Das aufsichtsbehördliche Verfahren wurde mit einer Warnung an den Vater abgeschlossen, zukünftig ohne vorhandene Rechtsgrundlage (Einwilligung der Sorgeberechtigten) Bilder des Sohnes zu veröffentlichen.

5.7 Überwachung von Müllbehältern

Der Mieter einer Wohnung in einem Mehrfamilienhaus berichtete davon, dass die Zugangstüren zum Haus und den Müllbehältern mit **Transpondern** ausgestattet wurden, die einerseits den Bewohnerinnen und Bewohnern namentlich zugeordnet wurden und andererseits geeignet seien, Zutrittsereignisse zu protokollieren.

Nach Schilderung verschiedener Mieterinnen und Mieter sei das System nach ihrer Kenntnis verbaut worden, um sehen zu können, wer wann bei den Müllbehältern gewesen sei, da in der Vergangenheit offenbar Müll nicht ordnungsgemäß entsorgt wurde.

Die Hausverwaltung erläuterte hierzu, dass der gegenüber den Mieterinnen und Mietern erfolgte Hinweis zur Überwachungsmöglichkeit der Müllanlage erfolgt sei, um zusätzliche Entsorgungskosten und höhere Betriebskosten zu vermeiden. Tatsächlich würde die vom System zur Verfügung stehende Protokollierungsmöglichkeit jedoch nicht genutzt, sodass keine aktive Überwachung stattfinde. Der Hinweis hätte lediglich einen erzieherischen Hintergrund gehabt.

Anhand der vorliegenden Beschwerde war erkennbar, dass der erfolgte Hinweis und die bestehende Möglichkeit einer Protokollierung zu einem Überwachungsdruck bei den betroffenen Mieterinnen und Mietern führten. Darüber hinaus darf bezweifelt werden, dass eine **Zugangsprotokollierung** das geeignete Mittel für eine ordnungsgemäße Müllentsorgung ist, da hierdurch weiterhin nicht nachvollzogen werden kann, wer tatsächlich was wie entsorgt hat.

Was ist zu tun?

Für natürliche Personen sollte zunächst Transparenz dahin gehend bestehen, ob personenbezogene Daten von ihnen erhoben und in welchem Umfang sie verarbeitet werden. Im Rahmen der Informations- und Transparenzpflichten sind betroffene Personen darüber zu informieren, welche Daten zu welchem Zweck und auf welcher rechtlichen Grundlage verarbeitet werden.

5.8 Bestandskundin oder nicht?

Auch in diesem Jahr erreichten uns wieder zahlreiche Beschwerden über den Erhalt von E-Mails zum Zweck der **Direktwerbung**.

Wie in verschiedenen Beiträgen 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 ihre Beziehung zu dem Verantwortlichen beruhen, in den Abwägungsprozess einzubeziehen.

Im Fall von Bestandskunden 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 im § 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 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 keine Einwilligung der betroffenen Person erforderlich ist.

Im Rahmen eines in diesem Berichtszeitraum geführten Verfahrens teilte das verantwortliche Unternehmen zunächst mit, dass die vorliegenden Kundendaten aus einer Reihe von vergangenen Bestellungen stammen würden.

Rechenschaftspflicht

Der Verantwortliche ist für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich und muss dessen Einhaltung nachweisen können.

Nachdem die Beschwerdeführerin dies jedoch bestritt, verwies die Rechtsnachfolgerin des ursprünglichen Unternehmens auf die bestehende Verpflichtung zur Löschung von personenbezogenen Daten nach Ablauf der gesetzlichen Aufbewahrungsfristen und räumte ein, dass sämtliche ursprünglichen Bestellvorgänge inzwischen gelöscht wurden, sodass nicht mehr belegt werden

konnte, dass es sich bei der betroffenen Person tatsächlich um eine Bestandskundin handelte und sich die Werbung auf ähnliche Waren bezog.

Da die gesetzlichen Aufbewahrungsfristen für steuerrechtlich relevante Bestellvorgänge zehn Jahre beträgt und die vom Unternehmen erwähnten Bestellvorgänge demnach offenbar vor über zehn Jahren erfolgten, kann auch nicht mehr davon ausgegangen werden, dass die vernünftigen Erwartungen der betroffenen Person dahin gehen, dass sie jetzt entsprechende Werbung von der Rechtsnachfolgerin des ursprünglichen Unternehmens erhält.

Was ist zu tun?

Nach Ablauf der gesetzlichen Aufbewahrungsfristen sind sämtliche Kundendaten zu löschen, wenn keine aktuelle Einwilligung zur Weiterverarbeitung von personenbezogenen Daten beispielsweise zum Zweck der Direktwerbung vorliegt.

5.9 Neues Gewerbe – alte Kundendaten

Im Rahmen einer weiteren Beschwerde berichtete der Eigentümer einer Ferienwohnung, dass er von seinem früheren Verwalter der Wohnungseigentümergemeinschaft ein postalisches Werbeschreiben für die Vermietung seiner Ferienimmobilie erhielt.

Nach seiner Schilderung würde der Absender die Tätigkeit als Hausverwalter seit über drei Jahren nicht mehr ausüben. Da dieser in dem Anschreiben unter einem neuen Firmennamen auftrat, sei davon auszugehen, dass er seine alten Kundendaten nutze, um für seine neue Firma zu werben.

Zweckbindung

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Nachdem sich der Verantwortliche im Rahmen einer Stellungnahme für seinen Fehler entschuldigt und eingeräumt hatte, bedauerlicherweise alte Kundendaten verwendet zu haben, die sich noch in seinem Bestand befanden, wurde er gemäß Art. 58 Abs. 2 Buchst. a DSGVO davor gewarnt, dass er bei einer **fortdauernden Nutzung alter Kundendaten** für Zwecke seines neuen Gewerbes **gegen datenschutzrechtliche Vorschriften verstoße**.

Darüber hinaus wurde ihm ein Hinweis dahin gehend erteilt, dass personenbezogene Daten zu löschen sind, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Sollte eine Löschung wegen gesetzlicher Aufbewahrungsfristen derzeit noch nicht möglich sein, sind die Daten beispielsweise durch eine Archivierung in einem nicht direkt zugänglichen System zu sperren.

5.10 Satellitenortung I: Erreichbarkeit von Beschäftigten und Leistungskontrolle

Immer häufiger erreichen uns Beschwerden von Beschäftigten zu **GPS-Trackern**, die vom Arbeitgeber in den Firmenfahrzeugen verbaut werden. Oft werden die Beschäftigten nicht ausreichend über das **Tracking** informiert, da einige Arbeitgeber davon ausgehen, dass die mittels der GPS-Geräte erhobenen Standortdaten keine personenbezogenen Daten im Sinne von Art. 4 Nr. 1

DSGVO darstellen, da ja nur der Standort des Fahrzeugs geortet werde. Regelmäßig ist es dem Arbeitgeber jedoch möglich nachzuvollziehen, welcher Beschäftigte an welchem Datum ein bestimmtes Firmenfahrzeug gefahren ist, sodass die Standortinformationen personenbezogen sind. Grundsätzlich kann sich eine **GPS-Ortung** auf die berechtigten Interessen des Arbeitgebers nach Art. 6 Abs. 1 Buchst. f DSGVO oder auf Art. 6 Abs. 1 Buchst. b DSGVO stützen, wenn diese zur Erfüllung des Arbeitsvertrags erforderlich ist. Dabei sind jedoch auch die Interessen und Rechte der Beschäftigten zu berücksichtigen.

Globales Satellitennavigationssystem

Bei GPS (Global Positioning System) handelt es sich um ein satellitengestütztes Navigationssystem. Neben GPS gibt es auch noch weitere solche Systeme, die allerdings eine untergeordnete Rolle spielen, z. B. GLONASS (Russland) oder Beidou (China).

Aufgrund einer Beschwerde prüften wir das GPS-Tracking in den Fahrzeugen eines Unternehmens, das Hausmeister- und Reinigungsarbeiten durchführt. Das Unternehmen gab an, dass das in den Fahrzeugen verbaute GPS-System den aktuellen Standort, die Fahrstrecke sowie Geschwindigkeit und Uhrzeit erfasse. Die Daten würden für 365 Tage gespeichert werden.

Das Unternehmen legte mehrere Zwecke dar, zu denen die GPS-Ortung gebraucht werde. Zum einen benötige man die GPS-Ortung, **um kurzfristige Aufträge und Noteinsätze zu disponieren**, wobei es zu kurzfristigen Umdisponierungen maximal zwei bis dreimal im Monat, wenn nicht noch seltener komme. Die Beschäftigten seien angehalten, während der Arbeit nicht das Handy zu benutzen, da bei den Kundinnen und Kunden nicht der Eindruck entstehen solle, die Beschäftigten würden während der Arbeitszeit am Handy spielen. Die Erforderlichkeit konnte jedoch nicht ausreichend nachgewiesen werden. Zum einen konnten die beschriebenen „Noteinsätze" keine derartige Dringlichkeit erkennen lassen, die eine Ortung des aktuellen Standorts erforderlich machen. Auch die eher geringe Anzahl an Beschäftigten und ein geografisch nicht weitläufiger Einsatzbereich sprachen dafür, dass es nicht auf den aktuellen Standort der Beschäftigten für Umdisponierungen ankam. Vielmehr ergab der Sachverhalt, dass es insbesondere darum ging, Kapazitäten umzudisponieren. Sollte es in seltenen Ausnahmefällen doch darauf ankommen, den aktuellen Standort eines Beschäftigten zu erhalten, ist es zumutbar, dass eine telefonische Erreichbarkeit der Beschäftigten sichergestellt wird.

Ferner sollten die GPS-Daten nach den Angaben des Unternehmens zur **anlassbezogenen repressiven Mitarbeiterkontrolle** dienen, da es in der Vergangenheit zu mehreren Fällen von umfangreichem Arbeitszeitbetrug kam. In der Interessenabwägung ist aber zu berücksichtigen, dass personenbezogene Daten von Beschäftigten zur Aufdeckung von Straftaten nur dann verarbeitet werden dürfen, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Wichtig ist, dass der begründete Verdacht eines Arbeitszeitbetrugs bereits vorliegen muss und dann zu prüfen ist, ob der Einsatz eines GPS-Trackings tatsächlich geeignet, erforderlich und verhältnismäßig ist, um den Verdacht aufzuklären. Unzulässig ist es, Standortdaten auf Vorrat zu speichern, um diese nachträglich auswerten zu können, falls sich irgendwann mal der Verdacht eines Arbeitszeitbetrugs ergibt. Wichtig ist zudem, dass der Verdacht dokumentiert wird und sich auf einen konkreten Beschäftigten oder zumindest eng abgrenzbaren Personenkreis von Beschäftigten beschränkt. Es dürfen nicht alle Beschäftigten unter einen Generalverdacht gestellt werden. Dieser Zweck rechtfertigt daher keine dauerhafte Ortung und Speicherung der Standortdaten. Dies ist, wenn überhaupt, nur im begründeten Einzelfall zulässig und muss zeitlich begrenzt sein.

Des Weiteren diene die GPS-Ortung dem **Diebstahlschutz außerhalb der Arbeitszeit**. Hier ist zu beachten, dass ein GPS-Tracker keinen Diebstahl verhindern kann. Vielmehr ermöglicht es eine GPS-Ortung lediglich, im Falle eines Dieb-

stahls das entwendete Fahrzeug wieder aufzufinden. Daher rechtfertigt dieser Zweck keine Speicherung der Standortdaten, sondern nur die anlassbezogene Ortung.

Das Unternehmen deaktivierte letztendlich die Speicherung und löschte alle historischen Tracker-Daten aus der Software. Das Unternehmen gab an, dass eine Ortung mittels der GPS-Tracker nur noch vorgenommen werde, wenn es zu einem Diebstahl eines Fahrzeugs komme. Sofern es zukünftig zu Verdachtsfällen bezüglich eines Arbeitszeitbetrugs kommen sollte, werde man vorab eine entsprechende Verhältnismäßigkeitsprüfung vornehmen und dies entsprechend schriftlich dokumentieren. Zudem seien die Beschäftigten über die Änderungen bei dem Einsatz der GPS-Tracker transparent informiert und die entsprechenden Datenschutzerklärungen angepasst worden. Das Verfahren konnte damit abgeschlossen werden.

Was ist zu tun?

GPS-Tracker für Firmenfahrzeuge sind heutzutage schnell und kostengünstig zu bekommen. Leider werden die datenschutzrechtlichen Aspekte von vielen Verantwortlichen dabei vernachlässigt. Verantwortliche sollten sorgfältig prüfen, ob eine GPS-Ortung zu den verfolgten Zwecken tatsächlich erforderlich ist und dabei auch die Interessen und Rechte der Beschäftigten berücksichtigen.

5.11 Satellitenortung II: Sicherheit auf Autobahnen

Aufgrund einer Beschwerde wurde ein Prüfverfahren gegen ein Unternehmen eingeleitet, welches insbesondere Arbeiten auf Autobahnen in Schleswig-Holstein ausführt. Zu diesem Zweck sei in den Einsatzfahrzeugen (z. B. Lkws, Transporter oder Räumfahrzeuge) ein System verbaut, welches zur Steuerung aller fachlichen und organisatorischen Abläufe im Straßenbetriebsdienst diene, hier im Speziellen im Autobahnbetriebsdienst. Die Fahrzeuge seien keinen einzelnen Beschäftigten zugeordnet, sondern würden in der Regel von Teams genutzt werden.

Das System erhebe **Telemetriedaten** im Zusammenhang mit dem Einsatz des Fahrzeugs, die zunächst nicht personenbezogen sind. Bei den erfassten Telemetriedaten handle es sich u. a. um die aktuelle Position, Geschwindigkeit, gefahrene Kilometer sowie gegebenenfalls Zusatzinformationen wie Fahrbahntemperatur oder andere Sensordaten. Diese Daten werden nur erfasst, wenn das Fahrzeug in Bewegung ist. Sobald ein in dem Fahrzeug sitzendes Mitglied des Teams eine vordefinierte Leistung aktiviere (z. B. Mähen Grünstreifen oder Fahrbahn streuen), werden die Telemetriedaten der aktivierten Leistung zugeordnet. Dabei wird ein sogenannter Arbeitsbericht erstellt, aus dem auch der Name des bedienenden Beschäftigten hervorgeht, sodass hier eine Verarbeitung personenbezogener Daten vorliegt.

Das Unternehmen legte dar, dass die Telemetriedaten in Verbindung mit den erstellten Arbeitsberichten zum einen gemäß Art. 6 Abs. 1 Buchst. b DSGVO zur Erfüllung des Vertrags mit dem Auftraggeber erforderlich seien. Im Laufe des Verfahrens setzte sich das Unternehmen erneut mit dem Auftraggeber zusammen, um den Vertrag zu prüfen. Dabei kam man zu dem Ergebnis, dass eine personenbezogene Dokumentation nicht erforderlich ist, um den Vertrag zu erfüllen.

Es verbleibe jedoch ein berechtigtes Interesse des Unternehmens im Sinne von Art. 6 Abs. 1 Buchst. f DSGVO, da man die personenbezogenen Arbeitsberichte in Verknüpfung mit den Telemetriedaten insbesondere zur **Nachvollziehbarkeit von Vorgängen und zur Fehleranalyse** benötige. Dies diene lediglich der Qualitätssicherung und nie der Überwachung von

Beschäftigten. Hierbei sei zu berücksichtigen, dass an den Autobahnbetriebsdienst besonders hohe Qualitätsanforderungen zu stellen sind, da es letztendlich um die Sicherheit und den Schutz von Gesundheit und Leben der Beschäftigten sowie der Teilnehmenden am Straßenverkehr gehe.

Die GPS-Ortung ist im vorliegenden Fall daher nur ein Teil von einem relativ komplexen Verarbeitungsvorgang. Aufgrund der besonderen Anforderungen an die Abläufe im Straßenbetriebsdienst und die damit einhergehenden Sicherheitsaspekte haben wir im vorliegenden Fall die Erforderlichkeit der GPS-Ortung bejaht und keine überwiegenden Interessen der Beschäftigten gesehen, die der Verarbeitung entgegenstehen.

Das Verfahren ist jedoch noch nicht ganz abgeschlossen, da die Speicherdauer der personenbezogenen Daten ursprünglich auf 30 Jahre ausgelegt war. Dies wurde mit der Laufzeit des Vertrags mit dem Auftraggeber begründet. Da sich aus dem Vertrag nunmehr keine Verpflichtung mehr zur Speicherung der personenbezogenen Daten ergibt, ist noch zu klären, welche Speicherdauer nunmehr als erforderlich angesehen werden kann.

5.12 Informationsverknüpfung führt zu Identifizierbarkeit

Das ULD erreichte eine Beschwerde über eine für die Datenverarbeitung verantwortliche Person, die sich zwar um **Anonymisierung** bemühte, dies jedoch nicht ausreichend gelang.

Im Rahmen einer Beerdigung war die Verantwortliche als Trauerrednerin engagiert worden. Im Anschluss an die Feierlichkeiten veröffentlichte sie diverse Informationen **bei Social Media** zum Zweck der **Eigenwerbung**. Zu diesen Informationen gehörte ein Bild, auf dem der Sarg mit dem Vornamen und dem ersten Buchstaben des Nachnamens der verstorbenen Person zu sehen war. Daneben wurde ein Text einer Angehörigen veröffentlicht, in dem diese sich bei der Verantwortlichen bedankte. Auch hier wurden nur der Vorname und der erste Buchstabe des Nachnamens abgedruckt. Zudem ergänzte die Verantwortliche noch den Standort der Feierlichkeiten – eine kleinere Stadt in Schleswig-Holstein.

Ein Angehöriger der verstorbenen Person wurde auf den Social-Media-Kanal der Verantwortlichen aufmerksam und forderte sie auf, die Bilder und den Text zu löschen. Dem kam die Trauerrednerin jedoch nicht nach, was zur Einreichung einer Beschwerde führte.

Zwar hat die Verantwortliche versucht, nur weitestgehend anonymisierte Informationen zu veröffentlichen. Jedoch ließen sich die einzelnen Daten hier so kombinieren, dass Personen plötzlich identifizierbar wurden. Es lagen damit keine anonymisierten Daten vor. Es mag zwar der Grundsatz gelten, dass die Anwendung der DSGVO nur für lebende natürliche Personen in Betracht kommt. Allerdings sind die entsprechenden Vorschriften maßgeblich, wenn die veröffentlichten Angaben Bezug zu lebenden Angehörigen haben. Folglich ist dann Zurückhaltung bei der Datenverarbeitung geboten, wenn auch ein Vorname und der erste Buchstabe des Nachnamens für die Leserschaft eine Identifizierung ermöglicht.

Da ein Personenbezug vorlag, weil eine Identifizierbarkeit der angehörigen Person möglich war, bedurfte die Veröffentlichung der Informationen einer Rechtsgrundlage nach der DSGVO. Mangels einer Einwilligung des Angehörigen beschränkte sich die Prüfung auf Art. 6 Abs. 1 Buchst. f DSGVO. Demnach ist die Verarbeitung nur rechtmäßig, wenn diese zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Bei der Interessenabwägung fiel ins Gewicht, dass die Veröffentlichung von **Angaben zu einem Trauerfall** bereits eine **sensible Thematik** betraf. Dabei sollten trauernde Angehörige nach Möglichkeit auch bestimmen können, ob Dankesschreiben für Mitwirkende an einer Beerdigung der Öffentlichkeit zugänglich sind.

Letztlich galt es auch zu berücksichtigen, dass selbst bei einer Rechtfertigung der Veröffentlichung nach Art. 6 Abs. 1 Buchst. f DSGVO ein Widerspruch des Angehörigen gegen die Verarbeitung nach Artikel 21 DSGVO in Betracht kam.

Nachdem die Verantwortliche auf die Rechtslage hingewiesen wurde, zeigte sie sich kooperativ und entfernte den Eintrag von ihrem Social-Media-Kanal. Das Prüfverfahren konnte daher abgeschlossen werden.

5.13 Sportwetten im Internet – Auskunftsanspruch

Das ULD erreichten 2025 diverse **Beschwerden gegen Wettanbieter mit Sitz in Malta**. Hintergrund der Beschwerden waren gar nicht oder nur unvollständig beantwortete Auskunftsersuchen gemäß Artikel 15 DSGVO. Den Betroffenen ging es insbesondere darum, eine **detaillierte Aufschlüsselung ihrer Gewinne und Verluste** zu erhalten.

Maßgebend war ein Vorlagebeschluss des Bundesgerichtshofs (BGH) an den Gerichtshof der Europäischen Union (EuGH) zur Vorabentscheidung aus dem Jahr 2024. Der BGH führt darin aus, dass die Veranstaltung öffentlicher Sportwetten in Deutschland ohne die erforderliche Lizenz verboten sei. Demnach seien alle Sportwettenverträge, die vor Erteilung einer Lizenz durch die Glücksspielbehörde geschlossen wurden, nichtig und der Sportwettenanbieter sei grundsätzlich zum Ersatz der Verluste der Spielerinnen und Spieler verpflichtet. Zur genauen Bezifferung des Schadensersatzes benötigten die Betroffenen nun die detaillierte Aufschlüsselung ihrer Gewinne und Verluste, da die Verluste nur in der Höhe erstattet werden, soweit sie die Gewinne übersteigen. Der einfachste Weg, an diese Aufstellung zu gelangen, bestand in der Geltendmachung eines Auskunftsersuchens gemäß Artikel 15 DSGVO, da es sich bei der Aufschlüsselung um personenbezogene Daten handelt.

Gemäß Art. 15 Abs. 1 DSGVO haben betroffene Personen das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Soweit dies der Fall ist, hat die betroffene Person ein **Recht auf Auskunft** über diese personenbezogenen Daten und auf diverse Informationen – beispielsweise etwa die Verarbeitungszwecke, die Kategorien der personenbezogenen Daten, die verarbeitet werden, und die Dauer der Speicherung.

Die gegen die Sportwettenanbieter geltend gemachten Auskunftsersuchen wurden häufig gar nicht beantwortet. In den Fällen, wo eine Auskunft erteilt wurde, erfolgte in der Regel lediglich eine sehr oberflächliche und unvollständige Beantwortung. Die Verantwortlichen begründeten dies mit der angeblichen Komplexität und dem Aufwand der Anfrage oder der Behauptung, die Daten würden nur zur Vorbereitung einer Klage benötigt, und bezogen sich dabei nicht selten auf maltesisches Recht, wonach die Auskunft für derlei Fälle eingeschränkt werden könne.

Eine Einschränkung des Auskunftsrechts ist zwar nicht von vornherein ausgeschlossen. So sind in Art. 15 Abs. 4 DSGVO und in Artikel 23 DSGVO Beschränkungsmöglichkeiten vorgesehen, beispielsweise wenn die Auskunft Rechte und Freiheiten anderer Personen beeinträchtigen würde. Es ist jedoch höchst fraglich, ob dies vorliegend einschlägig wäre.

Die beim ULD eingegangenen Beschwerden wurden zuständigkeitshalber an die maltesische Aufsichtsbehörde, den Information and Data Protection Commissioner (IDPC), weitergeleitet. Von den maltesischen Kollegen bekamen wir zwischenzeitlich eine Mitteilung, dass ein Verantwortlicher gegen die Entscheidung des IDPC gerichtlich vorgegangen sei. Die maltesische Aufsichtsbehörde hat daher beschlossen, die Ermittlungen gegen diesen Verantwortlichen bis zum Abschluss der Entscheidung des Datenschutzgerichts auszusetzen. Zum gegenwärtigen Zeitpunkt ist nicht absehbar, wann und wie die Entscheidung ausfallen wird. Bis zum Ergehen der Entscheidung werden Auskunftsersuchen wahrscheinlich weiterhin im bisherigen Umfang beantwortet.

Das ULD informierte die betroffenen Beschwerdeführer über den geschilderten Verfahrensstand und bezüglich der Zuständigkeit des IDPC.

5.14 Weitergabe von Beschäftigtendaten an das Ordnungsamt

Ein ehemaliger Beschäftigter wandte sich an uns, da er ein Schreiben vom Ordnungsamt bekommen hatte, in dem ihm vorgeworfen wurde, die zulässige Höchstgeschwindigkeit überschritten zu haben. Der Beschwerdeführer vermutete, dass seine privaten Kontaktdaten von seinem ehemaligen Arbeitgeber bzw. dem Unternehmen, welches für die Verwaltung der Dienstwagen zuständig war, an das Ordnungsamt weitergegeben wurden. Der Beschwerdeführer gab jedoch an, dass er das Fahrzeug mit dem angegebenen KFZ-Kennzeichen nie selbst gefahren sei und er an dem Datum, an dem die Ordnungswidrigkeit begangen wurde, schon seit mehreren Monaten nicht mehr für das Unternehmen gearbeitet habe. Es stellte sich daher die Frage, aus welchem Grund seine Daten an das Ordnungsamt weitergegeben wurden, obwohl er als Fahrer des Fahrzeugs nicht in Betracht kam.

Im Rahmen des eingeleiteten Verwaltungsverfahrens stellte sich heraus, dass es durch eine Verkettung von mehreren Versäumnissen zu der unberechtigten Weitergabe der Daten gekommen ist. Das besagte Unternehmen teilte mit, dass es sich bei dem fraglichen Fahrzeug um ein **Poolfahrzeug** handle. Dieses sei dem Beschwerdeführer als Verwalter zugeordnet gewesen, da das von ihm geführte Team das Fahrzeug nutzen konnte. Beim Ausscheiden des Beschwerdeführers aus dem Unternehmen sei zunächst vergessen worden, ihn aus der entsprechenden Datenbank als Verwalter zu löschen. Als dann das Schreiben vom Ordnungsamt kam, sei von der Sachbearbeitung übersehen worden, dass es sich um ein Poolfahrzeug handle. Es wurde daher einfach der in der Datenbank (fälschlicherweise) als Verwalter geführte Beschwerdeführer als Fahrer benannt, anstatt anhand des Fahrtenbuchs den tatsächlichen Fahrer des Poolfahrzeugs zu ermitteln.

Grundsätze für die Verarbeitung personenbezogener Daten

Der Verantwortliche hat gemäß Art. 5 Abs. 1 Buchst. d DSGVO sicherzustellen, dass personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit").

Um diese Fehler zukünftig zu verhindern, ergänzte das Unternehmen die bestehende Arbeitsanweisung für die Rückgabe von Dienstfahrzeugen um den Punkt, dass auch weitere Dienstfahrzeuge im Verantwortungsbereich des jeweiligen Nutzers geprüft werden müssen. Zudem sei die geführte Datenbank übersichtlicher gestaltet worden, um leichter erkennen zu können, dass es sich um ein Poolfahrzeug handle. Die fälschlicherweise noch gespeicherten Daten des Beschwerdeführers wurden selbstverständlich unverzüglich gelöscht.

