SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 19/3545**
19. Wahlperiode 18. Februar 2022

Bericht

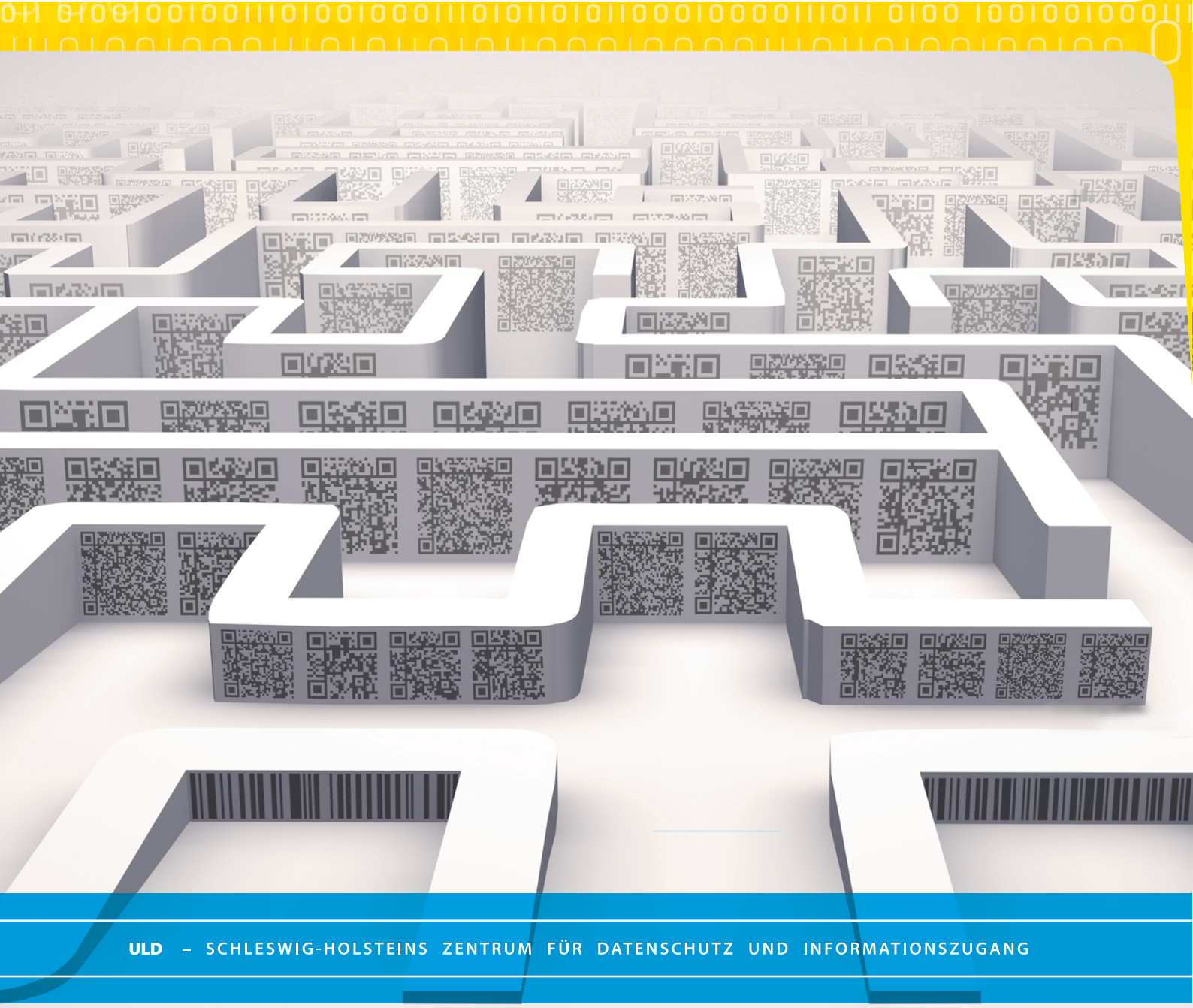
des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein

Tätigkeitsbericht 2022

ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

TÄTIGKEITSBERICHT
2022



ULD – SCHLESWIG-HOLSTEINS ZENTRUM FÜR DATENSCHUTZ UND INFORMATIONSZUGANG

Tätigkeitsbericht 2022
des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

BERICHTSZEITRAUM: 2021

REDAKTIONSSCHLUSS: 31.12.2021

LANDTAGSDRUCKSACHE 19/3545

(40. TÄTIGKEITSBERICHT DER LANDESBEAUFTRAGTEN FÜR DATENSCHUTZ)

Marit Hansen

Landesbeauftragte für Datenschutz 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

Umschlaggestaltung: Martin Papp, Eyekey Design, Kiel

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

Fotos:

Titelbild: ULD/stock.adobe.com

Umschlag innen: Hand: jannoon028@freepik.com

Inhaltsverzeichnis

01

KERNPUNKTE

Datenschutz in Zeiten der Pandemie
Zahlen und Fakten
Evaluierung der Datenschutzgesetze
Informationsfreiheit „by Design“

1 Datenschutz und Informationsfreiheit

Im Jahr 2021 ist viel passiert – auch im Bereich Datenschutz und Informationsfreiheit. Wie jedes Jahr stelle ich Ihnen die **wichtigsten Entwicklungen und interessante Fälle** vor, die Ihnen einen Einblick in die Arbeit des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) geben.

Eigentlich hätte man nun – mehr als drei Jahre nach Geltung der Datenschutz-Grundverordnung – erwarten können, dass die **Umsetzung von Datenschutzanforderungen zur Selbstverständlichkeit** geworden ist. Das müsste doch ebenso für die Behörden und Unternehmen im Land gelten wie für die globalen Konzerne, deren Produkte und Dienstleistungen auch in Europa verbreitet sind. Leider ist dies im europäischen Konzert der Aufsichtsbehörden noch nicht so gut gelungen, wie ich es mir erhofft hatte.

Defizite sehe ich auch im Punkt der Digitalisierung, die durch die Coronapandemie in Deutschland einen erheblichen Schub bekommen hat, weil beispielsweise Homeoffice, Videokonferenzsysteme und die E-Akte einen neuen Stellenwert erhalten haben. Doch ein Mehr an Digitalisierung ist noch nicht gleichbedeutend mit der Beherrschung der damit verbundenen Risiken. Hier fehlt es seit Jahrzehnten an der ausreichenden **Professionalisierung**, und das rächt sich jetzt. Die Auswirkungen sieht man z. B. an der gestiegenen Zahl der Datenpannenmeldungen an meine Behörde, die zu einem großen Teil mit nicht ausreichend geschützten IT-Systemen zu tun hatten.

Hier zeigen sich erhebliche Versäumnisse: Einerseits fehlt es aufseiten der Anwender in Behörden und Unternehmen an **Know-how und Bewusstsein über Risiken** und deren Beherrschung – und man darf schon dankbar über diejenigen sein, die über so viel Wissen und über definierte Abläufe verfügen, dass sie die festgestellten Verletzungen des Schutzes personenbezogener Daten an uns melden. Andererseits haben sich zahlreiche Anbieter in ihren Produkten oder Diensten auf **IT-Komponenten mit unklarem Sicherheits- oder Datenschutzniveau** verlassen.

Problem erkannt, Gefahr gebannt? Keineswegs. Diese Probleme sind nicht kurzfristig zu lösen, denn die **Komplexität heutiger IT-Systeme** steht in vielen Fällen einer adäquaten Beherrschung der Risiken entgegen. Es mag für viele wie ein Labyrinth an nur schwer zu durchschaubaren Regeln und technischen Komponenten wirken – so haben wir es auf dem Titelbild der Druckfassung dieses Berichts visualisiert.

Digitalisierung im Blindflug darf nicht passieren. Ich hoffe, dass die Erschütterungen in der IT-Community, die durch die sich häufenden bekannt gewordenen Sicherheitslücken ausgelöst wurden, dazu führen, dass Informationstechnik künftig zu einem besser kontrollierbaren Werkzeug wird. Zusätzlich gilt für das Systemdesign: Auch in puncto Datenschutzfunktionalität ist dringend nachzubessern.

Für die Verantwortlichen und Auftragsverarbeiter im Land bedeutet dies, ihr **Datenschutzmanagement** ernst zu nehmen und auf seine Wirksamkeit zu überprüfen.

Anregungen dazu finden Sie in diesem Bericht. Ich wünsche allen eine interessante Lektüre!

Marit Hansen

Landesbeauftragte für Datenschutz Schleswig-Holstein

1.1 Datenschutz in Zeiten der Pandemie

Rückblende: Im April 2020 veröffentlicht die Konferenz der unabhängigen Datenschutzaufsichtsbehörde des Bundes und der Länder die Entschließung **„Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie“:**

https://www.datenschutzkonferenz-online.de/media/en/Entschließung Pandemie 03_04_2020_final.pdf

Kurzlink: *https://uldsh.de/tb40-1-1*

Damals konnte wohl noch keiner ahnen, welchen Verlauf die Pandemie und die Debatten zu Bekämpfungsmaßnahmen nehmen würde. Die damals aufgeführten **Grundsätze gelten auch heute noch** in einer fortgeschrittenen Phase der Pandemie. Dass es einer Rechtsgrundlage für die Verarbeitung personenbezogener Daten bedarf. Dass die Eignung und die Erforderlichkeit der geplanten Maßnahmen kritisch zu überprüfen sind. Dass eine Zweckbindung wesentlich ist. Dass nicht mehr notwendige Daten unverzüglich zu löschen sind. Dass die Maßnahmen befristet sein sollten. Und dass Gesundheitsdaten gegen eine missbräuchliche Verwendung und vor Fehlern in der Verarbeitung zu schützen sind.

Aus Datenschutzsicht hat einiges ganz gut geklappt, aber vieles auch nicht. Fehlerfrei kommt wohl kaum ein Staat durch eine Pandemie. Doch es hakt immer noch an drei miteinander zusammenhängenden Punkten:

- Einbeziehung von **Datenschutzkompetenz** bereits bei der Planung der Maßnahmen,
- Klärung der vorhersehbaren **Praxisfragen** in Bezug auf eine etwaige Verarbeitung personenbezogener Daten, bevor neue Regelungen in Kraft gesetzt werden,
- **Bereitstellen von Hilfen** wie z. B. Musterdokumenten oder Informationsblättern.

In unserer täglichen Arbeit macht dies Probleme: Sobald neue Regeln erlassen wurden, prasseln auf uns Nachfragen ein, wie sie wohl gemeint sind: Welche Daten müssen von den Verpflichteten geprüft werden? Wie sind erfolgte Prüfungen zu dokumentieren? Dürfen oder müssen auf Nachfrage Daten herausgegeben werden, und wenn ja, an wen? Wann müssen Daten gelöscht sein?

Wir bemerken auf der einen Seite einen „Viel hilft viel“-Ansatz, bei dem die Verpflichteten vor Ort aus Angst, bei etwaigen Prüfungen der Ordnungsbehörden ihr korrektes Verhalten nicht belegen zu können, **(zu) viele Daten abfragen und speichern** – damit verstoßen sie aber häufig gegen das Datenminimierungsgebot des Datenschutzrechts und haben auch öfter Probleme, die Sicherheit der personenbezogenen Daten gewährleisten zu können. Auf der anderen Seite gibt es Verpflichtete, die **völlig überfordert** sind: sowohl von den Verpflichtungen aus Gründen des Pandemieschutzes als auch von Datenschutzfragen, die vorher bei ihnen gar keine Rolle spielten. Um hier Wildwuchs und Datenschutzverletzungen zu vermeiden, sind klare Regeln und vor allem Praxishinweise erforderlich.

Vor allem sollte man sich in der Gesetzgebung ebenso wie bei der Entwicklung von technischen Unterstützungswerkzeugen vor Augen führen, wie dies **ganz konkret in der Praxis funktionieren** soll. Gern unterstützen wir bei dieser Aufgabe im Rahmen unserer Zuständigkeit.

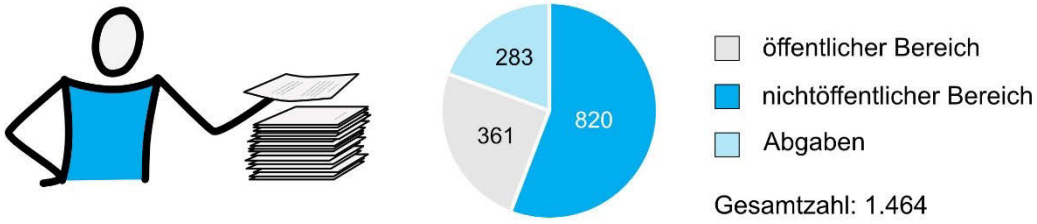
Was ist zu tun?

Gerade wegen der hohen Komplexität der Pandemieregeln und der großen Geschwindigkeit, in der sie verändert werden, darf die Praxistauglichkeit nicht vernachlässigt werden. Wir wünschen uns drei Dinge für die Zukunft: Datenschutzkompetenz einbeziehen – Praxisfragen der Datenverarbeitung vorab klären – Hilfestellung für die Umsetzung geben.

1.2 Zahlen und Fakten zum Jahr 2021

Die Anzahl der **Beschwerden** hat sich im Jahr 2021 **etwa auf demselben Stand** wie im Vorjahr eingependelt und ist nicht wieder auf das Niveau von 2019 zurückgegangen. Eine leichte Zunahme war für den nichtöffentlichen Bereich zu verzeichnen, während die Zahl bezüglich der Beschwerden über (vermutete) Datenschutzverstöße bei öffentlichen Stellen abnahm. Auffällig war allerdings, dass uns im Berichtsjahr **deutlich mehr Verletzungen des Schutzes personenbezogener Daten** gemeldet wurden. Somit sind die Zahlen der Datenpannenmeldungen seit Geltung der Datenschutz-Grundverordnung (DSGVO) kontinuierlich gestiegen. Im Folgenden sind die genauen Zahlen dargestellt:

2021 erreichten uns 1.464 schriftliche **Beschwerden** (Vorjahr: 1.497), von denen 283 (Vorjahr: 278) 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 musste



Zahl der bearbeiteten Beschwerden im Jahr 2021

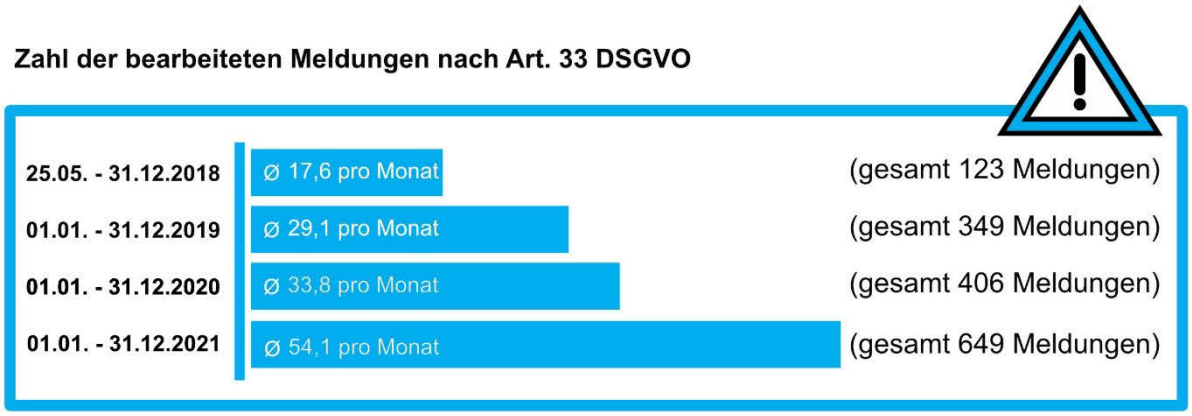
Da bei uns erhobene Beschwerden zunehmend einen grenzüberschreitenden Sachverhalt oder Verantwortliche in anderen Mitgliedstaaten betreffen, werden regelmäßig Fälle an die zuständigen Aufsichtsbehörden anderer Mitgliedstaaten zur alleinigen oder federführenden Bearbeitung abgegeben. Im Jahr 2021 betraf dies insbesondere die Aufsichtsbehörden in Frankreich, Malta und Schweden.

Insgesamt wurden in eigener Zuständigkeit 1.181 (Vorjahr: 1.219) Beschwerden bearbeitet, davon richteten sich **mehr als zwei Drittel der Beschwerden gegen Unternehmen** und andere nichtöffentliche Stellen (820; Vorjahr: 812), der Rest gegen Behörden (361; Vorjahr: 407). Dazu kamen 712 (Vorjahr: 808) Beratungen für den öffentlichen und den nichtöffentlichen Bereich.

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

Die Zahl von 649 (Vorjahr: 406) **gemeldeten Verletzungen des Schutzes personenbezogener Daten** nach Artikel 33 DSGVO, § 41 LDSG oder § 65 BDSG i. V. m. § 500 StPO (Datenpannen) ist im Vergleich zum Vorjahr um 60 % gestiegen. Das zeigt uns, dass vielen Verantwortlichen ihre Pflicht zur Datenpannenmeldung mittlerweile bekannt ist. Dennoch erfahren wir auch immer wieder von Datenpannen, bei denen die Verantwortlichen der Meldepflicht nicht nachgekommen sind.

Zahl der bearbeiteten Meldungen nach Art. 33 DSGVO



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

- 60 Warnungen (Vorjahr: 42),
- 51 Verwarnungen (Vorjahr: 50),
- 4 Anordnungen zur Änderung oder Einschränkung der Verarbeitung (Vorjahr: 13),
- 4 Geldbußen (Vorjahr: 0).

Nach unserem Eindruck wird die Dienststelle der Landesbeauftragten für Datenschutz in **Gesetzgebungsvorhaben** auf Landesebene weitgehend eingebunden, wenn Aspekte des Datenschutzes oder des Informationszugangs betroffen sein könnten. Dies geschah im Berichtsjahr über die Ministerien parallel zur Anhörung von Verbänden oder über die Ausschüsse im Landtag in 25 (Vorjahr: 25) neuen Gesetzgebungsvorhaben; ein Teil der Vorjahresbeteiligungen erstreckte sich zudem auf das Jahr 2021.

1.3 Schleswig-Holstein und die Digitalisierung

Digitalisierung ist ein **Schwerpunktthema** für uns – sowohl mit Blick auf den Datenschutz als auch auf die Informationsfreiheit. Die Landesbeauftragte für Datenschutz ist Mitglied im Beirat „KI@Gesellschaft“ (39. TB, Tz. 1.3) und steht mit ihrer Dienststelle zur Verfügung, um bei strategischen Planungen des Landes zu künstlicher Intelligenz, Open Source, digitaler Souveränität oder anderen Fragen der Digitalisierung zu beraten und dort Expertise einzubringen. Beispiele dafür finden sich in diesem Bericht, z. B. die Zusammenarbeit mit dem zentralen IT-Management (Tz. 6.1.1), Beratung im Bereich KI (Tz. 6.1.2) und Stellungnahmen zum Digitalisierungsgesetz (Tz. 6.1.4 und Tz. 12.1).

Im Ergebnis wird die Digitalisierung der Verwaltung und der anderen öffentlichen Bereiche unter dem Vorzeichen der digitalen Souveränität (39. TB, Tz. 2.1) zu einem Umbau führen, der zurzeit vorbereitet und behutsam umgesetzt wird. Dies ist nicht nur für Schleswig-Holstein relevant, sondern hier ist eine **länderübergreifende Kooperation** in verschiedenen Fach- und Infrastrukturverfahren sinnvoll, wie dies bereits praktiziert und vermutlich künftig eine noch größere Rolle spielen wird. Auch die jeweils beteiligten Datenschutzaufsichtsbehörden werden hier einen **Schulterschluss** suchen (Tz. 2.5).

Was ist zu tun?

Auf die Kompetenz des ULD sollte bei strategischen Planungen von Digitalisierungsprojekten weiterhin zurückgegriffen werden.

1.4 Evaluierungen der neueren Gesetze zu Datenschutz und Informationsfreiheit

Viele neue Gesetze enthalten mittlerweile **Evaluierungsklauseln**: Nach einer festgelegten Zeit sollen die Erfahrungen mit den jeweiligen Regeln abgefragt werden, und der Gesetzgeber kann auf dieser Basis im Bedarfsfall im Feinen nachjustieren oder in größerem Umfang Änderungen vornehmen.

Wie bereits im letzten Tätigkeitsbericht geschrieben, hat die **Evaluierung der DSGVO im Jahr 2020** den Anfang gemacht (39. TB, Tz. 1.4). Im Jahr 2021 stand die **Evaluierung des Bundesdatenschutzgesetzes** an. Auch die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, die täglich mit dem BDSG arbeiten, haben sich an der Evaluierung beteiligt.

Unsere gemeinsame Stellungnahme steht unter dem folgenden Link zur Verfügung:

https://www.datenschutzkonferenz-online.de/media/st/20210316_DSK_evaluierung_BDSG.pdf

Kurzlink: *https://uldsh.de/tb40-1-4a*

Das Bundesministerium des Innern und für Heimat, das für die Evaluierung zuständig war und dafür **Leitfragen in einem Fragebogen** bereitgestellt hatte, hat unseren Bericht und zahlreiche weitere Beiträge entgegengenommen. Die Zusammenfassung der Evaluierung durch das BMI ist hier verfügbar:

https://www.bmi.bund.de/SharedDocs/evaluierung-von-gesetzen/evaluierung-bdsg.html

Kurzlink: *https://uldsh.de/tb40-1-4b*

Im Ergebnis kommt das BMI zum Schluss, dass „die überwiegende Zahl der Regelungen des BDSG als sachgerecht, praktikabel und normenklar angesehen werden kann“. Es sollen aber zu einigen Regelungen **Klarstellungen**, Umformulierungen oder Anpassungen **geprüft** werden.

Liegt für das **Landesdatenschutzgesetz Schleswig-Holstein** eine ähnliche Situation vor? Im letzten Bericht hatten wir darauf hingewiesen, dass die gesetzlich vorgegebene Evaluierung ausstand. Das Ministerium für Inneres, ländliche Räume, Integration und Gleichstellung (MILIG) hat im Jahr 2021 eine **Befragung** durchgeführt, mit der Einschätzungen der maßgeblichen Rechtsanwender gesammelt wurden. Auch wir haben zu den Fragen und weiteren Punkten Stellung bezogen. Teile der Stellungnahme zum BDSG waren auch für das LDSG relevant, soweit sie sich auf Regelungen bezogen, die in beiden Gesetzeswerken gleich formuliert sind.

§ 16 IZG-SH

Die Landesregierung überprüft die Auswirkungen dieses Gesetzes mit wissenschaftlicher Unterstützung. Sie legt dem Landtag dazu in den Jahren 2020 und 2025 einen Bericht vor. Die oder der Landesbeauftragte für Datenschutz ist vor der Zuleitung der Berichte an den Landtag zu unterrichten; sie oder er gibt dazu eine Stellungnahme ab.

Fortschritte zur **Evaluierung des Informationszugangsgesetzes Schleswig-Holstein** (IZG-SH), die zum Jahr 2020 hätte durchgeführt werden sollen, sind uns nicht bekannt. Hier warten wir noch auf einen Bericht, zu dem wir dann eine Stellungnahme abgeben werden.

Eine Orientierung könnte die Evaluierung des rheinland-pfälzischen Landestransparenzgesetzes aus dem Jahr 2021 bieten (Landtag Rheinland-Pfalz, Drucksache 2018/678):

https://dokumente.landtag.rlp.de/landtag/drucksachen/678-18.pdf

Kurzlink: *https://uldsh.de/tb40-1-4c*

Zu bedenken ist aber bei der **Konzeption einer derartigen Evaluierung**, dass die dabei abgefragten Informationen oder Zahlen auch bei den Rechtsanwendenden – insbesondere den informationspflichtigen Stellen – verfügbar sind. Auch sollte nach Möglichkeit die Evaluierung selbst nicht einen zu großen Aufwand bei diesen Stellen auslösen. So kann es durchaus sein, dass die Evaluierungskonzepte aus anderen Bundesländern nicht auf Schleswig-Holstein übertragbar sind.

Schließlich ist ein weiterer Punkt zu etwaigen **Verbesserungspotenzialen in Gesetzen** hervorzuheben, der in den bisherigen Evaluierungen unter den Tisch fallen könnte. Denn Datenschutzregelungen finden sich nicht nur in den speziellen Datenschutzgesetzen wie DSGVO, BDSG oder LDSG, sondern spielen auch in anderen Gesetzgebungsprozessen auf Landesebene eine wesentliche Rolle. Dies gilt insbesondere dann, wenn **Öffnungs- oder Spezifikationsklauseln der DSGVO** genutzt werden sollen oder es sich um **Gesetzgebungsverfahren im Bereich Justiz und Inneres** handelt.

Wir beobachten, dass auch in Schleswig-Holstein dabei noch zu wenig die **Vorgaben des europäischen Datenschutzkonzepts und die dort eingeführte Terminologie** berücksichtigt werden. Wir haben im Berichtsjahr mehrfach auf dieses Problem hingewiesen, wenn wir zu Gesetzgebungsvorhaben angehört wurden – sind aber offensichtlich mit unseren Mahnungen nicht immer durchgedrungen. Nach unserer Auffassung ist damit **fraglich**, ob die **europarechtlichen Vorgaben** korrekt umgesetzt wurden, und es entstehen ebenso **Schutzlücken wie Regelungslücken**.

Das deutlichste Beispiel ist die **„Verarbeitung“**, die nunmehr zum Oberbegriff für alle Arten der Verarbeitung geworden ist und insbesondere die auch im Landesrecht noch häufig verwendeten Begriffe „Erhebung“, „Nutzung“, „Übermittlung“

und die vormals restriktiver definierte „Verarbeitung“ einschließt. Auch Begriffe wie **„pseudonymisiert“ oder „anonymisiert“** wurden früher in unserem Landesrecht teilweise in anderen Definitionen verwendet, als dies nach der Datenschutzreform der Fall ist.