5.15 Bewerbungsgespräch mit unerwarteten Folgen

Im Laufe des Jahres meldete sich ein Betroffener und schilderte folgenden Sachverhalt:

Er habe sich bei einem Unternehmen auf einen Remote-Arbeitsplatz beworben. Er recherchierte zu dem Unternehmen und da ein Handelsregistereintrag und eine relativ seriöse Website existierte, sei er davon ausgegangen, dass es sich um ein vertrauenswürdiges Jobangebot handelte. Er habe zügig online ein Bewerbungsgespräch mit dem neuen Arbeitgeber geführt, wobei der Eindruck von Seriosität und Vertrauenswürdigkeit bestehen geblieben sei. Kurze Zeit später erhielt er eine Zusage, dass er die Stelle antreten könne. Der Petent sei für das Aufsetzen des Arbeitsvertrages darum gebeten worden, einige persönliche Unterlagen und Daten zu übersenden. Er sei dem nachgekommen und habe alle notwendigen Informationen zur Verfügung gestellt. Er bekam sodann einen Arbeitsvertrag und einen

QR-Code. Mit dem QR-Code habe er auf Bitte des neuen Arbeitgebers zu einer Filiale der Deutschen Post Kontakt aufgenommen, um ein PostIdent-Verfahren durchzuführen.

PostIdent-Verfahren

Beim PostIdent-Verfahren handelt es sich um eine sichere Methode zur Identitätsprüfung für Onlineverträge (z. B. Handyvertrag, Kontoeröffnung), bei dem Mitarbeitende der Deutschen Post die Echtheit einer Person bestätigen – entweder persönlich in einer **Postfiliale** (mit Coupon und Ausweis), direkt bei der Person **zu Hause durch einen Postboten** (Übergabe von Dokumenten) oder modern über einen **Videochat**. Die Person legt ein gültiges Lichtbilddokument (Personalausweis, Reisepass) vor, die Daten werden abgeglichen und die Bestätigung wird digital an den Vertragspartner übermittelt.

Auch dies habe er gemacht, da ihm ein Laptop und Diensthandy in Aussicht gestellt worden sei. Er wartete sodann auf weitere Nachricht seines neuen Arbeitgebers, hörte jedoch nie wieder etwas von ihm. Nach einigen Tagen Funkstille sei er skeptisch geworden und habe sich im Internet informiert. Dort fand sich inzwischen eine Meldung der BaFin darüber, dass das Unternehmen, bei dem sich der Petent vermeintlich beworben habe, Opfer eines Identitätsdiebstahls geworden sei. Betrüger hätten sich die Identität des Unternehmens zu eigen gemacht und Tätigkeiten angeboten, die darin bestanden, auf den eigenen Namen ein Zahlungskonto zu eröffnen und dieses für Geldtransaktionen an Dritte zur Verfügung zu stellen.

Der Petent habe sich sodann umgehend an die Bank gewandt, die aus dem PostIdent-Coupon hervorging, und erfahren, dass er tatsächlich ein Konto eröffnet hätte, welches nun leider für Geldwäsche verwendet würde. Er ließ daraufhin umgehend das Konto sperren und wandte sich an die Strafverfolgungsbehörden. Zudem erhob er Beschwerde beim ULD, da die Verarbeitung seiner personenbezogenen Daten eine Verletzung der Artikel 5 und 6 DSGVO darstelle. Zudem bestehe die Befürchtung, dass die personenbezogenen Daten in betrügerischer Weise weiterverwendet werden könnten.

Das ULD konnte dem Petenten hier leider im Wesentlichen nicht behilflich sein, da sich die Betrüger nicht ausfindig machen ließen bzw. nicht ausreichend Anknüpfungspunkte für ein erfolgreiches datenschutzaufsichtsbehördliches Handeln vorlagen. Es gibt für Unternehmen auch kaum Möglichkeiten, sich vor **Identitätsdiebstahl** zu schützen. Es stellte sich beispielsweise heraus, dass die Website des Unternehmens gar nicht von dem Unternehmen selbst betrieben wurde, sondern von den Betrügern. Es sollte der Anschein von Seriosität und Vertrauen erweckt werden. Der Betrieb eines eigenen Webauftritts kann den parallelen Betrieb betrügerischer Webauftritte gegebenenfalls etwas erschweren, jedoch nicht gänzlich ausschließen.

Was ist zu tun?

Es ist immer höchste Vorsicht geboten, sobald Sie aufgefordert werden, im Rahmen von Arbeitsverhältnissen ein PostIdent-Verfahren durchzuführen. Aus dem PostIdent-Coupon ergibt sich stets der Vertragspartner, für welchen Sie sich legitimieren. Stimmt der Vertragspartner mit dem Namen des Arbeitgebers nicht überein, handelt es sich höchstwahrscheinlich um Betrug.

5.16 Gezielte Videoüberwachung mit Tonaufzeichnung von Beschäftigten

Aufgrund einer Beschwerde wurde die Videoüberwachung im Lager eines Unternehmens geprüft. Das Unternehmen gab an, dass im Lager neun **Videokameras** in Betrieb seien und auch die Tonaufnahmefunktion der Kameras aktiviert sei. Die Videoüberwachung solle zum einen der **Prävention und der Aufklärung von Diebstählen** sowie der **Einhaltung von Brandschutzvorschriften** dienen. Es habe seit einiger Zeit Verluste am Inventar und an Warenbeständen in Höhe von ca. 25.000 Euro gegeben, die man auf mögliche Diebstahlereignisse zurückführe. Ferner lege der Vermieter des Lagerhauses einen hohen Wert auf Einhaltung des Brandschutzes. Einzelne Mitarbeitende hätten jedoch gegen das absolute Rauchverbot mehrfach verstoßen. Aus diesen Gründen seien die Videokameras installiert worden, die 24 Stunden in Betrieb seien und die Aufnahmen für 14 Tage speichern. Zudem gebe es auch eine Echtzeitübertragung, auf die die Geschäftsführung Zugriff habe. Aus den übersandten Screenshots ging hervor, dass teilweise auch dauerhafte Arbeitsplätze der Beschäftigten erfasst waren. Die Mitarbeitenden hätten Einverständniserklärungen unterschrieben.

Die Videoüberwachung gestaltet sich gleich aus mehreren Gesichtspunkten problematisch. Zum einen kommt eine Einwilligung der Beschäftigten im Sinne von Art. 6 Abs. 1 Buchst. a DSGVO regelmäßig nicht als Rechtsgrundlage für eine Videoüberwachung in Betracht. Eine **Einwilligung** muss freiwillig abgegeben werden, d. h., die Betroffenen müssen eine echte und freie Wahl haben und die Einwilligung auch verweigern oder zurückziehen können, ohne Nachteile zu erleiden. Insbesondere aufgrund des besonderen Abhängigkeitsverhältnisses zwischen Arbeitgebern und Beschäftigten ist die Freiwilligkeit oft nicht gegeben. Hinzu kommt, dass die Einwilligung für eine Videoüberwachung nicht praktikabel ist, da eine Weigerung oder ein Widerruf dazu führen würde, dass der Verantwortliche die Videoüberwachung faktisch nicht mehr weiterbetreiben könnte. Vorliegend wurden die Beschäftigten jedoch nicht einmal über das Bestehen eines Widerrufsrechts informiert. Eine wirksame Einwilligung lag daher bereits aus diesem Grund nicht vor.

Fraglich blieb, ob der Verweis auf eine Diebstahlsprävention ausreichte, um einen Kameraeinsatz zu rechtfertigen. Danach dürfen personenbezogene Daten von Beschäftigten zur Aufdeckung von Straftaten verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind, was in der Interessenabwägung zu berücksichtigen ist. Das Unternehmen hat jedoch keine dokumentierten tatsächlichen Anhaltspunkte für den Verdacht von Diebstählen durch einen Beschäftigten oder einen eng eingrenzbaren Personenkreis von Beschäftigten vorgelegt. Auch fehlte es an einem Nachweis darüber, dass der behauptete Schaden in Höhe von 25.000 Euro tatsächlich entstanden ist. Gerechtfertigt wäre selbst bei entsprechenden Nachweisen häufig keine auf Dauer angelegte, sondern nur eine zeitlich begrenzte Videoüberwachung.

Zu prüfen war letztlich Art. 6 Abs. 1 Buchst. f DSGVO. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn die Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Die Verhinderung und Aufklärung von Diebstählen kann zwar ein berechtigtes Interesse im Sinne von Art. 6 Abs. 1 Buchst. f DSGVO darstellen, jedoch fehlte es – wie oben bereits erwähnt – an Nachweisen dafür, dass tatsächlich ein Schaden in Höhe von 25.000 Euro entstanden ist. Ferner wurden außer der vermehrten Kontrolle durch Fachvorgesetzte keine milderen gleich geeigneten Maßnahmen ergriffen oder zumindest geprüft, um die vermuteten Diebstähle aufzuklären. So sind hier beispielhaft die Einsichtnahme in Personaleinsatzpläne, der Abgleich von Abwesenheits- und Anwesenheitslisten mit Warenverlusten oder stichprobenartige Tor- und Taschenkontrollen

zu nennen. Nicht ausgeschlossen werden konnte vorliegend auch, dass für die Warenverluste gar keine Diebstähle, sondern eventuell Fehlbuchungen oder Ähnliches der Grund waren. Es fehlte daher bereits an der Erforderlichkeit der Videoüberwachung.

Selbst wenn die Erforderlichkeit gegeben wäre, überwiegten die Interessen der Beschäftigten im vorliegenden Fall. Eine Videoüberwachung stellt den denkbar intensivsten Eingriff in das Recht der Beschäftigten auf informationelle Selbstbestimmung dar. **Eine Videoüberwachung ermöglicht es, das Gesamtverhalten der Beschäftigten zu beobachten (Monitoring) und reproduzierbar festzuhalten (Aufzeichnung).** Das Unternehmen überwachte im Lager nicht nur die Regale mit der Ware, sondern auch Packtische, an denen die Beschäftigten dauerhaft arbeiteten und sich der Überwachung dadurch auch nicht entziehen konnten. Besonders erschwerend kam hinzu, dass die **Tonaufnahmefunktion aktiviert** war. Dies ging jedoch nicht aus den übersandten Einverständniserklärungen hervor, sodass davon auszugehen war, dass die Beschäftigten hierüber **nicht transparent** informiert wurden. Die Videoüberwachung war daher unverhältnismäßig und damit unzulässig. Daran konnte auch der zweite angegebene Zweck des Brandschutzes nichts ändern. Effektivere und wirksamere Mittel wären hier die vermehrte Installation von Rauchmeldern oder einer automatischen Feuerlöschanlage.

Das Unternehmen deaktivierte im Laufe des Verfahrens nach und nach einzelne Kameras, die insbesondere die dauerhaften Arbeitsplätze der Beschäftigten erfassten, und schaltete die Tonaufnahmefunktion ab.

Tonaufzeichnung

Sofern eine Videoüberwachungskamera über eine Audiofunktion verfügt, ist diese zu deaktivieren. Andernfalls macht sich der Verantwortliche unter Umständen sogar nach § 201 Abs. 1 und Abs. 2 Strafgesetzbuch strafbar. Unter diesen Straftatbestand fällt das unbefugt heimliche Abhören oder Aufzeichnen des nichtöffentlich gesprochenen Wortes.

Nachdem das Unternehmen darauf hingewiesen wurde, dass auch für die restlichen Kameras derzeit keine Rechtsgrundlage ersichtlich ist, da insbesondere kein Nachweis für den behaupteten Schaden erbracht wurde, deaktivierte das Unternehmen letztendlich auch die restlichen Kameras. Allerdings wurde dies nicht aus dem Grund getan, dass man die fehlende rechtliche Grundlage anerkannte. Vielmehr wurde als Begründung angeführt, dass es derzeit keine ausreichenden WLAN-Kapazitäten für die Kameras gebe und sie deshalb deaktiviert wurden. Das Unternehmen zeigte damit und auch in den vorherigen Stellungnahmen nur wenig Unrechtsbewusstsein.

Die gezielte Überwachung von den Beschäftigten an deren dauerhaften Arbeitsplätzen sowie die Tonaufzeichnung ohne eine rechtliche Grundlage stellten einen schweren datenschutzrechtlichen Verstoß dar, sodass das Verfahren an das zuständige Referat zur Prüfung der Einleitung eines Bußgeldverfahrens abgegeben wurde.

5.17 Datenpannen in der Wirtschaft – Meldungen nach Artikel 33 DSGVO

5.17.1 Zugang zu Räumen mit Generalschlüsseln

Mit großer Macht kommt große Verantwortung – das gilt auch für Inhaberinnen und Inhaber von Generalschlüsseln in Unternehmensgebäuden. Diesbezüglich erreichte uns im Frühjahr die Datenpannenmeldung eines Unternehmens. Inhalt der Meldung war ein Vorfall in den Räumlichkeiten der Personalabteilung, bei dem es zu einem unberechtigten Zutritt eines Technikers gekommen war.

Dieser Haustechniker erschien zu einem vereinbarten Termin in der Personalabteilung, wobei er

das Büro der Sachbearbeiterin verschlossen vorfand. Da er zur Abholung von Unterlagen in der Personalabteilung erschienen war, nutzte er seinen Generalschlüssel, um sich selbst in den Räumlichkeiten nach den Unterlagen umzusehen. Dabei versicherte er im Nachhinein aber, nicht in die Schränke der Personalsachbearbeiterin, sondern lediglich auf die direkt einsehbaren Oberflächen geschaut zu haben.

Zwar war der Großteil der Unterlagen in verschlossenen Schränken sicher verstaut, dennoch lagen auch vereinzelt Unterlagen mit personenbezogenen Daten auf dem Schreibtisch der Mitarbeiterin, welche folglich theoretisch von dem Haustechniker hätten eingesehen werden können.

Trotz der Zurückhaltung des Technikers konnte eine unberechtigte Einsichtnahme in personenbezogene Daten nicht ausgeschlossen werden, welche aufgrund des hier betroffenen Fachbereichs auch teilweise von hoher Sensibilität gekennzeichnet waren. Im Rahmen der Aufarbeitung versicherte der Techniker an Eides statt, keine personenbezogenen Daten eingesehen zu haben.

Dennoch nahm das Unternehmen diesen Vorfall zum Anlass, um die eigenen organisatorischen Prozesse nachzubessern. Hierbei wurde u. a. das Schlüsselkonzept angepasst, um ein ähnlich gelagertes missbräuchliches Verwenden des Generalschlüssels zukünftig zu vermeiden.

Mit den von dem Unternehmen getroffenen Maßnahmen konnten wir das Verfahren abschließen.

Was ist zu tun?

Mit der Macht von Generalschlüsseln öffnen sich wortwörtlich Tür und Tor – leider auch für mögliche Datenschutzverletzungen. Mit klar definierten Zugriffsregelungen, Schlüsselkonzepten und flächendeckenden Schulungen der Mitarbeitenden kann aber auch diese Gefahr nachhaltig gebannt werden.

5.17.2 Besucherfotos aus Fotobox gespeichert

Fotografische Andenken an einen erlebnisreichen Ausflugstag können eine Bereicherung für die Besucherinnen und Besucher sein – solange sie auch nur für die jeweiligen Gäste persönlich zugänglich sind. Mit dieser Thematik beschäftigte sich ein Museum, das uns im vergangenen Jahr eine Datenpannenmeldung zukommen ließ.

Im Rahmen einer Veranstaltung wurde über zwei Tage für die Besucherinnen und Besucher eine Fotobox aufgestellt, in welcher diese Bilder von sich in Verkleidungen selbstauslösend erstellen und direkt ausdrucken konnten. Soweit alles im Rahmen datenschutzrechtlicher Grenzen. Allerdings wurden die Bilder im Nachgang durch den externen Anbieter der Fotobox gespeichert und dem Museum über einen Link zur Verfügung gestellt, um auf Wunsch Bilder von dessen Systemen herunterzuladen. Dieser Link wurde an die Mitarbeitenden des Museums versandt, da sich auch einige Mitarbeitenden selbst haben fotografieren lassen und ein Interesse an der digitalen Version der Bilder bestand. Allerdings wurden damit auch alle Bilder der Besucherinnen und Besucher zur Verfügung gestellt.

Da sich die Gäste der Veranstaltung die Bilder direkt nach Anfertigung ausdrucken und mitnehmen konnten, sahen wir keinen begründbaren Zweck in der weiteren Speicherung der Aufnahmen.

Im Rahmen des Verfahrens wurden alle Mitarbeitenden, die den Link zu den Aufnahmen bekommen hatten, aufgefordert, diesen Link und alle Downloads der Bildmaterialien zu löschen. Des

Weiteren wurde der Link gesperrt, sodass kein Zugriff mehr möglich war. Ergänzend hierzu wurden die Mitarbeitenden diesbezüglich erneut sensibilisiert.

Unter der Voraussetzung, dass bei künftigen Nutzungen derartiger Fotoboxen eine Speicherung von Bildaufnahmen von Beginn an deaktiviert wird, konnten wir den Vorgang abschließen.

Was ist zu tun?

Der Grundsatz der Datenminimierung zieht seine Kreise auch im Bereich vermeintlich harmloser Freizeitangebote. Ein kritisches Hinterfragen von Speicheroptionen bei Besucherangeboten wie Fotoboxen ist daher ein zu beachtender Schritt in der Veranstaltungsplanung. So garantieren Sie eine Veranstaltung, die zwar den Besucherinnen und Besuchern, aber nicht Ihrem Datenschutzbeauftragten in Erinnerung bleibt.

5.18 Videoüberwachung

5.18.1 Allgemeine Entwicklungen

Immer mehr Personen fühlen sich im Alltag durch **Videoüberwachungskameras** beeinträchtigt. Im Vergleich zum Vorjahr ist die Anzahl von Beschwerden über Videoüberwachungsanlagen **um rund 25 Prozent gestiegen**. Seit mehreren Jahren nehmen diese Zahlen ständig zu. Ein aktueller Austausch der Aufsichtsbehörden im Arbeitskreis Videoüberwachung der Datenschutzkonferenz ergab, dass auch die Aufsichtsbehörden der anderen Länder und des Bundes stetig steigende Fallzahlen im Bereich der Videoüberwachung zu verzeichnen haben.

Der Großteil der bei uns eingegangenen Beschwerden richtet sich gegen nichtöffentliche Stellen. Dies umfasst insbesondere Beschwerden gegen die **Videoüberwachung durch Unternehmen sowie durch Privatpersonen in ihrem häuslichen Umfeld**. Rund zwei Drittel der Beschwerden richten sich gegen **Videoüberwachungsanlagen im nachbarschaftlichen Kontext**. Nach unserer Beobachtung liegt der hauptsächliche Grund für den Anstieg der Beschwerden in der zunehmenden Verbreitung von Videoüberwachungsanlagen auf Privatgrundstücken durch ein immer größer werdendes Angebot an günstigen und einfach handhabbaren Kameras.

Die Beschwerdeführenden sind zumeist Nachbarn aus dem direkten Umfeld, die in der Regel eine Überwachung von Nachbargrundstücken und/oder des öffentlichen Raumes vermuten und sich durch die Installation in ihren Rechten verletzt fühlen. **Für Außenstehende ist der exakte Erfassungsbereich einer Kamera selten klar wahrnehmbar.** Man kann nicht erkennen, ob benachbarte Flächen oder der öffentliche Raum erfasst werden, sodass ein Überwachungsdruck entstehen kann. Von Bedeutung ist in diesem Zusammenhang, dass allein das Vorhandensein und die Ausrichtung einer Videoüberwachungskamera noch keinen datenschutzrechtlichen Verstoß begründet. Durch das Ergreifen technischer Maßnahmen, beispielsweise mit einer **Schwärzungs- oder Verpixelungsfunktion**, können benachbarte Flächen von der Erfassung ausgenommen und eine Videoüberwachung im häuslichen Umfeld datenschutzkonform betrieben werden.

Im Rahmen unserer Befugnisse können wir Videoüberwachungsanlagen nur auf Grundlage des Datenschutzrechts, in erster Linie nach der DSGVO, bewerten. Die von der Videoüberwachung beeinträchtigten Persönlichkeitsrechte der betroffenen Personen – z. B. im Fall eines

gefühlten Überwachungsdrucks – sind parallel durch das Zivilrecht geschützt. Unabhängig von der datenschutzrechtlichen Bewertung einer Videoüberwachung können zivilrechtliche Abwehr- und Unterlassungsansprüche bestehen. Zur Überprüfung etwa bestehender derartiger Ansprüche müssen die Beschwerdeführenden Klage einreichen; dies liegt in der Verantwortung der Zivilgerichte und nicht beim ULD.

Neben den Beschwerden über Videoüberwachung im nachbarschaftlichen Kontext hat meine Dienststelle eine Vielzahl an Beschwerden erhalten, die sich u. a. auf die **Videoüberwachung in Sportvereinen, Reitanlagen und Kleingärten, in Taxis, in Restaurants und in Schwimmbädern** beziehen. Auch bei diesen Beschwerden zeigt sich insbesondere die **Problematik der fehlenden Transparenz**: Für die Beschwerdeführenden sind die überwachten Bereiche nicht klar erkennbar, sodass Unsicherheiten entstehen. Häufiger Beschwerdegegenstand ist in diesem Zusammenhang eine **nicht vorhandene oder nicht ausreichende Hinweisbeschilderung**. Im Rahmen der Verfahren erwirken wir sodann u. a. die Installation einer rechtskonformen Hinweisbeschilderung.

Neben der Bearbeitung von Beschwerden haben wir in diesem Jahr im Bereich der Videoüberwachung auch diverse Beratungen vorgenommen. Hierzu gehörte im öffentlichen Bereich u. a. die Beratung von Kommunen, beispielsweise zu einer geplanten Videoüberwachung von Schulen oder anderen öffentlichen Einrichtungen. Im nichtöffentlichen Bereich erstreckten sich die Beratungen zu einem Großteil auf die Videoüberwachung im häuslichen Umfeld.

5.18.2 Zwischen Tomaten und Technik – Videoüberwachung in Kleingärten

Dieses Jahr haben uns mehrere Beschwerden erreicht, die sich auf Videoüberwachungskameras in Parzellen von Kleingärten beziehen. Betreiber der in Rede stehenden Videoüberwachungskameras sind die jeweiligen Pächterinnen und Pächter der Parzellen. Beschwerdeführende sind regelmäßig die direkt angrenzenden Pächterinnen und Pächter („Nachbarn"), die den genauen Erfassungsbereich der Kameras nicht erkennen können und sich durch die Installation in ihren Rechten verletzt sehen.

Die Gründe für die Installation von Videoüberwachungskameras in Kleingartenparzellen liegen häufig darin, den eigenen Besitz, insbesondere in Zeiten der Abwesenheit, zu sichern.

Wie die Videoüberwachung des selbst bewohnten privaten Grundstücks unterfällt die Videoüberwachung einer gepachteten Kleingartenparzelle in der Regel nicht der Datenschutz-Grundverordnung. Dies liegt daran, dass die DSGVO nicht für die Datenverarbeitung für persönliche oder familiäre Tätigkeiten gilt. Bei der Überwachung der allein oder mit der Familie genutzten Parzelle handelt es sich um eine solche persönliche oder familiäre Tätigkeit, sodass die Anforderungen der DSGVO nicht berücksichtigt werden müssen. Insofern sollte bei der Installation einer Kamera dafür Sorge getragen werden, dass nur die eigene Parzelle erfasst wird. Darüber hinausgehende Bereiche wie angrenzende Parzellen oder gemeinschaftlich genutzte Flächen müssen beispielsweise durch **Schwärzung** von der Erfassung ausgenommen werden. Die **Überwachung von angrenzenden Parzellen oder gemeinschaftlich genutzten Flächen** durch Pächterinnen und Pächter **ist grundsätzlich unzulässig**.

In den von uns überprüften Fällen haben wir keine Verstöße gegen das Datenschutzrecht festgestellt. Auch wenn teilweise Kameras auf benachbarte Parzellen oder Gemeinschaftsflächen ausgerichtet zu sein schienen, konnte stets nachgewiesen werden, dass nur die eigene Parzelle mit Bude, Pool oder Beeten erfasst war. In diesen Fällen, in denen das Datenschutzrecht eingehalten wird, machen wir zusätzlich darauf aufmerksam, dass die Pächterinnen und Pächter schon durch die sichtbare Ausrichtung einer Kamera Sorge dafür tragen sollten, dass sich angrenzende „Nachbarn" und Nutzerinnen und Nutzer von Gemeinschaftsflächen und des angrenzenden öffentlichen Raums nicht durch die Kamera beeinträchtigt fühlen.

5.18.3 Kamera an Bord – Videoüberwachung in Taxis

Nach einer Feier schnell und sicher nach Hause? In dieser Situation nehmen sich wohl viele Personen ein Taxi – das ist ja meist eine schnelle und sichere Beförderungsmöglichkeit. Aber gehört hierzu auch, dass man als Gast im Fahrgastraum von einer Videoüberwachungskamera beobachtet wird?

Das ULD hat in diesem Jahr mehrere Hinweise und Beschwerden zu Videoüberwachungskameras in Taxis erhalten. In all diesen Eingaben wurde beschrieben, dass mindestens eine Videoüberwachungskamera auf den Fahrgastraum gerichtet war und so zumindest der Eindruck einer Überwachung entstanden ist.

In einem Fall erreichte uns eine Beschwerde eines Fahrgastes, der nach dem Besuch einer Feier gemeinsam mit Freunden die Heimfahrt in einem Großraumtaxi angetreten hatte. Er teilte uns mit, dass im Fahrgastraum eine Kamera installiert gewesen sei, ohne dass es dazu eine Information per Hinweisschild gegeben hätte.

Im Rahmen des aufsichtsbehördlichen Verfahrens hat sich gezeigt, dass die in Rede stehende Kamera in dem Großraumfahrzeug vom Fahrzeughersteller serienmäßig verbaut ist und dem Fahrer die Möglichkeit bietet, den hinteren Fahrgastraum über ein Display einzusehen. Im Verfahren wurde von dem Verantwortlichen vorgetragen, dass die Kamera dauerhaft deaktiviert sei und daher nicht zum Einsatz komme. Zudem wies er seine Bemühungen nach, die Kamera deinstallieren zu lassen.

In diesem aufsichtsbehördlichen Verfahren wurde die in Rede stehende Kamera daher mit einer Attrappe gleichgesetzt, da durch die dauerhafte Deaktivierung keine Datenverarbeitung stattfand. Dies hat zur Einstellung des Verfahrens geführt. Damit verbunden haben wir empfohlen, im Fahrgastraum auf die Deaktivierung der Kamera hinzuweisen. Unabhängig von der konkreten Konfiguration kann von einer solchen Videokamera ein Überwachungsdruck ausgehen, durch den die Rechte und Freiheiten der betroffenen Personen eingeschränkt werden können.

Generell zeigte sich auch bei weiteren Hinweisen betreffend Kameras in Taxis, die uns erreicht haben, die folgende Lage: Auf der einen Seite stehen betroffene Fahrgäste, die sich während der Fahrt von der Kamera überwacht fühlen und in deren Rechte eingegriffen wird. Auf der anderen Seite stehen Taxi-Unternehmer und das Fahrpersonal, welche die Kamera zur **Abschreckung von Gewalt, Diebstahl und Vandalismus** sowie zum **Schutz vor Übergriffen** und das gewonnene Videomaterial zur Aufklärung etwaiger Vorfälle nutzen möchten.

Art. 6 Abs. 1 Buchst. f DSGVO

Die Verarbeitung personenbezogener Daten ist gemäß Art. 6 Abs. 1 Buchst. f DSGVO rechtmäßig, wenn die Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Eine Videoüberwachung in einem Taxi kann auf der Grundlage des Art. 6 Abs. 1 Buchst. f DSGVO rechtmäßig betrieben werden. Eine **anlasslose, permanente Überwachung des Fahrgastraumes** wird jedoch regelmäßig als **unzulässig** bewertet. Insofern haben wir in den vorliegenden Fällen darauf hingewirkt, dass die dauerhafte Überwachung unterbleibt. **Zulässig hingegen ist eine anlassbezogene, zeitlich begrenzte Überwachung**, die manuell von der Taxifahrerin oder dem Taxifahrer in einer mutmaßlichen Gefahrensituation ausgelöst werden kann.

Auch bei der Videoüberwachung in Taxis müssen die **Informationspflichten** nach Artikel 13 DSGVO beachtet werden. Auf die Videoüberwachung muss in geeigneter Weise hingewiesen werden. In der Praxis erfolgt dies über eine Hinweisbeschilderung im Fahrgastraum.

5.18.4 Privatsphäre auf dem Teller – Videoüberwachung in Restaurants

Immer wieder erhalten wir Anfragen und Beschwerden zu Videoüberwachungskameras in Restaurants. In aller Regel richten sich die Beschwerden gegen Videoüberwachungskameras, die im Gastraum installiert sind. So erreichte uns auch in diesem Jahr eine Beschwerde, die sich gegen eine Videoüberwachung im Innen- und Außenbereich eines Restaurants richtete. Ein Gast des Restaurants fühlte sich von den Kameras beobachtet, insbesondere während des Bezahlprozesses bei der Eingabe seiner PIN.

Aufgrund der Schilderungen des Beschwerdeführers wurde ein aufsichtsbehördliches Verfahren eingeleitet, um zu prüfen, ob die in Rede stehende Videoüberwachung rechtmäßig war. Im Laufe des Verfahrens zeigte sich, dass der Verantwortliche aufgrund verschiedener Vorkommnisse – wie z. B. Einbrüchen, Diebstählen und Vandalismus – neben einer Alarmanlage und Glasbruchmeldern eine Vielzahl an Kameras auf seinem weitläufigen Gelände installiert hat. Aus diesem Grund entschieden wir uns in diesem konkreten Fall für eine Datenschutzprüfung vor Ort, insbesondere um alle relevanten Informationen direkt bei dem Verantwortlichen erheben zu können.

Die Prüfung vor Ort ergab, dass die in Rede stehende Videoüberwachung grundsätzlich rechtmäßig betrieben wurde. Jedoch bedurfte es zur Herstellung eines vollumfänglichen datenschutzkonformen Zustandes einzelner Anpassungen. Hierzu gehörte u. a., dass Tische, die zum längerfristigen Verweilen einladen, mindestens während der Betriebszeiten von der Erfassung ausgenommen werden. Der Verantwortliche setzte dies sogleich um, sodass eine konstruktive Zusammenarbeit zur Herstellung eines datenschutzkonformen Zustandes führte.

Generell gilt, dass eine Videoüberwachung einen starken Eingriff in das allgemeine Persönlichkeitsrecht der betroffenen Personen darstellt. Gäste eines Restaurants haben grundsätzlich ein Interesse daran, dass ihr Verhalten nicht von einer Videokamera erfasst und aufgezeichnet wird. Dies gilt besonders in öffentlich zugänglichen Räumen, in denen sich Personen typischerweise länger aufhalten und/oder miteinander kommunizieren.

Dies führt dazu, dass die **Videoüberwachung von Sitzgelegenheiten während der Betriebszeiten** in der Regel **unzulässig** ist. Ebenso ist die Videoüberwachung von Bereichen, die für das Personal zum Verrichten dauerhafter Arbeiten geeignet sind, regelmäßig unzulässig. Gegen eine Videoüberwachung dieser Bereiche außerhalb der Betriebszeiten, beispielsweise zum Einbruchschutz, bestehen üblicherweise keine Bedenken.

Die Erfassung von Eingangs- und Durchgangsbereichen stellt sich mit entsprechender Begründung der Erforderlichkeit hingegen oft als unproblematisch dar. Hierbei handelt es sich um Bereiche, in denen sich Gäste und auch das Personal in der Regel nur kurzfristig aufhalten, sodass von einer geringeren Eingriffsintensität auszugehen ist und die Persönlichkeitsrechte weniger stark beeinträchtigt werden.

5.19 Geldbußen für Datenschutzverstöße

5.19.1 Analyse von Kundendaten zu Werbezwecken mit Smart-Data-Verfahren

Im Berichtszeitraum wurde je eine Geldbuße gegen drei schleswig-holsteinische Kreditinstitute verhängt. Diese hatten unbefugt personenbezogene Daten von Kundinnen und Kunden zum Zweck der Profilbildung für zielgerichtete Werbemaßnahmen verarbeitet. In diesem Zusammenhang hatten die Kreditinstitute einem externen Dienstleister für die Entwicklung von Analyse- und Prognosemodellen mehrere Tausend Datensätze ihrer Kundinnen und Kunden zur Verfügung gestellt. Durch den Dienstleister wurden u. a. Zahlungsdaten, Stammdaten sowie Daten zum Wohnumfeld der Kundinnen und Kunden analysiert. Die Analyse zielte darauf ab

zu ermitteln, welche Kundinnen und Kunden besonders affin für spezifische Produkte des jeweiligen Kreditinstituts sein könnten. Die Ergebnisse der Analysen wurden den drei Kreditinstituten zur Verfügung gestellt. Auf der Grundlage dieser Berechnungsergebnisse sollte im nächsten Schritt eine gezielte werbliche Ansprache der Kundinnen und Kunden erfolgen.

Zu einer Nutzung der Daten und zu Werbemaßnahmen war es nicht mehr gekommen, weil die Kreditinstitute das Verfahren aufgrund der Warnung einer Datenschutzaufsichtsbehörde eines anderen Landes beendet hatten.

Gleichwohl gab es für die bereits erfolgte Analyse der Kundendaten keine rechtliche Grundlage – insbesondere lagen keine wirksamen Einwilligungen vor. Damit haben die drei Kreditinstitute gegen die Datenschutz-Grundverordnung verstoßen. Aufgrund der Verstöße wurden Geldbußen gegen die drei Kreditinstitute in einer Gesamthöhe von mehr als 250.000 Euro verhängt.

5.19.2 Veröffentlichung von Patientendaten durch einen Arzt in einer Antwort auf eine Internetrezension

Ein Arzt erhielt eine negative Bewertung im Internet. Die Bewertung wurde von der Lebensgefährtin eines seiner Patienten unter einem Pseudonym erstellt. Der Arzt verfasste hierauf eine ausführliche Antwort und ging darin auf die einzelnen Kritikpunkte ein. Die Antwort wurde unter der Rezension ebenfalls im Internet veröffentlicht. In der Antwort sprach er die Verfasserin der Rezension mit ihrem vollen Vor- und Nachnamen an und nannte außerdem den Nachnamen und die Initiale des Vornamens des Patienten. Damit konnten alle Informationen zur Erkrankung und Behandlung des Patienten, die der Arzt in seiner Antwort schilderte, dem Patienten zugeordnet werden. Dies gilt genauso für die Informationen aus der ursprünglichen Rezension. Es lag also eine Veröffentlichung personenbezogener Daten vor, und da Informationen über eine Erkrankung und deren Behandlung enthalten waren, handelte es sich dabei um **Gesundheitsdaten**.

Die Veröffentlichung war rechtswidrig, da hierfür keine Rechtsgrundlage bestand. Zwar hatte der Arzt grundsätzlich ein berechtigtes Interesse, auf eine negative Bewertung zu antworten und seine Sichtweise darzustellen. Hierfür war aber die Offenlegung der Personendaten des Patienten nicht notwendig und damit nach der Datenschutz-Grundverordnung nicht erlaubt.

Wegen des Verstoßes haben wir gegen den Arzt eine Geldbuße verhängt. Parallel zu unserem Bußgeldverfahren hat der Patient auf dem Zivilrechtsweg eine Entschädigung durch den Arzt erstritten. Dies haben wir in unserem Bußgeldverfahren berücksichtigt. Die Schadensersatzzahlung hat sich mindernd auf die Höhe der von uns verhängten Geldbuße ausgewirkt.

Was ist zu tun?

Stellungnahmen zu Bewertungen im Internet sind grundsätzlich legitim. Sie dürfen grundsätzlich aber keine personenbezogenen Daten zu der Verfasserin oder dem Verfasser der Rezension oder zu Dritten enthalten. Ist die Person, die die Rezension erstellt hat, unbekannt, darf auch die Antwort auf die Bewertung keine Rückschlüsse auf ihre Identität ermöglichen. Auch wenn die Verfasserin oder der Verfasser der Rezension ihre oder seine Identität selbst offengelegt hat, ist Vorsicht geboten. Es muss darauf geachtet werden, dass durch die Antwort nicht weitere Informationen zu ihr oder ihm oder zu anderen identifizierbaren Personen offenbart werden.

06

KERNPUNKTE

Prüfleitfaden KI

Standard-Datenschutzmodell – ein Update

Datenpannen in Verbünden und verteilten Systemen

KI-Fachgespräch: „Frag' für 'nen Freund"

6 Systemdatenschutz

6.1 Landesebene

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

Auch 2025 war das ULD Gast in **der Konferenz der IT-Beauftragten (ITBK)**, in der das Zentrale IT-Management (ZIT) zusammen mit den IT-Beauftragten der Ressorts über aktuelle und geplante IT-Projekte von zentraler Bedeutung beraten. Ebenso hat das ULD auch 2025 am IT-Board in Sankelmark teilgenommen. In diesem zweitägigen Workshop der IT-Beauftragten der Ressorts und nachgeordneter Behörden zusammen mit dem ZIT wird jährlich über aktuelle Planungen und Arbeiten berichtet.

Ein Schwerpunkt dieses Jahres waren **Migrationen zu Open-Source-Produkten**, insbesondere im Bereich der Office-Software. Dies betraf insbesondere die Nutzung von E-Mails, bei der zeitgleich sowohl die Software für die Beschäftigten als auch die Hintergrundsysteme (E-Mail-Server) gewechselt wurden. Bei dieser Migration kam es neben längeren Umstellungszeiten (und somit verlängerten Zeiten bei Zugriff auf E-Mails) auch zu einer Datenpanne durch eine Fehlkonfiguration, bei der kurzzeitig E-Mails in falschen Postfächern sichtbar waren.

Ein weiterer Schwerpunkt war die **Bereitstellung von Alternativsoftware für einzelne Teile der Microsoft-Bürokommunikationssoftware (MS Office)**, die insbesondere im nachgeordneten Bereich in spezifischen Verfahren zur Anwendung kommt (lokale kleinere datenbankgestützte Verfahren). Durch den Wegfall der Software MS Office sind Migrationen notwendig, die nicht zentral erfolgen können. Die Hauptlast liegt daher bei den einzelnen Behörden.

Zentral werden hingegen Softwarefunktionen wie Kollaborationssoftware bereitgestellt, bei der ebenfalls Produkte von Microsoft durch Open-Source-Produkte ersetzt werden.

Jegliche Software-Umstellung ist mit Aufwand, Änderungen und möglichen Fehlern verbunden – unabhängig davon, ob es sich um Open-Source-Software handelt oder nicht. Durch den Einsatz von Open-Source-Software steigt aber die Unabhängigkeit von Marktbeteiligten und ihren Betriebsmodellen, da es typischerweise Alternativen gibt.

Es kann weiterhin eine **Entwicklung zu Cloud-Modellen** beobachtet werden. Dies ist zwar nicht per se sicherheits- oder datenschutzkritisch, bedarf aber einer genauen Analyse und Steuerung. Daher ist es von Vorteil, wenn das Land einer Entscheidung Dritter („Alles in die Cloud“) nicht ausgeliefert ist, sondern realistische alternative Handlungsoptionen hat (Stichwort digitale Souveränität, vgl. 42. TB, Tz. 6.2.4).

Im Bereich der zentralen Steuerung der Informationssicherheit war das ULD ab September wieder als Gast in der AG Informationssicherheit beteiligt. In dieser Arbeitsgruppe arbeitet die zentrale Steuerung der Informationssicherheit des Landes beim ZIT („Chief Information Security Officer“ (CISO)), die 2025 neu organisiert und mit weiteren Ressourcen hinterlegt wurde, mit den jeweils Zuständigen in den Ressorts und Behörden zusammen. Ebenfalls 2025 wurden zentrale Leitlinien im Bereich der Informationssicherheit neu gefasst und in Kraft gesetzt.

6.1.2 Zusammenarbeit mit dem ITV.SH

Auch in diesem Berichtsjahr wurde mit dem ITV.SH an der Erstellung und Überarbeitung von Dokumenten für das **Projekt „SiKoSH“** (siehe auch 43. TB, Tz. 6.1.2) gearbeitet: Diese Dokumente zum Aufbau eines Sicherheitsmanagements im kommunalen Bereich müssen kontinuierlich angepasst werden, denn sie berücksichtigen Texte und (Sicherheits-)Standards wie die des IT-Grundschutzes, die ihrerseits regelmäßig verändert werden. Gleichzeitig gibt es auch Veränderungen in der Methodik des IT-Grundschutzes, die berücksichtigt werden müssen.

Weitere Berührungspunkte waren Fragen der **Umsetzung des Onlinezugangsgesetzes (OZG)** für den kommunalen Bereich, bei der der ITV.SH eine wichtige Rolle einnimmt und stellvertretend für die Kommunen OZG-Verfahren pilotiert und sie diesen bereitstellt. Hier ist es sinnvoll, notwendige Arbeiten, z. B. zur Dokumentation, zentral und nur einmal zu bearbeiten.

Selbst wenn die technische Bereitstellung von Onlinediensten zentral erfolgt, sind es am Ende die kommunalen Behörden, die die Verwaltungsverfahren bearbeiten und die datenschutzrechtlich für die Verfahrensschritte bei der Bearbeitung verantwortlich sind. Hierbei gibt es typischerweise örtliche Unterschiede, z. B. bei eingesetzten Fachverfahren oder Dienstleistern, die zu beachten sind.

Die Kunst bei der Dokumentation und Bereitstellung von Informationen gemäß Artikel 13 DSGVO ist nun, alles Identische „vor die Klammer zu ziehen“ und gleichzeitig die örtlichen Unterschiede und Gegebenheiten berücksichtigen zu können. Dazu sind die Informationen entsprechend aufzuteilen.

Da an einigen Dienstleistungen auch zentrale, vom Land bereitgestellte Komponenten (z. B. Servicekonten oder Bezahlverfahren) beteiligt sind, sind diese entsprechend zu berücksichtigen. Im Ergebnis muss hier die technische Aufgabenteilung zwischen Land, ITV.SH und Kommunen sowie den beteiligten Dienstleistern auch in der datenschutzrechtlichen Verantwortlichkeit und in der Dokumentation und Information nachgebildet werden.

Was ist zu tun?

Die Zusammenarbeit mit dem ITV.SH bei der zentralen Bereitstellung von Verfahren und Diensten sollte fortgesetzt werden.

6.1.3 Prüfleitfaden KI – Zusammenarbeit mit dem Landesrechnungshof

In Zusammenarbeit mit dem ULD erarbeitet der Landesrechnungshof (LRH) derzeit einen **Prüfleitfaden für KI-Systeme**, um einen einheitlichen und nachvollziehbaren Prüfrahmen bereitzustellen. Das Ziel besteht darin, einen Prüfrahmen zu erarbeiten, der die datenschutzrechtlichen Anforderungen der Datenschutz-Grundverordnung (DSGVO) mit den Vorgaben des europäischen Rechtsrahmens für künstliche Intelligenz (KI-VO) sowie mit anerkannten Kriterien für vertrauenswürdige KI verbindet. Der Prüfleitfaden ist als **praxisorientierte Orientierungshilfe** geplant und erhebt keinen Anspruch auf Vollständigkeit oder die abschließende Regelung sämtlicher denkbarer Anforderungen.

Ein Schwerpunkt der Arbeiten liegt auf der Klärung der Frage, ob eine Anwendung, die vom Verantwortlichen eingesetzt wird, als KI-System im Sinne der KI-Verordnung einzuordnen ist. Hierzu werden klare Abgrenzungskriterien herangezogen. Insbesondere wird berücksichtigt, ob

es sich um ein automatisiertes, maschinenbasiertes System handelt, das Ziele verfolgt, Schlüsse ziehen kann und in der Lage ist, Vorhersagen, Entscheidungen oder Empfehlungen zu treffen bzw. Inhalte zu erzeugen. Ein Mindestmaß an eigenständigem Handeln wird vorausgesetzt. Weitere Eigenschaften wie eine Anpassungsfähigkeit im laufenden Betrieb oder eine Einflussnahme auf die Umwelt können vorliegen, sind jedoch nicht zwingend erforderlich.

Auf dieser Grundlage werden Aspekte der Risikoeinstufung von KI-Systemen mit zentralen Gewährleistungszielen verknüpft. Dabei stehen insbesondere die **Aspekte Vertraulichkeit, Integrität, Intervenierbarkeit, Nichtverkettbarkeit, Verfügbarkeit sowie Zielerreichung und Wirtschaftlichkeit** im Fokus. Ergänzend fließen übergreifende Anforderungen an **Fairness, Transparenz, Autonomie und Kontrolle, Verlässlichkeit, Sicherheit sowie Datenschutz** in die Betrachtung mit ein. Der Prüfleitfaden zielt dabei nicht auf die Vorgabe detaillierter Einzelmaßnahmen, sondern auf die strukturierte Einordnung relevanter Risiken und Schutzziele im jeweiligen Einsatzkontext ab.

Darüber hinaus werden **haftungsrechtliche Fragestellungen** beim Einsatz von KI-Systemen behandelt. Schwerpunkte sind dabei Verantwortlichkeiten, Haftungszurechnung sowie die Bedeutung angemessener Dokumentations- und Steuerungsstrukturen für Nachvollziehbarkeit und Rechenschaftspflichten.

Der Prüfleitfaden folgt einem lebenszyklusorientierten Ansatz und umfasst alle Phasen des Einsatzes von KI-Systemen: von Design und Entwicklung über Einführung und Betrieb bis hin zu Monitoring und Weiterentwicklung. Entlang dieses Lebenszyklus wird ein beispielhafter Prüfkatalog erarbeitet. Dieser strukturiert prüfrelevante Fragestellungen und unterstützt eine einheitliche Betrachtung von KI-Systemen über ihre gesamte Lebensdauer hinweg.

Mit dem Abschluss der Arbeiten wird im Frühjahr 2026 gerechnet.

6.2 Deutschlandweite und internationale Zusammenarbeit der Datenschutzbeauftragten

6.2.1 AK Technik

AK Technik

Der Arbeitskreis Technik (AK Technik) beschäftigt sich mit **technischen Fragestellungen**, die in der **Datenschutzberatung und Aufsichtspraxis** aufgeworfen werden. Auch Fragen der organisatorischen Datensicherheit gehören zum Aufgabenbereich. Neben Vertretern der Datenschutzaufsichtsbehörden des Bundes und der Länder gehören auch Vertreter des Datenschutzes aus den Kirchen und dem Rundfunk, der Medienaufsicht aus Bayern sowie Datenschutzaufsichtsbehörden im deutschsprachigen Ausland dem Arbeitskreis an.

Die Schwerpunkte der Arbeit des AK Technik lagen auch in diesem Jahr bei Arbeiten am Standard-Datenschutzmodell (SDM, Tz. 6.2.2) sowie zahlreichen Zuarbeiten, etwa im Bereich der künstlichen Intelligenz (Tz. 6.2.5) und der Umsetzung des OZG (Onlinezugangsgesetz). Hier gab es Beiträge zu einem Dokument der Datenschutzkonferenz (DSK), das einen standardisierten Prüfprozess für sogenannte „EfA-Onlinedienste nach Onlinezugangsgesetz" beschreibt. **EfA-Onlinedienste** sind Onlinedienste, die einmal entwickelt werden, dann aber durch zahlreiche Länder bzw. Kommunen als Onlinedienst genutzt bzw. für diese bereitgestellt und betrieben werden können („Einer für Alle").

Dokument zum Prüfprozess von Onlinediensten:

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

Kurzlink: *https://uldsh.de/tb44-6-2-1a*

Relevant in diesem Zusammenhang sind auch Gespräche mit der **FITKO (Föderale IT-Kooperation)**, die als „operativer Unterbau des IT-Planungsrats" auch mit der Konzeption und dem Betrieb von Verfahren und Kommunikationsstrukturen bei der Umsetzung der OZG-Dienste befasst ist. Dadurch ergeben sich zahlreiche Berührungspunkte zu den Bundesländern.

Im AK Technik entstand auch ein Dokument, dass die Grenzen des sogenannten **„Confidential Cloud Computing"** beleuchtet. Hierbei handelt es sich um Verfahren, die auch den Betreiber einer Cloud-Infrastruktur davon abhalten können bzw. sollen, Kenntnis der verarbeiteten Daten zu nehmen. Während dies bei ruhenden Daten (z. B. einem Onlinearchiv) oder Datenübertragungen (Stichwort SSL/TLS) vergleichsweise einfach umzusetzen ist, ist diese Anforderung bei der Verarbeitung von Daten im Hauptspeicher eines Servers, etwa bei der Bereitstellung eines Webdienstes, dem Durchsuchen von Datenbeständen oder dem Betrieb einer Datenbank, nur schwer umzusetzen. Confidential Cloud Computing kann hierbei den Kreis der Zugriffsberechtigten stark einschränken. Gegen ein Angreifermodell, in dem der Angreifer Zugriff auf Hardware, Software und kryptografische Schlüssel hat, hilft Confidential Cloud Computing allerdings nur eingeschränkt.

Hier ist das Dokument zu „Confidential Cloud Computing" abrufbar:

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

Kurzlink: *https://uldsh.de/tb44-6-2-1b*

Weitere Zulieferungen gab es für die Technology Expert Subgroup, insbesondere im Bereich der **Anonymisierung** und **Pseudonymisierung** (siehe auch Tz. 6.2.3) sowie zu Leitlinien für die Übermittlung von Telemetrie- und Diagnosedaten. Hier sind die Arbeiten aber noch nicht abgeschlossen.

Technology Expert Subgroup

Die **Technology Expert Subgroup** ist ein Fachausschuss des **Europäischen Datenschutzausschusses (EDSA)**, der sich auf europäischer Ebene mit technischen Fragestellungen beschäftigt. Aufträge für die Erstellung umfangreicher Dokumente erteilt der EDSA.

6.2.2 Standard-Datenschutzmodell – ein Update

Im Jahr 2025 wurde an der Modernisierung des SDM gearbeitet, nachdem die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, im Jahr zuvor die Bedeutung des SDM erneut herausgehoben hatte und die Datenschutzbeauftragten Deutschlands beschlossen hatten, mehr Ressourcen aus ihren Häusern für die Pflege und Weiterentwicklung der Methode bereitzustellen.

Die Aufträge der DSK

Die Aufträge der DSK Ende 2024 an die Unterarbeitsgruppe SDM (UAG SDM) hatten es in sich: Englischübersetzung des SDM, Erarbeitung einer neuen Gliederung für Maßnahmenbausteine, Überarbeitung des generischen Maßnahmenkatalogs, Erarbeitung eines Glossars mit Bereinigung begrifflicher Unzulänglichkeiten, Erarbeitung eines Leitfadens zur Anbindung externer SDM-Expertinnen und -Experten, Erarbeitung einer Checkliste zum Vergleich SDM mit anderen Vorgehensmodellen, Erarbeitung einer SDM-Sonderedition („SE"), Erarbeitung weiterer Bausteine sowie die Vorstellung des SDM auf der europäischen Bühne.

Bis auf die Checkliste und die Vorstellung des SDM auf EU-Ebene, die beide sinnvollerweise erst nach Abschluss der anderen Arbeiten erfolgen sollten, wurden die Arbeiten aufgenommen – mit bereits ersten Zwischenergebnissen. Das Jahr 2026 wird davon gekennzeichnet sein,

die Zustimmung der Gremien für die teilweise inzwischen vorliegenden Entwürfe zu erreichen.

Einblick ins Labor

Die neue Gliederung für Bausteine wurde am Beispiel des **Bausteins „Protokollierung“** erarbeitet und liegt als Entwurf vor. Während dieser Überarbeitung – sowie an der parallel durchgeführten Überarbeitung auch des generischen Maßnahmenkatalogs – entschied sich die Entwicklergruppe, eine Innovation des IT-Grundschutzes zu übernehmen. In Anlehnung an die **OSCAL-Orientierung des „Grundschutz++“** werden zukünftig auch SDM-Maßnahmen in Form von **Satzschablonen** formuliert. Eine solche Satzschablone ist eine **vordefinierte syntaktische Struktur**, die umgehend mehr Klarheit verschafft. Langfristig besteht das Ziel darin, Datenschutzprüfungen auf der operativen Ebene stärker zu automatisieren und „vollständiger“ durchführen zu können.

Intensiv hat sich die Arbeitsgruppe auch mit der Analyse beschäftigt, warum das SDM in der Praxis noch zu wenig genutzt wird. Das Ergebnis dieser Analyse lautete, dass das SDM zwar ein **sehr gutes Modell zur wechselseitigen Transformation von normativen und operativen Anforderungen**, aber **keine Schritt-für-Schritt-Methode für die konkrete typische Durchführung von Prüfungen und Beratungen** biete. Für erfahrene DSB reicht die Kenntnis des Modells, insbesondere mit der Anwendung des SDM-Würfels, um daraus dann eine für die eigene Organisation angepasste Methodik zu entwickeln. Weniger erfahrene DSB mit kleinen Zeitanteilen für den operativen Datenschutz möchten dagegen ungleich stärker durch die Prozesse geführt werden. Dabei muss dann immer klar sein, welcher Bezug zu Anforderungen der DSGVO besteht und welche konkrete Hilfe das SDM dafür vorgesehen hat. Deshalb stand das letzte Drittel des Jahres unter dem wegweisenden Motto „Vom Modell zur Methode“. Die Lösung wird in der **Herausgabe einer Sonderedition („SE“) des SDM** gesehen. Die Beratungen zur Sonderedition sind noch nicht abgeschlossen, ein erster belastbarer Entwurf des Konzepts liegt vor.

Im Rahmen der Arbeiten am Glossar wurde entschieden, dass begriffliche Klärungen zunächst im Modelltext herbeigeführt werden müssen und dass das Glossar nur passiv wiedergibt, was im Text steht. Klärungen im Methodentext herbeizuführen sind allerdings langwierig und unterliegen Beratungen des AK Technik und häufig auch der DSK. Eine besondere Zusatzfunktion des Glossars wird darin bestehen, verstärkt auch Quellen (z. B. SDM-Eigenentwicklung, DSK- oder EDSA-Beschluss, Gerichtsurteil) auszuweisen.