Unser Appell: Im **Sinne der Rechtssicherheit** sollten die Gesetze auf etwaige Schutzlücken und Regelungslücken überprüft werden. Diese Arbeit ist nicht trivial – so reichen vielfach rein editorische oder kosmetische Änderungen nicht aus, wenn Gesetzesanpassungen anstehen. Doch andernfalls können Probleme aufseiten der Rechtsanwendenden oder der betroffenen Personen entstehen. Das gilt es zu vermeiden.

Was ist zu tun?

Hat der Gesetzgeber bestimmt, dass Evaluierungen vorzunehmen sind, müssen sie durchgeführt werden. Ein Praxischeck bei den Rechtsanwendenden ist in jedem Fall zu begrüßen, um Klarstellungen zu erreichen oder Hilfestellungen geben zu können. Die europäischen Vorgaben zum Datenschutz müssen in der Gesetzgebung berücksichtigt werden.

1.5 Informationsfreiheit „by Design“

Die Landesbeauftragte für Datenschutz ist in Schleswig-Holstein nicht nur für Datenschutz, sondern **auch für Informationsfreiheit** zuständig. Die gesetzlichen Aufgaben und Befugnisse unterscheiden sich stark, doch es gibt viele Bezugspunkte zwischen den Themen Datenschutz und Informationsfreiheit.

Die Diskussion zu Datenschutz „by Design“ läuft seit Mitte der 1990er Jahre und hat mit der Verankerung in Artikel 25 DSGVO an Sichtbarkeit gewonnen. Dahinter steckt die Erkenntnis, dass die **Gestaltung von Systemen einen erheblichen Einfluss auf die Umsetzbarkeit von Datenschutzanforderungen** hat. Werden Datenschutzgrundsätze von Anfang an und über alle Phasen der Systementwicklung berücksichtigt, ermöglicht oder vereinfacht es den Verantwortlichen und anderen Nutzenden, die rechtlichen Anforderungen zu befolgen und Pannen zu vermeiden (siehe Tz. 2.4).

Diese Erkenntnis lässt sich auf andere Anforderungen übertragen – wie beispielsweise auf die Informationsfreiheit. Dafür werben wir seit Jahren, und bereits 2019 haben wir dazu gemeinsam mit anderen Informationsfreiheitsbeauftragten einen Impuls gegeben: Das **Positionspapier „Informationsfreiheit by Design“ der 37. Konferenz der Informationsfreiheitsbeauftragten** (IFK) in Deutschland am 12. Juni 2019 in Saarbrücken ist unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/artikel/1317-.html

Kurzlink: *https://uldsh.de/tb40-1-5a*

Zu **Informationsfreiheit „by Design“** zählt die Gesamtheit technischer und organisatorischer Instrumente unter Berücksichtigung des Stands der Technik, die der Wahrnehmung und Erfüllung der Rechte nach den Informationsfreiheits- und Informationszugangsgesetzen, Umweltinformationsgesetzen und Transparenzgesetzen des Bundes und der Länder dienen.

Informationsfreiheit „by Design“ unterstützt einerseits **informationspflichtige Stellen** bei der Erfüllung eines beantragten Informationszugangs sowie bei der Umsetzung von Veröffentlichungspflichten, andererseits wird für **Antragstellende** der Informationszugang erleichtert.

Im Jahr 2022 werden wir uns verstärkt solchen technischen und organisatorischen Maßnahmen und Gestaltungsoptionen widmen und dies in unserer Beratungs- und Schulungspraxis einfließen lassen. Dies soll nicht nur ein regionales Thema für unser Bundesland bleiben, sondern als **Vorsitz der IFK** laden wir alle anderen Beauftragten für Informationsfreiheit des Bundes und der Länder ein, hieran mitzuwirken

(Tz. 12.5). Auch verwandte Themen wie die Erhöhung von Transparenz in algorithmischen Systemen oder die Rolle von Datentreuhändern im Sinne einer kontrollierten Datenfreigabe (siehe Tz. 8.4 zum Einwilligungsmanagement) werden wir behandeln. Am 12.09.2022 wird Informationsfreiheit „by Design“ das Thema unserer Sommerakademie sein (Tz. 13.2).

Auch die Bemühungen des Landes Schleswig-Holstein um **mehr Transparenz** unterstützen wir (38. TB, Tz. 1.5). Dies umfasst beispielsweise eine konstruktive Begleitung von Gesetz- und Verordnungsentwürfen in den Bereichen Transparenzportal und Open Data.

Transparenzportal:
https://www.schleswig-holstein.de/DE/Landesregierung/Themen/Digitalisierung/Transparenzportal/transparenzportal.html

Kurzlink: *https://uldsh.de/tb40-1-5b*

Open Data:
https://www.schleswig-holstein.de/DE/Landesregierung/Themen/Digitalisierung/openData/openData_node.html

Kurzlink: *https://uldsh.de/tb40-1-5c*

Was ist zu tun?

Das Land Schleswig-Holstein ist auf einem guten Weg für mehr Transparenz und Informationsfreiheit. Wir unterstützen dabei gern.

02

KERNPUNKTE

Spyware und Sicherheitslücken
Überwachungsgesamtrechnung
DSK 2.0
Beschäftigtendatenschutz

2 Datenschutz und Informationsfreiheit – global und national

Der Schwerpunkt unserer Arbeit liegt in Schleswig-Holstein – aber das bedeutet, auch die internationalen und nationalen Entwicklungen im Auge zu behalten, die unsere Bürgerinnen und Bürger betreffen. Was für uns im Jahr 2021 besonders bedeutsam war, ist hier zusammengefasst: Spyware und Sicherheitslücken (Tz. 2.1), Umsetzung der europarechtlichen Vorgaben (Tz. 2.2), Überwachungsgesamtrechnung (Tz. 2.3), ganzheitliche Systemgestaltung (Tz. 2.4), DSK 2.0 (Tz. 2.5) sowie Beschäftigtendatenschutz (Tz. 2.6).

2.1 Spyware und Sicherheitslücken

In Deutschland und teilweise auch im Ausland ist das Volkszählungsurteil von 1983 noch immer einigermaßen bekannt – im Gegensatz zu einem anderen Urteil des Bundesverfassungsgerichts, in dem das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität** (kurz: IT-Grundrecht) begründet wurde (BVerfG, Urteil des Ersten Senats vom 27.02.2008 – 1 BvR 370/07). Im Vordergrund steht die Frage, unter welchen Bedingungen eine heimliche Infiltration von IT-Systemen erlaubt sein kann.

Der wichtige Punkt ist hierbei: Schon im Jahr 2008 hat das Bundesverfassungsgericht deutlich gemacht, wie wichtig die Gewährleistung von Vertraulichkeit und Integrität in der von uns Menschen eingesetzten Technik ist. In der Zwischenzeit sind die Abhängigkeiten von erwartungsgemäß funktionierender Informationstechnik wesentlich größer geworden. Die heutige enorme **Bedeutung von Smartphones oder Plattformen im Internet** für die persönliche Kommunikation und für alle möglichen Situationen des täglichen Lebens – man denke nur an die Nutzung zahlreicher Apps – ließ sich damals kaum erahnen. Und dennoch spricht das Urteil eine klare Sprache und ist heute **aktueller denn je**.

Umso einschneidender sind die Debatten um **Hintertüren in Software** oder **Umgehen von Verschlüsselung.** Und es bleibt nicht bei Worten, sondern die Taten sind nicht wegzudiskutieren. Dazu gehören die Erkenntnisse der geheimdienstlichen Überwachung, die dank Edward Snowden im Sommer 2013 bekannt wurden. Oder, wie im Berichtsjahr bekannt wurde, der Einsatz einer Überwachungssoftware namens „Pegasus“, über die Menschen auf der ganzen Welt ausspioniert wurden. Der Hersteller von „Pegasus“, die israelische NSO Group, rechtfertigte sich damit, dass die Software nur zum Zwecke der Bekämpfung von Terrorismus und Kriminalität verkauft würde.

Von der **Website der NSO Group** (https://www.nsogroup.com/):

NSO creates technology that helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe.

Wirklich? Die Aufklärung durch das „Pegasus-Projekt“, an dem mehr als 80 Journalistinnen und Journalisten in zehn Ländern mitgearbeitet haben, zeigte ein anderes Bild: Demnach gehörten zu den **überwachten Personen auch Rechtsanwältinnen und Rechtsanwälte, Oppositionelle, Politikerinnen und Politiker, Geschäftsleute und Pressevertreterinnen und -vertreter.** Auch in der EU ist die Überwachungssoftware nachweisbar zum Einsatz gekommen.

Die neue Bundesregierung kennt das IT-Grundrecht des Bundesverfassungsgerichts. Im Koalitionsvertrag wird versprochen:

Aus dem Koalitionsvertrag 2021–2025:

Für den Einsatz von Überwachungssoftware, auch kommerzieller, setzen wir die Eingriffsschwellen hoch und passen das geltende Recht so an, dass der Einsatz nur nach den Vorgaben des Bundesverfassungsgerichtes für die Online-Durchsuchung zulässig ist.

Eigentlich eine Selbstverständlichkeit, dass das geltende Recht nicht gegen die Vorgaben des Bundesverfassungsgerichts verstößt! Und das Problem liegt tiefer: Es gibt einen Markt für Überwachung, Firmen bieten weltweit ihre Spyware an und die eingesetzte Informationstechnik ist **anfällig für Überwachung im großen Stil.**

Die Idee, dass **Hintertüren** eingebaut werden, die nur „für die Guten" zur Verfügung stehen, hat noch nie funktioniert. Für eine ernsthafte, vertrauenswürdige und zuverlässige Digitalisierung, die unserer demokratischen Gesellschaft Nutzen bringt, brauchen wir ein **stabiles und kein brüchiges Fundament** in der Informationstechnik.

Was ist zu tun?

Es gilt, die Sicherheit zu erhöhen und insbesondere der Kultivierung von Sicherheitslücken und den Forderungen nach Hintertüren in der IT eine klare Absage zu erteilen. Deutschland sollte dies auch in europäischen und internationalen Rechtsetzungsverfahren und Standardisierungen deutlich vertreten.

2.2 Umsetzung der europarechtlichen Vorgaben zum Datenschutz

Den **25. Mai 2018** werden Datenschützer nicht so schnell vergessen, denn an dem Tag erlangte die **Datenschutz-Grundverordnung** (Verordnung (EU) 2016/679) Geltung und bis zu dem Tag waren auch Regelungen des Bundes- und Landesdatenschutzrechts anzupassen, soweit dies die europäische Richtlinie (EU) 2016/680 für den Bereich Justiz und Inneres betraf. Einige vertreten die Ansicht, dass sich für Deutschland gar nicht viel geändert hätte. Das ist insoweit nicht falsch, als Behörden und Unternehmen häufig schon eine gewisse Vorstellung vom Thema Datenschutz hatten. Auch das Instrument der Datenschutzbeauftragten im Unternehmen oder in öffentlichen Stellen war in Deutschland bekannt und überwiegend geschätzt. Wer bereits ein **Datenschutzmanagement** bei sich in der Organisation etabliert hatte, war auch gut dafür aufgestellt, die Änderungen aus Europa aufzunehmen und umzusetzen.

Dennoch ist ein vollständiges Durchdringen des Datenschutzrechts sowohl für diejenigen, die mit dem „alten BDSG" vertraut waren, als auch für Neulinge in dem Thema nicht simpel. Das liegt zum einen daran, dass die **nationalen Rechtsauslegungen und Begriffe** nicht immer auch der europäischen Auslegung entsprechen. Zum anderen sind die Datenschutzregeln mit dem Ziel einer Technikneutralität und einer gewünschten Robustheit für viele Jahre formuliert worden und weisen daher notgedrungen einen **hohen Abstrahierungsgrad** auf.

Durch die mittlerweile entwickelten Muster und Orientierungshilfen fällt zwar die Einhaltung der Datenschutzanforderungen bei Standarddatenverarbeitungen üblicherweise nicht schwer, doch für **Spezialfragen** kann es komplex werden. So komplex, dass auch Gerichte in den Mitgliedstaaten der EU dem Europäischen Gerichtshof (EuGH) Fragen zur Klärung im Sinne einer einheitlichen europäischen Anwendung vorlegen. Ende 2021 waren beim EuGH mehr als 30 solcher Vorabentscheidungsersuchen von Gerichten aus den Mitgliedstaaten, in denen jeweils mehrere Fragen gestellt waren, anhängig, die der EuGH in der nächsten Zeit beantworten wird. Aus Deutschland kommen besonders viele Fragen, aber es liegen auch **Vorabentscheidungsersuchen** aus den Ländern Belgien, Bulgarien, Finnland, Lettland, Litauen, Luxemburg, Niederlande, Österreich, Rumänien, Schweden und Ungarn vor.

In mehreren Verfahren zur neuen Rechtslage hat der EuGH bereits entschieden. Prominent ist das unter dem Namen **„Schrems II"** bekannte Urteil des EuGH vom 16.07.2020 (Rechtssache C-311/18), in dem der „Privacy Shield" (Beschluss 2016/1250) der Europäischen Kommission zur Übermittlung personenbezogener Daten in die USA für unwirksam erklärt wurde (39. TB, Tz. 2.5). Der EuGH betont, dass bei einem grenzüberschreitenden Datenverkehr ein angemessenes Datenschutzniveau beim Empfänger bestehen muss, was durch den Privacy Shield nicht garantiert war.

Die Datenschutzaufsichtsbehörden in Europa hatten schnell auf das Urteil reagiert und ausgearbeitet, welcher **ergänzenden Maßnahmen** („Supplementary Measures“) es bei einem geplanten Drittstaatentransfer bedarf, der sich beispielsweise auf Standardvertragsklauseln oder auf aufsichtsbehördlich genehmigte „Binding Corporate Rules“ (verbindliche interne Datenschutzvorschriften) stützen könnte. Nach der Veröffentlichung der Leitlinien im Sommer 2020 wurde eine öffentliche Konsultation durchgeführt. Nach Auswertung der eingehenden Stellungnahme wurde die überarbeitete finale Fassung im Juni 2021 bereitgestellt:

https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de

Kurzlink: *https://uldsh.de/tb40-2-2a*

Ebenfalls im Juni 2021 stellte die EU-Kommission **neu gefasste EU-Standarddatenschutzklauseln** vor:

https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

Kurzlink: *https://uldsh.de/tb40-2-2b*

In einer Pressemitteilung hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder klargestellt, dass auch bei Verwenden der neuen EU-Standardvertragsklauseln eine **Prüfung der Rechtslage im Drittland und zusätzlicher ergänzender Maßnahmen erforderlich** ist:

https://www.datenschutzkonferenz-online.de/media/pm/2021_pm_neue_scc.pdf

Kurzlink: *https://uldsh.de/tb40-2-2c*

Für weitere Leitlinien, die die Beziehung zwischen dem räumlichen Anwendungsbereich (Artikel 3 DSGVO) und den Regeln zum grenzüberschreitenden Datentransfer betreffen, lief Ende 2021 noch die Konsultationsphase:

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_de

Kurzlink: *https://uldsh.de/tb40-2-2d*

Im Ergebnis bedeutet dies: Das EuGH-Urteil muss umgesetzt werden. Doch wenn der geplante Empfänger im Drittland kein **angemessenes Datenschutzniveau** gewährleisten kann, darf der Transfer der personenbezogenen Daten nicht stattfinden.

Auch heute noch finden wir immer **Datenschutzerklärungen** auf Webseiten, die sich auf den Privacy Shield beziehen oder auch sonst nicht erkennen lassen, dass der Verantwortliche bei dem von ihm beschriebenen Datentransfer die neue **Rechtslage** kennt und die nötigen Prüfungen vorgenommen hat. Dies ist zumindest ein Indiz für ein nicht funktionierendes **Datenschutzmanagement**. Hier ist dringend Abhilfe geboten.

Was ist zu tun?

Die europarechtlichen Vorgaben müssen umgesetzt werden. Das betrifft auch den Einsatz von Produkten und die Nutzung von Dienstleistungen in der EU. Wo dies nicht der Fall ist, müssen die Verantwortlichen gegebenenfalls Änderungen bei den Herstellern bzw. Anbietern einfordern oder datenschutzkonforme Alternativen einsetzen.

2.3 Gesetzgebung unter dem Vorzeichen einer Überwachungsgesamtrechnung

Das Bundesverfassungsgericht hat im Urteil vom 02.03.2010 – 1 BvR 256/08 zur Vorratsdatenspeicherung ausgeführt, die „Freiheitswahrnehmung der Bürger“ dürfe „nicht total erfasst und registriert werden“. Die Einführung der Vorratsdatenspeicherung zwinge den Gesetzgeber „**in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen**

zu größerer Zurückhaltung“. Das war eine Alarmleuchte zur Begrenzung der zunehmenden Datensammlungen aus Gründen der Sicherheitspolitik.

Gibt es also eine **rote Linie**, die ein Staat nicht überschreiten darf, weil es dann zu viel wird mit den Datensammlungen? Und muss man nicht das Thema im weiteren Sinne betrachten: also nicht nur den Fokus auf Datensammlungen beschränken, sondern sich insgesamt Gedanken über ein mögliches Übermaß an Überwachung machen? Besonders spannend ist aber die Frage, was diese Überlegung für die Praxis der bestehenden und entstehenden Sicherheitsgesetze mit Regelungen zu einer Überwachung bedeuten soll, die es auf den Ebenen des Bundes, der einzelnen Länder oder auch im internationalen Kontext gibt. Vorgeschlagen – und nun auch im Koalitionsvertrag der Bundesregierung aufgenommen – ist eine Evaluation der Sicherheitsgesetze, die in eine **Überwachungsgesamtrechnung** einfließt.

Dies soll zunächst einen besseren Überblick über die möglichen Auswirkungen auf die Rechte und Freiheiten ermöglichen. „Rechnung“ – das klingt nach einer exakten Matheformel, als ob man einen numerischen Schwellwert definieren und exakt berechnen könnte, der zum Ausdruck bringt, ob mit dem nächsten verabschiedeten Sicherheitsgesetz eine **rote Linie überschritten** wäre. Oder ob dies schon geschehen ist.

Mehrere Forschungsgruppen sind in den vergangenen Jahren dieser Frage nachgegangen, darunter auch das Forum Privatheit (Tz. 8.1) mit unserer Beteiligung. Die Idee der Überwachungsgesamtrechnung ist aus unserer Sicht spannend, auch wenn viele **Fragen der Implementierung** zu klären wären, z. B. welche Rechtsbereiche umfasst sein sollten, ob auch herausgabepflichtige oder beschlagnahmefähige Datensammlungen Privater einzubeziehen sind, ob allein der Gesetzestext oder auch die konkrete Praxis auszuwerten ist und ob Effekte der grenzüberschreitenden Zusammenarbeit einbezogen werden sollen. Nach unserer Auffassung würde allerdings ein **pseudo-mathematischer Ansatz eine Objektivität lediglich vortäuschen** und könnte sogar zu einer überschießenden Legitimierung neuer Sicherheitsgesetze – also einem **Whitewashing** – missbraucht werden.

Aus dem Koalitionsvertrag 2021–2025:

Die Eingriffe des Staates in die bürgerlichen Freiheitsrechte müssen stets gut begründet und in ihrer Gesamtwirkung betrachtet werden. Die Sicherheitsgesetze wollen wir auf ihre tatsächlichen und rechtlichen Auswirkungen sowie auf ihre Effektivität hin evaluieren. Deshalb erstellen wir eine **Überwachungsgesamtrechnung** und bis spätestens Ende 2023 eine unabhängige wissenschaftliche Evaluation der Sicherheitsgesetze und ihrer Auswirkungen auf Freiheit und Demokratie im Lichte technischer Entwicklungen. Jede zukünftige Gesetzgebung muss diesen Grundsätzen genügen. Dafür schaffen wir ein unabhängiges Expertengremium (Freiheitskommission), das bei zukünftigen Sicherheitsgesetzgebungsvorhaben berät und Freiheitseinschränkungen evaluiert.

In jedem Fall sollten Ansätze, die ein Korrektiv darstellen können, in den **Instrumentarien für Gesetzgeber** bei der Arbeit zur Überwachungsgesamtrechnung diskutiert werden. Dazu gehören beispielsweise Befristungen von möglicherweise kritischen Regelungen, Festlegungen von Zugriffsbeschränkungen und Zweckbindungen, der Richtervorbehalt, Klarstellungen bezüglich des Kernbereichs betroffener Personen, Verwertungsverbote, verstärkte Transparenz- und Informationspflichten gegenüber betroffenen Personen (z. B. mit Kontrollquittungen oder Benachrichtigungen (siehe 37. TB, Tz. 4.3.4)), eine verpflichtende **Gesetzes-(Datenschutz-)Folgenabschätzung,** Vorschriften zur wissenschaftlichen Evaluation mit klaren Kriterien oder auch die Einführung von Kontrollgremien. Der letzte Punkt findet sich als **„Freiheitskommission“** im Koalitionsvertrag der Bundesregierung.

Was ist zu tun?

Wir werden die Arbeiten zur Überwachungsgesamtrechnung interessiert verfolgen und auf die Relevanz für und Übertragbarkeit auf das Land Schleswig-Holstein auswerten.

2.4 Ganzheitliche Systemgestaltung für Datenschutz und Informationsfreiheit

Eingebauter Datenschutz bei der Systemgestaltung: Zwar noch keine Selbstverständlichkeit, aber die DSGVO hat die Weichen dafür gestellt. In den nächsten Jahren wird – so hoffen wir – dies nicht mehr die Ausnahme sein, sondern sich mehr und mehr in der Praxis und auf dem Markt durchsetzen. Bei Informationsfreiheit (siehe Tz. 1.5, Tz. 13.2) streben wir ebenfalls an, dass „by Design“ zu einem Standardkriterium für die Entwicklung wird. Geht das denn überhaupt: **sowohl Datenschutz als auch Informationsfreiheit bei der Systemgestaltung** von Anfang an zu berücksichtigen?

In der Tat gibt es **zahlreiche Spannungsfelder** bei der Entwicklung von Systemen. Das ist auch gar nichts Ungewöhnliches. Gerade in den Bereichen Datenschutz und Informationsfreiheit kennt man die Situation, dass unterschiedliche öffentliche und private Interessen gegeneinander abgewogen werden müssen. Auch muss stets eine Ausstrahlung auf andere Rechtsgebiete im Blick gehalten werden. Außerdem spielen häufig Anforderungen, die nicht rechtlich im selben Maße festgeschrieben sind, eine Rolle, um eine faire und verträgliche Gestaltung von Systemen zu erreichen.

Müssen nun die Datenschutz- oder Informationsfreiheitsbeauftragten – und sämtliche Systementwicklerinnen und -entwickler – über ihren jeweiligen Tellerrand schauen und quasi zu Universalgelehrten werden, um jeder möglichen Anforderung samt etwaiger Interdependenzen und Auswirkungen Rechnung zu tragen? Das ist wohl nicht möglich. Aber möglich ist es, sich etwaiger Gegensätze bewusst zu werden und Wege zu suchen, damit eine **datenschutzkonforme Verfahrensgestaltung nicht in einen unauflösbaren Widerspruch zu anderen wichtigen Erwägungen gerät**. Es lohnt sich also nicht nur, die Best Practices als Musterbeispiele für eine der wichtigen Anforderungen zu propagieren, sondern gleichermaßen den Blick zu weiten, um zumindest naheliegende Konfliktlinien zu identifizieren und Lösungen zu suchen.

Typische vermeintliche (aber doch oft auflösbare) Gegensätze werden uns immer wieder in den Bereichen „Datenschutz und Sicherheit“ (siehe auch Tz. 2.3), „Datenschutz und Freiheit“ und „Datenschutz und Nutzbarkeit“ genannt. Auch können Wechselwirkungen mit Informationsfreiheit, Umweltschutz, Datenzugang, Forschung, Wirtschaftlichkeit oder etwa Kartellrecht bestehen.

Das Oberthema für die Gestaltung von Systemen ist **„Fairness und Vertrauenswürdigkeit by Design“**. Dies betrifft nicht nur die Entwicklung informationstechnischer Systeme, sondern auch den Bereich der rechtlichen oder technischen Normgebung. Außerdem geht es darum, die Kluft zwischen Forschung und Praxis zu überbrücken: Neue Erkenntnisse müssen kurzfristig in der Gesetzgebung und Normierung ankommen, taugliche Lösungsansätze müssen schneller bekannt und nutzbar gemacht werden, um den Stand der Technik voranzubringen. Und vor allem ist der interdisziplinäre Diskurs und eine Folgenabschätzung wichtig, damit alle wesentlichen Aspekte Eingang finden und unerwünschte Effekte nach Möglichkeit vermieden werden.

Was ist zu tun?

Mit der zunehmenden Digitalisierung wird deutlich, dass Fairness und Vertrauenswürdigkeit im Systemdesign eine größere Rolle spielen müssen. Wir werden dazu unsere Impulse in den notwendigen gesellschaftlichen Diskurs geben und im uns möglichen Rahmen Forschung und Praxis unterstützen.

2.5 DSK 2.0

DSK – das ist die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Hier diskutieren die Behördenvertreterinnen und -vertreter Fachfragen, treffen Festlegungen oder veröffentlichen Beschlüsse. Die

DSK ist sozusagen das deutsche **Pendant zu dem Europäischen Datenschutzausschuss (EDSA**), in dem die Vertreterinnen und Vertreter der Mitgliedstaaten zusammenkommen. Mit einem wesentlichen Unterschied: Die Datenschutz-Grundverordnung regelt diese europäische Zusammenarbeit, beschreibt das Kohärenzverfahren zur einheitlichen Anwendung der DSGVO bis hin zur Streitbeilegung (siehe Kapitel VII der DSGVO). Eine derartige gesetzliche Regulierung gibt es für die deutsche DSK nicht.

Das bedeutet aber nicht, dass nicht ebenfalls zusammengearbeitet und Kohärenz angestrebt wird. Bereits im letzten Tätigkeitsbericht haben wir den **Arbeitskreis „DSK 2.0“** erwähnt (39. TB, Tz. 2.3). Dieser Arbeitskreis zielt darauf ab, die Potenziale zur Fortentwicklung der DSK und des Austausches zwischen den Datenschutzaufsichtsbehörden auszuloten und gegebenenfalls Vorschläge für eine Neugestaltung zu erarbeiten.

Mit Interesse haben wir im Koalitionsvertrag der Bundesregierung gelesen, dass eine Institutionalisierung der Datenschutzkonferenz im BDSG geplant ist.

Aus dem Koalitionsvertrag 2021–2025:

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

Gerne bringen wir uns ein, um das Ideenkorsett auf Bundesebene mit auch für die Länder praxistauglichen Lösungen zu füllen.

Wir müssen aber nicht auf Änderungen im BDSG warten, um die heutige vertrauensvolle Kooperation in der DSK fortzusetzen und in konkreten Fällen beispielsweise auf das Instrument der Amtshilfe (Art. 57 Abs. 1 Buchst. g DSGVO) zurückzugreifen. Im Zertifizierungsbereich, der alle Behörden betrifft, haben wir zudem im Jahr 2020 eine Verwaltungsvereinbarung (39. TB, Tz. 9.2) abgeschlossen, die u. a. die Möglichkeit der gegenseitigen Unterstützung für Genehmigungen von Zertifizierungskriterien umfasst.

2.6 Beschäftigtendatenschutz – neuer Anlauf?!

Digitalisierung verändert die Arbeitswelt (siehe auch Tz. 8.2). Die **Interessen der Beschäftigten** und die **Interessen der Arbeitgeber** sind oft nicht deckungsgleich, auch nicht im Bereich Datenschutz. Wie sieht ein fairer Ausgleich zwischen diesen Interessen aus? Wie lässt sich ein wirksamer Datenschutz im Arbeitsleben in der Praxis umsetzen?

Man könnte meinen, es wäre eine unendliche Geschichte: die **Diskussion über das Ob und Wie eines Beschäftigtendatenschutzgesetzes**. Die (Dienst-)Ältesten im Datenschutz erinnern sich an Debatten, die vor mehreren Jahrzehnten stattgefunden haben, und ein paar mehr Leute kennen noch Entwurfsfassungen wie aus dem Jahr 2010, der sogar von der Bundesregierung beschlossen und in den Bundestag eingebracht, aber nie verabschiedet wurde. Als später ein neuer Bundestag gewählt wurde und die nächste Legislaturperiode begann, war der alte Entwurf Makulatur, d. h., er wurde nicht erneut eingebracht.

Mit der Datenschutz-Grundverordnung wurden die Karten neu gemischt. In jedem Fall können auch die Beschäftigten ihre Datenschutzrechte nach der DSGVO wahrnehmen. Insgesamt sind aber die Situationen der Arbeitswelt nicht vollständig mit dem europäischen Gesetzeswerk geregelt, sondern die DSGVO lässt dem **nationalen Gesetzgeber einigen Spielraum**.

Art. 88 Abs. 1 DSGVO

Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext […] vorsehen.

In dieser Situation hatte die vorherige Bundesregierung eine Expertenkommission beim Bundesministerium für Arbeit und Soziales zur Fortentwicklung des Beschäftigtendatenschutzes installiert, in die auch die Landesbeauftragte für Datenschutz Schleswig-Holstein berufen wurde (39. TB, Tz. 2.4). In intensiven Diskussionen

wurden Thesen und Empfehlungen erarbeitet, die pandemiebedingt jedoch verzögert fertiggestellt und so erst im Januar 2022 an den Bundesarbeitsminister übergeben werden konnten.

Diese Empfehlungen enthalten nicht nur **Vorschläge für gesetzliche Regelungen und rechtliche Konkretisierungen** für ein Mehr an Rechtssicherheit und einen effektiven Datenschutz, sondern nehmen auch **weitere Instrumente** in den Blick, die für die verschiedenen beteiligten Akteure – Arbeitgeber, Beschäftigte, Personalvertretungen, Gewerkschaften, Datenschutzbeauftragte, Aufsichtsbehörden und das Bundesministerium für Arbeit und Soziales – relevant sein können. Dazu gehören die Unterstützung von Best-Practice-Ansätzen, Veröffentlichung von Musterdokumenten, Selbstaudits zur regelmäßigen Bestandsaufnahme des Datenschutzniveaus in der Organisation, Bereitstellung von Datenschutz-Prüfkriterien für Auswahl und Einsatz sowie Hilfestellungen für Datenschutz „by Design“ und „by Default“ für informationstechnische Systeme, die im Arbeitsleben eine Rolle spielen können.

Einen Gesetzentwurf hat die Expertenkommission nicht vorgelegt. Das ist vielleicht sogar ganz gut, denn das Dokument mit den Thesen und Empfehlungen, dessen Erarbeitung die vorherige Bundesregierung in Auftrag gegeben hatte, wird nun nicht dasselbe Schicksal erleiden wie der Gesetzentwurf aus dem Jahr 2010. Im Gegenteil: Da der Koalitionsvertrag der 2021 gewählten Bundesregierung das Thema Beschäftigtendatenschutz auf ihre Agenda gesetzt hat, kann es nun **mit neuem Schwung** behandelt werden.

Aus dem Koalitionsvertrag 2021–2025:

Wir schaffen **Regelungen zum Beschäftigtendatenschutz**, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen.

Nach der Veröffentlichung der Dokumente der Expertenkommission zum Beschäftigtendatenschutz werden wir auf unserer Webseite darauf hinweisen.

Was ist zu tun?

Die Empfehlungen zum Beschäftigtendatenschutz sollten sowohl bei Gesetzgebungsverfahren für diesen Bereich als auch bei Überlegungen für Verbesserungen in der Praxis einfließen.

03

KERNPUNKTE

Datenschutzgremium

Service für Abgeordnete zu Datenschutz und Informationsfreiheit

3 Landtag

Für den Datenschutz im parlamentarischen Bereich ist das Datenschutzgremium zuständig, an dessen Sitzungen die Landesbeauftragte für Datenschutz mit Gaststatus teilnimmt (Tz. 3.1). Bewährt hat sich die Möglichkeit für die Abgeordneten des Schleswig-Holsteinischen Landtages, sich bei uns zu allen auftretenden Datenschutz- und Informationsfreiheitsfragen beraten zu lassen (Tz. 3.2).

3.1 Datenschutzgremium

Manchmal erreichen uns Anfragen zu Sachverhalten, die Verarbeitungen personenbezogener Daten betreffen, die in **Wahrnehmung parlamentarischer Aufgaben** geschehen. Die Landesbeauftragte für Datenschutz mit ihrer Dienststelle ist für die Aufsicht in diesem Bereich allerdings nicht zuständig. So ist es im Landesdatenschutzgesetz (LDSG) geregelt.

> **§ 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.

Aus diesem Grund geben wir solche Anfragen an das zuständige Kontrollgremium weiter, das sich in seinen regelmäßigen Sitzungen mit solchen Fragen oder Beschwerden sowie aktuellen Themen beschäftigt: das **Datenschutzgremium des Schleswig-Holsteinischen Landtages**. Mitglieder des Datenschutzgremiums sind Repräsentanten jeder im Landtag vertretenen Fraktion oder Gruppe. Die Landesbeauftragte für Datenschutz nimmt als Gast an den Sitzungen teil.

Zu den Themen, mit denen sich das Datenschutzgremium beschäftigt hat, gehören die möglichen Auswirkungen des Urteils des Europäischen Gerichtshofs (EuGH) vom Juli 2020 (39. TB, Tz. 3.1). Demnach ist der **Petitionsausschuss des Hessischen Landtages** *„insoweit, als dieser Ausschuss allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet, als ‚Verantwortlicher' im Sinne von Art. 4 Nr. 7 der Verordnung 2016/679 einzustufen"* (EuGH, Urteil vom 09.07.2020, C-272/19). In dem vorliegenden Fall ging es um ein Auskunftsersuchen eines Petenten nach Artikel 15 DSGVO. Nun ergeben sich Fragen nach möglichen Auswirkungen des Urteils auf Parlamente und ihre Gremien in Bund und Ländern sowie in den anderen Mitgliedstaaten der EU. Von dieser möglichen Ausstrahlung über den eigentlich entschiedenen Sachverhalt hinaus hängt es ab, ob in Schleswig-Holstein rechtliche Anpassungen zur Klarstellung wünschenswert oder notwendig sind. Zu diesem Punkt steht man im Austausch mit Zuständigen auf Ebene des Bundes und der anderen Länder, um zu einem länder- und mitgliedstaatlich übergreifenden Verständnis zu kommen. Der Diskurs dazu wird fortgesetzt.

3.2 Liebe Abgeordnete: Fragen Sie uns gern!

Die Landesbeauftragte für Datenschutz ist zwar nicht Aufsichtsbehörde für den parlamentarischen Bereich, unterstützt aber gern bei **Fragen zu Datenschutz und Informationsfreiheit**. So besteht für alle Mitglieder des Landtages oder ihre Teams die Möglichkeit, sich bei uns vertrauensvoll beraten zu lassen. Jedes Jahr nehmen einige Abgeordnete diesen Service in Anspruch.

§ 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; [...]

Die Fragen ergeben sich oft direkt aus der praktischen Arbeit der Parlamentarier: Die Abgeordnetentätigkeit ist generell dadurch charakterisiert, dass die zu diskutierenden oder zu regelnden Sachverhalte möglichst gut durchdrungen und die damit verbundenen Facetten in den Blick genommen werden (siehe auch Tz. 2.4). Bürgerinnen und Bürger sprechen ihre Abgeordneten auf alle möglichen Angelegenheiten an und erwarten schnelle Antworten. Außerdem tun sich immer wieder konkrete Probleme in Bezug auf personenbezogene Daten oder Informationstechnik auf. Dies alles spiegelt sich auch in den Themen wider, **die von den Parlamentariern nachgefragt** werden. So geht es vielfach darum, wie sich bestimmte Datenverarbeitungen rechtskonform realisieren lassen, wo sich Risiken auftun und wie man diesen Risiken am besten begegnen kann.

Gerne stehen wir für die Bereiche Datenschutz und Informationsfreiheit **als Ansprechpartner für die Abgeordneten** zur Verfügung und versuchen dem Bedarf – im Rahmen unserer Ressourcen – nachzukommen. Hervorzuheben ist, dass von dem zumeist unmittelbar praxisbezogenen und lösungsorientierten Informationsaustausch alle Seiten profitieren – auch wir.

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 nehmen.

04

KERNPUNKTE

Die Wichtigkeit behördlicher Datenschutzbeauftragten
Gesetzliche Prüfpflichten im Polizeibereich
Datenpannen in der Verwaltung
Datenschutzerklärungen auf Webseiten

4 Datenschutz in der Verwaltung

4.1 Allgemeine Verwaltung

4.1.1 Die behördlichen Datenschutzbeauftragten: wichtig!

Die behördlichen Datenschutzbeauftragten haben vielfältige Aufgaben. Dazu gehört auch die **Zusammenarbeit mit der Aufsichtsbehörde** (Art. 39 Abs. 1 Buchst. d DSGVO). In diesem Sinne unterstützen wir gern die behördlichen Datenschutzbeauftragten, die wiederum von den Verantwortlichen bei Datenschutzfragen einzubeziehen sind.

Die Vorteile dieser Konstellation bestehen darin, dass das konkrete Wissen über die Verarbeitung personenbezogener Daten vor Ort vorhanden ist, dass es wohl weniger Berührungsängste der Beschäftigten in den Behörden gegenüber dem eigenen behördlichen Datenschutzbeauftragten gibt und dass im Bedarfsfall stets eine Rückkopplung mit dem ULD möglich ist. Leider klappt dies nicht immer. Besonders schwierig kann es werden, wenn – wie es häufiger in den letzten Jahren vorgekommen ist – die **behördlichen Datenschutzbeauftragten von den Verantwortlichen nicht einbezogen** wurden, obwohl sich viele Verarbeitungen personenbezogener Daten veränderten oder neu eingeführt wurden. Fast alle waren beispielsweise betroffen von der Umsetzung von Homeoffice und Videokonferenzen oder der Verarbeitung von Gesundheitsdaten oder Kontaktdaten, was jeweils von Anfang an durch geeignete technische und organisatorische Maßnahmen zu begleiten war.

Sicherlich hat die Coronapandemie die Verantwortlichen vor einige Herausforderungen gestellt, besonders wenn ein schnelles Agieren notwendig wurde, um Digitalisierungslösungen einzuführen, wodurch der übliche Vorlauf der Beratungen und Planungen sehr verkürzt wurde oder diese Phasen ganz übergangen wurden. Das war jedenfalls für das Jahr 2020 noch weitgehend nachvollziehbar. Für das Jahr 2021 hat sich dies allerdings nicht grundlegend geändert: Nach unserem Eindruck ist in Schleswig-Holstein noch nicht verinnerlicht, dass man mit **den behördlichen Datenschutzbeauftragten eine wichtige Instanz** vor Ort hat, deren Kompetenz es zu nutzen gilt, um Recht und Gesetz zu erfüllen und die Risiken zu beherrschen (siehe 38. TB, Tz. 1.3).

Seit einiger Zeit wird uns von den Datenschutzbeauftragten vor Ort berichtet, dass sie zunehmend Angriffen ausgesetzt sind, wenn sie korrekt gemäß den rechtlichen Regelungen und der höchstrichterlichen Rechtsprechung (hier besonders zu Schrems II, siehe 38. TB, Tz. 11.5) die Verantwortlichen beraten. Das **verbale Eindreschen auf den Datenschutz** kann dann auch persönlich werden. Damit wird den behördlichen Datenschutzbeauftragten die Arbeit schwer gemacht, engagierte Menschen werden abgeschreckt. Dabei brauchen wir für ein gutes Datenschutzniveau in der Fläche kompetente und motivierte Datenschutzbeauftragte.

Was ist zu tun?

Die Verantwortlichen sollten ihre Datenschutzbeauftragten, wie gesetzlich vorgesehen, einbeziehen und deren Rolle als Mehrwert schätzen.

4.1.2 Empfehlung der Konferenz der Datenschutzbeauftragten der obersten Landesbehörden für ein Datenschutzkonzept

Nicht nur im kommunalen Bereich, sondern auch auf Ebene der Landesbehörden arbeiten die behördlichen Datenschutzbeauftragten erfolgreich zusammen. Die behördlichen Datenschutzbeauftragten der obersten Landesbehörden haben dazu eine **Datenschutzbeauftragten-Konferenz** etabliert.

Im Rahmen dieser Zusammenarbeit wurde ein **Musterdatenschutzkonzept** entwickelt, mit dem Behörden Datenschutzprozesse einführen und in ihre Organisationsstruktur integrieren können. Dieses Datenschutzkonzept geht zum einen auf typische **operative Datenschutzaufgaben** ein, z. B. die Informationspflichten zur Verarbeitung personenbezogener Daten und die Bearbeitung von Anträgen betroffener Personen zur Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 22 DSGVO, beispielsweise der Rechte auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung sowie den Widerruf von Einwilligungen. Zum anderen nimmt das Datenschutzkonzept wichtige Punkte zur Analyse und Dokumentation von Verarbeitungstätigkeiten auf, die insbesondere die **Mitwirkung der behördlichen Datenschutzbeauftragten** bei der Gestaltung neuer Verfahren, etwa im Rahmen von Schwellwertanalysen und Datenschutz-Folgenabschätzungen, betreffen.

Ein Schwerpunkt in dem Datenschutzkonzept liegt auf der **Zusammenarbeit mit dem Informationssicherheitsmanagement** in den Behörden, um unnötige Doppelarbeit und Doppeldokumentation zu vermeiden und stattdessen Synergien nutzen zu können. Dabei werden aber die Besonderheiten des Datenschutzes und die Unterschiede zwischen Informationssicherheit und Datenschutz, die man sich immer wieder bewusst machen sollte, nicht aus den Augen verloren: So gibt es beispielsweise Unterschiede im Hinblick auf die Risikobetrachtung, die aus Datenschutzperspektive die Rechte und Freiheiten der betroffenen Personen und gegebenenfalls Dritter im Fokus hat und sich nicht immer und auch nicht vollständig mit der Risikoanalyse aus Sicht der Informationssicherheit deckt.

Stets gilt es, die richtige Kombination aus technischen und organisatorischen Maßnahmen auszuwählen und zu implementieren, die die Anforderungen sowohl des Datenschutzes als auch der Informationssicherheit erfüllen. Naturgemäß kann ein **Musterkonzept** nicht alle spezifischen Aspekte und organisatorischen Besonderheiten einer Behörde behandeln. Es ist daher **als Blaupause** zu verstehen, die entsprechend ergänzt und gegebenenfalls abgewandelt werden kann. Vor allem aber verdeutlicht das Musterkonzept die gesetzlich festgelegte, aber nach unserer Erfahrung noch nicht allseits bekannte Rolle der behördlichen Datenschutzbeauftragten.

Was ist zu tun?

Die obersten Landesbehörden sollten sich an dem vorgelegten Musterkonzept orientieren.

4.1.3 Übermittlung von Impfnachweisen durch Arbeitgeber an Pflegeeinrichtungen

Vorbemerkung: Die Pandemiesituation ist durch immer wieder sich geänderte Rechtsnormen charakterisiert (siehe Tz. 1.1). Die Beiträge in diesem Bericht beziehen sich auf die jeweils geltenden Regeln, die nach Redaktionsschluss zum 31.12.2021 anders aussehen können.

Verschiedene Unternehmen entsenden ihre Beschäftigten regelmäßig in voll- oder teilstationäre Einrichtungen zur Betreuung älterer, behinderter oder pflegebedürftiger Menschen, damit diese dort ihre Arbeitsleistung erbringen. Die Betreiber der Pflegeeinrichtungen sind bei der Beschäftigung externer Arbeitskräfte wiederum verpflichtet zu prüfen, ob für diese **aus Gründen der**

Pandemiebekämpfung ein Betretungsverbot auszusprechen ist. Der Zugang zu den Pflegeeinrichtungen ist hingegen zulässig, wenn eine vollständige Schutzimpfung gegen das Coronavirus SARS-CoV-2, ein Genesenennachweis hinsichtlich des Vorliegens einer vorherigen Infektion mit dem Coronavirus SARS-CoV-2 oder ein Testnachweis nach den Vorgaben der COVID-19-Schutzmaßnahmen-Ausnahmenverordnung (SchAusnahmV) vorliegt. Externe Beschäftigte in voll- und teilstationären Einrichtungen sind zudem täglich in Bezug auf eine Infektion mit dem Coronavirus zu testen; bei Personen, die nach der SchAusnahmV geimpft oder genesen sind, genügt eine Testung alle 72 Stunden sowie anlass- und symptombezogen. Entsprechendes galt nach der Corona-Bekämpfungsverordnung Schleswig-Holstein in der Fassung vom 13.11.2021.

In einer Beratungsanfrage bat ein Unternehmen um Prüfung, ob **vorhandene Impf- oder Genesenennachweise der eigenen Beschäftigten vorab kopiert** und an den Betreiber einer Pflegeeinrichtung übersandt werden dürfen. Dieser Prozess sollte die Prüfung des Impfstatus vor Ort vereinfachen und die Beschäftigten in die Lage versetzen, von der eingeschränkten Testverpflichtung zu profitieren.

Für die Beurteilung war zunächst maßgeblich, dass es sich bei den Angaben aus den Impf- und Genesenennachweisen um Gesundheitsdaten handelt, die im Wesentlichen nur auf Grundlage einer Einwilligung der Beschäftigten oder eines Gesetzes verarbeitet werden dürfen. Eine Einwilligung der Beschäftigten bedurfte insbesondere einer freiwilligen Erklärung in dem Bewusstsein, dass die Erbringung der Arbeitsleistung auch ohne eine Einwilligung möglich bleibt und auch im Übrigen bei Verweigerung der Einwilligung keine arbeitsrechtlichen Konsequenzen drohen.

Die Einholung derartiger Erklärungen, die die genannten Anforderungen umsetzen, konnte das anfragende Unternehmen nicht belegen. Eine Legitimation dafür, die Impf- und Genesenennachweise von den Beschäftigten zu kopieren und an den Betreiber der Pflegeeinrichtung zu übermitteln, ergab sich auch nicht aus einer besonderen gesetzlichen Vorschrift. Das für diesen Kontext einschlägige Bundesdatenschutzgesetz verlangt dabei eine strenge Prüfung der Erforderlichkeit einer Datenverarbeitung sowie eine Abwägung mit den schutzwürdigen Belangen der betroffenen Beschäftigten.

§ 26 Abs. 3 Bundesdatenschutzgesetz

Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Das **Kopieren der Gesundheitsdaten** war bereits deshalb **nicht** zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht **erforderlich**, weil

- den Beschäftigten nach der Corona-Bekämpfungsverordnung Schleswig-Holstein in der Fassung vom 13. November 2021 die Wahlmöglichkeit verblieb, anstelle der Impf- oder Genesenennachweise einen Testnachweis beizubringen,
- der Betreiber der Pflegeeinrichtung nach den landesrechtlichen Vorgaben in der Fassung vom 13. November 2021 vor Ort Testungen für externe Beschäftigte anzubieten und auf dieses Angebot am Eingang hinzuweisen hat und den Beschäftigten somit selbst für den Fall, dass sie ihren Impf- oder Genesenennachweis nicht mitführen, eine schnelle Klärung mittels eines aktuellen Tests möglich bleibt,
- die freie Entscheidung bei den Beschäftigten verbleiben musste, ihre Impf-, Genesenen- oder Testnachweise direkt dem Betreiber der Pflegeeinrichtung vorzulegen und schließlich
- es nach den landesrechtlichen Vorgaben in der Fassung vom 13. November 2021 genügte, dass die externen Beschäftigten dem Betreiber der Pflegeeinrichtung die entsprechenden Nachweise für eine Sichtkontrolle vorlegen. Die Anfertigung von Kopien der Nachweise externer Beschäftigter ist selbst für die Betreiber von Pflegeeinrichtungen nach der Corona-Bekämpfungsverordnung Schleswig-Holstein nicht vorgesehen.

Eine Voraberhebung der Impf-, Genesenen- und Testnachweise bei den eigenen Beschäftigten

durch Arbeitgeber mag in der vorliegenden Konstellation praktisch erscheinen. Allerdings muss den Beschäftigten **nach den gesetzlichen Vorgaben eine Wahlmöglichkeit verbleiben**, wie ihre Gesundheitsdaten verarbeitet werden. Etwaige Verzögerungen bei der Arbeitsaufnahme im Einzelfall infolge der Einholung eines aktuellen Testergebnisses bei der Pflegeeinrichtung vor Ort fallen regelmäßig nicht übermäßig ins Gewicht. Zusätzlich stehen anlass- und symptombezogene Tests bei externen Beschäftigten im Ermessen der Betreiberinnen und Betreiber von Pflegeeinrichtungen und sind vom Arbeitgeber der externen Beschäftigten nicht beeinflussbar.

4.1.4 Offenlegung von Impfwünschen gegenüber allen Beschäftigten

In dem Berichtszeittraum hat uns eine Beschwerde zum folgenden Sachverhalt erreicht: Alle Beschäftigten waren per intern versandter E-Mail darauf hingewiesen worden, dass sie sich bei **Interesse an einer Impfung** gegen COVID 19 in eine Liste eintragen könnten. In der Liste war anzugeben, welche der drei genannten Impfstoffe aus Sicht der jeweiligen Beschäftigten infrage kamen. Es waren Spalten für die Eintragung von Name, Vorname und des in Betracht kommenden Impfstoffs vorgesehen. Die **Liste** war in einem **für alle Beschäftigte zugänglichen Laufwerksordner** gespeichert.

Für die Erhebung der Daten mittels einer für alle Beschäftigten einsehbaren und beschreibbaren Liste lag keine Rechtsgrundlage vor. Beamtenrechtliche Regelungen, die nach dem Landesdatenschutzgesetz auch für Tarifbeschäftigte gelten, waren nicht anwendbar. Es hätte **andere Möglichkeiten** gegeben, den Bedarf an Impfstoffen zu ermitteln. Zur Abfrage des konkreten Bedarfs wäre es in diesem Fall ausreichend gewesen, eine anonyme Befragung durchzuführen, was eine Verarbeitung personenbezogener Daten vermieden hätte. Eine Einwilligung der Beschäftigten kam ebenfalls nicht als Rechtsgrundlage in Betracht. Unabhängig von der Frage der Freiwilligkeit einer im Beschäftigtenverhältnis erteilten Einwilligung lagen in diesem Fall ohnehin nicht die Voraussetzungen für wirksam erteilte Einwilligungen vor. So erhielten die Beschäftigten beispielsweise keine Informationen darüber, dass sie eine Einwilligung erklären sollen. Auch erfolgte keine Belehrung über das Widerrufsrecht.

In diesem Fall sprach das ULD daher eine Verwarnung aus. In die Abwägung hinsichtlich der Entscheidung über die Verhängung einer Verwarnung wurde berücksichtigt, dass **der behördliche Datenschutzbeauftragte intern nicht einbezogen** worden ist.

Was ist zu tun?

Die Abfrage eines Impfinteresses durch Arbeitgeber hat so zu erfolgen, dass die Antworten nicht für alle Beschäftigten zugänglich sind, wie dies durch die für alle Beschäftigten beschreibbaren Liste der Fall war.