Auch die Klärung der Anbindung von externen SDM-Expertinnen und -Experten an die UAG SDM, die außerhalb der Gremien der Datenschutzbehörden agieren, ist vorangekommen. Bislang wurde nur ein „Patenmodell“ angeboten, wonach Externe sich ein Mitglied aus dem Kreis der UAG SDM suchen mussten, über das externe Zuarbeiten in die Entwicklungen der UAG SDM eingespeist werden konnten. Diese nach wie vor bestehende Lösung wurde bislang noch nie gewählt. Es liegt deshalb ein Entwurf vor, wonach zunächst eine Grundsatzentscheidung der DSK zur Möglichkeit externer Zuarbeiten für die UAG SDM herbeigeführt werden soll. Wenn diese vorliegt, sieht das Konzept vor, bestimmte Formen der Zusammenarbeit zu erproben. Dies kann in der gemeinsamen Durchführung eines „SDM-Tages“ bestehen und bis zur gemeinsamen Bearbeitung von Bausteinen reichen.

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

https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V31.pdf

Kurzlink: *https://uldsh.de/tb44-6-2-2a*

6.2.3 EDSA-Guidelines zu Pseudonymisierung und Anonymisierung – ein Update

Im Tätigkeitsbericht des Vorjahres wurde bereits über die Arbeiten an zwei Leitlinien des Europäischen Datenschutzausschusses (EDSA) zu den Themen Pseudonymisierung und Anonymisierung berichtet (43. TB, Tz. 6.2.4). An der Erstellung beider Leitlinien sind wir beteiligt. Die Arbeiten sind weit fortgeschritten, aber noch nicht abgeschlossen.

Die **Leitlinie zur Pseudonymisierung** behandelt die Frage, wie die Vorgaben der DSGVO zur Pseudonymisierung (Art. 6 Buchst. e, Art. 25 Abs. 1, Art. 32 Abs. 1 Buchst. a DSGVO) praktisch umgesetzt werden können, sodass die eingesetzten Pseudonymisierungsverfahren die Vorgaben der Definition in Art. 4 Nr. 5 DSGVO erfüllen.

Zu Beginn des Jahres erfolgte eine öffentliche Konsultation durch den EDSA, deren Ergebnisse in eine neue Fassung eingearbeitet werden sollen. Unterbrochen wurden die Arbeiten durch ein Urteil des EuGH (C-413/23 P), das sich mit Fragen der Pseudonymisierung und des Personenbezugs in der Verordnung (EU) 2018/1725 befasst. Diese regelt die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Europäischen Union. Da das Urteil auf die Regelungen der DSGVO übertragbar ist, wird derzeit die Leitlinie angepasst, um die Aussagen des Urteils zu berücksichtigen.

In der **Leitlinie zur Anonymisierung** wird betrachtet, wann es sich bei Daten um „personenbezogene Daten" im Sinne von Art. 4 Nr. 1 DSGVO handelt, und es werden entsprechende Kriterien entwickelt. Aus technischer Sicht hätte man gerne einen Prüfalgorithmus, mit dem eindeutig über einen Personenbezug entschieden werden kann.

Doch so einfach ist die Welt nicht: eine Schwierigkeit bei der Entscheidung „Personenbezug ja/nein" besteht darin, dass im zugehörigen Erwägungsgrund 26 auch Aspekte genannt sind, die einer Auslegung und Einschätzung bedürfen. Beispielsweise sollen für eine Entscheidung „alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern".

Dies führt zu der Frage, wie der Begriff „nach allgemeinem Ermessen wahrscheinlich" in konkrete Prüfschritte übersetzt werden kann. Und zu der Frage, ob es über „Aussondern" hinaus weitere Möglichkeiten gibt, einen direkten oder indirekten Personenbezug herzustellen, welche das sind und wie man diese Möglichkeiten überprüft. Die Kunst ist dabei, bei der Beschreibung alle realistischen Fälle zu erfassen, ohne dabei fernliegende Fälle mit einzuschließen.

Auch die Arbeiten an dieser Leitlinie wurden zwischenzeitlich unterbrochen: Zum einen sollen gemäß einer neuen Verfahrensregelung Dritte frühzeitig und vor der Erstellung von Leitlinien eingebunden werden. Dieser Verfahrensschritt passt zwar nicht zum derzeit fortgeschrittenen Entwurfsstadium, ist aber dennoch Ende 2025 „nachgeholt" worden; die Ergebnisse müssen eingearbeitet werden. Zum anderen gibt es seit dem Herbst 2025 Änderungsvorschläge für die DSGVO (Tz. 2.5), die insbesondere die Definition des Personenbezugs betreffen. Da dies ein zentraler Punkt ist, ist der Abschluss der Leitlinien erst sinnvoll, wenn die Rechtslage feststeht.

Zwischenzeitlich haben einige Datenschutzbehörden in Deutschland in einem Modellverfahren versucht, den bisherigen Stand beider Leitlinien auf konkrete Verfahren anzuwenden, beispielsweise auf die Anonymisierungen von Daten aus dem Straßenverkehr oder die Pseudonymisierung von Daten für ein fiktives KI-Training. Schwerpunkte waren hier die realistische Beschreibung fiktiver Fälle, ihre Einordnung in den Rechtsrahmen (beispielsweise Regelungen des Straßenverkehrsrechts und der medizinischen Forschung) und die Beschreibung von Anonymisierungs- und Pseudonymisierungsverfahren. Der letzte Schritt, nämlich die Beurteilung, ob die beschriebenen Verfahren den Anforderungen der Leitlinien genügen, kann erst nach der Fertigstellung der Leitlinien abgeschlossen werden.

Der Abschluss beider Leitlinien wird 2026 erwartet.

6.2.4 Orientierungshilfe RAG-Systeme

Im Berichtszeitraum war das ULD aktiv an der Erarbeitung der „Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode" der Datenschutzkonferenz beteiligt. Dieses Papier beleuchtet die datenschutzrechtlichen Anforderungen beim Einsatz von **Retrieval Augmented Generation (RAG)** – einer neueren KI-Technologie, bei der große Sprachmodelle durch gezielten Zugriff auf z. B. organisationsinterne Wissensbestände ergänzt werden, um kontextspezifische und überprüfbare Antworten zu erzeugen. Die RAG-Methode ist dabei eine Alternative zum Nachtrainieren von KI-Modellen mit zusätzlichen Informationen.

Die Orientierungshilfe hat sich als äußerst praxisrelevant erwiesen, da viele innovative Unternehmen und Behörden derzeit erste konkrete Anwendungsfälle mit RAG-Systemen entwickeln oder entsprechende Services implementieren möchten. Sie bietet nicht nur eine verständliche Definition und technische Grundlagen der RAG-Methode, sondern insbesondere rechtliche und technische Hinweise, wie die Grundsätze der DSGVO in diesem Kontext umgesetzt werden können.

Ein zentrales Anliegen unserer Mitarbeit war es, datenschutzrechtliche Schwerpunkte schon in diesem frühen Entwicklungsstadium der Technologie zu setzen. Dabei konnten wesentliche Hinweise zur **Sicherstellung von Transparenz, Zweckbindung, Datenminimierung** und zur **Wahrung der Betroffenenrechte** eingebracht werden – mit dem Ziel, den weiteren technologischen und regulatorischen Entwicklungsprozess in datenschutzfreundliche Bahnen zu lenken.

Die Orientierungshilfe wurde von der Fachöffentlichkeit mit großem Interesse aufgenommen. Da das Papier angesichts der dynamischen Entwicklung der KI-Technologie gegebenenfalls mittelfristig einer Anpassung bedarf, können Rückmeldungen für eine Überarbeitung sehr hilfreich sein. Auch vor diesem Hintergrund wird die frühzeitige Bereitstellung dieser praxisorientierten Hilfestellung als wichtiger Beitrag bewertet, um die Potenziale der Technologie nutzbar zu machen, ohne datenschutzrechtliche Risiken aus dem Blick zu verlieren.

Ausblickend bietet die aktuelle Orientierungshilfe eine solide Grundlage, die in weiteren Iterationsschritten noch stärker auf spezifische Einsatzszenarien und weiterführende technische Entwicklungen eingehen kann. Insbesondere eine weiter gehende **Spezialisierung von Modellen auf spezifische Fachdomänen** und die **datenschutzfreundliche Gestaltung von Trainingsprozessen** könnten dazu beitragen, die Vorteile von RAG-Systemen noch stärker auszuschöpfen und datenschutzkonform zu realisieren.

Die Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode ist hier abrufbar:

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

Kurzlink: *https://uldsh.de/tb44-6-2-4a*

Was ist zu tun?

Jedes Feedback zur Orientierungshilfe mit Kritikpunkten, Änderungs- und Konkretisierungswünschen ist herzlich willkommen und kann an das ULD gegeben werden.

6.2.5 Orientierungshilfe zu Maßnahmen bei Entwicklung und Betrieb von KI-Systemen

Mit der zunehmenden Entwicklung von KI-Anwendungen und -Services in verschiedenen Bereichen stellen sich auch immer mehr Fragen zur konkreten Umsetzung von datenschutzrechtlichen Anforderungen. Das ULD hat aktiv an der Erstellung der „Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen“ der Datenschutzkonferenz mitgewirkt. Diese 28-seitige Orientierungshilfe richtet sich gezielt an Hersteller sowie Betreiber von KI-Systemen und geht damit über das traditionelle Adressatenfeld datenschutzrechtlich verantwortlicher Stellen hinaus. Die Ausrichtung auf Entwicklungsteams und Betreiber ist eine direkte Reaktion auf den erkennbaren Beratungsbedarf und zahlreiche Anfragen aus dieser Gruppe, die in der Praxis zunehmend vor datenschutzrechtliche Herausforderungen bei der Entwicklung und Nutzung von KI-Systemen gestellt werden. Damit dient die Orientierungshilfe auch der Anforderung aus Artikel 25 DSGVO und unterstützt den Datenschutz durch Technikgestaltung.

Ein zentrales Merkmal der Orientierungshilfe ist ihre **strukturierte Gliederung entlang des Lebenszyklus eines KI-Systems**. Die Arbeitshilfe gliedert die datenschutzbezogenen Anforderungen in vier aufeinanderfolgende Phasen – **Design, Entwicklung, Einführung sowie Betrieb und Monitoring** – und ordnet zu jeder Phase die relevanten technischen und organisatorischen Maßnahmen systematisch an. Durch diese lebenszyklusorientierte Darstellung erhalten unterschiedliche Beteiligte entlang der Entwicklungs- und Betriebsprozesse jeweils präzise Hinweise, welche Anforderungen in ihrem Tätigkeitsbereich zu beachten sind.

Die Orientierungshilfe verfolgt dabei konsequent eine Analyse anhand der **Gewährleistungsziele des Standard-Datenschutzmodells (SDM)**. Die sieben Gewährleistungsziele werden jeweils in den einzelnen Phasen erläutert und mit konkreten technischen Maßnahmen verknüpft. Diese Strukturierung unterstützt auch Personen mit wenig Vorkenntnissen im Datenschutz dabei, die Hintergründe und rechtlichen Grundlagen der Anforderungen zu verstehen und praktisch umzusetzen.

Trotz der komplexen und vielseitigen Anforderungen, die mit dem Einsatz von KI-Technologien verbunden sind, ist es gelungen, die Orientierungshilfe auf kompakten 28 Seiten zu verfassen. Für viele Anwenderinnen und Anwender sind die wesentlichen Passagen für ihre konkrete Aufgabe klar und prägnant zusammengefasst, sodass sie die relevanten datenschutzrechtlichen Aspekte schnell erfassen und in der Praxis anwenden können.

Die Orientierungshilfe konnte bereits in mehreren Fällen erfolgreich als praxisnahe Hilfestellung empfohlen werden, insbesondere wenn die Gesprächspartner einen fundierten ersten Überblick über datenschutzrechtliche Anforderungen an KI-Systeme suchten und diese in ihren Entwicklungs- oder Implementierungsprozessen berücksichtigen wollten. Sie leistet somit einen wichtigen Beitrag, datenschutzkonforme Gestaltung und Innovation in der KI-Entwicklung zu fördern.

Die Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen ist hier verfügbar:

https://www.datenschutzkonferenz-online.de/media/oh/DSK-OH_KI-Systeme.pdf

Kurzlink: *https://uldsh.de/tb44-6-2-5a*

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

6.3.1 Erkenntnisse aus Datenpannenmeldungen

Weiterhin beschäftigen uns Meldungen nach Artikel 33 DSGVO über Datenschutzverletzungen, umgangssprachlich „Datenpannenmeldungen“, sehr.

Ein Schwerpunkt liegt bei typischen internen Fehlern, etwa einer **Fehlbedienung eines Geräts**, einer **Fehleingabe einer E-Mail-Adresse** oder **Verwechslungen beim postalischen Versand**, die dann zu einer unbefugten Datenoffenbarung führen. Auch eine **fehlerhafte Konfiguration der Berechtigungsverwaltung**, die zu weite Einsichtsrechte in Datenbestände erlaubt, gehört dazu. Nicht immer lassen sich technische Maßnahmen finden, um dies zukünftig zu vermeiden; hier ist die Stärkung organisatorischer Prozesse, z. B. Kontrollen nach dem Vieraugenprinzip, zielführend.

Handelt es sich um technische Konfigurationen, z. B im Berechtigungsmanagement, ist neben der richtigen Festlegung der Sollvorgaben (etwa im Rechtemanagement: „Wer soll was dürfen?“) auch die richtige Umsetzung („Was wurde konfiguriert?“) zu prüfen. Dies sollte nicht nur auf der Ebene der Konfiguration („Welche Konfigurationseinstellungen wurden vorgenommen“?) erfolgen, sondern es ist, soweit möglich, auch die tatsächliche Wirksamkeit zu überprüfen: Wird das Ziel durch die vorgenommene Konfiguration tatsächlich erreicht? Typisches Beispiel ist die Überprüfung, ob Personen, Nutzergruppen oder Geräte, die keine Zugriffsberechtigung haben sollen, tatsächlich nicht zugreifen können oder ob die programmierten Back-up- und Löschzyklen tatsächlich eingehalten werden.

Durch Überprüfungen können Fehlkonfigurationen erkannt werden: Nicht immer wirkt eine Konfiguration wie erwartet oder wie gedacht. Dies kann an Softwarefehlern oder aber an falschen Annahmen über die genaue Wirkungsweise der Konfiguration liegen. Gerade im Berechtigungsmanagement auf Dateiebene (z. B. NTFS-Berechtigungen im Windows-Umfeld) oder im Management von Berechtigungsgruppen (z. B. in Verzeichnisdiensten) lauern Fehlerquellen. Wenn diese nicht erkannt werden, sind Datenschutzverletzungen vorprogrammiert.

Ein weiterer Schwerpunkt lag auf **Verletzungen des Schutzes der Verfügbarkeit von Daten** – sie waren schlicht gelöscht, unbefugt verschlüsselt oder sind als Nachrichten nicht übertragen worden. Ursachen waren zum einen Cyberangriffe mit Verschlüsselungstrojanern (vgl. 42. TB, Tz. 6.3.2), aber auch Fehlbedienungen (Tz. 4.1.4) oder Konfigurationsfehler. Dies kann große negative Auswirkungen auf Betroffene haben, wenn es keine Datensicherungen (Backups) gibt oder ein Fehlen von Nachrichten schlicht unbemerkt bleibt: Absender von elektronischen Anträgen oder Bewerbungen gehen davon aus, dass sie den Empfänger erreichen. Handelt es sich um Erstkontakte, so werden ausbleibende Nachrichten von den Empfängern nicht vermisst. Erst nach längerer Zeit fragen dann die Absender nach ausbleibenden Antworten – möglicherweise über den gleichen, nicht funktionierenden Kommunikationsweg. Bis diese Art von Kommunikationspanne erkannt wird und aufgeklärt ist, kann wertvolle Zeit vergehen. Und auch die Ermittlung der Ursache, an welcher Stelle genau es gehakt hat, kann schwierig sein (Tz. 6.3.2).

Weiterhin ein Klassiker sind **unbefugte Zugriffe auf E-Mail-Konten**, die meist durch Missbrauch (z. B. Versand von Spam im Namen des Kontoinhabers) erkannt werden. Im Raum steht dann aber nicht nur die missbräuchliche Verwendung durch Dritte, sondern auch ein unbefugter Datenzugriff: Wer mit einem fremden E-Mail-Konto Spammails versenden kann, kann auch die E-Mails lesen, umleiten, Kennwörter ändern usw. Daher ist der Spamversand erst der Anfang der Datenschutzverletzung, und es muss ermittelt werden, ob unbefugte lesende Zugriffe erfolgten.

Die Ursache sind meist abgefangene Zugangsdaten (Stichwort **Phishing**), gepaart mit der

Möglichkeit, allein mit Nutzernamen und Passwort über das Internet auf (cloudbasierte) E-Mail-Systeme zugreifen zu können. Wie bereits im 42. TB, Tz. 6.3.2 und 43. TB, Tz. 6.3.1 ausgeführt, sind daher zusätzliche Sicherungsmaßnahmen zu ergreifen, beispielsweise eine **Zwei-Faktor-Authentifizierung** oder die Begrenzung des Zugriffs auf bestimmte Netze (z. B. über ein VPN oder IP-Adresskreise) oder bestimmte Endgeräte (z. B. dienstlich genutzte Geräte).

Auch die **Sensibilisierung** der Kundinnen und Kunden oder Beschäftigten gegen diese Art von Angriffen kann helfen, sie aber nicht unterbinden: Während der Rat „kein Passwort-Recycling, sondern unterschiedliche Passwörter für unterschiedliche Nutzerkonten" vergleichsweise leicht durch die Nutzerinnen und Nutzer umzusetzen ist, ist dies beim Ratschlag „Falle nicht auf Phishing herein!" nicht der Fall: Mittlerweile sind Phishing-E-Mails sprachlich so ausgereift und überzeugend, dass sie wirklich schwer zu erkennen sind. Kombiniert mit täuschend ähnlichen gefälschten Webdiensten und Eingabefenstern für Zugangsdaten muss man schon genau aufpassen, um nicht in die Falle zu tappen.

Was ist zu tun?

Um Datenschutzverletzungen zu vermeiden, sind sorgfältige technische Konfiguration, zeitnahes Einspielen von Sicherheitspatches und zusätzliche Sicherheitsmaßnahmen beim Zugriff auf Cloud-Dienste notwendig.

6.3.2 Datenpannen in Verbünden und verteilten Systemen

Im vergangenen Jahr erreichten uns verschiedene Meldungen nach Artikel 33 über Datenpannen, die in Verbundsystemen aufgetreten waren. Meist handelte es sich um Nachrichten in Onlineportalen, die aus technischen Gründen nicht korrekt weitergeleitet wurden. Aufgefallen ist dies meist durch Nachfragen von Betroffenen beim Empfänger, der die Nachrichten aber nicht erhalten und daher nicht bearbeitet hat.

Insbesondere bei Webformularen, deren Inhalte an andere Institutionen oder Behörden weitergeleitet werden, führen **Fehler in der Weiterleitung** schnell zu Problemen. Um dies nachvollziehen zu können, sei zunächst der technische Ablauf kurz erläutert: Nutzerinnen und Nutzer rufen ein Webformular auf, geben entsprechende Inhalte ein und laden gegebenenfalls Anhänge hoch. Während der Eingabe können Inhalte auf Vollständigkeit geprüft werden; ebenso können nicht lesbare Anhänge oder nicht unterstützte Dateiformate abgelehnt werden. Mit dem Ende des Dialogs und dem Absenden endet der Kontakt des Portals zu den Nutzenden.

Nach dem Absenden der Eingabe wird technisch eine Nachricht (Datenpaket) erzeugt und dem Empfänger direkt übermittelt (z. B. über E-Mail-artige Systeme) oder zum Abruf bereitgestellt. Wer der Empfänger ist, hängt von den Eingaben (z. B. zuständige Behörde des Wohnortes) ab. Je nach Empfänger und technischer Anbindung kommen zur Übermittlung zwei Möglichkeiten in Betracht. Der Abruf kann direkt durch den Empfänger oder durch einen beauftragten Dritten erfolgen, der dann seinerseits für die Weiterleitung an den Empfänger zuständig ist. Diese Option wird häufig gewählt, wenn die Anzahl möglicher Empfänger sehr groß ist (z. B. alle Kommunalverwaltungen in Deutschland): Damit nicht sämtliche möglichen Empfänger und ihre technische Adressierung in dem Portalsystem verwaltet werden müssen, kommen Zwischenstellen, z. B. Landesdienstleister, zum Einsatz. Diese rufen die Nachrichten ab und sind dann ihrerseits dafür zuständig, sie an den richtigen Empfänger zu übermitteln. Der Empfänger verarbeitet schließlich die Nachrichten eigenständig

weiter, z. B. in einem zentralen Posteingang oder direkt in seinen Fachverfahren.

Technische Fehler bei der Übermittlung können dabei an verschiedenen Stellen auftreten: Zum einen können Adressierungsinformationen veraltet oder falsch sein, sodass das Portal die Nachrichten nicht den korrekten Empfängern zuordnen oder zustellen kann. Zum anderen kann es Probleme bei der Weiterleitung in nachfolgenden Systemen geben, z. B. bei beauftragten Dritten (Stichwort Landesdienstleister) oder innerhalb der Empfängerorganisation, etwa bei der Übertragung in Fachverfahren. Man kann die Fehlermöglichkeiten etwa mit dem Versand bei Briefen oder Paketen vergleichen – auch hier gibt es zahlreiche Fehlerquellen, die von unleserlichen oder falschen Anschriften über Fehlsortierungen, kaputte Fahrzeuge, vergessene Zustellungen bis hin zu Irrläufern im Hause des Empfängers reichen.

Zu dem Zeitpunkt, zu dem die Fehler auftreten oder bemerkt werden, gibt es keinen Kontakt zu den Absendenden der Nachricht – diese können über Fehler nicht benachrichtigt werden. Stattdessen haben sie nach dem Absenden der Nachricht eine Meldung erhalten, dass die Nachricht erfolgreich abgesendet wurde. Diese besagt aber nicht, dass die Nachricht erfolgreich beim Empfänger angekommen ist – ähnlich wie ein Einlieferungsbeleg einer Paketsendung auch keine Aussage über die Auslieferung treffen kann. Und anders als bei Paketen oder E-Mails tragen die Nachrichten auf der Außenseite keine Absenderkennung. Die Betroffenen haben auf die technischen Fehler der Nichtzustellung keinen Einfluss. Sie rechnen mit einer korrekten Zustellung, und erst wenn diese scheitert, erfahren sie von einer Nichtzustellung.

Daher ist es wichtig, **dass der Zustellprozess reibungslos läuft**. Dies ist umso wichtiger, wenn Betroffene auf eine schnelle Bearbeitung angewiesen sind (etwa bei Leistungen wie Wohngeld) und zukünftig ausschließlich Onlineverfahren eingesetzt werden. Die Möglichkeiten, auf technische Fehler zu reagieren, sind eingeschränkt. Sie bestehen in erster Linie darin, Fehler zu protokollieren, die Protokolle zu überprüfen und daraus Handlungen abzuleiten, z. B. einen erneuten Versand, die Information der Empfänger (etwa wenn diese wiederholt Nachrichten nicht abrufen) oder eine manuelle Ermittlung der korrekten technischen Empfängeradresse. Hier musste in der Vergangenheit nachgesteuert werden, wenn an der Zustellung beteiligte Stellen nicht die richtigen Schlüsse aus den Fehlerprotokollen gezogen haben: Anders als in der Paketwelt werden Nachrichten in den Zwischensystemen nur eine begrenzte Zeit vorgehalten oder nach erfolgreicher Übertragung an das nächste System automatisch gelöscht. Wenn dann später das Fehlen einer Nachricht bemerkt wird, ist diese im absendenden System meist nicht mehr vorhanden. Wenn eine Nachricht gar nicht zugestellt werden kann, müsste man sie analysieren, um den Absender ermitteln und informieren zu können. Eine Inhaltsanalyse ist aber aus gutem Grund nicht vorgesehen.

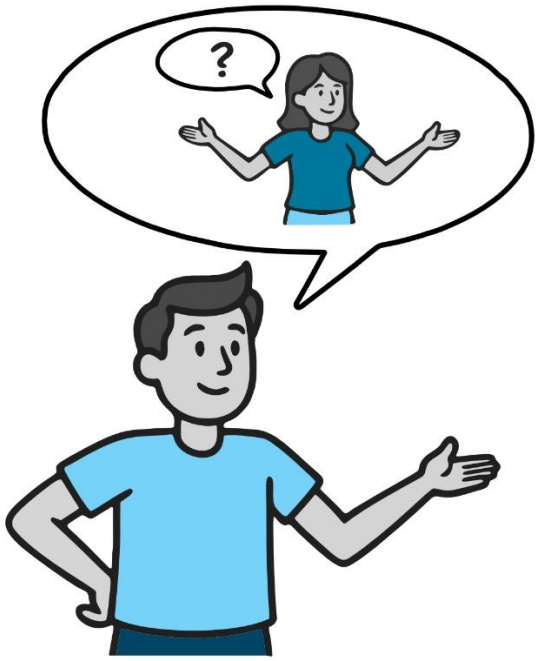
Was ist zu tun?

Bei der Verarbeitung von Nachrichten in Portal- und Verbundsystemen ist wegen der Vielzahl von Beteiligten und Datenübertragungen besonders darauf zu achten, dass Fehler protokolliert, durch ein fortlaufendes Monitoring erkannt und abgestellt werden.

6.3.3 KI-Fachgespräch: „Frag' für 'nen Freund"

Die zunehmende Integration von KI-Anwendungen in Unternehmen und Behörden stellt nach wie vor hohe Anforderungen an alle Beteiligten. Neben der dynamischen technischen Entwicklung führen neue gesetzliche und regulatorische Vorgaben zu zusätzlichen Anforderungen an die Planung, Entwicklung und den Einsatz von IT-Anwendungen. Somit stehen Organisationen vor der Herausforderung, technische Innovationen und rechtliche Anforderungen frühzeitig miteinander zu verknüpfen. Gleichzeitig sind Aufsichtsbehörden darauf angewiesen, Einblicke in die praktischen Fragestellungen und Erfahrungen aus der Umsetzung von KI-Technologien zu erhalten, um praxisnahe und umsetzbare Hinweise geben zu können.

Vor diesem Hintergrund hat sich das Veranstaltungsformat „Frag' für 'nen Freund" als geeigneter Rahmen für einen **offenen und fachlichen Austausch zwischen Organisationen und Aufsichtsbehörden** bewährt. Die Veranstaltung bietet Gelegenheit, Fragen zu neuer KI-Technologie, rechtlichen Rahmenbedingungen und praktischen Fragen der Umsetzung zu stellen und gemeinsam zu diskutieren. Durch den direkten Dialog können unterschiedliche Sichtweisen eingebracht und bestehende Unklarheiten frühzeitig angesprochen werden.