4.1.5 Datenbekanntgabe während öffentlicher Ratssitzung und Veröffentlichung im Internet

In einer Beschwerde ging es darum, dass während einer Ratssitzung der Name einer Bürgerin bekannt gegeben worden sei, die sich mit einer bestimmten Anregung in kommunalen Belangen an ihre Stadt gewandt hatte. Ihre Daten waren auch im Zusammenhang mit der Tagesordnung der Sitzung im Internet veröffentlicht worden.

In dem eingeleiteten Verfahren führte die Stadt aus, dass der **Öffentlichkeitsgrundsatz** sowie die gebotene Transparenz und Kontrollmöglichkeit durch die Bürgerinnen und Bürger eine direkte Kommunikation mit Verfasserinnen und Verfassern derartiger Anregungen erfordere, was die Offenlegung der Person auch im Internet

voraussetze – soweit kein gegenteiliges Interesse deutlich werde. Darüber hinaus vertrat die Stadt die Auffassung, dass die Bürgerin mit der Abgabe der Anregung eine **konkludente Einwilligung** erklärt habe, sie sei mit der Veröffentlichung ihrer personenbezogenen Daten einverstanden.

Diese Wertung teilen wir nicht. Für die Einhaltung des Öffentlichkeitsgrundsatzes war in dem vorliegenden Fall zwar die Durchführung einer öffentlichen Sitzung der Gemeindevertretung notwendig. Bereits hinsichtlich der formulierten Anregung der Bürgerin war aber zu prüfen, ob zwingend deren namentliche Benennung in der Sitzung erfolgen musste. Die inhaltliche Befassung mit dieser Anregung konnte unabhängig von der Person der Bürgerin erfolgen: Für die **Entscheidungsfindung der Ratsmitglieder** war es **nicht relevant zu wissen, welche Person diese Anregung abgegeben** hat. Die Bürgerin hatte auch keinen Antrag gestellt, über den die Gemeindevertretung hätte entscheiden müssen. Die namentliche Nennung der Bürgerin und in diesem Zusammenhang die Veröffentlichung ihrer personenbezogenen Daten im Internet waren nicht erforderlich gewesen.

Die Anregung der Bürgerin bezog sich zudem auf eine allgemeine kommunale Begebenheit. Auch von einer (konkludent erteilten) Einwilligung konnte nach unserer Auffassung nicht ausgegangen werden. Einer **wirksamen Einwilligung** hinsichtlich der Veröffentlichung der Anregung nebst **namentlicher Nennung im Internet** hätte eine angemessene **Unterrichtung** über den damit verfolgten Zweck vorausgehen müssen. Weiterhin hätte eine **Belehrung** über die Widerruflichkeit erfolgen müssen. Eine Einwilligung hätte darüber hinaus freiwillig sein müssen, d. h., die Bürgerin hätte eine echte Wahl gehabt haben müssen. Die Anforderungen an eine wirksame Einwilligung waren nicht erfüllt.

Was ist zu tun?

Die Veröffentlichung personenbezogener Daten kann nur dann auf § 35 Abs. 1 Satz 1 der Gemeindeordnung gestützt werden, wenn die Einhaltung des Öffentlichkeitsgrundsatzes dies zwingend erfordert. Bei der Beteiligung von Bürgerinnen und Bürgern ist im Hinblick auf deren Rechte, insbesondere das Recht auf informationelle Selbstbestimmung, ein besonderer Sorgfaltsmaßstab anzusetzen.

4.1.6 Benachrichtigung per E-Mail über offenen Verteiler an Ratsmitglieder

Ist die Benachrichtigung von Ratsmitgliedern unter Verwendung eines **offenen E-Mail-Verteilers** datenschutzrechtlich zulässig? In dem konkreten Fall ging es darum, dass eine Stadt für die Einladung zu einer gemeinsamen öffentlichen Sitzung zweier kommunaler Ausschüsse einen offenen E-Mail-Verteiler verwendete und die Einladungen über die „CC“-Funktion an die Mitglieder verschickte. Bei den E-Mail-Adressen der Empfänger handelte es sich um private E-Mail-Adressen (überwiegend mit Namensbezug) sowie um öffentlich zugängliche E-Mail-Adressen.

Durch die Verwendung eines offenen E-Mail-Verteilers werden die genutzten E-Mail-Adressen für alle Adressaten ersichtlich. Die damit einhergehende Übermittlung der personenbezogenen Daten (E-Mail-Adressen mit Namensbezug) erfordert eine Rechtsgrundlage. Eine gesetzliche Rechtsgrundlage kommt grundsätzlich nicht in Betracht. Sofern die Verwendung des offenen Verteilers auch nicht auf eine Einwilligung gestützt werden kann, ist die Verwendung des offenen Verteilers nicht mit den datenschutzrechtlichen Anforderungen vereinbar.

Etwas anderes kann im Einzelfall gelten, wenn die übermittelten E-Mail-Adressen den Empfängern einander bereits bekannt waren (z. B. durch rechtskonform ausgestaltete Mitgliederlisten, eigene E-Mail-Korrespondenz) oder öffentlich zugänglich sind.

Für das datenschutzkonforme Versenden von E-Mails an E-Mail-Verteiler gibt es (neben der Einholung einer Einwilligung) grundsätzlich zwei

Möglichkeiten. Zum einen kann eine **Mailinglisten-Software** genutzt werden, um E-Mails an einen Verteiler zu schicken, ohne dass die Empfänger alle anderen E-Mail-Adressen mitlesen können. Ein An- und Abmelden von den Verteilern kann dabei den betroffenen Personen ermöglicht werden. Zum anderen können die **E-Mail-Adressen im „BCC"-Feld** („Blind Carbon Copy") eingegeben werden, sodass sie für die Empfänger nicht sichtbar sind.

Was ist zu tun?

E-Mails dürfen nur bei Vorliegen einer Rechtsgrundlage an einen offenen Verteiler versandt werden. Anderenfalls sollte eine Mailinglisten-Software oder die „BCC"-Funktion genutzt werden.

4.1.7 Überarbeitungsbedürftige Datenschutzerklärungen auf Webseiten

Die öffentliche Verwaltung nutzt bereits seit vielen Jahren eigene Webseiten für die Informationen der Bürgerinnen und Bürger. Dort stehen vielfach auch ausfüllbare Formulare bereit, es gibt Downloadbereiche, Services zur Terminplanung werden angeboten, und künftig – wie vom Onlinezugangsgesetz gefordert – werden immer mehr **digitale Verwaltungsleistungen** hinzukommen.

Im Jahr 2020 haben wir begonnen, Datenschutzerklärungen auf den Webseiten von Verwaltungen, insbesondere von Kommunalverwaltungen, in Augenschein zu nehmen. Dabei haben wir festgestellt, dass **keine der geprüften Datenschutzerklärungen den Vorgaben der DSGVO im Hinblick auf die dort geforderten Informationen entsprochen** hat:

- Viele Datenschutzerklärungen waren augenscheinlich mit aus dem Internet abrufbaren Mustern **„zusammengeklickt"** worden. Die darin enthaltenen Informationen stimmten nicht damit überein, wie tatsächlich personenbezogene Daten über die Webseite verarbeitet wurden. Einerseits wurde so über Verarbeitungen informiert (z. B. angeblich eingebundene Google-Dienste), die gar nicht erfolgten. Andererseits fehlten aber auch Informationen über stattfindende Verarbeitungen.
- Weiterhin fehlten oft eindeutige **Informationen über die Rechte der betroffenen Personen** oder es wurde über die Möglichkeit informiert, bestimmte Rechte wahrzunehmen, die nicht zu der Datenverarbeitung durch die Webseite passten.
- Auf das **Beschwerderecht** der betroffenen Personen nach Artikel 77 DSGVO wurde häufig nicht hingewiesen.
- Sofern mittels der Webseiten weitere Funktionalitäten bereitgestellt wurden, die eigene Verarbeitungsvorgänge auslösen, wie z. B. von Fremdanbietern eingebundene Terminplaner oder Kontaktformulare, wurde nicht erläutert, um welche **Fremdanbieter** es sich handelt und welche Verarbeitungsvorgänge diese vornehmen.
- Auch die rechtlichen Vorgaben für die **Nutzung von Cookies** (siehe Tz. 7.2) wurden regelmäßig nicht umgesetzt. Teilweise wurde auf Cookies hingewiesen, die beim Besuch der Webseite gar nicht gesetzt wurden.

Wegen der Häufigkeit der vorgefundenen Missstände haben wir die Vorsitzenden der verschiedenen **Arbeitskreise der behördlichen Datenschutzbeauftragten der Städte, Gemeinden und Kreise** gebeten, alle in ihren Arbeitskreisen organisierten Datenschutzbeauftragten zu informieren und auf die Notwendigkeit der Überprüfung der Webseiten ihrer Verwaltung hinzuweisen, damit vorhandene Mängel abgestellt werden.

Was ist zu tun?

Das größere Angebot digitaler Verwaltungsdienstleistungen führt dazu, dass viele Webseiten ausgebaut werden. Dabei ist sicherzustellen, dass die Einbindung solcher Services datenschutzkonform geschieht und die nach Art. 13 Abs. 1 und 2 DSGVO erforderlichen Informationen in der dort geforderten eindeutigen und einfachen Sprache für die betroffenen Personen bereitgestellt werden.

Wir werden unsere Prüfungen von Webseiten der Verwaltung insbesondere in Bezug auf eingebundene Services, Cookies und Datenschutzinformationen fortsetzen.

4.1.8 Speicherfristen für Daten auf Meldescheinen

Hintergrund einer Beschwerde war die **Verwendung eines (einzigen) Formulars „Meldeschein/Gästekarte“**, mit dem Vermieter/Vermittler im touristischen Bereich die erforderlichen Angaben zur Erfüllung der melderechtlichen Vorgaben und zusätzlich im Zusammenhang mit der Kurabgabe erheben sollten. Die Beschwerde führende Person sollte dieses Formular für die Datenerhebung ihrer Gäste verwenden und monierte, dass sie dadurch die **Löschverpflichtung** für Meldescheine nach § 30 Abs. 4 Satz 1 des Bundesmeldegesetzes **nicht einhalten** kann. Demnach sind ausgefüllte Meldescheine vom Tage der Anreise der beherbergten Person an **ein Jahr** aufzubewahren und innerhalb von drei Monaten nach Ablauf der Aufbewahrungsfrist zu vernichten. Von der Kommune habe die Beschwerde führende Person jedoch die Auskunft erhalten, die Formulare seien **fünf Jahre** aufzubewahren.

§ 30 Abs. 3 Bundesmeldegesetz

Durch Landesrecht kann bestimmt werden, dass für die Erhebung von Fremdenverkehrs- und Kurbeiträgen weitere Daten auf dem Meldeschein erhoben werden dürfen.

Nach § 30 Abs. 3 des Bundesmeldegesetzes kann durch Landesrecht bestimmt werden, dass für die Erhebung von Fremdenverkehrs- und Kurbeiträgen weitere Daten auf dem Meldeschein erhoben werden dürfen. Die Kommune hatte vorliegend hiervon Gebrauch gemacht, indem auf Grundlage einer Satzung über die Erhebung einer Kurabgabe die Abfrage zusätzlicher Angaben erfolgt.

Die Kommune war zunächst fälschlich der Auffassung, dass die bundesrechtliche Löschverpflichtung durch die Erhebung von Angaben bezüglich der Kurabgabe außer Kraft gesetzt wird. Diese **Löschverpflichtung** bezieht sich auf die Angaben nach § 30 Abs. 2 des Bundesmeldegesetzes. Soweit Angaben in Bezug auf die Kurabgabe betroffen sind, die über diesen Datensatz hinausgehen, mochte gegebenenfalls eine längere Aufbewahrungsfrist in Betracht kommen.

§ 30 Abs. 2 Bundesmeldegesetz

Die Meldescheine enthalten vorbehaltlich der Regelung in Absatz 3 ausschließlich folgende Daten: Datum der Ankunft und der voraussichtlichen Abreise, Familiennamen, Vornamen, Geburtsdatum, Staatsangehörigkeiten, Anschrift, Zahl der Mitreisenden und ihre Staatsangehörigkeit in den Fällen des § 29 Absatz 2 Satz 2 und 3 sowie Seriennummer des anerkannten und gültigen Passes oder Passersatzpapiers bei ausländischen Personen.

Nach den Vorgaben der Satzung zur Erhebung einer Kurabgabe sah die Kommune vor, dass zusätzlich folgende Daten zu sämtlichen bzw. allen „aufgenommenen Personen“ zu erheben sind: Nachweise bezüglich des Grades einer Schwerbehinderung bzw. eine Notiz hierzu, Namen, Vornamen, Heimatanschriften sowie Altersangaben, soweit das 18. Lebensjahr noch nicht vollendet ist. Damit bestand im Vergleich mit den Daten, die für die Ausfüllung der Meldescheine

erhoben werden müssen, allenfalls eine **marginale Übereinstimmung der Felder im Datensatz**.

Die zwingende Löschung der Daten aus den Meldescheinen, die nicht mit den Angaben zur Erhebung der Kurabgabe übereinstimmten, konnte auch nicht mit dem Vorbringen der Kommune entkräftet werden, dass für alle Daten steuerrechtliche Aufbewahrungsfristen gelten würden. Mit der Erhebung der Daten zur Erfüllung melderechtlicher Vorgaben und der Daten in Bezug auf die Kurabgabe in einem einzigen Formular wurde den Vermietern die **Löschverpflichtung nach dem Bundesmeldegesetz erschwert**.

Nach Eröffnung eines Prüfverfahrens und Erörterung der Rechtslage hat die Kommune im Ergebnis die **Erhebungspraxis geändert**, sodass die Daten zu den Meldescheinen und zur Kurabgabe getrennt erfasst werden. Auf diese Weise können die Vermieter den Löschpflichten bezüglich der Angaben in den Meldescheinen nachkommen und eine gegebenenfalls längere Aufbewahrung der Daten in Bezug auf die Erhebung der Kurabgabe gewährleisten.

Was ist zu tun?

Der Gedanke, Angaben zu Meldescheinen und Kurabgaben in einem einzigen Formular zu erfassen, mag sich am Ziel orientiert haben, den Vermietern die Erfüllung ihrer gesetzlichen Pflichten zu vereinfachen. Allerdings führte die praktische Umsetzung in diesem Fall zu einer Komplikation für die Vermieter. Die Kommunen sollten vor der Einführung neuer Prozesse daher prüfen, ob mit der beabsichtigten Vereinfachung gesetzliche Vorschriften von den Beteiligten noch eingehalten werden können. Dazu sind insbesondere unterschiedliche Zwecke und Aufbewahrungsfristen in den Blick zu nehmen.

4.1.9 Zweitwohnungssteuer und Erhebung von Einkommensteuerdaten

In mehreren Beschwerden wandten sich Bürgerinnen und Bürger an das ULD hinsichtlich der Verwendung von **Fragebögen** durch die für die Erhebung von Zweitwohnungssteuer zuständigen Behörden.

Begriff: Zweitwohnungssteuer

Bei der Zweitwohnungssteuer handelt es sich um eine örtliche Aufwandsteuer, die auf Grundlage einer Satzung erhoben wird. Dabei wird der Eigengebrauch der Immobilie zunächst vermutet, kann aber von der steuerpflichtigen Person widerlegt werden. Zweitwohnungssteuer wird etwa dann nicht erhoben, wenn eine Vermietung als Ferienwohnung an Dritte erfolgt.

Eine Fremdnutzung der Immobilie muss der Steuerpflichtige belegen. Wurden z. B. Vermietungstage in der Steuererklärung angegeben, so kann gegebenenfalls die Beifügung von Angaben zu den Vermietungszeiten, zu den gezahlten Mietentgelten und zu den Namen der Mieterinnen und Mieter erforderlich sein. Mittels der Fragebögen ermitteln die zuständigen Kommunen die bestehenden Sachverhalte und **überprüfen**, ob eine **Zweitwohnungssteuerpflicht** besteht.

Beschwerdegegenstand waren dabei Aufforderungen der Kommunen, zur näheren Prüfung eine **Kopie der Anlage V zur Erklärung der Einkommensteuer** dem Fragebogen beizufügen. Es bestand die Fragestellung, ob zur Wahrnehmung der behördlichen Aufgaben sämtliche Angaben aus dieser Anlage V erforderlich sind, um die Grundlagen für die Erhebung von Einkommensteuer zu ermitteln. Diese Anlage gibt Aufschluss über die Einkünfte aus Vermietung und Verpachtung. Das Gebot der Erforderlichkeit ergibt sich vor allem aus § 3 des Landesdatenschutzgesetzes.

§ 3 Abs. 1 Landesdatenschutzgesetz

Die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.

Die Anlage V zur Einkommensteuererklärung enthält Angaben zu Einkünften aus dem Grundstück, wie z. B. Lage des Grundstücks oder der Eigentumswohnung nebst Anschrift, Nutzungsart, Höhe der Mieteinnahmen für Wohnungen und für andere Räume, Einnahmen für an Angehörige vermietete Wohnungen, Einnahmen aus der Vermietung von Garagen und Werbeflächen, vereinnahmte Umsatzsteuer und vom Finanzamt erstattete oder verrechnete Umsatzsteuer, öffentliche Zuschüsse, Werbungskosten, Anteile an Einkünften wie etwa aus Grundstücksgemeinschaften und Einkünfte aus Untervermietungen. Offensichtlich sind **nicht alle diese Daten für den verfolgten Zweck relevant**.

Bei der näheren Prüfung wurde nach Anhörung der Kommunen präzisiert, welche Angaben aus der Anlage V zur Überprüfung der Zweitwohnungssteuerpflicht erforderlich sind. Im Ergebnis sind die **Werbungskosten bezüglich der Erhaltungsaufwendungen und Fahrtkosten** maßgeblich. Informationen vor allem zu Umsatzsteuerangaben, Kosten der Geldbeschaffung und Zinsen haben für die Ermittlung keine Bedeutung.

Die öffentlichen Stellen haben für die Zukunft ihre **Fragebögen entsprechend angepasst** und erheben fortan nur die erforderlichen Daten.

Was ist zu tun?

Die für die Erhebung der Zweitwohnungssteuerpflicht zuständigen Kommunen sollten ihre Fragebögen überprüfen und den Steuerpflichtigen eine Schwärzung der nicht erforderlichen Informationen ermöglichen. Hierzu sind Hinweise in den Fragebögen hilfreich.

4.1.10 Veröffentlichung von Abwägungstabellen in baurechtlichen Verfahren

Im Rahmen einer Beschwerde wurde vorgetragen, dass im Zusammenhang mit einem **Bauleitplanverfahren** personenbezogene Daten (Namen, Anschriften) mit den jeweiligen Einwendungen von Bürgerinnen und Bürgern in sogenannten Abwägungstabellen im Internet veröffentlicht worden seien. In dem daraufhin gegen die betreffende Stadt eingeleiteten Beschwerdeverfahren stellte sich heraus, dass die **Veröffentlichung der Namen und Anschriften der Bürgerinnen und Bürger** in der Tabelle entgegen der sonstigen Verfahrensweise (u. a. vorherige Anonymisierung der Daten) der Stadt erfolgte. Nach Bekanntwerden des Vorfalls wurde die Veröffentlichung seitens der Stadt umgehend unterbunden.

Für die Nennung von Namen und Anschriften betroffener Bürgerinnen und Bürger besteht in einem Bauleitverfahren regelmäßig dann keine Berechtigung, wenn die mit der Entscheidung befassten Gremien eine **Erörterung und Entscheidungsfindung auch ohne identifizierende Angaben** der Bürgerinnen und Bürger durchführen können. Entsprechende Einwendungen von Bürgerinnen und Bürgern in einem Bauleitverfahren sind insoweit **grundsätzlich anonymisiert bzw. pseudonymisiert** an die Gremien zu übermitteln. Ausnahmen von diesem Grundsatz kann es im Einzelfall nur dann geben, soweit dies für die Entscheidungsfindung (der zu beteiligenden Gremien) erforderlich ist. Dies kann beispielsweise für personenbezogene Angaben zutreffen, auf die die Einwendungen der Bürgerinnen und Bürger gestützt werden (z. B. Beeinträchtigung eines Gewerbebetriebes, Beeinträchtigung als Anwohner nebst Angabe der Anschriften). Es ist daher für die jeweilige personenbezogene Angabe zu prüfen, ob diese für die Gewichtung und Abwägung der Belange erforderlich ist. Dabei ist den Einwendungen von natürlichen Privatpersonen infolge der

Anwendbarkeit der Datenschutzvorschriften höheres Gewicht beizumessen als den Einwendungen von Unternehmen zu betriebsbezogenen Gründen.

Für die erfolgte Veröffentlichung der Namen und der Anschriften der betroffenen Bürgerinnen und Bürger in Abwägungstabellen im Internet war **keine Rechtsgrundlage** ersichtlich. Die Veröffentlichung stand auch nicht mit der Durchführung einer Entscheidungsfindung im Zusammenhang.

Weiterhin wurde mit der Beschwerde vorgetragen, dass die personenbezogenen Daten der betroffenen Bürgerinnen und Bürger an ein Planungsbüro übermittelt worden seien. Die **Einbeziehung eines Planungsbüros in einem Bauleitplanverfahren verstößt nicht generell gegen datenschutzrechtliche Vorgaben**. Die Behörde hat etwa die Möglichkeit, bei der Verarbeitung personenbezogener Daten die Dienste eines Planungsbüros in Anspruch zu nehmen, was gegebenenfalls im Wege einer Auftragsverarbeitung zulässig ist. Beispielsweise kann ein Planungsbüro mit der Erstellung einer Abwägungstabelle beauftragt werden.

Bei der Erhebung von personenbezogenen Daten, wozu auch Einwendungen gegen bauplanungsrechtliche Vorgaben zählen, sind die Anzuhörenden zu unterrichten. Diese **Unterrichtung** kann beispielsweise in Form einer amtlichen Bekanntmachung erfolgen, mit der die öffentliche Auslegung bekannt gemacht und der z. B. ein Formblatt hinsichtlich der datenschutzrechtlichen Informationspflichten beigefügt wird.

4.2 Polizei und Verfassungsschutz

4.2.1 Gesetzliche Prüfpflichten als Garant für besseren Datenschutz?

„*WDSKegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatischen Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung.*“ – Mit diesen Worten betont das Bundesverfassungsgericht in seinem sogenannten Volkszählungsurteil aus dem Jahr 1983 die wichtige Rolle, die **eine unabhängige Datenschutzkontrolle im rechtsstaatlichen Gefüge** spielt. Sie treffen heute mehr zu als je zuvor.

Die Prüfpraxis der unabhängigen Datenschutzaufsichtsbehörden ist insbesondere von zwei Faktoren abhängig:

- ihrer personellen Ausstattung und
- gesetzlichen Prüfpflichten.

Seit 1983 hat der Umfang an automatisierter Verarbeitung personenbezogener Daten massiv zugenommen. Die Aufsichtsbehörden und behördlichen Datenschutzbeauftragten (bDSB) sind aber personell nicht im selben Umfang mitgewachsen. **Regelmäßige anlasslose Kontrollen der vorhandenen Systeme können nicht sichergestellt werden.** In letzter Konsequenz bedeutet dies, dass datenschutzrechtliche Kontrollen im Verhältnis zum Umfang der Datenverarbeitung dem sprichwörtlichen „Feigenblatt“ gleichen. Dies ist insbesondere dort problematisch, wo die unabhängige Kontrolle als Korrektiv für eingriffsintensive, meist intransparente Datenverarbeitungen verfassungsrechtlich geboten ist.

Ein Ansatz zur Lösung dieses Problems sind **Pflichtprüfungen** der Datenschutzaufsicht, die sich aus der Rechtsprechung ergeben und zunehmend vom Gesetzgeber geregelt werden. Ein Beispiel dafür findet man in der Entscheidung des Bundesverfassungsgerichts vom 24.04.2013 zum Antiterrordateigesetz (ATDG). Dort heißt es auszugsweise: *„Angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz kommt deren regelmäßiger Durchführung besondere Bedeutung zu und sind solche Kontrollen in angemessenen Abständen – deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf – durchzuführen.“*

Seit dieser Entscheidung sind auf Landes-, Bundes- und europäischer Ebene viele weitere Pflichtprüfungen hinzugekommen. Unmittelbar betroffen ist das ULD derzeit von **zwei Prüfpflichten auf Bundesebene, fünf vonseiten der EU-Gesetzgebung sowie zwei Pflichten**

auf Landesebene. Letztere sind in Schleswig-Holstein durch die Novellierung des Landesverwaltungsgesetzes (LVwG) hinzugekommen und betreffen elf verschiedene Maßnahmen. Dazu gehören die verdeckten Maßnahmen im Bereich der Gefahrenabwehr sowie die Datenübermittlung in Drittstaaten (siehe Tabelle). Für den Bereich der Strafverfolgung gibt es diese gesetzliche Prüfpflicht noch nicht, hier gelten aber die verfassungsrechtlichen Gründe für Pflichtprüfungen gleichermaßen. Es ist daher anzunehmen, dass weitere gesetzliche Prüfpflichten hinzukommen werden.

Darüber hinaus gibt es noch **weitere Pflichtprüfungen**, die der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) durchführt. Von diesen Prüfungen ist regelmäßig auch die Datenverarbeitung einzelner oder aller Länder betroffen, was die Beteiligung der dortigen Datenschutzaufsichtsbehörden erforderlich macht.