Seit der ersten Veranstaltung im November 2024 hat „Frag' für 'nen Freund" bereits fünfmal stattgefunden und stößt weiterhin auf großes Interesse. Die Termine werden dabei abwechselnd unter den Titeln „Frag' für 'nen Freund" und „Frag' für 'ne Freundin" durchgeführt. Die Vorstellung von aktuellen Fragen und auch Lösungsansätzen aus öffentlichen und nichtöffentlichen Stellen im Land steht im Mittelpunkt und regt immer wieder weiter gehende Fragen und Überlegungen in der wachsenden Gruppe an Teilnehmenden an. Typische Fragestellungen betreffen die **Anbindung und Nutzung großer Sprachmodelle (Large Language Models, LLMs)** sowohl im Eigenbetrieb als auch bei Dritten. Ebenso wurden **verschiedene Nutzungsszenarien** (z. B. als Werkzeug für allgemeine Textgenerierung und -analyse oder die Nutzung als spezifischer Wissensspeicher in Form eines RAG, siehe Tz. 6.2.4) diskutiert. Häufige Fragen waren auch, ob und gegebenenfalls nach welchen Regeln vorhandene Datenbestände zum **KI-Training** genutzt werden dürfen – eine Fragestellung, die im Hinblick auf Zweckänderungen auch jenseits von KI-Training, etwa bei der Ausbildung, bei Weiterbildungen oder bei Sammlungen in Form von Musterbeispielen oder internen Wissenssammlungen, eine Rolle spielt. Ebenso gab es Fragen nach Umfang und Intensität von KI-Schulungen für Beschäftigte.

Die Veranstaltungsreihe hat sich für viele Interessierte als sehr wertvoll erwiesen und wird fortgeführt. Sie bietet den Teilnehmenden die Möglichkeit, sich zu aktuellen technologischen Entwicklungen auszutauschen, voneinander zu lernen und Kontakte zu knüpfen. Unternehmen, Behörden und Aufsichtsbehörden treten dabei in einen direkten fachlichen Austausch auf Augenhöhe und befassen sich gemeinsam mit praktischen Fragestellungen rund um den **Einsatz neuer KI-Technologien**.

Unter diesem Link gibt es weitere Informationen:

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

Kurzlink: *https://uldsh.de/tb44-6-3-3a*

Was ist zu tun?

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

07

KERNPUNKTE

Änderungen zum Medienstaatsvertrag

Aktuelles aus dem AK Medien

7 Neue Medien

7.1 Änderungen zum Medienstaatsvertrag

Im Arbeitskreis Medien der Datenschutzaufsichtsbehörden des Bundes und der Länder war das ULD an der Erarbeitung von Hinweisen beteiligt, welche bei den Erörterungen zu den beabsichtigten **Änderungen des Medienstaatsvertrags (MStV)** einflossen. Der MStV ist eine von den Ländern unterzeichnete Übereinkunft und „enthält Regelungen für die Veranstaltung und das Angebot, die Verbreitung und die Zugänglichmachung von Rundfunk und Telemedien in Deutschland". Die Regelungen gelten sowohl für den öffentlich-rechtlichen als auch für den privaten Rundfunk.

Der neunte Medienänderungsstaatsvertrag enthält eine neue Bestimmung, die den Landesmedienanstalten in deren Funktion als Aufsichtsbehörden über Rundfunkanbieter **technische Mittel** an die Hand gibt, mit deren Hilfe **Text-, Audio- und Bildinhalte in Rundfunk und Telemedien automatisiert auf potenzielle Verstöße gegen die Bestimmungen des Medienstaatsvertrags abgeglichen werden** können. Dies soll auch die Verarbeitung personenbezogener Daten einschließlich besonderer Datenkategorien umfassen, soweit dies zur Wahrnehmung der Aufsichtstätigkeit erforderlich ist. Ein solches technisches Instrument kann ein KI-System sein, das automatisiert als Crawler Websites analysiert. Ermittelte Informationen sollen von den Landesmedienanstalten zur Verfolgung von Ordnungswidrigkeiten genutzt und bei Anhaltspunkten für die Erfüllung von Straftatbeständen an die zuständigen Strafverfolgungsbehörden weitergegeben werden dürfen.

Die Datenschutzaufsichtsbehörden haben die geplante Regelung gemeinsam mit Vertretern der Landesmedienanstalten erörtert und Empfehlungen für Präzisierungen ausgesprochen. Das ULD wies auf folgende Punkte hin:

- Der Regelungsansatz zeigt folgende Vorgehensweise auf: Die Prüfung beginnt mit einer allgemeinen Recherche im Internet hinsichtlich möglicher Verstöße mithilfe eines technischen Mittels. Dabei erfolgt eine Miterhebung öffentlich verfügbarer personenbezogener Daten zur abschließenden Bewertung eines möglichen Verstoßes. Wird nach dieser allgemeinen Recherche ein potenzieller Rechtsverstoß festgestellt, werden weitere Angaben zur Identität des Anbieters ermittelt. Ein alternativer Ansatz sollte darin bestehen, bereits die **Recherche auf konkrete Fälle zu beschränken**, wobei Prüfanlässe etwa auf der Grundlage von Beschwerden und Hinweisen entstehen können.
- Die Datenverarbeitung sollte vor diesem Hintergrund auf **konkrete und zureichende Anhaltspunkte für einen Verstoß** und damit auf Einzelfälle begrenzt werden. In Betracht kommt etwa die Prüfung, ob maßgebliche Verletzungen von Vorgaben des MStV (§ 109 MStV) oder des Jugendmedienstaatsvertrags (JMStV) im Fokus stehen.
- Recherchemaßnahmen müssen vor allem **erforderlich und verhältnismäßig** sein. Eine Orientierung können die Bestimmungen zur automatischen Kennzeichenerfassung geben (§ 163g StPO), welche bereits höhere Anforderungen für die Strafverfolgungsbehörden beinhalten.
- Bezüglich einer zweckändernden Verarbeitung recherchierter Informationen für den Fall, dass Anhaltspunkte für Straftaten bestehen, sollte sich die damit verbundene **Datenweitergabe an die Strafverfolgungsbehörden am Standard des § 24 BDSG orientieren**. Eine Datenweitergabe ist demnach zulässig, wenn dies im Einzelfall zur Verfolgung von Straftaten erforderlich ist, was auch für die Verarbeitung besonderer Datenkategorien gilt.

7.2 Aktuelles aus dem AK Medien

Immer wieder Thema ist im AK Medien die Problematik des Betriebs einer Facebook-Fanpage. Ein wichtiges Urteil dazu wurde am 25.11.2021 vom Schleswig-Holsteinischen Oberverwaltungsgericht gefällt, in welchem der Betrieb einer Facebook-Fanpage durch die Wirtschaftsakademie Schleswig-Holstein GmbH zum maßgeblichen Zeitpunkt im Dezember 2011 als Verstoß gegen datenschutzrechtliche Vorschriften angesehen wurde (40. TB, Tz. 7.3).

Mit Bescheid vom 17.02.2023 untersagte der damalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) dem **Presse- und Informationsamt der Bundesregierung (BPA)** den Betrieb der **Facebook-Fanpage**. Der BfDI stellte im Bescheid fest, dass eine **gemeinsame Verantwortlichkeit des BPA und Facebook** (heute Meta) auch dann vorliege, wenn die Statistikfunktion (sogenannte Insights) abgeschaltet werde. Die gemeinsame Verantwortlichkeit bestehe zumindest weiterhin durch das Setzen von Cookies. Eine wirksame Vereinbarung zur gemeinsamen Verantwortlichkeit zwischen dem BPA und Meta liege nicht vor. Ferner werde keine wirksame Einwilligung nach § 25 Abs. 1 TTDSG (heute: TDDDG) eingeholt.

Der Bescheid des BfDI ist unter dem folgenden Link abrufbar:

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2023/Bescheid-Facebook-Fanpage.pdf?__blob=publicationFile&v=1

Kurzlink: *https://uldsh.de/tb44-7-2a*

Das BPA klagte gegen den Bescheid. Mit dem Urteil vom 17.07.2025 entschied das Verwaltungsgericht Köln (VG Köln), dass keine gemeinsame Verantwortlichkeit vorliege, jedenfalls sofern die Statistikfunktion deaktiviert ist. Für das Setzen von Cookies und die Einholung von Einwilligungen sei Meta allein verantwortlich. Das VG Köln führte aus, dass kein ausreichender Ursachen- und Wirkungszusammenhang zwischen dem Betrieb der Facebook-Fanpage durch das BPA und dem mit der Speicherung und dem Auslesen der Cookies verbundenen Fernzugriff auf die Endgeräte der Nutzenden bestehe. Nach dem Urteil des VG Köln darf das BPA die Facebook-Fanpage zunächst weiterbetreiben.

Das **Urteil des VG Köln vom 17.07.2025 (Az. 13 K 1419/23)** ist unter dem folgenden Link abrufbar:

https://nrwe.justiz.nrw.de/ovgs/vg_koeln/j2025/13_K_1419_23_Urteil_20250717.html

Kurzlink: *https://uldsh.de/tb44-7-2b*

Mit dem Urteil ist die Angelegenheit jedoch noch nicht abgeschlossen. Die jetzige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat gegen das Urteil **Berufung eingelegt**, sodass das Verfahren dem Oberverwaltungsgericht Münster (OVG Münster) vorgelegt wird. Ein Anliegen der BfDI sei es, die bislang weder gesetzlich noch höchstrichterlich geklärten **Bedingungen für eine rechtskonforme Nutzung abschließend und unmissverständlich zu klären** und dabei digitale Kommunikation mit Bürgerinnen und Bürgern zu ermöglichen.

Wann es eine Entscheidung des OVG Münster geben wird, ist noch nicht absehbar. Für öffentliche Stellen sind soziale Medien in der heutigen Zeit ein wichtiger Kanal, um Informationen bereitzustellen. Bei der Nutzung von sozialen Medien, wie dem Betrieb einer Facebook-Fanpage, sind jedoch die datenschutzrechtlichen Vorgaben einzuhalten. Auch nach dem Urteil des VG Köln gibt es leider noch keine endgültige Rechtssicherheit, sodass **öffentliche Stellen sorgsam prüfen** sollten, ob ein datenschutzkonformer Betrieb einer Facebook-Fanpage möglich ist.

08

KERNPUNKTE

Plattform Privatheit

DatenTRAFO – Neue Datenschutz-Governance

Transparenz für das Internet der Dinge

TRUMAN – Vertrauenswürdige KI-Anwendungen

AnoMed – Anonymisierung für medizinische Anwendungen

8 Modellprojekte und Studien

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

Im Jahr 2025 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), Transparenzprobleme des Internets der Dinge (Tz. 8.3) sowie im Bereich der künstlichen Intelligenz (Tz. 8.4). Zudem setzte das ULD sein Engagement zu Anonymität für Medizinforschung mit Gesundheitsdaten fort (Tz. 8.5).

8.1 Plattform Privatheit: Forschung für ein selbstbestimmtes Leben in der digitalen Welt

Viele Jahre wirkt das ULD nun schon in der Plattform Privatheit (vormals: Forum Privatheit) mit. Dabei handelt es sich um ein vom BMFTR gefördertes, bundesweites Vernetzungsprojekt, dessen oberstes Ziel es ist, mit interdisziplinärer Forschung die informationelle Selbstbestimmung aller Bürgerinnen und Bürger zu stärken. Zudem unterstützt die Plattform Privatheit eine technologische Entwicklung, die dem Gemeinwohl dient. Die Plattform Privatheit vernetzt und begleitet eine Vielzahl interdisziplinärer Projekte, in denen Wissenschaftlerinnen und Wissenschaftler aus unterschiedlichen Disziplinen rechtliche, technische und organisatorische Lösungen entwickeln, die es den Menschen ermöglichen, im digitalen Alltag ihre Grundrechte und europäischen Werte zu wahren.

So hilft die Plattform Privatheit mittlerweile mehr als 30 Projekten bei der Vernetzung, darunter auch den vom BMFTR geförderten Projekten mit ULD-Beteiligung. Veröffentlichungen zu datenschutzrelevanten Schnittstellenthemen sind ebenso wie die Tagungsbände der Jahreskonferenz in Berlin, an der Interessierte online oder vor Ort teilnehmen können, kostenlos.

Weitere Informationen über die Plattform Privatheit lassen sich der Website entnehmen:

https://www.plattform-privatheit.de

Kurzlink: *https://uldsh.de/tb44-8-1a*

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

Das Projekt „Neue Datenschutz-Governance – Technik, Regulierung und Transformation (DatenTRAFO)" entwickelt Vorschläge, wie Datenschutz in der Praxis umgesetzt werden kann, wird vom BMFTR gefördert und läuft vom 1. September 2023 bis 31. August 2026. Bei DatenTRAFO war das Jahr 2024 von den neuen EU-Regelungen geprägt, insbesondere der Verordnung 2024/1689 zu künstlicher Intelligenz (KI-Verordnung), die die

Regelungen der DSGVO im Bereich der künstlichen Intelligenz ergänzt und erweitert.

KI-Verordnung

Die EU hat im Jahr 2024 die KI-Verordnung beschlossen, die nun in den kommenden Jahren von Behörden und Unternehmen angewendet werden muss. In bestimmten Bereichen verbietet sie den Einsatz von KI-Systemen, z. B. zur Erkennung von Gesichtern auf Videos von Überwachungskameras in Echtzeit. Allerdings gibt es dabei zahlreiche Ausnahmen, wie etwa für den besonders grundrechtssensiblen Bereich der polizeilichen Überwachung.

DatenTRAFO hat insbesondere die sogenannte **Grundrechte-Folgenabschätzung** und das **Risikomanagementsystem** der KI-Verordnung untersucht. Anders als die DSGVO, die sich nur an Verantwortliche richtet, also an die Stelle, die über eine Datenverarbeitung entscheidet, verpflichtet die KI-Verordnung auch diejenigen, die KI-Systeme entwickeln und in der KI-Verordnung als **Anbieter** bezeichnet werden. Das gilt auch für die Abwägung von Grundrechtsrisiken für Nutzende. Von einem solchen Modell könnten auch die DSGVO und die darin vorgesehene **Datenschutz-Folgenabschätzung** profitieren. Eine Risikoabwägung würde für Verantwortliche leichter, wenn sie auf eine Abschätzung von Risiken seitens des Herstellers zurückgreifen könnten. Zudem bestehen zwischen der **Grundrechte-Folgenabschätzung** und der **Datenschutz-Folgenabschätzung** zahlreiche Überschneidungen, sodass durch eine Angleichung der Regelungen eine Entlastung für Unternehmen bei gleichzeitiger Wahrung der Rechte der betroffenen Personen erreicht werden könnte.

In der aktuellen Diskussion zur Reform von DSGVO und KI-Verordnung werden diese Punkte noch nicht ausreichend berücksichtigt. Die Bundesregierung und die Länder haben jedoch vorgeschlagen, in der DSGVO zukünftig **Pflichten auch für Hersteller von bestimmten Diensten und Produkten einzuführen**.

Was ist zu tun?

Die DSGVO sollte um Pflichten für Hersteller von Diensten und Produkten erweitert werden. Wird dies umgesetzt, kann auch die Grundrechte-Folgenabschätzung durch die bereits bewährte Datenschutz-Folgenabschätzung abgelöst werden, da sie ohnehin für viele KI-Systeme vorzunehmen ist. Dies entlastet Unternehmen und sichert die Grundrechte betroffener Personen.

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

Vernetzte Geräte werden zunehmend allgegenwärtig und bringen Vorteile und Nachteile des **Internets der Dinge** (englisch: „Internet of Things", IoT) direkt zu den Menschen (43. TB, Tz. 8.3). Seit 2023 befasst sich das vom Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) geförderte Projekt **„Toolgestützte, moderierte und bürgerzentrierte Community-Plattform zur Privacy-Einstufung von IoT-Produkten – Unboxing.IoT.Privacy"** mit Aspekten der Transparenz und des Datenschutzes bei solchen Geräten.

Eines der Projektziele ist es, **Transparenz** über die Datenverarbeitung solcher Geräte zu unterstützen. Vielfach fehlen schlicht relevante Informationsquellen für interessierte Verbraucherinnen und Verbraucher, potenziell Betroffene oder datenschutzrechtlich Verantwortliche. Geeignete Informationen sollten am besten schon für die

Kaufentscheidung oder den Vertragsschluss mit dem Dienstleister vorliegen, damit eine angemessene Bewertung und Risikoeinschätzung erfolgen können. In neueren europäischen Rechtsakten werden diese Transparenz- und Datenschutz-Problemstellungen teilweise angesprochen, wenn auch nicht explizit mit Datenschutz als Zielsetzung. So nimmt die Cyberresilienz-Verordnung (englisch: „Cyber Resilience Act", CRA) Hersteller, Importeure und Verkäufer u. a. von IoT-Geräten in die **Pflicht**, nicht nur bestimmte Sicherheitseigenschaften zu gewährleisten, sondern auch Informationen bereitzustellen, die direkt oder mittelbar datenschutzrechtlichen Transparenzzielen dienen (dazu 43. TB, Tz. 8.3).

Mit der **Datenverordnung** (englisch: „Data Act", DA) hat der europäische Gesetzgeber weitere Regelungen geschaffen, die gleichsam Hersteller und weitere Akteure zur Informationsbereitstellung verpflichten. Ein Hauptziel des DA ist es, die bei der Gerätenutzung anfallenden **Daten bereitzustellen und deren Nutzung zu ermöglichen**. Dafür sind Geräte u. a. künftig so zu gestalten, dass Nutzende die anfallenden Daten einfach auslesen können. Weiter haben Nutzende ein Recht auf Zugänglichmachung, wenn die Daten bei einem Anbieter eines verbundenen Dienstes (Dateninhaber) vorliegen. Hersteller bzw. Diensteanbieter haben künftig u. a. über Art, Format, Umfang der erhobenen Produktdaten und erzeugten Dienstdaten, Identität des Dateninhabers sowie Modalitäten über die Zugriffsmöglichkeiten zu informieren.

Datenverordnung

Die Datenverordnung (englisch: „Data Act") ist Teil der Datenstrategie der EU-Kommission und enthält Regeln für Zugang, Nutzung und Weitergabe von Daten aus vernetzten Geräten. Nutzerinnen und Nutzer können entscheiden, ihre Daten selbst zu erhalten oder diese an Dritte weiterzugeben. Haben nutzergenerierte Daten einen Personenbezug, so richtet sich deren Verarbeitung nach der DSGVO.

Die Datenverordnung bezieht sich dabei auf „Daten", unabhängig davon, ob ein Personenbezug besteht. Für personenbezogene Daten geht im Falle eines Widerspruchs zwischen DSGVO und Datenverordnung erstere vor. In einfach gelagerten Fällen besteht weitgehender Gleichlauf zwischen Rechten und Pflichten aus DSGVO und Datenverordnung. Dies ist etwa der Fall, wenn Nutzende eines IoT-Geräts zugleich die jeweils einzigen von der Verarbeitung betroffenen Personen sind, wie etwa bei vernetzten Sportuhren.

Sobald Drittbetroffene involviert sind, wie z. B. weitere Hausbewohner, die von Sensoren erfasst werden, steigt die Komplexität. Eine korrekte Fallbeurteilung setzt dann zwingend eine saubere Zuordnung der Rollen nach DA und DSGVO im konkret vorgesehenen Einsatzszenario voraus (siehe Abb. 3 auf der nächsten Seite).

Erst aus der genauen Rollenzuordnung ergeben sich die Rechte und Pflichten zwischen den Akteuren. Herausforderungen im Spannungsfeld zwischen DSGVO und DA können sich etwa für Dateninhaber ergeben.

Insbesondere betrifft dies die Bereitstellungspflicht für personenbezogene Daten, die Diensteanbieter während der Erbringung eines verbundenen Dienstes abgerufen oder generiert haben. Datenschutzrechtlich bedarf es einer gültigen Rechtsgrundlage. Gleichzeitig besteht gemäß dem DA die Bereitstellungspflicht zumindest für nicht personenbezogene Daten. Dateninhaber gelangen so in die undankbare Lage, über den Personenbezug von Daten befinden zu müssen, obwohl sie die Umstände der Erhebung kaum kannten oder beeinflussen konnten. Eine denkbare rechtliche Lösung wäre, dass verbundene Dienste strikt im Rahmen einer Auftragsverarbeitung für die Nutzenden der Geräte tätig werden, sodass Letztere allein datenschutzrechtlich Verantwortliche wären. Diese Lösung widerspräche aber dem politischen Ziel, die Daten aus vernetzten Geräten weiteren Zwecken zuzuführen. Hier werden denkbare Lösungsansätze noch zu bewerten sein.

Interessant sind hier insbesondere vertragliche Regelungen, da Dateninhaber ohnehin für die Datennutzung einen Vertrag mit den Nutzenden benötigen. Dann könnte im selben Streich eine gemeinsame Verantwortlichkeit geregelt werden.

Einen Link mit weiteren Informationen finden Sie unter:

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

Kurzlink: https://uldsh.de/tb44-8-3a

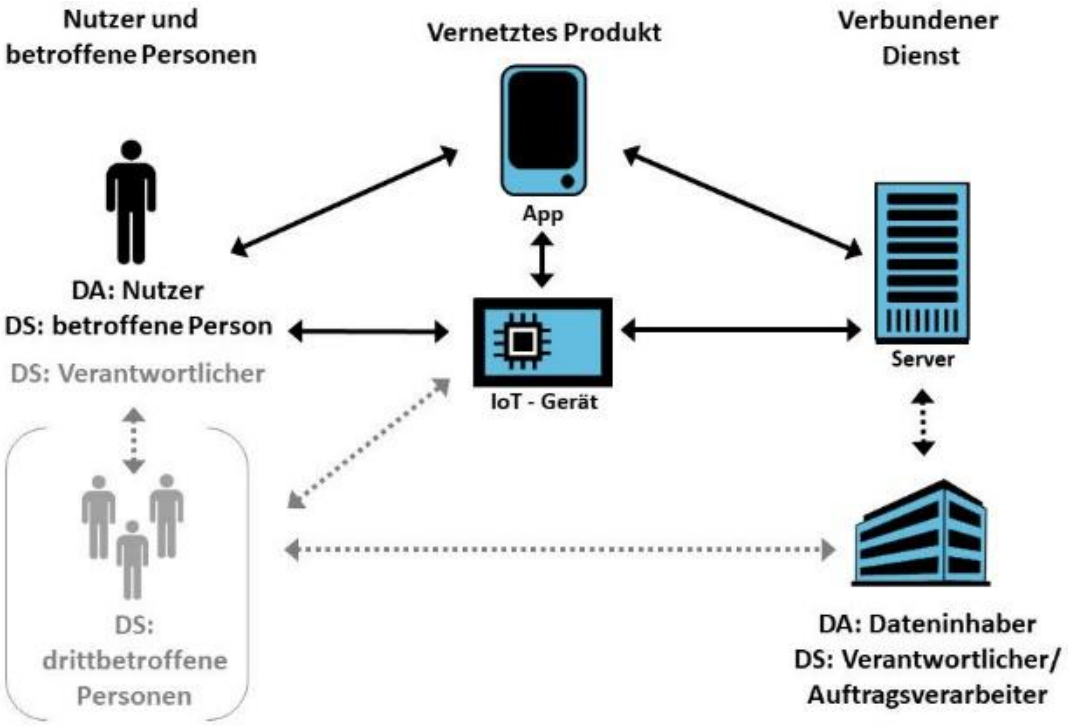


Abb. 3: Akteure und Rollen beim Einsatz von IoT-Geräten

8.4 Projekt TRUMAN – Der Mensch im Mittelpunkt: vertrauenswürdige KI-Anwendungen

In den letzten Jahren sind die Entwicklungen im Bereich der künstlichen Intelligenz (KI) in vielen Branchen weit vorangeschritten und haben zu wichtigen Erkenntnissen und Durchbrüchen in Bereichen wie Gesundheitswesen, Verkehr, Finanzen und Fertigung geführt. KI wurde zu einem wichtigen Wachstumsmotor für den gesamten Bereich der Informationstechnologie. Zugleich wirft der Einsatz von KI viele Fragen auf, die einer Lösung bedürfen, insbesondere wenn durch KI Rechte von Individuen berührt werden. Das von der Europäischen Kommission finanzierte Projekt **„TRUstworthy huMAN-centric artificial intelligence – TRUMAN"** zielt darauf ab, vertrauenswürdige und datenschutzkonforme KI-Systeme zu entwickeln, die den **Anforderungen der DSGVO und der KI-Verordnung** entsprechen. Im Mittelpunkt stehen technische und organisatorische Maßnahmen, die Transparenz und menschliche Kontrolle sicherstellen. Hinsichtlich der technischen Umsetzung soll die Vertrauenswürdigkeit von KI erhöht werden, indem Robustheit, Erklärbarkeit sowie menschliche Kontrollierbarkeit in allen Phasen des KI-Lebenszyklus (Datengewinnung, Modelltraining, Ausführung) integriert werden.

Das Projekt sucht für die sich aus KI stellenden datenschutzrechtlichen Herausforderungen Lösungen, die rechtliche, ethische und technische An-

forderungen in Einklang bringen. Für den Datenschutz sollen die Gewährleistungsziele u. a. durch dezentrale Lerntechniken und mehr Verständlichkeit und Transparenz gestärkt werden. Als mögliche Maßnahmen für Datenschutz durch Technikgestaltung werden u. a. föderiertes Lernen, synthetische Datenerzeugung und Differential-Privacy-Mechanismen betrachtet.

Ein Alleinstellungsmerkmal von TRUMAN ist die Integration des Projektziels „Explainability and Usability", das sich auf die verständliche Vermittlung der internen Vorgänge der KI sowie von Datenschutz- und Sicherheitsmaßnahmen konzentriert. Ziel ist es, Verantwortlichen sowie Nutzenden leicht nachvollziehbare Informationen über die Art der Datennutzung, die Funktionsweise der Sicherheits- und Datenschutzmechanismen und die möglichen Datenschutzrisiken anzubieten. Das Systemverhalten soll aus Nutzendenperspektive erklärbar sein bzw. verständlich werden. Diese „usable explanations" unterstützen Verantwortliche bei der Einhaltung des Transparenzgebots und bezwecken gleichzeitig eine gestärkte Vertrauenswürdigkeit von KI-Systemen, die diese Methoden unterstützen.