Sind gesetzliche Prüfpflichten also die Lösung, um das Datenschutzniveau insgesamt zu verbessern? Die Notwendigkeit regelmäßiger Pflichtprüfungen betont die Wichtigkeit der betroffenen Bereiche in Bezug auf eine Datenschutzkontrolle. Die Verantwortlichen und die behördlichen Datenschutzbeauftragten können sich auf die wiederkehrenden Prüfungen einstellen und in besonderem Maße auf ein funktionierendes Datenschutzmanagement achten. Jedoch verschärfen gesetzliche Prüfpflichten die **Knappheit der personellen Ressourcen** sowohl bei den Aufsichtsbehörden als auch den behördlichen Datenschutzbeauftragten. Man könnte sogar argumentieren: Wären die Personalressourcen ausreichend bemessen, würde es gesetzlicher Prüfpflichten in vielen Fällen nicht bedürfen. Aufgrund der momentanen Lage sorgen die gesetzlich geforderten Prüfungen jedoch dafür, dass in vielen anderen Bereichen noch weniger oder so gut wie gar nicht mehr geprüft werden kann.

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

Mit der Zunahme solcher Pflichten kann sich außerdem ihr Nutzen abschwächen, da auch in den betroffenen Bereichen die Stichproben ressourcenbedingt immer kleiner ausfallen könnten. Es könnte sogar der Effekt entstehen, dass solche Datenschutzprüfungen, zu denen die Aufsicht aufgrund der Undurchsichtigkeit der Datenverarbeitung verpflichtet wurde, nur selektiv zu mehr Transparenz führen und sich der **Kontrast dieser quasi „gut ausgeleuchteten Bereiche" zu anderen weiterhin wenig transparenten Datenverarbeitungen** verstärkt.

Die Relation zwischen gesetzlichen Prüfpflichten und der personellen Ausstattung der aufsichtführenden Stellen hat bereits das Bundesverfassungsgericht gesehen. In seinem bereits erwähnten Urteil zum ATDG wird im Zusammenhang mit den Pflichtprüfungen darauf hingewiesen, dass der gestiegene Aufwand bei der Ausstattung der Aufsichtsbehörden „zu berücksichtigen" ist.

Der Landesgesetzgeber spielt die entscheidende Rolle bei der personellen Ausstattung seiner Aufsichtsbehörde. Dabei müssen auch gesetzliche Prüfpflichten berücksichtigt werden, die durch den Bund sowie die europäische Rechtsetzung normiert werden. Effektiver Datenschutz kann dabei jedoch nicht allein durch eine Stärkung der Aufsichtsbehörde erreicht werden. Auch die Datenschutzbeauftragten in den Behörden vor Ort müssen personell so verstärkt werden, dass sie in der Lage sind, ihren gesetzlichen Aufgaben, zu denen ebenfalls die Durchführung von anlassunabhängigen Prüfungen gehört, vollumfänglich nachzukommen. Im **Bereich der behördlichen Datenschutzbeauftragten** der Landespolizei finden aufgrund der dünnen Personaldecke derzeit beispielsweise lediglich Einzelfallüberprüfungen aufgrund von Beschwerden statt. Die Zunahme von Pflichtprüfungen lässt auf der Seite der Aufsichtsbehörde ebenfalls immer weniger Spielraum für anlasslose Kontrollen zu.

Gesetzlich vorgeschriebene Pflichtprüfungen können dann einen Beitrag zu einem besseren Datenschutzniveau leisten, wenn dadurch die **zentrale Aufgabe anlassloser Kontrollen** nicht eingeschränkt wird. Das Fehlen anlassloser Kontrollen in den Behörden und durch die Aufsichtsbehörde fällt häufig lange Zeit nicht auf, doch dies kann sich rächen, wenn sich Probleme bezüglich der Datenschutzkonformität aufbauen, die dann „plötzlich" als „Datenschutzskandal" in das öffentliche Interesse rücken. Dies gilt es zu vermeiden.

Was ist zu tun?

In dem Maße, wie Prüfpflichten zunehmen, muss auch die personelle Ausstattung der Aufsichtsbehörden wachsen. Die präventive Wirkung anlassloser Kontrollen darf nicht unterschätzt werden. Behörden müssen ihren Datenschutzbeauftragten dafür ausreichende Ressourcen zur Verfügung stellen.

4.2.2 Ermittlung einer Beifahrerin bei einer Verkehrsordnungswidrigkeit

In einem Fall haben wir im Berichtszeitraum gegenüber einer Polizeidirektion eine Verwarnung ausgesprochen. Hintergrund war eine Anfrage aus einem anderen Bundesland, bei der im Rahmen einer Verkehrsordnungswidrigkeit der Fahrer eines Dienstwagens ermittelt werden sollte.

Im Zuge der Ermittlungen gegen den beschuldigten Fahrer wurde auch die Identität der Beifahrerin ermittelt. Dazu wurden Personen im Arbeitsumfeld des Beschuldigten befragt sowie weitere **personenbezogene Daten der Beifahrerin** (z. B. Lichtbild, Meldedaten) bei der Amtsverwaltung des Wohnorts erhoben. Diese Daten wurden dann an das anfragende Bundesland übermittelt. Aufgrund einer Beschwerde wurde der Vorgang durch das ULD überprüft. Dabei wurde festgestellt, dass die Verarbeitung der personenbezogenen Daten der Beifahrerin unrechtmäßig erfolgt ist – ein klarer datenschutzrechtlicher **Verstoß**.

Doch was konnte nun getan werden, um einerseits die negativen Folgen für die betroffene Person nach Möglichkeit zu verringern und andererseits für die Zukunft derartige Fehler zu vermeiden?

Der Vorgang wurde durch den behördlichen Datenschutzbeauftragten (bDSB) sowie den verantwortlichen Direktionsleiter engagiert **aufgearbeitet**. In diesem Zusammenhang wurden die unrechtmäßig verarbeiteten Daten gemäß den Vorgaben des LDSG soweit wie möglich gelöscht. Wo dies nicht möglich gewesen wäre, ohne das zugrunde liegende OWI-Verfahren zu gefährden, wurden die Daten für eine weitere Verwendung gesperrt. Das anfragende Bundesland wurde nachträglich über die unzulässige Datenübermittlung informiert und darauf hingewiesen, dass die personenbezogenen Daten der Beifahrerin nach § 34 Abs. 5 LDSG zu löschen bzw. zu sperren seien. In die interne Aufarbeitung wurden außerdem die handelnden Beamten sowie ihre Vorgesetzten einbezogen.

Im Ergebnis handelt es sich um einen klaren Verstoß gegen datenschutzrechtliche Vorschriften. Der Vorgang ist aber auch ein gutes Beispiel für die **Aufarbeitung und Korrektur**. Die Polizeidirektion hat gut mit der Aufsichtsbehörde zusammengearbeitet und alle erforderlichen Maßnahmen ergriffen. Auf diese Weise konnte der **Schaden begrenzt** werden. Die Mitarbeitenden wurden sensibilisiert und die Situation wurde als Chance betrachtet, die eigenen Abläufe zu verbessern. Eine gute interne Aufarbeitung bildet die beste Grundlage dafür, zukünftige Verstöße zu verhindern.

Was ist zu tun?

Auch über Direktionsgrenzen hinweg eignen sich derartige Sachverhalte sehr gut dafür, Beamtinnen und Beamte zu schulen und für datenschutzrechtliche Fragestellungen zu sensibilisieren. Die Art und Weise, wie verantwortliche Führungskräfte und behördliche Datenschutzbeauftragte Verstöße aufarbeiten, trägt maßgeblich dazu bei, die internen Prozesse zu verbessern. So können künftige Verstöße vermieden werden.

4.2.3 Abruf von Personalausweisbildern bei Verkehrsordnungswidrigkeiten

Im Berichtszeitraum erreichte uns eine Beschwerde zu folgendem Sachverhalt: Der Beschwerdeführer erhielt im Rahmen einer **Verkehrsordnungswidrigkeit** am 30. Dezember 2020 ein Schreiben mit einem Anhörungsbogen des zuständigen Landkreises, das auf den 23. Dezember 2020 datiert war. Am 4. Januar 2021 beauftragte er seinen Anwalt, mit dem Kreis Kontakt aufzunehmen. Dies erfolgte am 5. Januar 2021. Am 6. Januar 2021 stellte die Bußgeldstelle beim Einwohnermeldeamt einen **Antrag auf Übermittlung eines Personalausweis- oder Passfotos**. Der Beschwerdeführer sah sich durch diesen Abruf in seinen Rechten verletzt. Der Abruf sei nicht erforderlich gewesen, da er bereit war, am Verfahren mitzuwirken, und so schnell wie möglich auf die Anhörung des Kreises reagiert habe. Auf eine vorherige Beschwerde beim Kreis wurde dem Petenten mitgeteilt, dass der Abruf von Bildern datenschutzrechtlich das mildeste Mittel sei, um den Fahrer zu ermitteln. Außerdem würde auch das ULD auf seiner Webseite diese Verfahrensweise grundsätzlich befürworten.

Eine Prüfung des Sachverhalts ergab, dass der Abruf der Personalausweisdaten – exakt zwei Wochen nach dem Datum des Anhörungsschreibens – datenschutzrechtlich problematisch gewesen war. Der Abruf von Bilddaten beim zuständigen Einwohnermeldeamt dient der Ermittlung des Fahrers. Äußert sich der Halter eines Fahrzeugs nicht zu dem festgestellten Verstoß, muss die Bußgeldbehörde auf anderem Weg den Fahrer ermitteln. Regelmäßig wird in solch einem Fall anhand von Personalausweis- oder Passfotos überprüft, ob der Halter oder ein Familienangehöriger gefahren ist. Der Abruf der Bilder im Rahmen der Fahrerermittlung ist dabei weniger eingriffsintensiv als z. B. eine Befragung von Nachbarn oder Familienangehörigen. Selbstverständlich gilt aber: Der Abruf ist trotzdem **nur dann zulässig, wenn der**

Fahrer auf anderem Weg nicht ermittelt werden konnte. Im ersten Schritt muss versucht werden, den Fahrer im Rahmen des Anhörungsverfahrens zu ermitteln.

Im vorliegenden Fall war der Beschwerdeführer bereit gewesen, Angaben zur Sache zu machen. Der **Abruf der Bilddaten** erfolgte somit **verfrüht**, da das Anhörungsverfahren im zugrunde liegenden Zeitraum faktisch nicht abgeschlossen werden konnte.

Im Ergebnis hat der Kreis **Änderungen für das Anhörungsverfahren** angekündigt. Die interne Frist, bevor Personalausweis- oder Passfotos zum Zweck der Fahrerermittlung abgerufen werden, soll verlängert werden. Auf diese Weise wird sichergestellt, dass auch in speziellen Konstellationen – wie in diesem konkreten Fall – den Betroffenen die Möglichkeit gegeben wird, ihre Rechte wahrzunehmen.

Was ist zu tun?

Auch andere Behörden, die Verkehrsordnungswidrigkeiten ahnden, sollten prüfen, ob ihre internen Fristen angepasst werden müssen. Dies kann saisonal oder generell geregelt werden.

4.3 Justiz

4.3.1 Gesetz zur ambulanten Resozialisierung und zum Opferschutz (ResOG SH)

Im Berichtszeitraum hat der Schleswig-Holsteinische Landtag ein Gesetz zur ambulanten Resozialisierung und zum Opferschutz verabschiedet. Das Gesetz regelt die Organisation, die Praxis und auch die Datenverarbeitung der Ambulanten Sozialen Dienste der Justiz und weiterer Einrichtungen der Resozialisierung.

Wir haben zu dem Gesetzentwurf Stellung genommen und an einer Anhörung im Innen- und Rechtsausschuss des Landtags teilgenommen. Im Laufe des Gesetzgebungsverfahrens sind durch den Landtag einige **Verbesserungen** vorgenommen worden, mit denen unsere wesentlichen Kritikpunkte ausgeräumt wurden:

- Im Gesetzentwurf waren weitreichende Befugnisse zur zweckändernden Übermittlung von Daten an Dritte durch **Bewährungshelferinnen und Bewährungshelfer** vorgesehen. Durch eine Änderung wurde nun klargestellt, dass die Übermittlungsbefugnisse nicht für Geheimnisträgerinnen und Geheimnisträger gelten.
- Für den Schutz sogenannter besonderer Kategorien personenbezogener Daten, wie etwa Angaben zur Gesundheit, zur Religionszugehörigkeit oder zur rassischen und ethnischen Herkunft sind spezifische Anforderungen für technische und organisatorische Maßnahmen aufgenommen worden.
- Eine missverständlich formulierte und daher zu weitreichende Regelung zur Datenübermittlung an private Dritte wurde gestrichen.

Ein grundlegender Kritikpunkt, der nicht nur für dieses, sondern für eine Vielzahl bereichsspezifischer Landesgesetze gilt, wurde im Gesetzgebungsverfahren leider nicht ausgeräumt: Die **Terminologie** in diesem und in anderen Fachgesetzen ist nicht an das neue Datenschutzrecht angepasst. Es werden vielfach noch die Begrifflichkeiten aus dem früheren LDSG verwendet, die mittlerweile im LDSG nicht mehr enthalten und somit nicht mehr legal definiert sind. Dies betrifft insbesondere den neuen Begriff der Verarbeitung nach der DSGVO und der JI-Richtlinie. An dessen Stelle werden im ResOG SH und in anderen neuen Fachgesetzen noch häufig die Begriffe „Erheben“, „Speichern“, „Nutzen“ und „Übermitteln“ verwendet. Hierdurch können Regelungslücken entstehen (siehe auch Tz. 1.4).

4.3.2 Meldungen über Datenpannen in der Justiz

Vor zwei Jahren hatten wir darüber berichtet, dass aus dem Bereich der Justiz nur eine Meldung einer Verletzung des Schutzes personenbezogener Daten bei uns eingegangen war. Im Berichtszeitraum hat sich die Anzahl der Meldungen leicht erhöht; es sind **insgesamt fünf Meldungen** eingegangen. Im Vergleich zu den Meldungen, die aus anderen öffentlichen Stellen des Landes eingehen, ist die Zahl immer noch sehr gering. Die Meldungen kommen aus unterschiedlichen Gerichten und auch aus dem Bereich der Staatsanwaltschaften, sodass wir davon ausgehen, dass die Meldepflicht inzwischen in der Justiz dem Grunde nach bekannt ist. Ob tatsächlich jede Datenpanne erkannt, intern kommuniziert oder an uns als Aufsichtsbehörde gemeldet wird, bleibt angesichts der niedrigen Anzahl der Meldungen fraglich.

Aus diesem Grund weisen wir nochmals auf die **Meldepflicht nach der DSGVO, nach der Strafprozessordnung und dem Bundesdatenschutzgesetz** hin. Im Bereich der Justiz sind Verletzungen des Schutzes personenbezogener Daten häufig mit einem Risiko für die Rechte und Freiheiten der betroffenen Personen verbunden, da oftmals besondere Kategorien personenbezogener Daten verarbeitet werden, strafrechtliche Verurteilungen bekannt werden können oder die Daten geeignet sind, den Ruf der betroffenen Person zu schädigen, oder zu anderen Nachteilen führen können.

Der Europäische Datenschutzausschuss hat eine Leitlinie veröffentlicht, die Beispiele zu Datenpannenmeldungen enthält und Verantwortliche dabei unterstützt, das Risiko solcher Verletzungen zu bewerten (Tz. 11.2). Sie ist unter dem folgenden Link abrufbar:

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_de

Kurzlink: *https://uldsh.de/tb40-4-3-2*

Erwägungsgrund 75 der DSGVO

Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, [...] wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

Was ist zu tun?

Auch im Bereich der Justiz müssen die Verantwortlichen sicherstellen, dass die Beschäftigten für die Meldepflicht in Bezug auf Verletzungen des Schutzes personenbezogener Daten sensibilisiert sind, damit diese Vorfälle erkannt und korrekt an die Aufsichtsbehörde kommuniziert werden. Neben der Meldung ist wesentlich, geeignete Maßnahmen zu treffen, um etwaige negative Auswirkungen für die betroffenen Personen abzumildern. Zu prüfen ist auch, ob die betroffenen Personen zu benachrichtigen sind.

4.4 Soziales

4.4.1 Homeoffice – Risiken für den Sozialdatenschutz

Was ist bei Heim- bzw. Telearbeit mit Sozialdaten zu beachten? Im 37. TB, Tz. 4.5.2 hatten wir die wichtigsten Punkte als Empfehlungen dargestellt. Wie notwendig es ist, insbesondere für den Transport und die Verwahrung der konventionellen Datenträger verbindliche Vorgaben festzulegen und deren Einhaltung zu kontrollieren, zeigen die zwei folgenden Beispiele.

Der erste Fall betrifft ein Jugendamt. Ein Mitarbeiter wollte Jugendhilfeakten im Homeoffice bearbeiten. Die Akten enthielten u. a. Namen, Anschriften, Geburtsdaten, Anamnesebögen zur kindlichen Entwicklung, Mitteilungen der Polizei zu begangenen Straftaten, Anklagen der Staatsanwaltschaften und vertrauliche Berichte der Kinder- und Jugendpsychiatrie. Der Mitarbeiter verwendete für den **Transport der Akten seinen privaten Rucksack**. Auf dem Weg nach Hause legte der Mitarbeiter auf einer **Parkbank** eine Pause ein, um zu telefonieren. Als er den Heimweg fortsetzte, vergaß er den Rucksack samt Akten. Erst Wochen später wurden die Akten dem Jugendamt zurückgegeben. Das Fehlverhalten des Mitarbeiters war der verantwortlichen Stelle zuzurechnen, da nicht eindeutig geregelt war, in welchen Fällen und wie der Transport derartig sensibler Akten erfolgen darf. Es fehlte zudem an Vorgaben etwa zur Beschränkung der Aktenanzahl, Beschränkungen des zu transportierenden Aktenumfangs in Bezug auf die Dauer einer häuslichen Arbeit, Anforderungen an die Dokumentation einer Mitnahme von Akten in den häuslichen Bereich oder Regelungen zu einer vorherigen Rücksprache mit Vorgesetzten. Auch war nicht ersichtlich, ob und inwieweit eine Kontrolle der verwendeten Transportverhältnisse auf deren Eignung erfolgte.

Auch im zweiten Fall ging ein Rucksack mit dienstlichen Unterlagen verloren. Diesmal betraf es ein Jobcenter. Der Rucksack wurde offenbar **aus einem nicht verschlossenen Auto entwendet**. Die Mitarbeiterin hatte die Unterlagen nicht direkt nach Hause gebracht, sondern war noch einmal in die Stadt gefahren, um etwas zu erledigen. Betroffen waren in diesem Fall sogar 50 Personen. Wieder fehlte es an den entsprechenden Vorgaben.

https://www.datenschutzzentrum.de/tb/tb37/kap04_5.html

Kurzlink: *https://uldsh.de/tb40-4-4-1*

Welche **negativen Folgen** diese Datenschutzverstöße für die Betroffenen hatten, lässt sich nur erahnen. Wir haben wegen dieser Datenschutzverstöße Verwarnungen ausgesprochen. Den Beschäftigten drohen dienstrechtliche Konsequenzen.

Was ist zu tun?

Für die Heim- bzw. Telearbeit mit Sozialdaten benötigen die Beschäftigten verbindliche schriftliche Vorgaben mit konkreten Festlegungen, um insbesondere bei dem Transport und der Verwahrung die Sicherheit der Datenträger sicherzustellen. Die oder der behördliche Datenschutzbeauftragte sollte bei der Kontrolle der Einhaltung dieser Vorgaben eingebunden werden.

4.5 Schutz des Patientengeheimnisses

4.5.1 Zulässigkeit der Erhebung von Patientendaten per Corona-Fragebögen in Zahnarztpraxen

Auch in Schleswig-Holstein haben im letzten Jahr einzelne Zahnarztpraxen von Patientinnen und Patienten verlangt, dass diese einen sogenannten **Corona-Fragebogen** ausfüllen. Patienten sollte u. a. angeben, ob sie aktuell unter Symptomen wie Fieber, Atemproblemen, Kopfschmerzen, Übelkeit/Erbrechen, Durchfall, Husten, Muskel- und Gelenkschmerzen, Halsschmerzen oder Schnupfen leiden. Auch nach Vorerkrankungen wurde gefragt.

Sind dies zulässige Fragen in einer Zahnarztpraxis? Es kommt darauf an, warum gefragt wird. Außerdem hat sich die Rechtslage im Laufe des Berichtsjahrs geändert: Für den vorgetragenen Sachverhalt war die Rechtslage vor der Änderung des Infektionsschutzgesetzes vom 23.11.2021 maßgeblich.

Bei den abgefragten Daten zu möglicherweise vorliegenden Symptomen und zu etwaigen Vorerkrankungen handelt es sich um **Gesundheitsdaten**, mithin um besondere Kategorien von personenbezogenen Daten. Die Verarbeitung dieser Daten ist nur zulässig, wenn hierfür eine ausreichende Befugnis vorliegt, die sich insbesondere aus einer Rechtsvorschrift oder der Einwilligung der betroffenen Person ergeben kann. Eine Zahnarztpraxis ist auf der Grundlage des Behandlungsverhältnisses befugt, von den Patientinnen und Patienten die Daten zu erheben, die **für die medizinische Diagnose oder für die Versorgung oder Behandlung erforderlich** sind (Art. 9 Abs. 2 Buchstabe h DSGVO bzw. § 22 Abs. 1 Nr. 1 Buchstabe b BDSG).

Die Verwendung derartiger Corona-Fragebögen bzw. die damit verbundene Erhebung und Speicherung von Gesundheitsdaten ist dann zulässig, wenn dies im Rahmen der Anamnese erfolgt und die Daten zur Durchführung der zahnmedizinischen Behandlung erforderlich sind. Dieser Einschätzung wurde auch von der Zahnärztekammer Schleswig-Holstein (und von der ebenfalls befragten Ärztekammer Schleswig-Holstein) nicht widersprochen.

Nicht zulässig war es allerdings, die umfangreichen Datensammlungen mit derartigen Fragebögen auf die Landesverordnung zur Bekämpfung des Coronavirus SARS-CoV-2 zu stützen. In diesen Fällen teilten wir den Zahnarztpraxen mit, dass die Erhebung und Speicherung von Gesundheitsdaten zumindest **in dem beabsichtigten Umfang unzulässig** war. Bereits gesammelte Daten waren zu **löschen**; die geprüften Zahnarztpraxen sahen nach unserem Hinweis von der Verwendung derartiger Corona-Fragebögen ab.

Was ist zu tun?

(Zahn-)ärztinnen und -ärzte müssen beachten, dass im Rahmen eines Arzt-Patienten-Verhältnisses die Erhebung und Speicherung von Gesundheitsdaten erfolgen darf, soweit dies für die medizinische Diagnose oder für die Versorgung oder Behandlung der Patientin oder des Patienten erforderlich ist.

4.5.2 (Keine) Kopie von Ausweisdaten durch Apotheken bei Abgabe von FFP-Masken

Ab dem 1. Januar 2021 konnten Bürgerinnen und Bürger, die das 60. Lebensjahr vollendet hatten oder bei denen eine bestimmte Vorerkrankung bzw. ein Risikofaktor vorlag, **in einer Apotheke kostenfreie Schutzmasken** erhalten. So stand es in der Verordnung zum Anspruch von Schutzmasken zur Vermeidung einer Infektion mit dem Coronavirus SARS-CoV-2 (Coronavirus-Schutzmasken-Verordnung – SchutzmV) vom 14.12.2020. Diese Maßnahme sollte einfach und unkompliziert dazu beitragen, die Coronapandemie in den Griff zu bekommen.

In den Apotheken herrschte nicht nur ein großer Andrang, sondern auch große Unsicherheit, ob bzw. wie die Abgabe der Schutzmasken zu dokumentieren ist. Schließlich galt es doch, eine unberechtigte Mehrfachabgabe von Schutzmasken zu verhindern, oder etwa nicht?

Einige Apothekerinnen und Apotheker wollten sichergehen, notierten daher den **Namen und die Anschrift ihrer Kunden** und ließen diese den Erhalt der kostenfreien Schutzmasken in einer **Kundenliste mit Unterschrift** bestätigen. Andere Apothekerinnen und Apotheker **kopierten sogar die vorgelegten Personalausweise**. Diese Datensammelei gefiel nicht jedem Kunden, aber wer sich weigerte, bekam keine Schutzmasken.

Wir haben darauf hingewiesen, dass die Coronavirus-Schutzmasken-Verordnung keine rechtliche Verpflichtung – und auch **keine Erlaubnis** – für die Apotheken vorsah, durch die Speicherung von Kundendaten oder durch das Kopieren von Personalausweisen eine missbräuchliche Mehrfachabgabe von Schutzmasken zu verhindern. Wie hätte auch eine Kundenliste oder die Kopie eines Personalausweises schon helfen können? Schließlich konnten und durften die Daten der einzelnen Apotheken nicht untereinander abgeglichen werden.

Die von uns in Schleswig-Holstein kontaktierten Apotheken handelten unverzüglich: Bereits **erfasste Kundendaten wurden gelöscht**. Die Kundenlisten und Kopien von Personalausweisen wurden vernichtet.

Was ist zu tun?

Auch in Apotheken dürfen personenbezogene Daten nur verarbeitet werden, wenn hierfür eine ausreichende Befugnis vorliegt, die sich z. B. aus einer Rechtsvorschrift oder der Einwilligung der betroffenen Person ergeben kann.

4.5.3 Telefax in Arztpraxen noch möglich?

Patientendaten unterliegen der ärztlichen Schweigepflicht und aufgrund ihrer Sensibilität als besondere Kategorien personenbezogener Daten (Gesundheitsdaten) einem hohen Schutzbedarf. Im Berichtsjahr wurde bundesweit diskutiert, ob Patientendaten per Fax übermittelt werden dürfen. Zu oft liest man schließlich von **Datenpannen aufgrund einer fehlerhaften Faxübertragung**.