Die Beiträge des ULD zu datenschutzrechtlichen Aspekten erfolgen vor allem zu zwei zentralen Projektzielen. Das Projektziel **„Human-in-the-Loop – Verteiltes dynamisches Lernen"** fokussiert sich auf KI und maschinelles Lernen. Es dient als Ausgangspunkt für das weitere Projekt und definiert Eigenschaften und Spezifikationen für KI-Techniken und die zu erforschenden Lösungen. Die drei Schlüsselbegriffe für dieses TRUMAN-Projektziel sind:

- „Human-in-the-Loop (HITL)", da der Mensch eine wichtige Rolle bei der Verbesserung von KI-Systemen spielt und Aufsicht und Kontrolle durch Menschen und die faktische und technische Möglichkeit dazu in allen Phasen des KI-Lebenszyklus erforderlich sind.
- „Verteilt", da Daten oft dezentral am Standort des Diensteanbieters, Verbrauchers oder eines vernetzten Geräts entstehen und ein zentrales Sammeln und Zusammenführen datenschutzrechtlich unerwünscht ist.
- „Dynamisch", da Daten im Laufe der Zeit kontinuierlich anfallen und sich weiterentwickeln.

Im Rahmen des Projektziels **„Vertrauenswürdigkeit durch Erklärbarkeit und Benutzerfreundlichkeit"** ergründet das Projektkonsortium, wie menschenzentrierte KI-Systeme ergänzt werden können, um die Erklärbarkeit des Systemverhaltens aus Sicht der Nutzenden zu verbessern. Dazu sollen Schutzziele und Metriken für vertrauenswürdige KI-Systeme ermittelt und nachvollziehbar definiert werden. Diese erfassen und abstrahieren die Anforderungen, die sich aus einschlägigen Gesetzen, der Rechtsprechung oder Leitlinien der für KI zuständigen Aufsichtsbehörden und Ethikgremien ergeben. Absehbar werden sich inhärente Zielkonflikte aufzeigen lassen – etwa zwischen **Datenrichtigkeit und Vollständigkeit in Abwägung mit Datenminimierung**. Derartige Konflikte werden aufgezeigt und mögliche Methoden zum Ausgleich bzw. zur Begrenzung der Risiken gesucht und bewertet. Schließlich werden auch Aspekte der Benutzerfreundlichkeit von KI aufgegriffen.

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

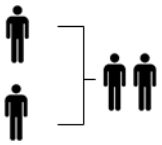
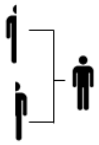
Kurzlink: *https://uldsh.de/tb44-8-4a*

8.5 Projekt AnoMed – Kompetenzcluster Anonymisierung für medizinische Anwendungen

Der Kompetenzcluster **„Anonymisierung für medizinische Anwendungen – AnoMed“** geht nun in die zweite Runde. Der Cluster wurde durch das Bundesministerium für Technologie und Raumfahrt sowie der Europäischen Union (NextGenerationEU) (43. TB, Tz. 8.4) gefördert und für eine Fortsetzung der Förderung um drei Jahre ausgewählt. Das Folgeprojekt setzt zum 1. Januar 2026 unter Koordination der Universität Lübeck die Arbeit mit neuen Forschungsfragen und -schwerpunkten rund um Anonymisierung und Pseudonymisierung sowie von Gesundheitsdaten fort. Im Konsortium trägt das ULD mit vorwiegend datenschutzrechtlicher Expertise bei. Das Projekt befasst sich mit vielversprechenden **Technologien zum Schutz von Gesundheitsdaten**, die insbesondere auf Differential Privacy oder maschinellem Lernen basieren.

Mit dem **Europäischen Raum für Gesundheitsdaten** (European Health Data Space, EHDS) wurde eine Blaupause für weitere Datenräume geschaffen und dessen Umsetzung kommt eine Vorreiterrolle für andere Datenräume zu. Die Europäische Datenstrategie sieht weitreichende Sekundärnutzungen von Daten für Gemeinwohl, Wirtschaft und Verwaltung vor. Die zur Forschung benötigten Daten sind meist personenbezogen und teils hochsensibel. Um sie für Datenräume nutzbar zu machen, ist es erforderlich, sie zu anonymisieren oder anderweitig ausreichende Schutzmaßnahmen zu treffen. Wo eine Anonymisierung nicht möglich ist, wird im Gesundheitsdatenraum eine pseudonyme Bereitstellung von Daten vorgesehen.

Datenräume bringen eine Vielzahl von Datenquellen für eine integrierte Analyse zusammen. Die Integration kann **horizontal** (gleiche Datenkategorien von vielen Personen) oder **vertikal** (Daten zu einer Person werden aus mehreren Quellen zusammengeführt) erfolgen:

horizontale  Integration	Die gleichen Daten von vielen Personen werden zusammengeführt.	z. B. europäisches Lagebild, gespeist aus nationalen Daten
vertikale Integration 	Verschiedene Daten (Aspekte) der gleichen Person werden zusammengeführt.	z. B. Zusammenhang von Gesundheit, Ernährung, Fitness

Verschiedene Integrationsarten erfordern dabei verschiedene Datenschutzstrategien und Maßnahmen.

Im Projekt wurden hierzu **Pseudonymisierungsstrategien** für horizontale und vertikale Integration vorgeschlagen. Sie zielen darauf ab, Verknüpfungsmöglichkeiten zu minimieren und nur innerhalb einer Analyse zu ermöglichen. Je nach Integrationstyp müssen zu verschiedenen Zeitpunkten verschiedene Akteure Pseudonyme kreieren und verwalten.

In Datenräumen sollen pseudonyme Daten nur in sogenannten sicheren Verarbeitungsumgebungen analysiert werden. Das AnoMed-Team hat beschrieben, welche technischen und organisatorischen Maßnahmen zur Sicherung solcher physischen oder virtuellen Verarbeitungsumgebungen eingesetzt werden können, um eine Identifizierung zu verhindern. Ein Beispiel ist die Methode der föderierten Analyse, die es erlaubt, alle Daten an ihren Quellen zu belassen und trotzdem horizontal integrierte Analysen (z. B. Statistiken) zu erstellen.

Ob Daten erfolgreich anonymisiert worden sind oder ob eine Re-Identifizierung von Personen doch noch möglich ist, ist nicht immer bestimmbar. Zum Beispiel können neue Zusatzdaten, neue Identifizierungsmethoden oder Vervielfachung der verfügbaren Rechenleistung die Identifikation in vorher anonym geglaubten Daten ermöglichen. Um diese Situation kontrollierbar zu machen, hat das Projektteam in Analogie zur Informationssicherheit von Software das Zusammenspiel von verschiedenen Parteien in einem eigenen Ökosystem vorgeschlagen. Wesentlich dafür ist eine zentrale Anlaufstelle als Einrichtung des Datenraums mit der Aufgabe, Entwicklungen und Risiken zu beobachten. Die Einrichtung wäre mit einem CERT/CSIRT vergleichbar, das solche Aufgaben im Bereich der Informationssicherheit wahrnimmt. Eine wichtige Rolle nehmen auch Re-Identifizierungsforschende ein. Sie testen Anonymisierungsmethoden und Möglichkeiten einer Re-Identifizierung am Rande des Machbaren.

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

Kurzlink: https://uldsh.de/tb44-8-5a

09

KERNPUNKTE

Themen der AK Zertifizierung in Deutschland

Themen auf europäischer Ebene in der Expert Subgroup

Überarbeitung des Prüfkriterienpapiers

9 Zertifizierung und Akkreditierung

Bis 2018 hat das ULD selbst Datenschutz-Auditierungen und Zertifizierungen vorgenommen. Diese Expertise haben wir daraufhin auch in unsere Arbeit als Leiter des Arbeitskreises Zertifizierung der deutschen Datenschutzaufsichtsbehörden eingebracht und begleiten seitdem die Verfahren zu Akkreditierungen und Zertifizierungen im Datenschutzbereich in Deutschland und Europa.

9.1 Stand der Akkreditierung und Zertifizierung in Deutschland und der EU

Der in den vorherigen Berichtszeiträumen zu beobachtende Trend einer **Häufung von Anträgen** auf Genehmigung von Zertifizierungskriterien und Akkreditierungen von Zertifizierungsstellen in einzelnen Mitgliedstaaten, wie beispielsweise Deutschland, Luxemburg oder den Niederlanden, bzw. in einzelnen Bundesländern (Nordrhein-Westfalen, Bremen, Berlin) hat sich im abgelaufenen Berichtszeitraum weiter bestätigt.

Die **Qualität** der durch die zukünftigen Zertifizierungsstellen oder Programmeigner erstellten und eingereichten **Zertifizierungsprogramme** hat sich im abgelaufenen Berichtszeitraum zum Teil nochmals verbessert. Dennoch bleiben die Herausforderungen für alle Beteiligten aufgrund der anspruchsvollen Thematik und der Mehrstufigkeit des zu durchlaufenden Verfahrens sehr komplex und zeitintensiv. Hierbei prüfen die **Deutsche Akkreditierungsstelle (DAkkS)** und die jeweils zuständige Datenschutzaufsichtsbehörde die eingereichten Kriterienkataloge als Teil der Zertifizierungsprogramme zunächst auf ihre Anwendbarkeit und Eignung. Daraufhin genehmigt die jeweils zuständige Aufsichtsbehörde die **Kriterienkataloge**, vorbehaltlich einer positiven Stellungnahme durch den **Europäischen Datenschutzausschuss (EDSA)**. Aufgrund der engen Verzahnung unterschiedlicher Stellen – sowohl im deutschen als auch im europäischen Kontext – und einer Vielzahl ganz verschiedener Detailfragen, die sich in jedem Verfahren ergeben, ist eine enge Abstimmung aller Beteiligten notwendig.

Im abgelaufenen Berichtszeitraum konnten abermals deutschlandweit und auch in anderen EU-Staaten weitere Anträge auf Genehmigung nationaler und europäischer Zertifizierungskriterien erfolgreich abgeschlossen werden.

Was ist zu tun?

Auch weiterhin ist die Sicherstellung einer einheitlichen Bewertung von Kriterienkatalogen und Zertifizierungsprogrammen ein zentraler Aspekt im entsprechenden Verfahren. Um dies sicherzustellen und um das Instrument der Zertifizierung langfristig auf einem fachlich hohen Niveau zu verankern, ist es notwendig, die bestehenden Papiere zur Akkreditierung und Zertifizierung auch weiterhin zu überarbeiten und an neueste Entwicklungen anzupassen.

9.2 Themen des AK Zertifizierung in Deutschland

Die Koordinierung von Angelegenheiten der Zertifizierung und Akkreditierung erfolgt unter den deutschen Datenschutzaufsichtsbehörden im **Arbeitskreis Zertifizierung der Datenschutzkonferenz** (AK Zertifizierung), den das ULD auch im abgelaufenen Berichtszeitraum geleitet hat. Wie bereits in der Vergangenheit haben wir hierfür zunächst monatliche (im weiteren Jahresverlauf zweimonatliche) virtuelle Treffen abgehalten, auf denen wir uns über Themen und Entwicklungen auf deutscher, aber auch auf europäischer Ebene im Zusammenhang mit der Akkreditierung und Zertifizierung ausgetauscht haben.

Teil dieses Austausches ist, wie in der Vergangenheit auch, die **Deutsche Akkreditierungsstelle (DAkkS)**, die in enger Zusammenarbeit mit den nationalen Datenschutzaufsichtsbehörden die Akkreditierung von Zertifizierungsstellen vornimmt. Die Arbeit des AK Zertifizierung wurde auch im abgelaufenen Berichtszeitraum durch den **Unterarbeitskreis Prüfkriterien**, der von Nordrhein-Westfalen geleitet wird, unterstützt (zu dessen Arbeit siehe Tz. 9.4).

Der AK Zertifizierung ist ein wichtiges Instrument, um alle Aufsichtsbehörden in Deutschland auf dem **aktuellen Stand** im Bereich Akkreditierung und Zertifizierung zu halten. Neben möglichen Anträgen durch örtliche potenzielle Zertifizierungsstellen können auch europaweite Zertifizierungen Aufgabenbereiche nationaler Aufsichtsbehörden betreffen. Daher nahm der Austausch über aktuelle Entwicklungen einen großen Raum in den Sitzungen ein. Für eine mögliche Unterstützung anderer Dienststellen wurde im Rahmen der bestehenden Kooperationsvereinbarung eine Liste potenziell möglicher Gutachter erstellt und gepflegt.

Auch war Deutschland 2025 Ausrichter eines **europaweiten CEH-Workshops** in Berlin, in dessen Planung und Koordinierung der AK Zertifizierung maßgeblich eingebunden war (Tz. 9.3).

Und schließlich wurde erneut der jährliche Austausch der Gutachter der Datenschutzaufsichtsbehörden mit der DAkkS koordiniert.

9.3 Themen auf europäischer Ebene in der Expert Subgroup

Auf europäischer Ebene konnten im abgelaufenen Berichtszeitraum weitere Genehmigungsverfahren für Zertifizierungsprogramme aus Deutschland und Europa erfolgreich abgeschlossen werden. Bei der Bewertung und Prüfung dieser Programme konnten wir unsere umfangreiche Erfahrung abermals im Rahmen der für Fragen der Akkreditierung und Zertifizierung zuständigen **Compliance, e-Government und Health Expert Subgroup (CEH Expert Subgroup)** einbringen.

Die Arbeit der CEH Expert Subgroup erstreckte sich dabei – neben der eigentlichen **Prüfung und Genehmigung konkreter Kriterienkataloge** – weiterhin vor allem auf grundlegende Fragestellungen zur Akkreditierung und Zertifizierung. So waren erneut u. a. die **innereuropäische Zusammenarbeit** unter den Aufsichtsbehörden sowie Fragestellungen zum **Drittstaatentransfer personenbezogener Daten** gemäß Artikel 46 DSGVO zentrale Themen der CEH Expert Subgroup im Kontext datenschutzrechtlicher Zertifizierungen. Auch dieses Mal gelang es unter der Einbindung weiterer Expert Subgroups wie der **International Transfer Subgroup (ITS)** sowie der **Key Provision Subgroup (KEYP)**, Lösungen für diese zum Teil sehr komplexen Problemstellungen zu erarbeiten.

Im Jahr 2025 fand in Berlin ein dreitägiger **Workshop der CEH Expert Subgroup** statt. Ausrichter waren die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Landesbeauftragte für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen und wir. Eingeladen waren neben Vertretern der Aufsichtsbehörden aus ganz Europa auch die International Transfer Subgroup (ITS) und Zertifizierungsstellen. Die Vertreter der Zertifizierungs-

stellen konnten am ersten Tag des Workshops durch ihre Vorträge einen praxisnahen Einblick in die aktuelle Situation am Markt geben und auf diese Weise die Grundlage für eine intensive Befassung mit den unterschiedlichen Aspekten und Herausforderungen im Bereich der Akkreditierung und Zertifizierung für den zweiten und dritten Tag legen.

Was ist zu tun?

Die Zusammenarbeit unter den Datenschutzaufsichtsbehörden in Europa im Sinne einer Zertifizierung, die in der Praxis ohne große Hürden einsetzbar ist und zu einem Mehr an nachgewiesenem Datenschutz führt, ist fortzusetzen.

9.4 Überarbeitung des Prüfkriterienpapiers

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**)“ wurde durch den Unterarbeitskreis Prüfkriterien des AK Zertifizierung unter Mitwirkung des ULD auch im abgelaufenen Berichtszeitraum überarbeitet und weiterentwickelt. Hierbei wurden unter Beibehaltung der grundlegenden Struktur des Dokuments einige Abschnitte überarbeitet und erweitert.

Das Prüfkriterienpapier dient als **Grundlage zur Bewertung von Kriterienkatalogen**, die bei den Aufsichtsbehörden zur Genehmigung eingereicht werden. Es kann auch als **Orientierungshilfe für zukünftige Zertifizierungsstellen** dienen, um sie bei der Erstellung von Zertifizierungsprogrammen und insbesondere von Zertifizierungskriterien zu unterstützen.

Die umfangreichen Überarbeitungen der Ausführungen zu Artikel 25 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) sowie zu Artikel 28 DSGVO (Auftragsverarbeiter) sind abgeschlossen. Hierbei wurde insbesondere auf immer wieder aufkommende Diskussionen zu technisch-organisatorischen Maßnahmen in Zertifizierungsprogrammen und die zunehmende Anzahl von Zertifizierungsprogrammen für Auftragsverarbeitung Rücksicht genommen. Zu Artikel 25 DSGVO erfolgte eine konkretisierte Einarbeitung der **EDSA-Leitlinie 4/2019** zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Bei Artikel 28 DSGVO erfolgte eine Strukturanpassung mit besserer Abgrenzung der beiden möglichen Konstellationen „Zertifizierung eines Auftragsverarbeiters“ und „Zertifizierung eines Verantwortlichen, der Auftragsverarbeiter einbindet“. Beachtet wurde auch die **EDSA-Leitlinie 07/2020** zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, insbesondere bezüglich der fortlaufenden Kontrolle von Auftragsverarbeitern durch den Verantwortlichen. Die EDSA-Stellungnahme 22/2024 zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben, wurde eingepflegt. Aufgezeigt werden nunmehr Umsetzungsmöglichkeiten, z. B. Monitoring/Alerting, Festlegen von Indikatoren und Schwellenwerten, Vereinbarung von Vertragsstrafen usw. im Zusammenspiel mit Konzeptdokumenten.

Weiterhin werden in übersichtlicher Form als Tabelle nicht nur die gesetzlichen Tatbestandsmerkmale aufgeführt, sondern auch die Prüfthemen mit ihrer Umsetzung dargestellt.

Das entsprechende Papier konnte auch im abgelaufenen Berichtszeitraum in einigen Akkreditierungsverfahren Anwendung finden. Durch die

vorgenommenen Ergänzungen erhöht sich die **Praxistauglichkeit** des Papiers nochmals, sodass es den Verwender auch bei zukünftigen Akkreditierungsverfahren sinnvoll unterstützen kann. Weitere konkrete Erfahrungen bei der Anwendung des Papiers, Entwicklungen im Bereich der Akkreditierung sowie Vorgaben auf europäischer Ebene werden auch in zukünftige Überarbeitungen einfließen, um das Papier noch praxisnäher zu gestalten.

Das Papier wurde in seiner neuesten Version von der DSK Ende 2025 angenommen. Das Papier ist unter dem folgenden Link abrufbar:

https://www.datenschutzkonferenz-online.de/media/ah/DSK_Zertifizierungskriterien_Version_3_0.pdf

Kurzlink: *https://uldsh.de/tb44-9-4a*

Was ist zu tun?

Für eine weiter gehende praxisnahe Überarbeitung und Anpassung des Papiers wird der Unterarbeitskreis auch weiterhin die Entwicklungen auf deutscher und europäischer Ebene intensiv beobachten.

10

KERNPUNKTE

Fingerabdrücke im Web

Sicherheit von Webbrowsern

KI-Systeme und die Privatsphäre

10 Aus dem IT-Labor

10.1 Fingerabdrücke im Web – wie funktioniert Browser-Fingerprinting?

Website-Betreiber möchten Menschen, die ihre Website besuchen, nur allzu gern wiedererkennen. Die einen möchten ihnen auf diese Weise maßgeschneiderte Informationen anzeigen, die anderen maßgeschneiderte Werbung.

In jedem Fall werden Techniken dazu benötigt, einen Website-Besuch mit einem vorangegangenen zu verknüpfen. Cookies waren hier lange das Mittel der Wahl, um die Browser zu markieren. Doch Cookies lassen sich von Nutzerinnen und Nutzern steuern, löschen und blockieren. Einigen Website-Betreibern und insbesondere der Werbeindustrie ist das ein Dorn im Auge. Darum werden immer ausgefeiltere Techniken entwickelt, um Geräte auch ohne Cookies wiederzuerkennen.

Mit dem Begriff **„Fingerprinting"** bezeichnet man Techniken, die **Merkmale eines IT-Geräts erfassen** und daraus einen eindeutigen Fingerabdruck erstellen. Dazu wird auf technische System- und Konfigurationsdaten zurückgegriffen. Dabei sind für die Anbieter vor allem Eigenschaften wichtig, die eine starke Unterscheidbarkeit ermöglichen. Eine Bildschirmauflösung ist nicht besonders einzigartig. Die genaue Zusammensetzung der installierten Schriftarten eines PCs ist da schon interessanter (diese sind überraschend individuell). Auch winzige Geschwindigkeitsunterschiede bei Rechenoperationen liefern Anhaltspunkte zur Unterscheidung von Geräten. Das kann dazu führen, dass ein Browser auch dann wiedererkannt wird, wenn alle Cookies und ähnliche lokale Speicher gelöscht wurden.

Aus Sicht einer Website kann das hilfreich sein, um Kundeninteresse zu ermitteln: Mithilfe eines Fingerprints werden nicht nur Besuche mit erfolgreichem Log-in, sondern jeder Aufruf mit einem bestimmten Browser erfasst. Ein einzelner Website-Betreiber sieht auf diese Weise allerdings nur Besuche seiner eigenen Website.

Für Werbenetzwerke bieten sich hingegen mittels Fingerprinting Möglichkeiten, weiträumige Persönlichkeitsprofile zu erstellen: Werbenetzwerke sind über unzählige Websites verstreut, und ein wiedererkennbarer Fingerprint liefert **langfristige Informationen über das (website-übergreifende) Surfverhalten einzelner Personen**. Die Anbieter von Fingerprinting-Systemen werben damit, einen Browser selbst dann wiederzuerkennen, wenn man den Inkognito-Modus oder ein VPN verwendet.

Die **Browserhersteller** wiederum versuchen zum Teil, solche **Techniken zur Wiedererkennung einzuschränken oder zu behindern**. Das geschieht zum einen durch Blockieren von Webadressen, von denen bekannte Trackingskripte stammen, und zum anderen durch Einschränkungen in den Schnittstellen, über die auf identifizierende Maschinendaten zugegriffen werden kann. Auch Browsererweiterungen (Add-ons) widmen sich der Verteidigung gegen verschiedene Fingerprinting-Technologien. Nutzende können hier also auf mehreren Wegen der Profilbildung entgegenwirken.

Die Wirksamkeit der getroffenen Maßnahmen lässt sich nicht leicht prüfen. Am einfachsten ist es noch, wenn ein Fingerprinting-Anbieter auf seiner Website zu Werbezwecken selbstbewusst den Fingerprint selbst anzeigt, also den Hashwert seiner einzelnen Erkennungstechnologien. Ändert sich dieser beim nächsten Besuch, wurde man nicht wiedererkannt. Bleibt er gleich, sollte man tätig werden – zumindest dieser Anbieter kann das eigene IT-Gerät langfristig identifizieren.

Vorsicht ist geboten bei Testwebsites, die die „Einzigartigkeit" oder Unverwechselbarkeit (uniqueness) überprüfen. Dass ein Rechner mehr oder weniger einzigartig erscheint, klingt zunächst nach eindeutiger Wiedererkennung. Relevant ist hingegen, ob derselbe Fingerprint auch beim

nächsten Besuch auftaucht. Viele Gegenmaßnahmen vermischen die Ergebnisse nämlich mit Zufallswerten: Sie sind zwar weltweit einzigartig, erscheinen aber auch nur einmalig. Beim nächsten Besuch werden andere Zufallswerte verwendet – die Wiedererkennbarkeit geht gegen null.

Was ist zu tun?

Bei der Wahl des Browsers sollte die Widerstandsfähigkeit gegen Fingerprinting-Versuche berücksichtigt werden – manche Browser bieten hier einen deutlich besseren Schutz. Je nach Gewohnheiten können zusätzliche Browsererweiterungen sinnvoll sein. Vor allem sollten Browserhersteller die Systemhärtung gegen Fingerprinting-Technologien konsequent fortsetzen, um Nutzende langfristig zu schützen.

10.2 Sicherheit von Webbrowsern durch Filtermechanismen – neue Entwicklungen

In der Vergangenheit (41. TB, Tz. 10.1) haben wir bereits über den Plan der Firma **Google** berichtet, mit Manifest v3 die Erweiterungs-API seines Chrome-Browsers grundlegend zu überarbeiten – insbesondere den Teil, der besonders für Werbeblocker notwendig ist. Mit Chrome-Version 139 wurde Manifest v2 Mitte 2025 vollständig abgeschaltet. Google begründet diesen Schritt mit verbesserter Sicherheit und Performance. Doch die Realität ist eine erhebliche Einschränkung der Kontrollmöglichkeiten, vor allem für **Werbe- und Trackingblocker**.

Erweiterungs-API

Ein **A**pplication **P**rogramming **I**nterface für Erweiterungen ist eine Schnittstelle, über die Browsererweiterungen (Add-ons) auf Browserfunktionen zugreifen können. Möglich sind damit z. B. das Abfangen von Netzwerkanfragen, das Verwalten von Tabs oder das Anpassen von Website-Inhalten. Die Regelwerke Manifest v2 und v3 definieren hierfür genauer, welche APIs mit welchen Berechtigungen genutzt werden dürfen.

Das zentrale Problem liegt im Austausch der APIs: Die alte webRequest-API ermöglichte eine flexible, dynamische Filterung. Manifest v3 ersetzt sie durch declarativeNetRequest – ein starres Regelsystem ohne intelligente Anpassungsfähigkeit. Werbeblocker, die Manifest v3 unterstützen, müssen daher Kompromisse eingehen: Ihre Filterqualität sinkt, weil nur vordefinierte Regeln greifen. Kontextabhängige Heuristiken, die Entscheidungen im Einzelfall treffen, sind nicht mehr möglich.

Googles Argument für diese Umstellung ist sicherheitstechnisch nachvollziehbar: Die webRequest-API eröffnete Browsererweiterungen Zugriff auf den gesamten Netzwerkverkehr. Gleichzeitig ist nicht zu übersehen, dass die Änderung Werbe- und Trackingblocker besonders stark trifft – was Googles Werbegeschäft eher zugutekommt.

Die Browsermonokultur verschärft das Problem

Besonders problematisch ist Googles Marktposition: Mit **Chromium** hat der Konzern eine neue Browsermonokultur geschaffen. Die meisten modernen Browser – Microsoft Edge, Vivaldi, Brave – basieren auf Chromium und müssen Googles Vorgaben übernehmen. Ein Abweichen wäre technisch möglich, hätte aber erhebliche Konsequenzen: Die Erweiterungs-API müsste vollständig neu entwickelt und gepflegt werden.

Firefox und **Safari** bleiben damit die einzigen von Google **unabhängigen Browser**. Allerdings verfolgt Safari mit seiner Content Blocking API

schon seit Längerem einen ähnlich restriktiven Kurs wie Googles Manifest v3 – auch hier sind flexible Filtersysteme unmöglich. Firefox unterstützt zwar ebenfalls Manifest v3, behält aber als einziger Browser die umfassenden Funktionen von Manifest v2 bei.

Kontrollverlust der Nutzenden

Diese Entwicklung hat eine grundsätzliche Implikation: Chromium-Nutzende verlieren die Möglichkeit, ihren Netzwerkverkehr granular zu steuern. Zwar birgt die alte webRequest-API echte Sicherheitsrisiken – doch ob die radikale Ersetzung durch ein starres Regelsystem die beste Lösung ist, bleibt umstritten.

Wenn die Möglichkeiten zur dynamischen Filterung des Datenverkehrs eingeschränkt werden, verlieren Nutzende ein wichtiges Instrument zur Kontrolle ihrer persönlichen Daten im Internet. Dies könnte dazu führen, dass mehr persönliche Informationen – von Surfgewohnheiten bis hin zu sensiblen Interessen und detaillierten Nutzerprofilen – gesammelt und für gezielte Werbung oder Profiling genutzt werden.

10.3 KI-Systeme und die Privatsphäre

Sogenannte künstliche Intelligenz hält den Einzug in fast jedes System, das man sich vorstellen kann. Mit geringem Aufwand kann man professionell wirkende Texte, Bilder, Videos, Songs usw. generieren, ohne über eigene Fähigkeiten in diesem Bereich verfügen zu müssen. Immer realistischer werden die Ergebnisse und lassen sich teilweise kaum noch von echten kreativen Leistungen unterscheiden.

Sogenannte **„Deep Fakes"** stellen dabei eine **besondere Bedrohung der Persönlichkeitsrechte** dar. Mit nur wenigen Fotos als Vorlage kann man ein KI-System dazu bringen, die abgebildete Person realitätsnah in einen völlig anderen Kontext zu übertragen. Plötzlich sieht man ein Video von sich bei Handlungen, zu denen man womöglich nie bereit war. Auch die Stimme lässt sich so nachahmen, dass es kaum auffällt. Ob Fotos, Video- oder Tonaufzeichnungen noch die Realität wiedergeben, lässt sich durch einfache Inaugenscheinnahme längst nicht mehr verlässlich sagen, zumal die verwendeten Systeme sich immer weiterentwickeln und immer mehr Fehler wie die berühmten sechs Finger bereinigen.

Während die Gefahren dieser generativen Anwendungen noch leicht nachvollziehbar sind, denken nicht alle daran, dass solche Systeme auch in anderen Szenarien zum Einsatz kommen können. Mit nicht geringem Erfolg lassen sich KI-Systeme auch dazu bringen, schwarze Balken vor Augen, Unschärfen, Verpixelungen, Stimmverzerrungen und andere Veränderungen, die Menschen vor Identifizierung schützen sollten, wieder rückgängig zu machen. Die Ergebnisse sind dabei zwar nicht exakt, aber gut genug, um eine Erkennung zu ermöglichen. Für einen angemessenen Schutz von Persönlichkeitsrechten in Berichterstattungen sind solche Maßnahmen daher nicht mehr als hinreichend zu betrachten.

Auch in der **Mustererkennung** sind KI-Systeme in neue Dimensionen vorgestoßen und verbessern sich stetig. Der Aufwand, Browser und darüber deren Nutzende durch individuelle Parameter wie Einstellungen, Latenz usw. wiederzuerkennen (sogenanntes Browser-Fingerprinting, Tz. 10.1) und aus Abrufen und Klickverhalten auf Vorlieben zu schließen, sinkt mit einfach zu bedienenden KI-Tools massiv. Dass ein Webdienst auf „technisch notwendige" **Cookies** eingeschränkt wird oder ganz auf diese verzichtet, ist insofern kein Indiz mehr dafür, dass man nicht ausgeforscht wird. Vielleicht erkennt man Menschen auch inzwischen am zuverlässigsten daran, dass sie für sogenannte **CAPTCHA-Tests** besonders lange brauchen und eher Fehler machen.

Für andere Bereiche gibt es ebenfalls deutliche Auswirkungen: Die Verknüpfung von anonymisierten oder pseudonymisierten Daten mit anderen Datenquellen oder eine Korrelation von Daten mithilfe bisher unbekannter, aber durch KI-Anwendungen aufgedeckter Muster kann dazu führen, dass ein **Personenbezug** leicht

(wieder-)hergestellt werden kann. Der in einigen Gesetzgebungsverfahren vergangener Jahrzehnte noch angenommene sehr hohe Aufwand für solche Verknüpfungen ist durch die technische Entwicklung im KI-Bereich deutlich gesunken.

Die allgemeine Verfügbarkeit so mächtiger Auswertungswerkzeuge, wie KI-Systeme sie darstellen, dürfte auch in weitere Bereiche ausstrahlen. **Gefälschte Identitäten** etwa ließen sich damit mindestens erkennen, vielleicht sogar aufdecken. Personen, die noch nie Spuren von sich in sozialen Netzen hinterlassen haben, werden schließlich immer seltener. Dies betrifft dann nicht nur gewiefte Trickbetrügerinnen und -betrüger, sondern auch verdeckte Ermittelnde. Dem wird man allerdings auch mit rechtlichen Regelungen kaum beikommen.

11

KERNPUNKTE

Datenübermittlung in Drittländer zu medizinischen Zwecken

Chatkontrolle – Risiko für digitale Infrastruktur

11 Europa und Internationales

11.1 Anwendungshinweise der DSK zur Datenübermittlung in Drittländer zu medizinischen Zwecken

In Zusammenarbeit mit den anderen deutschen Datenschutzaufsichtsbehörden beteiligte sich das ULD an der Erstellung von Anwendungshinweisen zu den Anforderungen an Datenübermittlungen an Drittländer im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken. Die **Forschung im medizinischen Kontext** ist eine bedeutsame Thematik, insbesondere zur Erforschung von Krankheiten, der Entwicklung von Therapiemaßnahmen, zur Verbesserung von Diagnosen, Behandlungen und der Arzneimittelforschung. Eine Herausforderung besteht darin, dass zum Zweck der Medizinforschung **sensible Datenkategorien**, wie etwa Gesundheitsdaten, in Drittländer übermittelt werden sollen, die über kein dem europäischen Standard vergleichbares Schutzniveau verfügen.

Die Anwendungshinweise zeigen **wichtige Prüfschritte** auf, um im Vorfeld Fragen zur Zulässigkeit der Datenübermittlung beantworten zu können. Hierzu zählen vor allem folgende Punkte:

- Die Prüfung erfolgt in **zwei Stufen**. In **Stufe 1** ist zu untersuchen, ob für die Datenübermittlung eine **Rechtsgrundlage** besteht. In **Stufe 2** sind **Besonderheiten bezüglich der Übermittlungen in Drittländer** zu beachten, insbesondere die Heranziehung von Angemessenheitsbeschlüssen der Europäischen Kommission, die Berücksichtigung geeigneter Garantien und ergänzende Maßnahmen zur Gewährleistung der Datensicherheit und mögliche Ausnahmetatbestände für Übermittlungen im Einzelfall.
- In **Stufe 1** kann die **Einwilligung** der betroffenen Person eine Rechtsgrundlage sein. In diesem Zusammenhang ist aber bereits zu untersuchen, ob der Forschungszweck unter dem Gesichtspunkt der Datenminimierung auch durch anonyme Daten erreichbar ist.
- Hilfreich ist ein effektives **Einwilligungsmanagement**, bei welchem nach bestimmten Standards Einwilligungen erklärt und widerrufen werden können.
- Vor der Erklärung einer Einwilligung müssen der betroffenen Person Informationen zu dem Forschungsvorhaben, konkrete Zwecksetzungen und Datenempfänger bekannt sein, was z. B. durch Newsletter oder über eine leicht zugängliche Datenbank erreichbar wäre.
- Die frühzeitige Einbindung eines **Datenschutzbeauftragten** vor der Datenerhebung und -übermittlung sowie die vorherige Einholung des Votums einer **Ethikkommission** kann für die datenschutzrechtliche Beurteilung des Forschungsvorhabens hilfreich sein.
- Es ist zu empfehlen, stets eine **Datenschutz-Folgenabschätzung** vorzunehmen.
- Es kommt auch die vorherige Konsultation der zuständigen Datenschutzaufsichtsbehörde in Betracht.
- In **Stufe 2** ist die Existenz von **Angemessenheitsbeschlüssen** der Europäischen Kommission von Bedeutung, die bisher für 15 Länder bestehen. Gemessen am Beispiel der USA ist dabei zu prüfen, ob der Datenempfänger im Drittstaat über eine Zertifizierung nach der maßgeblichen Angemessenheitsentscheidung verfügt.
- In Stufe 2 können im Falle eines fehlenden Angemessenheitsbeschlusses – oder im Falle der USA bei fehlender Zertifizierung des Empfängers – geeignete Garantien in Form von **Standarddatenschutzklauseln** oder **Binding Corporate Rules** nötig sein. Nach der Rechtsprechung des Europäischen Gerichtshofs bedarf es in den letztgenannten Fällen zusätzlicher Maßnahmen, insbesondere technischer und organisatorischer Natur, um im Drittstaat mög-

liche unbefugte Zugriffe auf die Daten durch andere Unternehmen oder öffentliche Stellen zu unterbinden.

Die Anwendungshinweise der Datenschutzkonferenz können unter folgendem Link abgerufen werden:

https://www.datenschutzkonferenz-online.de/media/oh/20250917_DSK_OH_Datenuebermittlungen.pdf

Kurzlink: *https://uldsh.de/tb44-11-1a*

Die Empfehlungen für die Umsetzung von **Informationspflichten bei Datenübermittlungen an Drittländer** im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken sind hier zu finden:

https://www.datenschutzkonferenz-online.de/media/oh/20250917_DSK_OH_Datenuebermittlungen_Anlage.pdf

Kurzlink: *https://uldsh.de/tb44-11-1b*

Was ist zu tun?

Wer medizinische Forschungsprojekte plant oder durchführt, sollte die aufgezeigten Prüfschritte sowie die Empfehlungen zur Gestaltung der Informationspflichten berücksichtigen.

11.2 Wiedergänger Chatkontrolle – Risiko für die gesamte digitale Infrastruktur

Nachdem bereits im Jahr 2022/2023 die von der Europäischen Kommission vorgeschlagene Verordnung zur sogenannten **EU-Chatkontrolle** in den Fokus der datenschutzrechtlichen Diskussionen getreten war und wir damals hofften, dass diese Vorschläge aufgrund der erheblichen Risiken für die Grundrechte und die Sicherheit der Infrastrukturen begraben waren, flammte die Diskussion im Jahr 2025 erneut auf. Die dänische Regierung hatte als amtierende EU-Ratspräsidentschaft die Verordnung zur Chatkontrolle auf die Tagesordnung des EU-Rats gesetzt. Ziel der Verordnung ist es, die Bekämpfung von Kindesmissbrauch und Terrorismus zu intensivieren, indem Plattformbetreiber verpflichtet werden, **Kommunikation in privaten Messengerdiensten und Chats auf verdächtige Inhalte zu scannen**. Betroffen wären Messengerdienste, E-Mail-Dienste und Cloud-Speicher. Zwar ist das Ziel legitim, doch wirft der Ansatz erhebliche datenschutz- und grundrechtliche Fragen auf.

Die geplanten Prüfpflichten würden zu einer **generellen und unterschiedslosen Kontrolle sämtlicher Nachrichten** führen. Dies kollidiert mit den Artikeln 7 und 8 der EU-Grundrechtecharta sowie den zentralen datenschutzrechtlichen Prinzipien gemäß Artikel 5 DSGVO. Der EuGH hat vergleichbare Formen der **Massenüberwachung** (u. a. Vorratsdatenspeicherung) mehrfach als unverhältnismäßig eingestuft.

Ein zentrales Risiko der EU-Chatkontrolle liegt in der möglichen Schwächung oder Umgehung der **Ende-zu-Ende-Verschlüsselung**, die derzeit eine der wichtigsten Schutzmaßnahmen für die Sicherheit privater Kommunikation darstellt. Daraus resultieren diverse technische Herausforderungen. Die Einführung von Technologien, die Kommunikation auf verdächtige Inhalte hin scannen, könnte dazu führen, dass Anbieter gezwungen werden, die Verschlüsselungssysteme zu umgehen oder aufzuweichen, um den Scanprozess zu ermöglichen. Das könnte nicht nur das Vertrauen der Nutzenden in Kommunikationsdienste untergraben, sondern würde auch die Sicherheit der gesamten digitalen Infrastruktur gefährden.

Der **Grundsatz der Datenminimierung** sieht vor, dass Daten nur in dem Maße erhoben und verarbeitet werden, wie es für den jeweiligen Zweck notwendig ist. Die EU-Chatkontrolle könnte jedoch dazu führen, dass Kommunikationsanbieter Daten in einem viel größeren Umfang sammeln und analysieren, als es für die Bekämpfung von Kindesmissbrauch oder Terrorismus notwendig wäre.

Das Aufspüren „neuer" Missbrauchsinhalte oder Anbahnungsversuche setzt auf KI-basierte Klassifikatoren. Diese Systeme sind fehleranfällig und wenig transparent. Falschmeldungen könnten zur Weitergabe völlig unproblematischer privater Inhalte an Behörden führen – ein erhebliches Risiko für Betroffene und ein Verstoß gegen das Gebot der Richtigkeit und Fairness der Verarbeitung.

Die Datenschutzaufsichtsbehörden sind sich durchaus dessen bewusst, dass Sicherheitsbehörden wirksame Werkzeuge und rechtliche Möglichkeiten zur Bekämpfung und Vermeidung von sexuellem Missbrauch von Kindern benötigen. Dieses Ziel darf jedoch nicht auf Kosten der Privatsphäre von Millionen von Personen verfolgt werden, die dafür keinen Anlass gegeben haben. In der technischen Umsetzung bedeutet die Chatkontrolle eine Hintertür, die den Weg in die Überwachung sämtlicher Inhalte eröffnet. Das Missbrauchspotenzial ist enorm. **Hintertüren in der Verschlüsselung gefährden die Sicherheit** der Kommunikation aller Personen und könnten auch von Kriminellen missbraucht werden.

Die Pressemitteilung der Datenschutzkonferenz „Datenschutzbeauftragte fordern Nein der Bundesregierung zur Chatkontrolle – Private Kommunikation muss sicher und vertraulich bleiben" ist unter den folgenden Links abrufbar:

https://www.datenschutzzentrum.de/artikel/1517-Datenschutzbeauftragte-fordern-Nein-der-Bundesregierung-zur-Chatkontrolle.html

Kurzlink: *https://uldsh.de/tb44-11-2a*

https://www.datenschutzkonferenz-online.de/media/pm/20251008-DSK-PM_Nein-zur-Chatkontrolle.pdf

Kurzlink: *https://uldsh.de/tb44-11-2b*

Zwischenzeitlich haben sich die EU-Staaten nach langem Ringen nun darauf geeinigt, dass die Plattformbetreiber nicht verpflichtet werden, private Nachrichten automatisiert zu durchsuchen. Sie sollen aber freiwillige Kontrollen durchführen dürfen. Die EU-Kommission soll später prüfen, ob eine Verpflichtung doch nötig ist. Die Debatte um die Chatkontrolle geht also weiter.

12

KERNPUNKTE

Beanstandungen nach dem IZG-SH

Neue Kostenverordnung zum IZG-SH

Top-5-Themen und besondere Fälle

Beschlüsse der IFK

12 Informationsfreiheit

Diskussionen über Sinn und Zweck der Informationsfreiheit im Bund und einigen Bundesländern zeigten 2025, dass dieses Bürgerrecht weiterhin nicht für jeden eine Selbstverständlichkeit darstellt. In Schleswig-Holstein hat es sich seit dem Jahr 2000 etabliert. In den letzten 25 Jahren ist es bei vielen Behörden zum festen Bestandteil der Bürgerkommunikation geworden und trägt seinen Beitrag zur Transparenz der Verwaltungstätigkeit und damit zum Vertrauen in die Arbeit der öffentlichen Stellen bei.

12.1 Beanstandungen

§ 14 Abs. 5 IZG-SH regelt seit 2022, dass, wenn die oder der Landesbeauftragte für Informationszugang Verstöße gegen das IZG-SH feststellt, sie oder er diese gegenüber der informationspflichtigen Stelle beanstanden kann. Hiervon haben wir im Berichtszeitraum einmal Gebrauch machen müssen.

1. Ein Petent hatte bei der **Gemeinde Malente** die Einsicht in Stellungnahmen der Träger öffentlicher Belange zu einem **vorläufigen Bebauungsplan** nach dem IZG-SH beantragt. Die Gemeinde lehnte diese mit Verweis darauf ab, dass es sich um verwaltungsinterne, vorbereitende Schriftstücke handele. Die Ablehnung erfolgte zum einen nach § 9 Abs. 2 Nr. 4 IZG-SH, da sich der Antrag auf die Herausgabe eines noch nicht abgeschlossenen Schriftstücks im Sinne eines Planentwurfs beziehe. Zudem liege der Versagungsgrund des § 9 Abs. 1 Nr. 3 IZG-SH vor und das Interesse an der Vertraulichkeit der Beratungen von informationspflichtigen Stellen überwiege das öffentliche Bekanntgabeinteresse. Nach BVerwG vom 09.05.2019 (Az. 7 C 34/17, Rn. 13) sei der behördliche Entscheidungsprozess geschützt. Das Ergebnis selbst spiegele sich erst im Planentwurf und im Abwägungsbeschluss im Sinne des § 1 Abs. 7 BauGB wider.

Der Argumentation konnten wir nicht folgen. Die Äußerungen der Träger öffentlicher Belange sind für sich abgeschlossene Dokumente und in der Regel nicht unter Vorbehalt einer Überarbeitung oder Änderung übermittelt worden. Es handelt sich im Gegensatz zu der Voraussetzung des § 9 Abs. 2 Nr. 4 IZG-SH um abgeschlossene Schriftstücke.

Die Äußerungen sind auch als Grundlage für die Beratungen anzusehen und damit nicht im Rahmen des Beratungsprozesses nach § 9 Abs. 1 Nr. 3 IZG-SH geschützt. Nach Kommentaransicht und Rechtsprechung fallen die zur Entscheidung führenden Tatsachen, Sachinformationen und gutachterlichen Stellungnahmen nicht unter die in § 9 Abs. Satz 1 Nr. 3 IZG-SH geschützten Beratungen.

Schon im Tätigkeitsbericht 2002 des ULD (24. TB, Tz. 13.1) äußerten wir uns zu einem vergleichbaren Sachverhalt: „Zwar muss z. B. im Rahmen eines Bauleitplanverfahrens der Schutz des behördlichen Entscheidungsbildungsprozesses gewährleistet werden. Dieser Schutz gilt indes nicht für alle Arten von Unterlagen. Handelt es sich z. B. um Äußerungen von Trägern öffentlicher Belange, so sind dies – da es sich um extern erstellte Vorlagen handelt, deren inhaltliche Ergebnisse feststehen und von der Behörde nur noch bewertet werden müssen – Unterlagen, die unabhängig vom Stand des jeweiligen Verfahrens zugänglich zu machen sind."

Im Ergebnis wurden dem Antragsteller die beantragten Informationen ohne nachvollziehbare Gründe verwehrt, womit sein Anspruch auf Zugang zu Informationen im Sinne des § 3 IZG-SH verletzt wurde. Wir haben unter Abwägung der genannten Punkte und der Verstöße gegen das IZG-SH das Mittel der Beanstandung gewählt. Hiergegen hat die Gemeinde Malente Klage vor dem Verwaltungsgericht Schleswig eingereicht.

2. In unserem letzten Tätigkeitsbericht (43. TB, Tz. 12.1) hatten wir über eine Beanstandung gegenüber der **Gemeinde Heikendorf** berichtet. Betroffen waren Informationen über **Gemeinderatssitzungen und Anwaltsgutachten** im Auftrag der Gemeinde. Die Gemeinde Heikendorf bzw. das Amt Schrevenborn hatten gegen unsere Beanstandung **Klage beim Verwaltungsgericht** in Schleswig eingelegt. Das Verfahren ist dort weiterhin anhängig und noch nicht abgeschlossen.

Was ist zu tun?

Das Mittel der Beanstandung ist bei Verstößen gegen das IZG-SH weiterhin zu nutzen, um den informationspflichtigen Stellen, wenn sie bei der Umsetzung der Informationsfreiheit Fehler machen, diese nachdrücklich darzulegen.

12.2 Neue Kostenverordnung zum IZG-SH

Am 24. Januar 2025 wurde eine neue Landesverordnung über Kosten nach dem Informationszugangsgesetz für das Land Schleswig-Holstein (IZG-SHKostenVO) veröffentlicht. Wir waren im Vorfeld nicht eingebunden worden. Die Verordnung beruht auf § 13 IZG-SH, wonach Gebühren und Auslagen für die Bereitstellung von Informationen erhoben werden können. Zentrale Änderung ist die **Erhöhung der Gebühren**. Zwar sind die Gebühren unter Berücksichtigung des Verwaltungsaufwands zu bemessen, jedoch muss auch beachtet werden, dass das Recht auf Zugang zu Informationen wirksam in Anspruch genommen werden kann. Zu hohe Gebühren könnten für Antragstellerinnen und Antragsteller abschreckend wirken. In der alten Version der Verordnung betrug die Maximalgebühr 500 Euro. Diese wurde nun für außergewöhnlich aufwendige Maßnahmen zur Zusammenstellung von Unterlagen auf 700 Euro erhöht. Damit ging auch einher, dass die mittlere Gebühr für umfassende Auskünfte auf maximal 350 Euro erhöht wurde. Für die **Erteilung von mündlichen oder einfachen schriftlichen oder elektronischen Auskünften** blieb es bei der **Gebührenfreiheit**. Hierfür nehmen wir einen Aufwand von ca. 30 bis 45 Minuten an, wobei hierzu nicht zählt, wenn sich eine informationspflichtige Stelle zunächst mit den Grundlagen des IZG-SH befassen muss. Aber auch bei höherem Aufwand erlaubt § 4 der Verordnung, dass von der Erhebung von Kosten **ganz oder teilweise abgesehen werden kann**, wenn dies im Einzelfall aus Gründen der Billigkeit oder des öffentlichen Interesses geboten ist. Nach unserem Wissen machen viele informationspflichtige Stellen hiervon im Sinne der Bürgerfreundlichkeit Gebrauch.

Neu hinzugekommen ist die Regelung in § 2. Danach gilt, dass – soweit im Falle eines Informationsbegehrens **mehrere gebührenpflichtige Tatbestände** entstanden sind – die Gebühren einen Betrag von insgesamt 700 Euro nicht übersteigen dürfen. Werden mehrere Informationsbegehren in einem Antrag gemeinsam gestellt, sind sie unabhängig voneinander zu berechnen. Unklar bleibt dabei, wann mehrere Informationsbegehren vorliegen. Üblich ist es in der Praxis, dass zu einem Sachverhalt im Rahmen von Anträgen nach dem IZG-SH mehrere Fragen gestellt werden, die sich auf Teilinformationen zu einem Sachverhalt beziehen. Wir gehen davon aus, dass es sich hierbei weiterhin um ein Informationsbegehren handelt.

Was ist zu tun?

Informationspflichtige Stellen sind über die Regelungen zur Erhebung von Kosten zu beraten und über Neuigkeiten in dem Bereich zu informieren.

12.3 Top 5 der Themen in Schleswig-Holstein

Nach § 14 Abs. 1 IZG-SH kann eine Person, die der Ansicht ist, dass ihr Informationsersuchen zu Unrecht abgelehnt oder nicht beachtet worden ist oder dass sie von einer informationspflichtigen Stelle eine unzulängliche Antwort erhalten hat, die Landesbeauftragte für Informationszugang anrufen. Einige Beschwerdegründe von Petentinnen und Petenten wiederholten sich auch 2025 mehrfach. Die Top 5 der Beschwerden sind in vielen Teilen vergleichbar mit denen der letzten Jahre (vgl. u. a. 41. TB, Tz. 12.3; 42. TB, Tz. 12.2; 43. TB, Tz. 12.2).

Ein häufiger Beschwerdegrund war auch in diesem Jahr, dass die informationspflichtige Stelle nicht **innerhalb der gesetzlichen Frist** auf den Antrag auf Informationszugang antwortet. Nach § 5 Abs. 2 Satz 1 IZG-SH sind die Informationen der antragstellenden Person unter Berücksichtigung etwaiger von ihr angegebenen Zeitpunkte so bald wie möglich, spätestens jedoch mit Ablauf eines Monats nach Eingang des Antrags zugänglich zu machen. 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 (§ 5 Abs. 2 Satz 2 IZG-SH). Wird hiervon Gebrauch gemacht, ist dies der antragstellenden Person so bald wie möglich, spätestens aber innerhalb eines Monats nach Antragseingang unter Angaben der Gründe mitzuteilen.

Bei zahlreichen Beschwerden, die uns erreichen, erfolgte nach der Antragstellung gar keine Reaktion der angefragten informationspflichtigen Stelle. Erst durch unser Einschalten kam es dann zu einer Rückmeldung.

Mehrfach hatten Petentinnen und Petenten auf ihre Anträge die Rückmeldung erhalten, dass die Behörde durchaus zwar gewillt sei, Auskunft zu erteilen, aber dies erst aufgrund der Arbeitsbelastung in einer unbestimmten Zukunft möglich sei. Auch diesen Beschwerden sind wir nachgegangen, da Antragstellerinnen und Antragsteller ein Recht darauf haben, dass die Bescheidung des Antrags innerhalb der oben genannten Fristen erfolgt und bei einer Verlängerung der Frist klar mitgeteilt wird, dass diese nur um einen weiteren Monat erfolgt. Die Erfahrung zeigt, dass in vielen Fällen eine frühe Kontaktaufnahme zu antragstellenden Personen hilfreich ist. Auch wenn die Fristenregelung klar vom Gesetzgeber geregelt ist, kann es im persönlichen Gespräch möglich sein, aufgrund besonderer Umstände andere Absprachen zu treffen. Gar keine Reaktion zu zeigen ist die denkbar schlechteste Lösung, mit Anträgen nach dem IZG-SH umzugehen. Der Bürger fühlt sich dann zu Recht von der Behörde nicht ernst genommen.

Ob ein Antrag nach dem IZG-SH vorliegt, ist für eine öffentliche Stelle **nicht immer klar zu erkennen**. Eine Pflicht zur ausdrücklichen Berufung auf das Gesetz besteht nicht. Grundsätzlich schreibt das Gesetz auch keine besondere Form der Antragstellung vor, sodass diese sogar mündlich erfolgen kann. Manchmal werden auch Anträge auf Auskunft über eigene personenbezogene Informationen nach Artikel 15 DSGVO mit Anträgen nach dem IZG-SH vermischt. Grundsätzlich darf es nicht zulasten der antragstellenden Personen gehen, dass diese die Rechtsgrundlagen nicht konkret kennen. Die öffentliche Stelle ist in der **Pflicht**, die Anträge entsprechend im Sinne der Bürgerinnen und

Bürger auszulegen. Ist dies nicht möglich, so ist die antragstellende Person so bald wie möglich, spätestens aber innerhalb eines Monats aufzufordern, den Antrag zu präzisieren (§ 4 Abs. 2 Satz 2 IZG-SH). Dabei haben die informationspflichtigen Stellen die antragstellende Person bei der Stellung und Präzisierung von Anträgen zu unterstützen (§ 4 Abs. 2 Satz 3 IZG-SH).

Regelmäßig bestehen unterschiedliche Auffassungen zwischen der antragstellenden Person und der informationspflichtigen Stelle, ob diese tatsächlich **über die angefragten Informationen verfügt**. Nach § 2 Abs. 5 IZG-SH verfügt eine informationspflichtige Stelle über Informationen, wenn diese bei ihr vorhanden sind oder an anderer Stelle für sie bereitgehalten werden. Dabei kommt es nicht darauf an, ob eine andere Stelle auch über die Informationen verfügt oder gegebenenfalls sogar der eigentliche Urheber der Informationen ist.