Basierend auf der Veröffentlichung des **Landesbeauftragten für den Datenschutz bei der Präsidentin des Schleswig-Holsteinischen Landtages vom 17.07.1991** zur „Datensicherheit bei der Benutzung des Telefaxes-Dienstes der Deutschen Bundespost“ haben wir die Übermittlung von besonderen Kategorien personenbezogener Daten, die einer berufsrechtlichen Schweigepflicht unterliegen, per Fax beim Vorliegen folgender Voraussetzungen bislang als zulässig betrachtet:

- Es wird ein Dienstleister genutzt, auf den die Vorschriften zum „Postgeheimnis“ (hier: Telekommunikationsgeheimnis) Anwendung finden.
- Der Versender ist sich bewusst, dass er nicht nur die Verantwortung für das Sendegerät, sondern zumindest zum Teil auch für das Empfangsgerät trägt. Die Verantwortung endet nicht mit dem Versenden, sondern erst, wenn der beabsichtigte Empfänger die Sendung entgegennimmt.
- Der Versender muss vor dem Versand des Faxes sicherstellen, dass er die zutreffende, richtige und aktuelle Faxnummer des Empfängers hat.
- Der Versender versichert sich vor dem Versand, dass es bei der Eingabe der Fax-Nummer nicht zu einem Fehler gekommen ist.
- Der Versender des Faxes muss sich vor dem Versand des Faxes vergewissern, dass ausschließlich der gewünschte Empfänger das Fax entgegennimmt bzw. nur befugte Personen Zugang zu dem Faxgerät haben. Soweit erforderlich, ist insoweit die Versendung eines Faxes vorab telefonisch bei dem Empfänger anzukündigen.

Bereits im Rahmen unserer gemeinsam mit der Ärztekammer und der Zahnärztekammer durchgeführten Aktion „Datenschutz in meiner Arztpraxis“ wurde den Leistungserbringern geraten, im Gesundheitsbereich Patientendaten **nur in begründeten Ausnahmefällen und unter Beachtung der zuvor aufgezeigten Kriterien per Fax** zu übermitteln. Ein Ausnahmefall könnte sich durch eine Eilbedürftigkeit ergeben, wenn keine anderen, sicheren Kommunikationswege genutzt werden können.

Auch der Umstand, dass ein Faxversand häufig unverschlüsselt (wie bei der analogen Telefonie) erfolgt (siehe auch Tz. 10.2), war Gegenstand der Erörterung zwischen den Aufsichtsbehörden. Mit der **verschlüsselten Übertragung von Gesundheitsdaten** kann ein angemessener Schutz erreicht werden. Aus technischer Sicht stellt sich jedoch die Frage, was unter einem „verschlüsselten Fax“ zu verstehen ist. Nach unserer Einschätzung dürfte eine Verschlüsselung von Faxen zwischen beliebigen Faxgeräten allenfalls möglich sein, wenn ein Fax in eine E-Mail oder eine E-Mail in ein Fax umgewandelt werden kann.

Derzeit werten wir eine unverschlüsselte Faxkommunikation zwischen Leistungserbringern im Medizinbereich nicht pauschal und grundsätzlich als Verstoß gegen die Vorgaben des Art. 32 Abs. 1 DSGVO, sondern es erfolgt eine **Einzelfallprüfung** (siehe auch Tz. 10).

Was ist zu tun?

Bevor Patientendaten per (unverschlüsseltem) Fax versandt werden, ist zu prüfen, ob nicht ein anderer, sicherer Weg der Übermittlung möglich ist. Auch bei dem Versand von Patientendaten müssen durch entsprechende Vorkehrungen die Integrität und Vertraulichkeit der Verarbeitung personenbezogener Daten sichergestellt werden.

4.5.4 Bußgelder bei unsachgemäßem Umgang mit Gesundheitsdaten

Im Berichtszeitraum haben wir mehrere Bußgelder wegen eines unsachgemäßen Umgangs mit Patientendaten verhängt:

- In einem Fall wurden im Zuge der Aufgabe einer Arztpraxis die vorhandenen **Patientenunterlagen** einer Arztpraxis in **Altpapiercontainern** entsorgt, die zu einem von mehreren Praxen genutzten Geschäftsgebäude gehörten.
- In einem anderen Fall hatte eine Ärztin ihre Arztpraxis in ihrem Wohngebäude betrieben und die Patientenunterlagen auf ihrem **Grundstück in einem offenen Carport und in einem nicht abgeschlossenen Schuppen** gelagert.

In beiden Fällen entsprach der Umgang mit den Patientendaten nicht den Anforderungen der DSGVO an die Sicherheit der Daten. Gerade Gesundheitsdaten als besondere Kategorien personenbezogener Daten haben einen hohen Schutzbedarf. In beiden Fällen waren die Daten nicht gegen einen Zugriff durch Unbefugte gesichert. Im Fall der Aktenentsorgung im Altpapiercontainer bestand nicht nur ein abstraktes Risiko eines unbefugten Zugriffs, sondern es hat tatsächlich jemand in die Akten im ungesicherten Container geschaut – und dann die Polizei hierüber informiert.

- In einem dritten Fall hat ein Mitarbeiter eines **Testzentrums** für Corona-Schnelltests die Telefonnummer einer Testperson genutzt, um dieser abends nach dem Test **privat eine Nachricht per Messenger** zu schicken. Die Empfängerin der Nachricht hat sich daraufhin umgehend an die Polizei gewandt und Strafanzeige gestellt, weil sie mit der Kontaktaufnahme nicht einverstanden war. Eine Straftat lag zwar nicht vor, sodass die Polizei den Vorgang an uns abgegeben hat. Die zweckfremde, missbräuchliche Nutzung der Kontaktdaten stellte jedoch eine Ordnungswidrigkeit dar. Aus unserer Sicht war die Verhängung einer Geldbuße geboten, da das Vertrauen der getesteten Person in den sorgfältigen Umgang mit ihren Daten besonders gestört worden war.

Gesundheitsdaten sind besonders sensibel, weshalb für die Verantwortlichen auch besonders hohe Anforderungen an die Wahrung der Vertraulichkeit gelten. Verstöße hiergegen können das notwendige Vertrauen in das Gesundheitssystem empfindlich stören. Aus diesen Gründen ahnden wir solche Verstöße regelmäßig mit einem **Bußgeld**.

Was ist zu tun?

Beim Umgang mit Gesundheitsdaten ist besonders sorgfältig darauf zu achten, dass die Vertraulichkeit gewahrt wird. Bei Verstößen drohen Bußgelder.

4.5.5 Datenpannen im Medizinbereich: immer wieder Fehlversand von Patientenunterlagen

Schon im Vorjahr berichteten wir darüber, dass der **Fehlversand von Patientenunterlagen** eine der häufigsten Ursachen für eine Datenschutzverletzung darstellt (39. TB, Tz. 4.5.9). Dies hat sich leider nicht geändert.

Im Berichtsjahr 2021 lag in über 45 Prozent der Meldungen im medizinischen Bereich die Ursache der Datenschutzverletzung darin, dass Patientenunterlagen an falsche Personen versandt oder ausgehändigt wurden. Fast immer waren es individuelle Fehler einzelner Mitarbeiterinnen oder Mitarbeiter. So wurden beispielsweise bei der administrativen Aufnahme in eine medizinische Einrichtung falsche oder unvollständige Anschriften aufgenommen. Häufiger lag es jedoch daran, dass Beschäftigte beim Versand von Unterlagen die Adressdaten anderer Patientinnen oder Patienten verwendeten, was insbesondere immer dann geschah, wenn Beschäftigte mehrere Patientenfälle gleichzeitig

bearbeiten mussten. Erschreckend häufig wurden Patientinnen und Patienten vor Ort verwechselt, was dazu führte, dass gerade in Stresssituationen Rezepte, Atteste oder Arztberichte an falsche Personen ausgehändigt wurden. Ein Fehlversand bzw. die Aushändigung von Patientenunterlagen an Unbefugte ist keine Kleinigkeit und kann **schlimme Folgen für die betroffenen Personen** haben.

Erfreulich ist, dass der Fehlversand von Patientenunterlagen per Fax nicht mehr so häufig vorkommt. Offenbar haben auch Arztpraxen erkannt, wie schnell eine falsche Faxnummer eingetippt ist und dass es sichere Alternativen zum Faxversand gibt (siehe hierzu auch Tz. 4.5.3 und Tz. 10.2)

Was ist zu tun?

Verantwortliche müssen prüfen, ob ihre Beschäftigten, die für den Versand oder die Aushändigung von Patientenunterlagen zuständig sind, überlastet, überfordert oder nicht ausreichend geschult sind. Bei einem Fehlversand von Patientenunterlagen muss der Verantwortliche unverzüglich Kontakt mit dem unbeabsichtigten Empfänger aufnehmen und mit diesem die Rückgabe oder die datenschutzgerechte Löschung der Unterlagen vereinbaren. Die Meldung der Datenschutzverletzung an die zuständige Aufsichtsbehörde ist eine gesetzliche Pflicht.

4.5.6 Verspätete Meldung einer Fehlversendung von Impfhinweisen durch das MSGJFS

Informationen zur Terminvergabe für die Corona-Schutzimpfung in den Impfzentren kann man von dem Ministerium für Soziales, Gesundheit, Jugend, Familie und Senioren des Landes Schleswig-Holstein (MSGJFS) erhalten. Und es haben viele, sehr viele Leute das Ministerium per E-Mail um Informationen gebeten.

Ein Mitarbeiter des Ministeriums wollte sich die Arbeit anscheinend etwas leichter machen. Anstelle jedem Anfragenden einzeln zu antworten, fasste er die gewünschten Informationen in einer Antwort zusammen und sandte dann diesen Antworttext per E-Mail-Verteiler zeitgleich an **390 Anfragende**. Leider setzte er die E-Mail-Adressen dieser Anfragenden nicht in „BCC“, sondern in „CC“. Somit konnte **jeder Empfänger die E-Mail-Adressen der anderen Anfragende**n lesen, speichern und verwenden. Das gab Ärger und viele Beschwerden. Zu Recht, wie auch das Ministerium schnell erkannte.

Drei Tage später wurde ein anderer Mitarbeiter gebeten, uns als Aufsichtsbehörde „nicht nur eine Mitteilung zum Vorfall zu übermitteln, sondern auch ein formelles Verfahren einzuleiten und zu begleiten“. Dieser Mitarbeiter schickte uns daraufhin eine kurze E-Mail. Eine formelle Meldung der Verletzung des Schutzes personenbezogener Daten mit dem gesetzlich vorgesehenen Inhalt – wie in Artikel 33 DSGVO aufgeführt – blieb jedoch aus. Wir mussten ein Verwaltungsverfahren der Datenschutzaufsicht einleiten. Das Ministerium räumte ein, dass aufgrund einer innerbehördlichen Kommunikationspanne **erst nach unserer Aufforderung eine formale, vollständige Meldung** erfolgte.

Das Ministerium wurde nicht nur wegen der Verwendung des „offenen E-Mail-Verteilers“ verwarnt, sondern auch, weil die Meldung der Datenschutzverletzung nicht innerhalb der gesetzlich vorgesehenen Meldefrist erfolgte. Interne Kommunikationsprobleme oder das Hin- und Herschieben von Verantwortlichkeiten stellen keine Entschuldigung dar.

Ein Formular für die Meldung einer Verletzung des Schutzes personenbezogener Daten steht unter dem folgenden Link zur Verfügung:

https://www.datenschutzzentrum.de/meldungen/

Kurzlink: *https://uldsh.de/tb40-4-5-6*

Was ist zu tun?

Eine Verletzung des Schutzes personenbezogener Daten muss der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Datenschutzverletzung bekannt wurde, der Aufsichtsbehörde melden. Interne Verfahrensvorgaben für die Beschäftigten müssen sicherstellen, dass es nicht zu innerbehördlichen Kommunikationspannen kommen kann. Dem Datenschutzbeauftragten obliegt es, die Einhaltung der datenschutzrechtlichen Pflichten zu überwachen und den Verantwortlichen zu unterstützen.

4.5.7 Fehlende Mandantentrennung im Krankenhausinformationssystem (KIS)

Da staunte ein Patient zu Recht, als er in seiner Arztpraxis auf seinen Termin in einer psychiatrischen Klinik angesprochen wurde. Er selbst hatte gar nichts erzählt. Woher wusste die Sprechstundenhilfe dieses Arztes von seinem sensiblen Termin? Für den Patienten war dies eine unangenehme und peinliche Situation, die zu einer Beschwerde bei uns führte.

Auf Nachfrage wurde uns mitgeteilt, dass das Medizinische Versorgungszentrum (MVZ), zu dem auch die aufgesuchte Arztpraxis gehörte, gemeinsam mit diversen Kliniken für die Verarbeitung der Patientendaten ein Krankenhausinformationssystem (KIS) nutzt. Dieses KIS sah gleich zwei Funktionen vor, in denen Patiententermine eingetragen werden konnten. In diese Terminkalender wurden u. a. Patientenname, Termindatum, Terminkategorie und die Dauer der Anwesenheit gespeichert. Zudem war ein Bemerkungsfeld für Freitexteingaben vorgesehen. Es gab keine Einschränkung des Leserechts, keine Mandantentrennung. Auf diese Weise – quasi mit Blick in einen **übergreifenden Terminkalender** – hatte also die Sprechstundenhilfe des Arztes von dem **Termin des Patienten in der psychiatrischen Klinik** erfahren.

Erschwerend kam hinzu, dass in diesem gemeinsam genutzten Terminkalender seit 2014 alle Termine erfasst und niemals gelöscht worden waren. Auch die in dem Datenfeld „Bemerkungen“ notierten und zum Teil sehr detaillierten Ausführungen zu einem Termin (Diagnosen, Behandlungsnotwendigkeit, persönliche Anmerkungen usw.) waren noch da. Enthalten war also eine **umfassende Übersicht aller Termine der letzten sieben Jahre**. Zwar wurde protokolliert, wer sich diese Daten angeschaut hat, aber eine **Auswertung dieser Protokolldaten funktionierte nicht**.

In der „Orientierungshilfe Krankenhausinformationssysteme“ der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder steht, was zu beachten ist, wenn Krankenhäuser und Medizinische Versorgungszentren ein Krankenhausinformationssystem gemeinsam nutzen. Besonders wichtig ist die Mandantentrennung: Beschäftigte eines Krankenhauses (Mandant Nr. 1) dürfen nicht unbefugt auf Patientendaten eines anderen Krankenhauses (Mandant Nr. 2) oder des MVZ (Mandant Nr. 3) zugreifen können. Diese Vorgaben waren nicht beachtet worden. Der Patient hatte auch nicht seine Einwilligung dafür erklärt, dass Beschäftigte der Arztpraxen des MVZ und der vielen Kliniken bereichsübergreifend seine Termine sehen konnten.

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

Kurzlink: *https://uldsh.de/tb40-4-5-7*

Gemeinsam mit den Verantwortlichen wurde vereinbart, dass diese Terminkalender abgeschaltet und die gespeicherten Daten umgehend gelöscht werden. Zukünftig sollen Mitarbeiterinnen und Mitarbeiter nur noch den **Hinweis „Terminkollision“** erhalten, wenn ein Termin bereits anderweitig belegt ist.

Aus dieser Information darf aber nicht ersichtlich sein, wo bzw. wer den Termin bereits vergeben hat und ob es sich etwa um einen Behandlungstermin, einen Gesprächstermin für die Klärung einer Kostenfrage oder einen Besuchstermin handelt. Diese Lösung hat zudem den Vorteil, dass es keiner zusätzlichen Einwilligung der Patienten bedarf.

Was ist zu tun?

Wenn Krankenhäuser, Kliniken und Medizinische Versorgungszentren (MVZ) ein Krankenhausinformationssystem (KIS) gemeinsam nutzen, dann sind insbesondere die Vorgaben der „Orientierungshilfe Krankenhausinformationssystem – OH KIS“ zur Mandantentrennung zu beachten.

4.5.8 Einbruch / Diebstahl / Hackerangriff in der Arztpraxis

Bereits im letzten Tätigkeitsbericht schilderten wir, dass so manches Unheil von außen droht (siehe 39. TB, Tz. 4.5.10). Auch diesmal müssen wir über verschiedene Fälle berichten.

- In einer gynäkologischen Praxis wurden normalerweise alle Patientenunterlagen in verschlossenen Schränken verwahrt. Da jedoch am nächsten Tag der Umzug in die neuen Praxisräume erfolgen sollte, wurde ein Teil der Karteikarten für den Umzug in Kartons verpackt und über Nacht im Flur verwahrt. Ärgerlich, dass gerade in dieser **Nacht vor dem Umzug in die Praxis eingebrochen** wurde. Soweit man feststellen konnte, wurden keine Unterlagen gestohlen. Ob die Einbrecher Patientenakten gelesen oder Fotos gemacht haben, konnte aber nicht ausgeschlossen werden.
- Aus einer logopädischen Praxis wurden **drei Notebooks und ein iPad gestohlen**, die u. a. für die Erstellung von Therapieberichten verwendet wurden. Die Praxis versicherte zwar, dass auf diesen Geräten keine Patientendaten gespeichert waren. Aber auch in diesem Fall wurde von der Praxis eingeräumt, dass nicht auszuschließen sei, dass die Einbrecher Patientenakten gelesen oder Fotos gemacht haben.
- In einem weiteren Fall meldete eine Hausarztpraxis, dass ein **vermeintlich defekter und daher bereits ersetzter Server der Arztpraxis gestohlen** wurde. Betroffen von der Datenschutzverletzung wären die **Daten von ca. 40.000 Patienten**. Die Daten waren **nicht verschlüsselt**. Auf Nachfrage erklärte die Praxis, dass der Server im Oktober 2019 ausgetauscht, jedoch nicht fachgerecht von dem beauftragten IT-Dienstleister entsorgt wurde. Der Server stand zwei Jahre unbemerkt in der Praxis herum. Besonders heikel war, dass als Diebe offenbar nur Mitarbeiter der Praxis oder des Dienstleisters infrage kamen. Die Polizei ermittelt noch.
- In einer Vielzahl von Fällen berichteten Arztpraxen von **Hackerangriffen**. Wir erhielten Meldungen mit Überschriften wie „Emotet-Angriff“, „Ransomware-Angriff“, „Sicherheitsproblem Microsoft Exchange Server – Hafnium Exchange-Lücke!“, „Schadstoffware auf Praxisserver“ oder „Hacking-Angriff auf die Telefonanlage“. Nicht jeder Angriff führte zu einem Verlust der Vertraulichkeit von Patientendaten. Aber es zeigt, dass der Technikeinsatz für die Verarbeitung personenbezogener Daten Angriffsfläche für Angriffe aus dem Netz bietet. In allen Fällen haben wir versucht zu helfen.

Fast alle diese Fälle haben gemeinsam, dass die Patientendaten bzw. die Kenntnisnahme von Patientendaten nicht das eigentliche Ziel der Einbrecher oder Hacker waren. Das ändert aber nichts daran, dass das **Patientengeheimnis** gleichwohl in jeder der geschilderten Situationen in großer Gefahr war.

Was ist zu tun?

Es gilt weiterhin, dass ein ausreichender Einbruchschutz für Arztpraxen genauso selbstverständlich sein muss wie die erforderlichen Maßnahmen zur digitalen Informationssicherheit.

4.5.9 Freiwilliges Soziales Jahr (FSJ) im Krankenhaus contra ärztliche Schweigepflicht?

Die folgende Meldung einer Klinik über eine Datenschutzverletzung zeigt, wie schnell ein menschliches Fehlverhalten einzelner Beschäftigter schlimme Folgen für die Betroffenen haben kann: Eine Mitarbeiterin hatte unbefugt Informationen über eine Operation einer Patientin (die zudem selbst Beschäftigte der Klinik war) an unberechtigte Dritte (weitere Beschäftigte der Klinik) weitergegeben. Die betroffene Patientin war für diese Operation – einen Schwangerschaftsabbruch – stationär aufgenommen worden. Auf unsere Nachfrage wurde uns erklärt, dass es sich bei allen Beteiligten um Beschäftigte im Rahmen eines Freiwilligen Sozialen Jahres (FSJ) handelt. Man kannte einander und nun wurde fleißig getratscht. So machte die ungewollte Schwangerschaft im Wohnheim die Runde – sicherlich keine schöne Situation für die betroffene Person.

Als die Patientin hiervon erfuhr, wandte sie sich zunächst Hilfe suchend an die direkten Vorgesetzten. Diese empfahlen ihr ein klärendes Gespräch mit der Kollegin, unterrichteten jedoch nicht die Klinikleitung über die Datenschutzverletzung. Wir konnten nicht nachvollziehen, dass gerade Ärzte diesen **Vorfall anscheinend als nicht gravierend einstuften** und wohl auch nicht erkannten, welche **Folgen diese Datenschutzverletzung** für die betroffene Person hatte.

Das FSJ ermöglicht jungen Menschen einen Freiwilligendienst in sozialen Bereichen. Jugendliche, die ihre Schulpflicht erfüllt haben, können z. B. in Pflegediensten oder Krankenhäusern einen Einblick ins Berufsleben erhalten. Datenschutzrechtlich ist das FSJ mit einer Ausbildung vergleichbar. Ein FSJ darf aber nicht dazu führen, dass durch Unwissenheit oder fehlende Sensibilität der Schutz der Patientendaten gefährdet wird. Die Verantwortlichen haben daher eine besondere Pflicht, die Jugendlichen von Anfang an im Umgang mit dem Patientengeheimnis zu schulen. Die direkten Vorgesetzten müssen sich ihrer Verantwortung bewusst sein.

Die Klinikleitung teilte uns mit, dass alle FSJlerinnen und FSJler in schriftlichen Vereinbarungen **ausdrücklich zur Einhaltung der Schweigepflicht verpflichtet** werden. Die Freiwilligen würden zusätzlich eine Verpflichtungserklärung auf die Vertraulichkeit zur Wahrung des Datengeheimnisses unterschreiben und ein entsprechendes Merkblatt erhalten. Zu Beginn des FSJ erfolge im Rahmen eines Einführungskurses eine Einweisung zur Schweigepflicht. Diese Maßnahmen sind notwendig, reichen aber ganz offensichtlich nicht aus. Das Fehlverhalten einzelner Mitarbeiterinnen oder Mitarbeiter kann bei mangelnder Festlegung klarer dienstlicher Vorgaben zum Datenschutz der Klinik zugerechnet werden: **Der Verantwortliche ist eben verantwortlich.**

Patientendaten von Beschäftigten einer Klinik werden üblicherweise im Krankenhausinformationssystem (KIS) mit einem sogenannten **VIP-Kennzeichen** versehen. Die Kennzeichnung als „Very Important Person“ führt zu einem besonderen Umgang: Der Zugriff auf derartig gekennzeichnete Daten wird beispielsweise nur solchen Beschäftigten ermöglicht, die tatsächlich in die Behandlung eingebunden sind. Zudem müssen die Beschäftigten darüber in Kenntnis gesetzt werden, dass eine Protokollierung der Zugriffe auf diese Daten erfolgt. Die Klinikleitung sagte uns zu, zukünftig einzelfallbezogen **zu prüfen, ob FSJlerinnen und FSJler in die Behandlungen von Kolleginnen und Kollegen eingebunden** werden. Beschäftigte der Klinik sollen nun nicht nur zu Beginn ihrer Tätigkeit, sondern fortlaufend zum Datenschutz geschult werden.

Der Vorfall wurde zudem zum Anlass genommen, insbesondere die **Beschäftigten in Leitungsfunktionen** erneut auf die bestehenden Vorgaben zur Meldung von Datenschutzverletzungen hinzuweisen. Der Vorgesetzte, dem sich die Betroffene anvertraut hatte, wurde erinnert und entsprechend belehrt.

Was ist zu tun?

Unkenntnis von Beschäftigten im Umgang mit dem Patientengeheimnis und fehlende Sensibilität können zu Datenschutzverletzungen führen. Die Verantwortlichen müssen Beschäftigte von Anfang an schulen und diesen verbindliche und verständliche Regelungen für den Schutz von Patientendaten an die Hand geben. Die oder der betriebliche Datenschutzbeauftragte ist einzubinden.

4.6 Bildung

4.6.1 Dienstliche E-Mail-Adressen und Endgeräte für alle Lehrkräfte

Was lange währt, wird endlich gut.

Bereits im Jahre **2015** hatten wir die **Bereitstellung von dienstlichen E-Mail-Adressen für alle Lehrkräfte** an den Schulen in Schleswig-Holstein (vgl. 35. TB, Tz. 4.7.5) gefordert. Seit März 2021 verfügen alle Lehrkräfte an öffentlichen Schulen in Schleswig-Holstein über eine personalisierte dienstliche E-Mail-Adresse. Eine Vereinbarung zwischen dem Hauptpersonalrat der Lehrkräfte und dem Bildungsministerium legt fest, dass diese E-Mail-Adresse von den Lehrkräften zwingend für die dienstliche Kommunikation zu verwenden ist.

Damit verbunden sind zwei Vorteile: Zum einen müssen Lehrkräfte ihre bisher bei unterschiedlichen – teilweise auch außereuropäischen – Anbietern privat eingerichteten E-Mail-Adressen nicht mehr nutzen, um mit Schülerinnen und Schülern, Eltern oder anderen Stellen zu kommunizieren. Zum anderen, und dies ist besonders wichtig, dürfen Lehrkräfte bei Nutzung dieser dienstlichen E-Mail-Adressen auch personenbezogene Daten betroffener Personen (z. B. Schülerinnen und Schüler) versenden, soweit sie mit diesen dienstlichen E-Mail-Adressen untereinander kommunizieren, da diese Kommunikation ausschließlich im Landesnetz und nicht über das Internet erfolgt. Auch der E-Mail-Austausch mit anderen öffentlichen Stellen oder der eigenen Schulverwaltung über deren Landesnetzadressen kann jetzt im internen Landesnetz erfolgen. Aufgrund der Umsetzung in Form von Webmail-Funktionalität kann vermieden werden, dass die gesendeten und empfangenen E-Mail-Nachrichten auf lokalen Endgeräten der Lehrkräfte gespeichert sind, wo sie über ihren gesamten Lebenszyklus gegen unberechtigte Zugriffe zu sichern wären.