Andererseits stellt das IZG-SH auch **kein allgemeines Fragerecht** dar. Insbesondere Bitten um rechtliche Erläuterungen oder ergänzende Auswertungen von Informationen sind oftmals nicht vom IZG-SH gedeckt, wenn diese Informationen nicht schon etwa Teil eines Vermerks geworden sind. Auskunftspflichtig sind nach § 2 Abs. 1 IZG-SH nur Informationen, die sich auf einem Informationsträger befinden. Die reinen Gedanken, die sich etwa ein Sachbearbeiter gemacht hat, gehören nicht dazu, wenn er sie nicht in irgendeiner Form festgehalten hat.

Damit ging im Berichtszeitraum mehrfach die Frage einher, welcher **Aufwand bei der Zusammenstellung** etwa statistischer Informationen noch zumutbar ist, um die Informationen als verfügbar anzusehen. In einem Urteil des OVG Schleswig vom 23.07.2020 (Az. 4 LB 45/27) wurde eine Übersicht über Akten oder eine Liste von Vorgängen, die in dieser aggregierten Form bei der Stelle zwar nicht vorliegen, aber die Stelle sie aus den von ihr geführten Akten oder gespeicherten Informationen zusammenstellen könnte, als vorhandene Informationen angesehen. Somit können auch mit einfacher Datenbankrecherche ermittelbare Informationen als vorhanden angesehen werden. Dies stützt auch ein Urteil des EuGH vom 11.01.2017 (C-491/15 P): Danach liegen Informationen vor, die aus einer elektronischen Datenbank im Rahmen ihrer üblichen Nutzung mithilfe vorprogrammierter Suchfunktionen extrahiert werden können, auch wenn diese Informationen noch nicht in dieser Form angezeigt wurden oder von den Bediensteten der Organe nie gesucht worden sind. Hingegen stellt jede Information, deren Beschaffung eine Veränderung entweder der Organisation einer elektronischen Datenbank oder der derzeit für die Extrahierung von Informationen zur Verfügung stehenden Suchfunktionen erfordert, ein neues Dokument dar.

Die Grundlagen zum IZG-SH haben wir in einer Broschüre zusammengefasst, die regelmäßig aktualisiert wird:

https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-7-Informationszugang.pdf

Kurzlink: *https://uldsh.de/tb44-12-3a*

Was ist zu tun?

Den Beschwerden von Petentinnen und Petenten ist nachzugehen. Weiterhin sind informationspflichtige Stellen auf ihre Fehler hinzuweisen. Damit diese gar nicht erst auftreten können, werden wir die Schulungen bzw. Informationen über das IZG-SH für öffentliche Stellen intensivieren.

12.4 Besondere Fälle und Fragen

Im Berichtszeitraum hatten wir einige besondere Anfragen und Beschwerden, die über die typischen Fragestellungen (Tz. 12.3) hinausgingen.

1. In einem Verfahren war umstritten, ob **Vergabeunterlagen** nach dem IZG-SH herausgegeben werden mussten. Dabei berief sich die informationspflichtige Stelle auf die **Vergabeverordnung (VgV)**. Nach § 5 Abs. 2 Satz 2 VgV sind Interessensbekundungen, Interessensbestätigungen, Teilnahmeanträge und Angebote einschließlich ihrer Anlagen sowie die Dokumentation über Öffnung und Wertung der Teilnahmeanträge und Angebote auch nach Abschluss des Vergabeverfahrens vertraulich zu behandeln.

Das Verwaltungsgericht Berlin hat für das Informationsfreiheitsrecht in Berlin am 13.03.2025 eine Entscheidung zum Verhältnis zu § 5 Abs. 2 Satz 2 VgV gefällt (2 K 100/23). In der Entscheidung macht das Gericht deutlich, dass die Regelung der VgV vorgeht. „Der Schutz dieser Vorschrift erstreckt sich nicht nur auf die in § 5 Abs. 2 Satz 2 VgV genannten Unterlagen, sondern auf sämtliche Unterlagen, die den schutzwürdigen Inhalt wiedergeben. Da es sich bei der Preisgestaltung um den Kernbereich der Geschäftsgeheimnisse handelt […], umfasst die Vertraulichkeitspflicht auch die im aufgrund des Angebotes abgeschlossenen Vertrag enthaltene Preisangabe (vgl. Urteil der Kammer vom 9. März 2017 – VG 2 K 111/15 – juris Rn. 35).“ Allerdings bezieht sich die Aussage nur auf die in der VgV genannten Informationen („Interessensbekundungen, Interessensbetätigungen, Teilnahmeanträge und Angebote“ und deren Wiedergabe). Bezüglich des abgeschlossenen Vertrags wird nur auf die Preisangabe Bezug genommen.

Im Umkehrschluss verstehen wir die Rechtslage so, dass alle anderen Informationen weiterhin dem Informationsfreiheitsrecht unterfallen. Dies betrifft insbesondere Informationen, die vonseiten der öffentlichen Hand stammen und nicht als Betriebs- und Geschäftsgeheimnisse im Sinne des § 10 Satz 1 Nr. 3 IZG-SH von dem Träger im Rahmen des Verfahrens individuell übermittelt wurden. Dies dürfte z. B. die Leistungsbeschreibung der Ausschreibung, kann aber auch zumindest Teile der Kooperationsvereinbarung betreffen. Auch ist zu beachten, dass die VgV nur für Vergaben oberhalb der Schwellenwerte von § 106 GWB gilt. Darunter kann § 5 VgV nicht herangezogen werden.

2. Immer wieder kommt es dazu, dass informationspflichtige Stellen Anträge aufgrund von **Missbrauch** im Sinne des § 9 Abs. 2 Nr. 1 IZG-SH ablehnen. Im Berichtszeitraum wurde zum einen auf die Anzahl der Anträge abgestellt, um Missbräuchlichkeit anzunehmen. Eine andere Stelle erkannte in dem Umstand, dass die Antragstellerin aus dem beantragten Dokument zitiert, dass sie dieses schon besitze und daher der Antrag missbräuchlich sei.

Schon der Gesetzestext schreibt vor, dass der Missbrauch „offensichtlich“ sein muss. Hieran sind hohe Anforderungen zu stellen. Ein Missbrauch liegt vor, wenn deutlich ist, dass der Antrag nicht zur Informationsgewinnung dient, sondern insbesondere dazu, die Behörde mit Arbeit zu belasten. Die Rechtsprechung nimmt selbst bei einer mittleren zweistelligen Anzahl von Anträgen keinen Missbrauch an, sodass das Argument bei den uns vorgelegten Fällen in der Regel nicht griff.

Da das IZG-SH keine Voraussetzungen an das Interesse der antragstellenden Person stellt, kann der Nutzen der Informationen für die Person kein Kriterium für die Missbräuchlichkeit sein. Sinn des IZG-SH ist insbesondere die Transparenz der Behörde, wozu auch die Information gehören kann, ob ein Dokument dort vorhanden ist. Wenn aus einem Dokument zu deren genauen Bestimmung zitiert wird, so können wir hierin nicht ansatzweise eine Missbräuchlichkeit erkennen.

3. Eine Behörde verlangte mit Verweis auf das Landesverwaltungsgesetz (LVwG) von einer Antragstellerin zwingend ihre **Postanschrift**, um den Bescheid mit der Antwort zustellen zu können. Nach § 108 LVwG ist jedoch ausdrücklich gerade die elektronische Form des Bescheids zugelassen. Diese umfasst auch die einfache E-Mail. Soweit die Behörde meinte, dass nach § 147 Abs. 2 LVwG eine Zustellung per Post (oder per DE-Mail oder direkt über die Behörde) vor-

geschrieben sei und deswegen die Postanschrift abgefragt werden müsse, war dem zu entgegnen, dass dieser Paragraf sich lediglich auf die in § 146 LVwG geregelten Fälle bezieht, in denen die entsprechende Zustellung ausdrücklich durch Rechtsvorschrift oder behördliche Anordnung bestimmt ist. Dies war hier jedoch nicht der Fall. Eine behördliche Anordnung muss sich dabei an die allgemeinen Ermessensgrundsätze halten. Der Gesetzgeber hat das IZG-SH so ausgestaltet, dass möglichst niedrige Anforderungen an die Antragstellung gesetzt werden. Es ist nicht ersichtlich, welche der Zwecke einer Zustellung bei einer einfachen Auskunft nach dem IZG-SH herangezogen werden müssten, um eine Anordnung der Zustellung zu rechtfertigen. Nach § 6 Abs. 2 Satz 2 IZG-SH ist ausdrücklich für die Ablehnung des Antrags die elektronische Form auf Verlangen vorgesehen. Auch einfache elektronische Auskünfte werden vom Gesetz genannt (etwa § 13 Abs. 1 Nr. 1 IZG-SH).

4. In einem anderen Fall hatte eine Antragstellerin bei einer Behörde Zugang zu Bauplänen für ein Gebäude beantragt, das sie selbst gekauft hatte. Die Behörde hatte dies zunächst mit Verweis auf **Urheberrechte** nach § 10 Satz 1 Nr. 2 IZG-SH verweigert, obwohl wohl sogar die Einwilligung der Erben des Verkäufers vorlagen. Durch unsere Vermittlung konnte dann der Informationsanspruch durch Einsichtnahme vor Ort weitgehend erfüllt werden.

Was ist zu tun?

Personen, die der Ansicht sind, dass ihre Anträge nach dem IZG-SH nicht ordnungsgemäß beantwortet worden seien, sind weiterhin zu unterstützen. Die informationspflichtigen Stellen sind auf ihre Pflichten nach dem Gesetz hinzuweisen – gegebenenfalls in Form einer Beanstandung.

12.5 Beschlüsse der IFK

Im Rahmen des **Arbeitskreises Informationsfreiheit (AKIF)** und der Treffen der **Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK)** in Jena und Erfurt unter dem Vorsitz des Thüringischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit haben wir an mehreren Entschließungen mitgewirkt.

- **Mehr Transparenz und Open Data nach der Bundestagswahl!** (13.03.2025)

  https://www.datenschutzzentrum.de/uploads/ifk/Entschliessung_Bundestagswahl_13.03.2025.pdf

  Kurzlink: *https://uldsh.de/tb44-12-5a*

- **Abschaffung der Informationsfreiheit auf Bundesebene völlig falscher Weg!** (28.03.2025 als Pressemitteilung)

  https://www.datenschutzzentrum.de/uploads/ifk/20250328-PM_IFK.pdf

  Kurzlink: *https://uldsh.de/tb44-12-5b*

- **Protokolle der öffentlichen Sitzungen der Kommunalparlamente offenlegen!** (48. Sitzung am 18.06.2025 in Jena)

  https://www.datenschutzzentrum.de/uploads/informationsfreiheit/ifk/Entschliessung_48_IFK_Kommunalordnung.pdf

  Kurzlink: *https://uldsh.de/tb44-12-5c*

- **Transparenz bei Wahlleitungen klar regeln!** (48. Sitzung am 18.06.2025 in Jena)

  https://www.datenschutzzentrum.de/uploads/informationsfreiheit/ifk/Entschliessung_48_IFK_Wahlleiter.pdf

  Kurzlink: *https://uldsh.de/tb44-12-5d*

- **Privat finanzierte Forschung an Hochschulen muss transparenter werden!** (49. Sitzung am 26.11.2025 in Erfurt)

  https://www.datenschutzzentrum.de/uploads/informationsfreiheit/ifk/Entschliessung_49_IFK_Privat_finanzierte_Forschung_an_Hochschulen.pdf

  Kurzlink: https://uldsh.de/tb44-12-5e

Die **Protokolle und weiteren Informationen** zu den Sitzungen der IFK können hier abgerufen werden:

https://www.datenschutzzentrum.de/artikel/1347-Protokolle-der-Konferenz-der-Informationsfreiheitsbeauftragten-IFK.html

Kurzlink: *https://uldsh.de/tb44-12-5f*

Was ist zu tun?

Wir werden uns weiterhin intensiv in die Diskussionen und Entschließungen der IFK und dem zugehörigen Arbeitskreis einbringen.

13

KERNPUNKTE

Fortbildungen der DATENSCHUTZAKADEMIE

Schulkurse

Sommerakademie „Im Alarmmodus: Sicherheit und Datenschutz?“

13 DATENSCHUTZAKADEMIE Schleswig-Holstein

Die DATENSCHUTZAKADEMIE Schleswig-Holstein ist für die Konzeption und Organisation der Fortbildungsveranstaltungen zu den Themenbereich Datenschutz und Informationsfreiheit zuständig. Im Einklang mit der Datenschutz-Grundverordnung (DSGVO) wird so beispielweise den behördlichen und betrieblichen Datenschutzbeauftragten entsprechendes Fachwissen vermittelt.

13.1 Fortbildungsveranstaltungen im Programm der DATENSCHUTZAKADEMIE

Im Schulungsjahr 2025 hat sich die DATENSCHUTZAKADEMIE auf Grundlagenkurse in den folgenden Bereich konzentriert:

- behördlicher Datenschutz,
- betrieblicher Datenschutz
- Standard-Datenschutzmodell / Datenschutz-Folgenabschätzung,
- Datenschutz in der Personalverwaltung einer Behörde,
- technische Basiskenntnisse für Datenschutzbeauftragte.

Die Dauer der Fortbildungskurse lag bei einem Tag bis drei Tagen. Die Kurse im Bereich behördlicher und betrieblicher Datenschutz unterteilten sich in **rechtliche und technische Themen**. Die Teilnehmenden erlernten neue Inhalte und konnten sich untereinander vernetzen.

Die etablierten **Schulkurse „Entscheide DU – sonst tun es andere für Dich!"** erfreuen sich im Berichtszeitraum weiterhin großer Beliebtheit. **Mehr als 1.000 Schülerinnen und Schüler ab Klassenstufe 5** wurde vor Ort in ihren Schulen Datenschutz- und Medienkompetenz vermittelt. Der Fokus lag dabei u. a. auf dem Umgang mit ihren persönlichen Daten im Internet und in sozialen Medien.

Die aktuellen Fortbildungsveranstaltungen finden Sie unter dem folgenden Link:

https://www.datenschutzzentrum.de/akademie/

Kurzlink: https://uldsh.de/tb44-13-1a

13.2 Sommerakademie – jährliche Datenschutzkonferenz in Kiel

Die alljährlich an einem Montag im Spätsommer stattfindende Sommerakademie der DATENSCHUTZAKADEMIE stand im Jahr 2025 unter dem Motto **„Im Alarmmodus: Sicherheit und Datenschutz?"**. Teilnehmende aus dem gesamten Bundesgebiet haben den Weg nach Kiel gefunden, um über Datenschutz und Datensicherheit zu diskutieren.

Im Mittelpunkt stand das Verhältnis zwischen Sicherheit und Freiheit bezüglich der Befugnisse zur Überwachung. Aktuell schnürt die Politik **neue Sicherheitspakete in Bund und Ländern**. Es geht darin auch um zusätzliche Befugnisse zur Überwachung, beispielsweise auf Basis von biometrischer Gesichtserkennung oder verbunden mit dem Einsatz von künstlicher Intelligenz. Das

Verhältnis zwischen Sicherheit und Freiheit gehört zu den klassischen Grundthemen des Datenschutzes. Das Bundesverfassungsgericht und der Europäische Gerichtshof zeigen in ihren Entscheidungen immer wieder Grenzen auf, wenn der **Eingriff in die Grundrechte und Grundfreiheiten** überhandnimmt.

In der digitalisierten Welt mit Daten über jede und jeden und angesichts des fortwährenden Ausbaus von rechtlichen und technischen Überwachungsinstrumenten stellt sich die Frage, **wo die roten Linien verlaufen**. Unter welchen Bedingungen soll sich der Staat welcher Kontrollmöglichkeiten bedienen können? Wie kann es sein, dass verfassungs- oder europarechtswidrige Gesetze in Kraft treten? Vorgeschlagen wird ein Konzept zur Erfassung der Gesamtheit aller staatlichen Überwachungsmaßnahmen in Form einer **Überwachungsgesamtrechnung** – geht dies überhaupt und was ließe sich damit bewirken?

Es ist aber nicht nur der Staat: Auch Unternehmen installieren Überwachungswerkzeuge zur Kontrolle ihrer Beschäftigten oder werten Daten über das Verhalten von Nutzenden aus. Wieder spielt Sicherheit als Motiv für mehr Überwachung eine Rolle, denn zwingen nicht die neuen gesetzlichen Anforderungen im Bereich der Netz- und Informationssicherheit zu mehr Kontrolle? Ist der **Einsatz der fortschrittlichsten Überwachungstools** also quasi alternativlos? Und wie passt dies mit Datenschutzanforderungen wie dem Grundsatz der Datenminimierung zusammen?

Diesen Fragen gingen Expertinnen und Experten aus Praxis und Wissenschaft auf der Sommerakademie nach. Die Vorträge sind unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/sommerakademie/2025/

Kurzlink: https://uldsh.de/tb44-13-2a

Index

A

Abgeordnete **37**
Akkreditierung **115**
AnoMed **112**
Anonymisierung **48**, **76**, **92**, **94**, **112**
Arbeitskreis
  Datenschutz- und Medienkompetenz **65**
  Informationsfreiheit (AKIF) **136**
  Medien **104**
  Presse- und Öffentlichkeitsarbeit **20**
  Technik **91**
  Zertifizierung **116**
Ärztebewertung **59**
Auskunftspflicht **55**
  von Arztpraxen **58**
Auskunftsrecht
  bei Sportwetten **77**
  von Hinterbliebenen **56**
  von Kreditinstituten **55**
  von Patientinnen und Patienten **57**

B

Bankgeheimnis **55**
Beanstandungen
  Gemeinde Heikendorf **132**
  Gemeinde Malente **131**
Beschäftigtendaten **78**
Beschwerden **11**
Bildsymbole **10**
Bildung **62**
biometrische Gesichtserkennung **50**
Browser **121**, **122**
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) **23**
Bundesdatenschutzgesetz (BDSG) **17**, **23**
Bundesmeldegesetz (BMG) **42**
Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) **108**
Bürgerliches Gesetzbuch (BGB) **57**

C

CAPTCHA-Test **123**
CEH Expert Subgroup **116**
Chatkontrolle **128**
Chromium **122**
Confidential Cloud Computing **92**
Cookies **121**, **123**
Cyberresilienz-Verordnung (Cyber Resilience Act, CRA) **27**, **28**, **109**
Cybersicherheit by Design **27**

D

Datenminimierung **27**, **95**, **111**, **129**
Datenpannen **97**
  bei Schul-IT **43**
  bei Vollstreckungsankündigung **45**
  im Medizinbereich **60**
  in der Wirtschaft **81**
  in einer Hochschule **64**
  in Verbünden und verteilten Systemen **98**
  in Verwaltungs- und Büroräumen **45**
Datenschutz
  durch Technikgestaltung **52**
Datenschutz by Design und by Default **10**, **29**
DATENSCHUTZAKADEMIE Schleswig-Holstein **139**
Datenschutzbeauftragte **10**, **17**, **91**
  behördliche **41**
Datenschutz-Folgenabschätzung **108**
Datenschutzgremium **36**, **37**
Datenschutz-Grundverordnung (DSGVO) **10**, **29**, **68**, **70**, **81**, **85**, **90**, **110**
Datenschutzkompetenz **65**
Datenschutzkonferenz (DSK) **20**, **23**, **25**, **92**, **127**
Datenschutzreform **23**, **31**
Datenschutzverstöße **44**, **86**
DatenTRAFO **107**
Datenübermittlung in Drittländer **127**
Datenverordnung (Data Act) **14**, **15**, **109**

Department of Government Efficiency (DOGE) **9**
Deutsche Akkreditierungsstelle (DAkkS) **115**
digitale Souveränität **9**
digitaler Fitnesscheck **31**, **32**

E

Einwilligung **47**, **55**, **61**, **71**, **80**, **127**
elektronische Aufenthaltsüberwachung **50**
elektronische Fußfessel **50**
E-Mail **97**
  Phishing **97**
  Sozialdaten **56**
Ende-zu-Ende-Verschlüsselung **128**
Erweiterungs-API **122**
Europa **127**
Europäischer Datenschutzausschuss (EDSA) **92**, **115**, **117**
  Guidelines zu Pseudonymisierung und Anonymisierung **94**
Europäischer Gerichtshof (EuGH) **11**
European Health Data Space (EHDS) **112**

F

Facebook **71**, **104**
Fahrerlaubnisbehörde **47**
Festplatte **67**
Fingerprinting **121**
Firefox **122**
Föderale IT-Kooperation (FITKO) **92**
Föderale Modernisierungs-agenda **14**, **17**, **23**, **24**, **30**
Fotobox **82**

G

Geldbuße **86**, **87**
Gemeindeordnung **41**
Generalschlüssel **81**
Gesundheitsdaten **59**, **62**, **87**, **112**
Globales Satellitennavigationssystem (GPS) **74**
Google **122**
Grundrechte-Folgenabschätzung **108**

H

Halterdaten **69**
Herstellerverantwortung **27**, **29**, **30**, **32**, **108**, **109**
Human-in-the-Loop (HITL) **111**

I

Identifizierbarkeit **76**
Immigration and Customs Enforcement (ICE) **9**
Informationsfreiheit **9**, **13**, **23**, **37**, **131**
Informationspflichten **70**
Informationszugangsgesetz Schleswig-Holstein (IZG-SH) **13**, **131**
  neue Kostenverordnung **132**
International Transfer Subgroup (ITS) **116**
Internet **77**
Internet of Things (IoT) **108**
Internetrezension **59**, **87**
IoT-Geräte **108**
IT-Labor **121**
IT-Verbund Schleswig-Holstein (ITV.SH) **90**

J

JI-Richtlinie (EU 2016/680) **52**
Justiz **54**

K

Kennzeichenerfassung **70**
Key Provision Subgroup (KEYP) **116**
KI-Anwendungen **110**
KI-Fachgespräch „Frag' für 'nen Freund“ **100**
Kinderdatenschutz **32**
Kindertagesförderungsgesetz (KiTaG) **63**
Kindertagesstätte **62**
KI-Systeme **91**, **96**, **123**
  Prüfleitfaden **90**
KI-Verordnung (KI-VO) **30**, **90**, **108**, **110**
Koalitionsvertrag **23**, **24**
Konferenz der Informationsfreiheits-beauftragten in Deutschland (IFK) **136**
Konferenz der IT-Beauftragten (ITBK) **89**

Krankenhausinformationssystem (KIS) **61**, **62**
Kreditinstitut **55**, **86**
Kundendaten **73**, **86**

L

Landesdatenschutzgesetz (LDSG) **13**, **35**, **36**, **37**
Landesrechnungshof (LRH) **90**
Landesverfassungsschutzgesetz **54**
Landesverwaltungsgesetz **49**
Landtag **35**
Large Language Models (LLMs) **100**
Löschung **43**, **52**, **67**

M

Manifest v3 **122**
Medienkompetenz **65**
Medienstaatsvertrag (MStV) **103**
Meldungen **12**, **81**, **97**
Mobile Device Management (MDM) **44**
MS Office **89**
Müllanlage **71**

N

Netzwerk Medienkompetenz Schleswig-Holstein **65**
Neue Medien **103**
NIS-2-Richtlinie **27**

O

Omnibus-Verfahren **31**
Onlinezugangsgesetz (OZG) **90**, **91**
Open-Source-Produkte **89**
Ordnungsamt **78**
Orientierungshilfe
- KI-Systeme **96**
- RAG-Systeme **95**

Ortsbeiräte **42**
owi21 **52**
OWi-Verfahren **51**

P

Parlament **35**
Passwort **68**, **98**
Patientendaten **47**, **60**, **61**, **87**
Patientengeheimnis **56**
Patientenunterlagen **57**
Personalausweisgesetz (PAuswG) **69**
Personalausweiskopien **68**
Phishing **97**
Plattform Privatheit **32**, **107**
Polizei **49**, **50**
PostIdent-Verfahren **79**
Privacy-Enhancing Technologies (PETs) **107**
Produktdaten **14**, **15**
Projekte
- AnoMed **112**
- DatenTRAFO **107**
- Plattform Privatheit **32**, **107**
- SiKoSH **90**
- TRUMAN **110**
- Unboxing.IoT.Privacy **108**

Prüfpflichten **49**
Prüfungen **97**
Pseudonymisierung **92**, **94**, **112**

R

Recruiting-Videos **60**
Retrieval Augmented Generation (RAG) **95**
Rezepte **61**

S

Safari **122**
Satellitenortung
- Erreichbarkeit von Beschäftigten **73**
- Sicherheit auf Autobahnen **75**

Schuleingangsuntersuchung **42**
Schulgesetz **43**
Schul-IT **44**

Schwärzung **83**
Schweigepflicht **43**, **47**
Seniorenbeiräte **42**
SiKoSH **90**
Smart-Data-Verfahren **86**
Social Media **76**
Sommerakademie **139**
Sozialberichte **48**
Sozialdaten **56**
Sozialgesetzbuch (SGB) **55**
Sportwetten **77**
Standard-Datenschutzmodell (SDM) **92**, **96**
  SDM-Sonderedition (SE) **93**
  Unterarbeitsgruppe SDM (UAG SDM) **92**
Straßenverkehrsgesetz (StVG) **47**, **69**
Systemdatenschutz **89**

T

Technology Expert Subgroup (TECH ESG) **92**
Teilzeit- und Befristungsgesetz **46**
Telemetriedaten **75**, **92**
Tonaufzeichnung **81**
Tracking **73**, **122**
Transparenz **16**, **70**, **84**, **91**, **95**, **108**
Transponder **71**
TRUMAN **110**

U

Unabhängiges Landeszentrum für Datenschutz (ULD)
  Beratung **18**, **37**
  Informationsmaterialien **19**
  Öffentlichkeitsarbeit **19**
  Veranstaltungen **20**
Unboxing.IoT.Privacy **108**

V

Verfassungsschutz **49**
Verordnung über die Transparenz und das Targeting politischer Werbung (TTPW-VO) **15**, **16**
Verpixelung **83**, **123**
Versand
  von Arztbriefen **61**
  von Patientenunterlagen **57**
  von Sozialdaten **56**
  von Vollstreckungsankündigungen **45**
  von Willkommensbriefen **64**
Verwaltung **18**, **41**
Videoüberwachung **50**, **83**
  in Kleingärten **84**
  in Restaurants **86**
  in Taxis **85**
  von Beschäftigten **80**

W

Werbung **14**, **16**, **72**, **76**, **86**
Wirtschaft **67**

Y

YoungData **65**

Z

Zentrales IT-Management (ZIT SH) **89**
Zertifizierung **115**
  Prüfkriterienpapier **117**
Zugangsprotokollierung **72**
Zweckbindung **73**, **95**
Zwei-Faktor-Authentifizierung **98**

ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

Schleswig-Holsteins
Zentrum für Datenschutz
und Informationszugang

https://www.datenschutzzentrum.de/tb/