Das ULD hat die Umsetzung dieser technischen Dienstleistung in einem konstruktiven und vertrauensvollen Prozess mit dem **Bildungsministerium datenschutzrechtlich begleitet**.

Eine weitere datenschutzrechtliche Baustelle, die seit vielen Jahren zu Frust und Verdruss bei Lehrkräften und Schulleitungen geführt hat, wird ebenfalls demnächst geschlossen sein: Das Bildungsministerium hat sich dazu entschlossen, allen Lehrkräften der öffentlichen Schulen **dienstliche Endgeräte (Laptops und Tablets), die dem Sicherheitsstandard des Landes Schleswig-Holstein entsprechen**, für ihre Arbeit bereitzustellen. Diese dienstlichen Endgeräte können die Lehrkräfte einerseits für ihren schulischen Alltag im Rahmen der Bildungsvermittlung nutzen, andererseits können sie als Hilfsmittel für die Verarbeitung personenbezogener Daten der Schülerinnen und Schüler sowie Eltern dienen. Mit diesen Endgeräten können die Lehrkräfte beispielsweise die Dienste des Schulportals in Schleswig-Holstein in Anspruch nehmen.

4.6.2 Mängel in Datenschutzerklärungen von Schulwebseiten

Immer wieder erreichen uns Beschwerden von Bürgerinnen und Bürgern über fehlerhafte bzw. mangelhafte Datenschutzerklärungen auf Webseiten der Schulen. Die von uns daraufhin erfolgten Inaugenscheinnahmen führten zu ähnlichen Ergebnissen wie bei den **Webseiten** von anderen öffentlichen Stellen (siehe Tz. 4.1.7): Es gibt datenschutzrechtliche Defizite.

Im Regelfall haben wir den **zentralen Datenschutzbeauftragten des Bildungsministeriums für die öffentlichen Schulen** gebeten, mit den jeweiligen Schulleitungen Kontakt aufzunehmen, damit diese die Datenschutzerklärungen auf den Webseiten korrigieren.

Den Rückmeldungen des zentralen Datenschutzbeauftragten entnehmen wir, dass augenscheinlich vielen **Schulleitungen nicht bekannt war, welcher Dienstleister die Webseite** der Schule bereitstellt. Dies liegt offensichtlich daran, dass Schulen bereits vor langer Zeit Webseiten eingerichtet haben. Die Einrichtung hat im Regelfall der Schulträger für die Schulen beauftragt. Danach hat der Schulträger lediglich die jährlich anfallenden Kosten für das Webhosting getragen. Die inhaltliche Gestaltung und Aktualisierung der Webseite erfolgte und erfolgt bis heute durch Lehrkräfte der Schule. Die Schulträger haben im Regelfall keine Kenntnis darüber.

Wenn neue Schulleiterinnen und Schulleiter kommen, haben sie zumeist keine Kenntnis über die vertraglichen und datenschutzrechtlichen Verantwortlichkeiten im Zusammenhang mit dem Betrieb der schulischen Webseite. Insofern fallen ihnen die vorhandenen Defizite im Zusammenhang mit der Datenschutzerklärung auf der Schulwebseite häufig nicht auf.

Die Schulleiterinnen und Schulleiter sind aber für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Dies gilt auch für die Einhaltung der datenschutzrechtlichen Bestimmungen zur Information nach Art. 13 Abs. 1 und 2 DSGVO in Form einer Datenschutzerklärung auf der Webseite der Schule. Voraussetzung ist selbstverständlich, dass die Webseite selbst datenschutzkonform ist und beispielsweise auf die Einbindung unzulässiger Dienste verzichtet.

Was ist zu tun?

Fehlende oder fehlerhafte Informationen zur Verarbeitung personenbezogener Daten, die im Kontext mit dem Besuch oder der Benutzung einer schulischen Webseite einhergehen, stellen einen Verstoß gegen die Vorschriften der Datenschutz-Grundverordnung (DSGVO) dar. Um dies in das Bewusstsein der Schulleitungen zu rücken, empfehlen wir, dass das Bildungsministerium als oberste Fachaufsicht über die öffentlichen Schulen in Schleswig-Holstein alle Schulleiterinnen und Schulleiter auffordert, die Datenschutzkonformität ihrer Webseiten und die Datenschutzerklärungen zu prüfen.

4.6.3 Fehlversand von Informationen mit weitreichenden Folgen

In den Schulen ist es mittlerweile üblich, die Eltern über E-Mail-Verteiler mit Informationen zu versorgen. Solche Sammelnachrichten sollte man, insbesondere wenn E-Mail-Adressen von Privatpersonen berührt sind, ausschließlich so versenden, dass die **privaten E-Mail-Adressen nicht für alle Empfängerinnen und Empfänger sichtbar** sind. Dies ist beispielsweise durch Versand als sogenannte Blindkopie („Blind Carbon Copy“, „BCC“) möglich.

Diese Versandart ist unter Datenschutzgesichtspunkten als Standard zu betrachten, zumindest wenn die Daten von Privatpersonen betroffen sind. Im Schulbereich ist dies sogar explizit durch die **Dienstanweisung des Bildungsministeriums** für die Nutzung der Schulverwaltungsrechner geregelt.

Allein im Jahr 2021 wurde uns von den Schulen im Rahmen der Meldungen nach Artikel 33

DSGVO (sogenannte Datenpannenmeldungen) in zehn Fällen der irrtümliche Versand von E-Mails mit offenem E-Mail-Verteiler gemeldet. Regelmäßig war dies mit der Angabe verbunden, dass dies irrtümlich geschah.

Welche Auswirkungen es haben kann, wenn nicht sorgfältig darauf geachtet wird, solche E-Mail-Verteiler nur in „BCC“ zu nutzen, musste uns eine Schule im Rahmen einer Meldung nach Artikel 33 DSGVO mitteilen: Dort wurden **alle in offener Weise versandten E-Mail-Adressen der Eltern dieser Schule vermutlich von einem Elternteil an eine andere Person weitergeleitet**. Diese Person nutzte die E-Mail-Adressen dann für einen **Newsletter**. Zwar teilte diese Person den Eltern mit, dass sie den Datenschutz sehr ernst nehme und deshalb den Eltern angeboten habe, den Newsletter mittels E-Mail wieder abzubestellen. Allerdings fehlte auch für diese weitere Verarbeitung eine Rechtsgrundlage.

In diesem Fall wurden die E-Mail-Adressen der betroffenen Personen „nur“ für einen Newsletter missbräuchlich verwendet. Denkbar sind jedoch auch andere Szenarien, die zu tatsächlichen materiellen oder immateriellen Schäden für die betroffenen Personen führen können. In Anbetracht dessen, dass nach **Art. 82 Abs. 1 DSGVO** jede Person, der wegen eines Verstoßes gegen die Datenschutz-Grundverordnung ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen hat, sollte die Nutzung von E-Mail-Verteilern mit **äußerster Sorgfalt** erfolgen.

Was ist zu tun?

Das Bildungsministerium als oberste Fachaufsicht sollte die Schulleiterinnen und Schulleiter für etwaige Datenschutzprobleme beim E-Mail-Versand unter Hinweis auf die vorhandene Dienstanweisung sensibilisieren.

05

KERNPUNKTE

Test-, Genesenen- und Impfnachweise
Missbrauch von Kundendaten für private Zwecke
Datenpannen in der Wirtschaft
Videoüberwachung

5 Datenschutz in der Wirtschaft

5.1 Impfnachweispflicht im Unternehmen

Das ULD erreichten zahlreiche Nachfragen von Unternehmen und Beschäftigten zu Datenschutzfragen in Bezug auf den Nachweis einer erfolgten Schutzimpfung gegen das Coronavirus SARS-CoV-2 oder einer überstandenen Infektion beim Arbeitgeber.

Eine gesetzliche Regelung zur Verarbeitung eines Impfnachweises oder einer überstandenen Infektion erfolgte erst mit der Änderung des Infektionsschutzgesetzes (IfSG) im November 2021. Davor bestand eine rechtliche Unsicherheit über die erforderliche Rechtsgrundlage für die Erhebung und Dokumentation zu Nachweisen über eine Impfung oder Genesung. So wurde z. B. vertreten, dass der Impfstatus in den Fällen abgefragt werden durfte, in denen Beschäftigte mit Kundinnen und Kunden sowie anderen Beschäftigten Kontakt haben, weil hier die Schutzpflicht des Arbeitgebers zu der Verpflichtung führe, die Gesundheit der Beschäftigten durch geeignete Maßnahmen zu schützen. Eine Rechtsgrundlage dafür ergäbe sich nämlich bei Vorliegen der Voraussetzungen des § 26 Abs. 3 BDSG i. V. m. Art. 9 Abs. 2 Buchst. b DSGVO und aus den Schutzpflichten des Arbeitgebers. Arbeitgeber, die sich auf diese Rechtsgrundlage berufen wollten, mussten in einem ersten Schritt darlegen, dass die Verarbeitung des Impf- bzw. Genesenenstatus für den konkreten Verarbeitungszweck, z. B. Vorkehrungen der Arbeitssicherheit durch Schutzkleidung o. Ä., geeignet, erforderlich und unter Berücksichtigung der Beschäftigteninteressen verhältnismäßig war. In einem weiteren Schritt war dann darzulegen, dass kein Grund zu der Annahme bestand, dass die schutzwürdigen Interessen der Betroffenen die Interessen des Verantwortlichen an der Verarbeitung überwiegen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat am 31. März 2021 in einer Pressemitteilung deutlich gemacht, dass für eine Verarbeitung von pandemiebezogenen Gesundheitsdaten zwar eine Einwilligung der Beschäftigten grundsätzlich in Betracht kommt, diese allerdings nicht pauschal als freiwillig abgegeben betrachtet werden kann. Die erforderliche Abwägung ist schwierig und mit großer Rechtsunsicherheit verbunden. Darum wurde der Gesetzgeber aufgefordert, eine gesetzliche Grundlage zu schaffen. Alle Anfragenden wurden auf diese Situation hingewiesen.

Die Stellungnahme der DSK ist unter dem folgenden Link abrufbar:

https://www.datenschutzkonferenz-online.de/media/pm/20210331_pm_entschliessung_impfdaten.pdf

Kurzlink: *https://uldsh.de/tb40-5-1a*

Mit dem Gesetz zur Änderung des Infektionsschutzgesetzes und weiterer Gesetze anlässlich der Aufhebung der Feststellung der epidemischen Lage von nationaler Tragweite vom 22. November 2021 hat der Bundesgesetzgeber mit der Neufassung von § 28b IfSG Regelungen geschaffen, die **Vorgaben zur Verarbeitung des Impf-, Sero- und Teststatus von Beschäftigten** enthalten. Das ULD hat hierzu Hinweise veröffentlicht, die unter folgendem Link abrufbar sind:

https://www.datenschutzzentrum.de/artikel/1383-.html

Kurzlink: *https://uldsh.de/tb40-5-1b*

5.2 Verarbeitung von Test-, Genesenen- und Impfnachweisen in Gaststätten und Beherbergungsbetrieben

Das ULD erhielt eine Vielzahl an Beschwerden, die sich auf das Fotografieren, Scannen und Speichern von Test-, Genesenen- und Impfnachweisen, vornehmlich durch Gaststätten und

Beherbergungsbetriebe, bezogen. Weiterhin wurden Gäste von Beherbergungsbetrieben vermehrt dazu aufgefordert, diese Nachweise vorab per E-Mail zu übermitteln oder auf einen Server hochzuladen. In einzelnen Fällen wurde den Gästen mitgeteilt, dass ohne ein vorheriges Übersenden der Nachweise eine Buchung nicht möglich wäre.

Bei Informationen hinsichtlich des Test-, Genesenen- oder Impfstatus einer Person handelt es sich um Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO. Diese Daten unterliegen einem erhöhten Schutzbedarf.

Vorgaben hinsichtlich der Verarbeitung des Test-, Genesenen- und Impfstatus von Personen finden sich in der jeweils gültigen Corona-Bekämpfungsverordnung des Landes Schleswig-Holstein (Corona-BekämpfVO). Demnach gilt für bestimmte Einrichtungen, dass eine Beherbergung von Personen oder Bewirtung von Gästen innerhalb geschlossener Räume nur zulässig ist, wenn diese geimpft, getestet oder genesen sind. Die Betreiber dieser Einrichtungen müssen gewährleisten, dass diese Vorgaben eingehalten werden. Die Corona-BekämpfVO sieht vor, dass im Rahmen der Kontrolle der entsprechenden Nachweise auch eine Überprüfung der Identität mittels eines gültigen amtlichen Lichtbildausweises erfolgen muss, sofern die Person nicht persönlich bekannt ist.

Aus der Corona-BekämpfVO ergibt sich jedoch keine Verpflichtung, diese Nachweise in irgendeiner Form zu speichern oder sich diese vorab übermitteln zu lassen. Zur Erfüllung der Vorgaben aus der Corona-BekämpfVO reicht die kurze Einsichtnahme in die entsprechenden Nachweise aus. Zudem kann der Umstand vermerkt werden, dass kontrolliert wurde. Eine Rechtsgrundlage zur Verarbeitung dieser Daten kann sich nur aus Art. 6 Abs. 1 i. V. m. Art. 9 DSGVO (und gegebenenfalls weiteren landesrechtlichen Regelungen) ergeben.

Wie schon bei der Pflicht zur **Kontaktdatenerhebung** (39. TB, Tz. 5.3) zeigte sich auch bei der **Verarbeitung der Test-, Genesenen- und Impfnachweise**, dass die Speicherung oftmals aus Unwissenheit erfolgte. In vielen Fällen sahen sich die Verantwortlichen veranlasst, die Nachweise zu speichern, um im Falle einer Kontrolle die Einhaltung der Vorgaben der Corona-BekämpfVO belegen zu können. An den erhobenen Daten selbst bestand kein Interesse.

Aufgrund der Vielzahl der gemeldeten Verstöße und der Neuartigkeit der 3G-Regelung haben wir ein die Rechtslage klarstellendes Informationsschreiben erstellt und an die Gastronomie- und Beherbergungsbetriebe in Schleswig-Holstein übermittelt. Nach der Veröffentlichung des Informationsschreibens ging die Anzahl der Beschwerden hinsichtlich der Speicherung von Test-, Genesenen- und Impfnachweisen merklich zurück. Das Informationsschreiben ist unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/artikel/1380-.html

5.3 Abfrage von Corona-Daten vor Handwerkerservicetermin

Das ULD wurde im Berichtszeitraum darauf aufmerksam gemacht, dass ein Unternehmen im Rahmen von Serviceterminen im Handwerksbereich Corona-Daten der Kundinnen und Kunden abfragte. Hierzu wurde den Kundinnen und Kunden vorab ein Fragebogen zugestellt, der verschiedene Fragen zum Gesundheitszustand enthielt. So wurden neben der Frage nach dem Auftreten von Corona-Symptomen auch Informationen hinsichtlich erfolgter Kontakte zu Corona-Erkrankten, kürzlich erfolgter Reisen in ein Risikogebiet und des Gesundheitszustands von Haushalts- und Familienmitgliedern gestellt. Die Beantwortung der Fragen sollte telefonisch vor dem Termin erfolgen. Die Kundinnen und Kunden wurden darauf hingewiesen, dass ohne die Beantwortung der Fragen der Termin abgesagt werden würde. Begründet wurden diese Fragen mit dem Schutz der Servicemitarbeitenden vor einer möglichen Corona-Infektion.

Bei den abgefragten Informationen handelt es sich um Gesundheitsdaten, die einem höheren Schutzbedarf unterliegen. Eine Verarbeitung dieser Daten wäre hier nur rechtmäßig gewesen, wenn eine Einwilligung der betroffenen Kundinnen und Kunden vorgelegen hätte. Im vorliegenden Fall wurde jedoch die Erbringung der Dienstleistung an die Angaben der Kundinnen und Kunden zum aktuellen Gesundheitszustand ge-

koppelt, was keine freie Willensbekundung darstellt. Es lag demnach keine Rechtsgrundlage zur Verarbeitung der Gesundheitsdaten vor.

Anzuzweifeln waren auch die Erforderlichkeit der Daten und die Eignung der Gesundheitsfragen für den Zweck, die Servicemitarbeitenden vor einer Corona-Infektion zu schützen. Es bestand das Risiko, dass die Fragen nicht wahrheitsgemäß beantwortet worden wären, wenn ein Kunde ein starkes Interesse an der Erbringung der Dienstleistung gehabt hätte. Weiterhin sollten durch die Fragen zu Familien- und Haushaltsangehörigen auch Gesundheitsdaten von Personen erhoben werden, mit denen keine Geschäftsbeziehung bestand.

Durch das ULD wurde neben der **Löschung der erhobenen Gesundheitsdaten** verfügt, dass der Dienstleister derartige **Abfragen von Gesundheitsdaten zu unterlassen** habe. Als Alternative wird nun der Hinweis an die Kundschaft übermittelt, beim Auftreten von Corona-Symptomen den Dienstleister zu kontaktieren und ohne Angabe von Gründen eine Verlegung des Termins zu veranlassen.

5.4 Veröffentlichung von Teilaktbildern durch Fotostudio

Zum Beginn des Jahres 2021 ging bei uns eine Beschwerde eines Polizeibeamten ein, dass er von Freunden, seinem Kollegium und im Rahmen eines polizeilichen Einsatzes von einem Bürger auf ein Teilaktbild von ihm aufmerksam gemacht wurde, welches in verschiedenen Filialen eines Fotostudios aushing.

Der Betroffene berichtete hierzu, dass er zehn Jahre zuvor ein Fotoshooting besucht habe, bei dem „normale Bilder“ und ein Teilaktbild erstellt wurden. Hierbei sei ihm angeboten worden, sechs zusätzliche Fotodaten auf CD und ein Poster im Wert von 190 Euro gegen Erteilung einer Einwilligung kostenfrei zu erhalten.

Die entsprechende Vereinbarung habe er in Unkenntnis von Zweck, Art und Umfang der geplanten Verwendung der Bilder unterzeichnet, insbesondere sei ihm nicht klar gewesen, dass sich seine Zustimmung auch auf das Teilaktbild bezog und dieses umfänglichen Marketingmaßnahmen dienen sollte. Derzeit würde er auch einen Schadensersatzanspruch in erheblichem Umfang gegen das Unternehmen zivilrechtlich geltend machen.

Bei der Überprüfung der Vereinbarung stellten wir fest, dass die **zeitlich, örtlich und inhaltlich uneingeschränkte Nutzung aller beim Fotoshooting erstellten Bilder für Werbe- und Publikationszwecke** tatsächlich Bestandteil der Vereinbarung war.

Darüber hinaus handelte es sich hierbei um eine schuldrechtliche Vereinbarung, sodass die Nutzung der streitgegenständlichen Bilder als Gegenstand dieser Vereinbarung zunächst auf Grundlage des § 28 Abs. 1 Satz 1 Nr. 1 des zum damaligen Zeitpunkt geltenden BDSG rechtmäßig erfolgte. Da die Verarbeitung nach Inkrafttreten der Datenschutz-Grundverordnung auf Grundlage des Art. 6 Abs. 1 Buchst. b DSGVO erfolgen konnte, wurde von etwaigen Maßnahmen gegen das Fotostudio hierzu abgesehen.

Was ist zu tun?

Damit eine betroffene Person die Folgen ihrer Willenserklärung abschätzen kann, sind entsprechende Vereinbarungen vom Verantwortlichen hinreichend bestimmt und in einer verständlichen, klaren und einfachen Sprache zu formulieren.

5.5 Umgang mit Kundendaten im Fahrradgeschäft

In den vergangenen Monaten war in Schleswig-Holstein ein Fahrradboom zu beobachten, der in einem Fall allerdings ein datenschutzrechtliches Problem mit sich brachte: Aufgrund der hohen Auslastung einer Fahrradwerkstatt und des damit verbundenen Platzmangels wurden reservierte oder bereits verkaufte Räder nunmehr im Ladenbereich anstatt im für Kunden unzugänglichen Werkstattbereich abgestellt. Die vorliegende Beschwerde bezog sich darauf, dass an den Rädern die Auftragsformulare am Lenkrad der Fahrräder befestigt wurden und somit Fremde anhand der Auftragsformulare sehen konnten, welches Fahrrad für wen reserviert sei und wo dieser wohnen würde.

Auch Fahrradläden sind als Verantwortliche im Rahmen der Beachtung der Grundsätze der Integrität und Vertraulichkeit verpflichtet, Kundendaten in einer Art und Weise zu verarbeiten, die eine angemessene Sicherheit gewährleistet, und dabei insbesondere für einen Schutz vor unbefugter oder unrechtmäßiger Offenlegung gegenüber Dritten Sorge zu tragen.

Im Rahmen des durchgeführten Verfahrens teilte der Geschäftsführer mit, dass die Verfahrensweise nicht dem üblichen Betriebsablauf entspreche und dem situationsbedingt stark erhöhten Werkstattaufkommen mit dem damit verbundenen Platzmangel geschuldet sei. Der Vorfall wurde vom Geschäftsführer als Anlass genommen, den Betriebsablauf dahin gehend anzupassen, dass **Kundenräder** nunmehr **lediglich mit einer Auftragsnummer** statt mit Namen und Adressdaten versehen werden. Der dazugehörige Auftrag befindet sich jetzt in einem gesonderten Ordner, der nur für befugte Mitarbeitende zugänglich ist, sodass eine Offenlegung von Kundendaten gegenüber unberechtigten Dritten ausgeschlossen werden kann.

5.6 Löschung personalisierter E-Mail-Konten von Beschäftigten

Verfügen Beschäftigte über ein dienstliches personalisiertes E-Mail-Konto, stellt sich für den Arbeitgeber als Verantwortlichem bei deren Ausscheiden stets die Frage, wie mit dem E-Mail-Konto zu verfahren ist. Idealerweise wird der Umgang mit dienstlichen E-Mail-Konten im Vorhinein in einer Verfahrensbeschreibung geregelt. Eine einfache Lösung sind Funktionspostfächer, die bei einem Ausscheiden an den Nachfolger oder die Nachfolgerin übergeben werden. Handelt es sich um E-Mail-Adressen, die durch den Namen der beschäftigten Person gekennzeichnet sind, hat der Verantwortliche für deren unverzügliche Deaktivierung Sorge zu tragen.

In einem uns zur Kenntnis gelangten Fall hatte der Arbeitgeber den Posteingang eines personalisierten E-Mail-Kontos eines ausgeschiedenen Beschäftigten an einen anderen Beschäftigten weitergeleitet. Dadurch waren diesem auch E-Mails bekannt geworden, die mit privaten Inhalten an den ehemaligen Kollegen adressiert waren.

Grundsätzlich steht es dem Arbeitgeber frei, die private Nutzung eines dienstlichen E-Mail-Postfachs zuzulassen oder zu untersagen. Bei **personalisierten Postfächern** besteht aber stets die Möglichkeit, dass die oder der Beschäftigte **E-Mails mit privaten Inhalten** erhält, auch wenn das Konto von den Beschäftigten ausschließlich dienstlich genutzt wird. Solche E-Mails dürfen in jedem Fall nicht weiter inhaltlich zur Kenntnis genommen werden, sobald ihr privater Charakter deutlich wird. Dienstliche E-Mails kann sich ein Arbeitgeber zwar von den Beschäftigten vorlegen lassen, jedoch überschreitet eine automatisierte Weiterleitung in der Regel die Grenze der Erforderlichkeit für betriebliche Zwecke. Bei einem Ausscheiden einer oder eines Beschäftigten sollte daher ein personalisiertes E-Mail-Postfach umgehend mit dem Ausscheiden deaktiviert werden, damit dort keine weiteren E-Mails eingehen können.

Was ist zu tun?

Arbeitgeber sollten klare, schriftliche Vorgaben machen, wie bei einem Ausscheiden aus dem Betrieb mit dem E-Mail-Postfach und archivierten E-Mails der betroffenen Person zu verfahren ist. Ein personalisiertes Postfach ist mit dem Ausscheiden aus dem Betrieb zu deaktivieren, private E-Mails sind zu löschen. Den Beschäftigten ist schon vorab die Möglichkeit zu geben, private E-Mails zu löschen.

5.7 Nutzung von Daten aus der Hausverwaltung für Maklertätigkeit

Zahlreiche Immobilienunternehmen bieten neben der Hausverwaltung zum Teil selbst oder über Tochtergesellschaften Maklertätigkeiten an. Im Berichtszeitraum gab es hierzu einzelne Anfragen und Beschwerden, inwieweit solche Unternehmen auf personenbezogene Daten der Wohnungsverwaltung zugreifen dürfen, um für ihre Maklertätigkeiten zu werben.

Da die Verarbeitung der personenbezogenen Daten der Eigentümerinnen und Eigentümer lediglich für den Zweck der Wohnungsverwaltung erfolgt, würde eine solche Nutzung der Daten für Maklertätigkeiten eine Zweckänderung darstellen, die eine ausreichende rechtliche Befugnis erfordert.

Zweckbindung

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

Im Falle von selbstständigen Tochtergesellschaften handelt es sich um eine Datenübermittlung, die regelmäßig nicht erforderlich ist und somit ausschließlich auf Grundlage einer zuvor erteilten Einwilligung der betroffenen Person erfolgen darf.

Da auch im Falle einer Nutzung der Daten für werbliche Zwecke der Maklertätigkeit innerhalb eines Unternehmens nicht davon ausgegangen werden kann, dass eine solche Verwendung mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbar ist, wäre auch in diesen Fällen eine eigene rechtliche Grundlage für die werbliche Ansprache erforderlich. Hierbei ist u. a. zu beachten, dass Eigentümerinnen und Eigentümer vernünftigerweise nicht mit einer solchen Verwendung ihrer Daten aus der Wohnungsverwaltung rechnen müssen.

Im Rahmen eines von uns durchgeführten Verfahrens räumte ein Unternehmen den Zugriff auf E-Mail-Adressen von Eigentümern aus der Wohnungsverwaltung ein, um per E-Mail für seine Maklertätigkeit zu werben. Nach Mitteilung des Datenschutzbeauftragten habe es sich um eine rechtliche Fehleinschätzung der dortigen Geschäftsführung gehandelt. Das Unternehmen habe diese Fehleinschätzung nunmehr erkannt, bedaure dies und würde künftig **ohne Vorliegen einer entsprechenden Einwilligung der betroffenen Personen keine weiteren Werbemaßnahmen per E-Mail** mehr vornehmen. Da die entsprechenden Prozesse in Abstimmung mit dem Datenschutzbeauftragten angepasst und die Beschäftigten hierzu nochmals geschult wurden, konnte von weiteren Maßnahmen abgesehen werden.

5.8 Erhalt von Einladungen und Veranstaltungshinweisen nach Vereinsaustritt

Im Zusammenhang mit dem Vereinsaustritt hatte ein ehemaliges Mitglied die Löschung seiner Daten verlangt, was ihm umgehend vom Vorstand schriftlich bestätigt worden war. In der etwa einen Monat nach Erhalt der Löschbestätigung eingereichten Beschwerde beklagte die betroffene Person, dass ihre E-Mail-Adresse trotz der bestätigten Löschung weiterhin regelmäßig für den Versand von Einladungen und Veranstaltungshinweisen genutzt werde.

Im Rahmen des durchgeführten Verfahrens teilte der Vorstand mit, dass die personenbezogenen Daten zwar in der genutzten Mitgliedersoftware grundsätzlich gelöscht waren und daraus keine E-Mails mehr an die betroffene Person versandt wurden, es aber doch nicht ausgeschlossen werden könne, dass die betreffende **E-Mail-Adresse noch in einzelnen Verteilern des Vereins außerhalb der Mitgliedersoftware** gespeichert sei.

Nach Art. 17 Abs. 1 DSGVO haben betroffene Personen das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten gelöscht werden. Verantwortliche sind verpflichtet, die personenbezogenen Daten unverzüglich zu löschen, sofern einer der im § 17 Abs. 1 DSGVO aufgeführten Gründe zutrifft. Darüber hinaus haben betroffene Personen gemäß Art. 21 DSGVO ebenfalls das Recht, jederzeit Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einzulegen.

Im Verfahren konnte der Vorstand anhand der Absenderadressen nachvollziehen, aus welcher Quelle die E-Mails stammten und in welchen Verteilern die E-Mail-Adresse der betroffenen Person noch gespeichert war. Nach erfolgter Löschung in diesen Verteilern erhält das ehemalige Mitglied nun keine entsprechenden Einladungen und Veranstaltungshinweise mehr.

Was ist zu tun?

Der Verantwortliche hat rechtzeitig geeignete Vorkehrungen zu treffen, um jederzeit eine zügige und vollumfängliche Erfüllung der Betroffenenrechte sicherstellen zu können. Für die Umsetzung eines Löschantrags müssen sämtliche zugehörige Daten gelöscht werden.

5.9 Missbräuchliche Halterabfrage zur privaten Kontaktaufnahme

Ein junger Mann kam in der Kieler Innenstadt spontan mit einer jungen Frau ins Gespräch. Diese sah er später auf einem Parkplatz wieder, als sie in ihr Auto stieg. Hierbei notierte er sich ihr Kfz-Kennzeichen. Unter dem Vorwand, zwecks Kontaktaufnahme nach einem von ihm verursachten Schaden die Wohnanschrift zu benötigen, beantragte er kurz darauf bei der Zulassungsstelle eine Halterabfrage. Die hieraus erlangten Daten nutzte er, um der Frau zwei Postkarten zu schicken, in denen er auf das vorangegangene Gespräch verwies und um ein weiteres Treffen zum näheren Kennenlernen bat. Die junge Frau war hiervon jedoch gar nicht begeistert und reichte beim ULD Beschwerde ein.

Eine Halterabfrage bei der zuständigen Zulassungsbehörde ist nur zulässig, wenn der Empfänger darlegen kann, dass er diese 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. Zu anderen Zwecken, z. B. wie im vorliegenden Fall **zur privaten Kontaktaufnahme**, dürfen diese **Daten nicht übermittelt** werden.

Der junge Mann gab dem ULD gegenüber an, dass ihm dieser Umstand bewusst gewesen sei und er deshalb einen vermeintlich verursachten

Schaden als Grund für die Halterabfrage angegeben hätte. Generell zeigte er sich uneinsichtig, sagte aber zu, die erlangten Adressdaten nicht weiter zu verwenden und diese zu löschen.

Aufgrund der erfolgten unrechtmäßigen Verarbeitung personenbezogener Daten wurde hier eine Verwarnung nach Art. 58 Abs. 2 Buchst. b DSGVO ausgesprochen.

5.10 Missbrauch von Kundendaten für private Zwecke

Mehrere Beschwerden, die beim ULD eingingen, bezogen sich auf den Missbrauch von Kundendaten für private Zwecke. So wurden die im Rahmen der beruflichen Tätigkeiten erlangten **Handynummern** genutzt, um die Kundinnen oder Kunden **privat zu kontaktieren** und um ein näheres Kennenlernen oder auch ein persönliches Treffen zu bitten.

Art. 5 Abs. 1 Buchst. f DSGVO

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung.

Einer der Grundsätze für die Verarbeitung personenbezogener Daten sieht vor, dass diese in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung (Integrität und Vertraulichkeit). Hierzu hat der Verantwortliche geeignete technische und organisatorische Maßnahmen umzusetzen. Dies umfasst auch die Belehrung und Schulung der Mitarbeitenden hinsichtlich der datenschutzrechtlichen Bestimmungen im Umgang mit Kundendaten sowie das Aufzeigen von Konsequenzen bei Verstößen gegen diese.

In den vorliegenden Fällen hatten die Arbeitgeber ihre Beschäftigten bereits hinsichtlich der datenschutzrechtlichen Anforderungen belehrt. Gleichwohl verstießen einige Beschäftigte gegen die Vorgaben. Daraufhin wurden die Mitarbeitenden über ihr Fehlverhalten nochmals belehrt und bezüglich der Datenschutzregeln sensibilisiert, teilweise folgten personalrechtliche Konsequenzen durch die Arbeitgeber. Durch das ULD wurde eine unrechtmäßige Verarbeitung personenbezogener Daten festgestellt und gegenüber den Verantwortlichen ein Hinweis gemäß Art. 58 Abs. 1 Buchst. d DSGVO erteilt.

5.11 Datenpannen in der Wirtschaft

5.11.1 Nutzung von erbeuteten Daten

Auch im Jahr 2021 meldeten Unternehmen zahlreiche Verletzungen des Schutzes personenbezogener Daten ans ULD, bei denen Unbefugte Zugang zu E-Mail-Adressen sowie E-Mail-Inhalten erlangt hatten. Die unrechtmäßige Nutzung solcher Daten ließ in mehreren Fällen nicht lange auf sich warten: So gingen den betroffenen Personen sogenannte **Phishing-E-Mails** zu, in denen diese zur Eingabe ihrer Zugangsdaten oder zur Begleichung von Rechnungen auf ein Bankkonto der Absender aufgefordert wurden. Nicht immer ist eine solche Phishing-E-Mail für die Empfängerinnen und Empfänger als betrügerisch zu identifizieren, besonders dann nicht, wenn Zahlungsaufforderungen und E-Mails mit Kenntnis der erbeuteten E-Mail-Inhalte überzeugend gestaltet werden. Daher entstand bei mehreren betroffenen Personen ein finanzieller Schaden, da sie den Zahlungsaufforderungen nachgekommen waren.

Als ungewöhnlichen Weg, E-Mail-Adressen gewinnbringend einzusetzen, wurde in einem gemeldeten Sachverhalt die **Newsletter-Funktion eines Unternehmens** der Süßwarenbranche **missbraucht**. Hier wurden automatisiert ca. 150.000 E-Mail-Adressen zur Anmeldung für den Newsletter in das entsprechende Formular

eingefügt und in dem Feld zur (freiwilligen) Namensangabe ein eigener Link eingetragen, sodass die betroffenen Personen sämtlich eine E-Mail mit der Grußformel „Guten Tag Herr https://(...)Perfect Place for Sex Dating Online“ erhielten. Durch Öffnen des Links erfolgte eine einschlägige werbliche Ansprache, die bei direktem Versand übliche Spamfilter wohl kaum überwunden hätte. Glücklicherweise kam es jedoch nach den vorliegenden Erkenntnissen nicht zur Infizierung mit Schadsoftware. Das Unternehmen reagierte umgehend, löschte die ihm zugeflossenen E-Mail-Adressen und ergriff technische Maßnahmen zur Vermeidung eines erneuten gleichartigen Vorfalls: So wurden eine Captcha-Abfrage für die Newsletter-Anmeldung eingerichtet und die Nutzung des Formulars mit einer zeitlichen Taktungsbeschränkung belegt.

Über umfangreichere Datensätze verfügten Betrüger in einem anderen **Missbrauchsfall**, bei dem diese **fremde Identitäten zur Anmeldung von Accounts** bei einem Lotterieanbieter nutzten und auf diese Weise den mit dem Registrierungsprozess verbundenen Schufa-Identitätscheck erfolgreich durchliefen. Die für die Begleichung der Spieleinsätze verwendeten Bankdaten stammten jeweils von anderen Drittpersonen, Institutionen oder Unternehmen, die diese im Internet veröffentlicht hatten. Da zumindest mittelfristig mit einer Entdeckung der unrechtmäßigen Abbuchungen durch die Kontoinhaber zu rechnen war, wurden für den Missbrauch Lotteriespiele mit täglicher Ziehung sowie Online-Lose gewählt. Kurz vor der Auszahlung von möglichen Gewinnen erfolgte eine Änderung der Bankverbindung, um die erzielten Beträge auf das neue Konto auszahlen zu lassen. Ein finanzieller Schaden entstand den betroffenen Personen durch einen entsprechenden Ausgleich des Lotterieanbieters in diesem Fall nicht. Die verwendeten personenbezogenen Daten wurden auch in diesem Fall aus dem Produktivsystem des Unternehmens gelöscht, jedoch gesondert für den Fall der Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen verwahrt.

Die genannten Beispiele zeigen die Bedeutung der **Benachrichtigung betroffener Personen über die Verletzung des Schutzes personenbezogener Daten**, um sie in die Lage zu versetzen, selbst Maßnahmen zu ergreifen, um eigene Schäden aufgrund der Datenschutzverletzung zu vermindern oder auszuschließen. Eine Benachrichtigung erfolgte mehrfach auch dann, wenn von einem voraussichtlich hohen Risiko für die betroffenen Personen nicht auszugehen war, die Verantwortlichen sich jedoch im Sinne einer transparenten Information hierfür entschieden. Dies ist zu befürworten. In mehreren Fällen haben wir daher gegenüber Verantwortlichen, die ihrer Meldepflicht an uns nachgekommen waren, Empfehlungen zur Benachrichtigung der betroffenen Personen ausgesprochen, wenn eine missbräuchliche Nutzung der Daten möglich war, auch ohne dass von einem voraussichtlich hohen Risiko ausgegangen werden musste.

5.11.2 Datenpannen in Zusammenhang mit Beschäftigtendaten

Etwa 30 Meldungen von Verletzungen des Schutzes personenbezogener Daten im Jahr 2021 betrafen unmittelbar die Verarbeitung von Beschäftigtendaten. Wie bereits in den Vorjahren waren diese insbesondere auf fehlerhaft eingerichtete Zugriffsberechtigungen oder auf eine Ablage an einem falschen Speicherort zurückzuführen. Hinsichtlich der Speicherung von Beschäftigtendaten fehlten teilweise konkrete Vorgaben, jedoch wurden auch bestehende Vorgaben durch Mitarbeitende nicht beachtet. So war beispielsweise ein **unberechtigter Zugang möglich auf Bewerbungsdaten, von denen Kopien angefertigt** und im eigenen Bereich abgelegt worden waren, auf eine Liste über den **Impfstatus** von Beschäftigten sowie auf ganze **Personalakten**.

In mehreren Fällen erfolgte eine Versendung von personenbezogenen Daten von Beschäftigen an **falsche Empfänger**. Dies betraf sowohl die postalische Versendung als auch die Versendung per E-Mail. Hierdurch wurden sensible personenbezogene Daten aus Verdienstabrechnungen, Auflösungsverträgen und Beurteilungen der Arbeitsleistungen gegenüber externen Dritten, aber teilweise auch gegenüber unmittelbaren Kollegen offengelegt. Die Gründe für die fehlerhaften Zusendungen reichten hierbei von einer defekten Kuvertiermaschine über Versehen bei der manuellen Bearbeitung bis hin zu fehlerhaften Steuerzeilen für die Adressierung in der Software für die Erstellung der Dokumente. Letztere entstanden in einem Fall durch eine versehentliche Löschung bei einer Programmierung im Rahmen einer Anpassung, in einem anderen Fall dadurch, dass eine zuvor erfolgte Anpassung einer Standardsoftware nicht im

Patch- bzw. Update-Prozess berücksichtigt und somit **durch ein Update überschrieben** wurde. Da die jeweils durchgeführten Tests eine Prüfung der Adressierung der Dokumente nicht vorsahen, blieben die Fehler unbemerkt.

Auch die **automatische Vervollständigung von E-Mail-Adressen** war für eine fehlerhafte Auswahl von Adressaten von Bedeutung. Das entsprechende Risiko wäre hier deutlich zu vermindern, indem E-Mail-Adressen, die nicht mehr für aktuelle Schriftwechsel erforderlich sind, regelmäßig aus dem Adressbuch gelöscht würden. Obwohl dies zur Einhaltung des Grundsatzes der Datenminimierung angezeigt ist, passiert es in der Praxis nach den vorliegenden Erkenntnissen wohl eher selten.

Mehrfach wurden bei dem Versand von E-Mails Dokumente weitergeleitet oder aktiv angehängt, die personenbezogene Daten enthielten, die nicht für eine Übermittlung an die Empfänger bestimmt waren: So wurde einem Vorgesetzten ein **Attest über die Arbeitsunfähigkeit** eines Beschäftigten zugeleitet, aus dem sich Rückschlüsse auf dessen Erkrankung ziehen ließen. Einer E-Mail eines anderen Verantwortlichen wurde ein **Zwischenzeugnis** angehängt, das auf diese Weise **mehr als 300 Lieferanten** des Unternehmens zugestellt wurde. Versteckter erfolgte der ungewollte Versand in einem anderen gemeldeten Vorfall: Hier sollte den Empfängern tatsächlich eine Berechnungstabelle zugesandt werden, allerdings enthielt die angehängte Datei auf **weiteren Blättern der Tabellenkalkulation Gehaltsdaten** der Beschäftigten.

Erstaunen löste ein besonderer Fehlversand aus, bei dem ein Verantwortlicher einer der Landesbeauftragten für Datenschutz zugesandten Stellungnahme zu einer Anhörung (einen Datenschutzvorfall betreffend) als Anlage die Gewährung eines Arbeitgeberzuschusses für ein Leasingfahrrad einer Beschäftigten beifügte – was mit dem ursprünglichen Datenschutzvorfall nun gar nichts zu tun hatte, aber gleich einen neuen Fall begründete.

Soweit keine ausreichenden technischen und organisatorischen Maßnahmen getroffen waren, die eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, wurden gegenüber den Verantwortlichen Verwarnungen ausgesprochen. Zu berücksichtigen war hierbei, dass aufgrund der **hohen Sensibilität von Beschäftigtendaten** in besonderem Maße dafür Sorge zu tragen ist, dass diese rechtmäßig verarbeitet werden.

Was ist zu tun?

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung); dies betrifft auch die Speicherung von E-Mail-Adressen im Adressbuch des E-Mail-Programms. Die Einhaltung des Grundsatzes der Datenminimierung stellt zugleich eine organisatorische Maßnahme dar, die das Risiko eines Fehlversands von E-Mails vermindert, da sich die Anzahl der im Rahmen der „Autovervollständigung“ vorgeschlagenen Empfänger reduziert.

Auch sonst ist in Bezug auf Beschäftigtendaten Sorgfalt vonnöten, um Datenpannen durch beispielsweise fehlerhafte Zugriffsmöglichkeiten, falsche Adressaten oder inkorrekte Beifügung von Dokumenten zu vermeiden.

5.12 Bußgeld wegen unbefugter Zugriffe auf Kontodaten durch Mitarbeiter einer Bank

Durch eine Beschwerde wurden wir darauf hingewiesen, dass ein Mitarbeiter einer Bank über den Zeitraum von etwa einem Jahr **regelmäßig auf die Kontodaten des Beschwerdeführers zugegriffen** hatte. Der Beschwerdeführer hatte dies erfahren, weil er gegenüber der Bank eine Auskunft über die zu seiner Person verarbeiteten Daten verlangt und erhalten hatte.

Die Bank konnte ausschließen, dass es einen dienstlichen Grund für die Zugriffe gegeben hatte. Zwischen dem Mitarbeiter der Bank und

dem Beschwerdeführer bestand allerdings eine private Verbindung. Hierin lag offenkundig auch das Motiv des Bankmitarbeiters, sich regelmäßig über die Bewegungen auf dem Konto des Beschwerdeführers zu informieren. Somit konnte festgestellt werden, dass für die Kenntnisnahme der Kontodaten keine Rechtsgrundlage bestand und sie somit rechtswidrig war. Außerdem ließ sich aufklären, dass nicht die Bank, sondern der Mitarbeiter selbst für den unzulässigen Zugriff auf die Daten verantwortlich war.

Aufgrund des Verstoßes gegen die Datenschutz-Grundverordnung haben wir gegen den Mitarbeiter eine Geldbuße verhängt.

Was ist zu tun?

Der Zugriff auf personenbezogene Daten, die zu Geschäftszwecken oder zur Aufgabenerfüllung öffentlicher Stellen gespeichert werden oder zugänglich sind, ist zu privaten Zwecken unzulässig und stellt einen Verstoß gegen datenschutzrechtliche Vorschriften dar. Solche Verstöße kann die Aufsichtsbehörde mit einer Geldbuße ahnden. Daneben können den betroffenen Personen Schadensersatzansprüche zustehen. Unternehmen oder Behörden sind verpflichtet, ihre Datenbestände gegen solche unbefugten Zugriffe durch technische und organisatorische Maßnahmen zu schützen.

5.13 Videoüberwachung

5.13.1 Allgemeine Entwicklungen

Gegenüber den Vorjahren haben sich im Berichtsjahr die **Beschwerden und Anfragen zur Videoüberwachung um etwa 20 Prozent erhöht**.

Einen Schwerpunkt bildeten, wie in den Vorjahren, Beschwerden über Videoüberwachung in der Nachbarschaft. Weit mehr als die Hälfte der Beschwerden bezieht sich auf die Videoüberwachung durch Private auf ihren eigenen Grundstücken, an ihren Wohnungen oder an ihren Fahrzeugen. Hierüber haben wir bereits in den Vorjahren ausführlich berichtet (37. TB, Tz. 5.5.4). Im Berichtszeitraum mehrten sich Beschwerden über Videokameras in Fahrzeugen, die auch im geparkten Zustand ihre Umgebung überwachen. In manchen neueren Fahrzeugen sind solche Kameras bereits eingebaut.

Einen weiteren Schwerpunkt bildete im Berichtszeitraum die Videoüberwachung im Gesundheitswesen, insbesondere in Apotheken und in Krankenhäusern. In einem größeren Krankenhaus in Schleswig-Holstein wurde infolge einer Prüfung und anschließender Anordnung durch uns die vorher übermäßige Videoüberwachung in vielen Bereichen erheblich eingeschränkt. Dies betraf vor allem die Überwachung auf Fluren von Stationen.

Auch die Videoüberwachung in der Gastronomie hat uns durch mehrere Beschwerden im Berichtszeitraum beschäftigt. Während des pandemiebedingten Lockdowns haben wir zunächst alle Verfahren in diesem Bereich ausgesetzt und erst nach dessen Ende wieder aufgenommen. In einigen Fällen mussten wir die Überwachung während der Geschäftszeiten im Gastraum und in den Arbeitsbereichen, wie z. B. der Küche, untersagen.

In der deutlichen Mehrzahl der von uns geprüften Fälle reichten Hinweise an die Verantwortlichen auf die Rechtslage aus, um datenschutzkonforme Zustände herzustellen. Die Verantwortlichen haben die Hinweise aufgenommen, ihre Videoüberwachung daran angepasst und uns einen Nachweis darüber vorgelegt.

In einigen Fällen war es jedoch erforderlich, den Verantwortlichen **durch förmlichen Verwaltungsakt anzuweisen, die Videoüberwachung einzuschränken oder sonstige Änderungen vorzunehmen**. Die meisten dieser Anordnungen sind rechtskräftig und vom Verantwortlichen umgesetzt worden. In drei Fällen haben die Verantwortlichen gegen unsere Anordnung Klage erhoben. Hier sind Gerichtsverfahren anhängig. Ebenfalls noch beim Gericht anhängig ist die Untersagungsordnung

gegen die Videoüberwachung in mehreren Fitnessstudios (siehe Tz. 5.13.2).

Aufgrund der stetig steigenden Nachfrage haben wir das **Informationsangebot zur Videoüberwachung auf unserer Webseite ausgebaut**. Verantwortliche und betroffene Personen finden Informationen zu Datenschutzfragen bei einer Videoüberwachung unter dem folgenden Link:

https://www.datenschutzzentrum.de/video/

Kurzlink: *https://uldsh.de/tb40-5-13-1*

5.13.2 Videoüberwachung im Fitnessstudio, ein Dauerbrenner

Bereits in früheren Tätigkeitsberichten war die Videoüberwachung in Fitnessstudios ein wiederkehrendes Thema (35. TB, Tz. 5.6.2, 36. TB, Tz. 5.6.3, 37. TB, Tz. 5.5.6, 38. TB, Tz. 5.4.1). Seinerzeit wurden in verschiedenen Fitnessstudios einer Fitnessstudiokette sowohl der jeweilige Umkleidebereich, die Trainingsflächen und die Aufenthaltsbereiche mittels Videoüberwachung gefilmt. Gegen die von uns **im Jahr 2017 erlassene Untersagungsanordnung** für die Überwachung der Umkleidebereiche sowie Teile der Trainingsflächen ist ein Gerichtsverfahren anhängig: Die Klage des Betreibers gegen unsere Anordnung wurde in der ersten Instanz, dem Verwaltungsgericht, abgewiesen. Die **Entscheidung in der zweiten Instanz**, dem Oberverwaltungsgericht, **steht noch aus**.

In der Zwischenzeit mehren sich die Beschwerden gegen die von der Anordnung betroffene Kette sowie gegen weitere Fitnessstudios. In einem Fall mussten wir gegenüber einem Betreiber eines Fitnessstudios die Überwachung der Trainingsfläche untersagen. Bei einer Überprüfung der Videoüberwachung hatten wir festgestellt, dass die gesamte Trainingsfläche, auf der sich überwiegend fest platzierte Kardio- oder Krafttrainingsgeräte befanden, mit zwei Kameras aus verschiedenen Blickrichtungen überwacht wurde. Darüber hinaus wurden der Tresen- und der Eingangsbereich mittels Videokameras überwacht. Zur Begründung gab der Betreiber an, dass festgestellt worden sei, dass Mitglieder auch unbefugte Personen in das Fitnessstudio mitgenommen hätten und darüber hinaus insbesondere Hanteln mehrfach gestohlen worden seien. Auch habe es Sachbeschädigungen am Inventar gegeben. Zudem sei die Eingangstür mutwillig beschädigt worden, was ebenfalls durch die Kamera aufgenommen worden sei.

Die Überwachung im Eingangsbereich sowie im Bereich des Tresens und der Hantelablage war rechtmäßig. Hierfür kann sich der Betreiber auf sein berechtigtes Interesse berufen, dem keine überwiegenden schutzwürdigen Interessen der betroffenen Mitglieder und Beschäftigten entgegenstehen. Anders war die Überwachung der Trainingsflächen zu beurteilen. Hier war bereits zweifelhaft, ob eine Überwachung der gesamten Fläche überhaupt für die angegebenen Zwecke erforderlich war. Denn zur Verhinderung und Aufklärung der Mitnahme von unbefugten Personen in das Fitnessstudio reichte eine Ausrichtung einer Videoüberwachungskamera auf den unmittelbaren Eingangsbereich aus. Zur Aufklärung von Hanteldiebstählen genügte die Videoüberwachung des Aufnahme- und Ablageorts der Hanteln. Eine darüber hinausgehende Videoüberwachung, insbesondere der Trainingsbereiche, in denen sich Mitglieder sowie Beschäftigte überwiegend aufhalten, erschien nicht als erforderlich. Auch die schutzwürdigen Interessen sowohl der Mitglieder als auch der Beschäftigten wiegen in diesem Bereich schwerer. Sie halten sich hier für einen längeren Zeitraum auf. Eine Videoüberwachung bedeutet, dass sie beim Training oder bei der Arbeit beobachtet und dauerhaft aufgezeichnet werden. In der Gesamtbetrachtung war daher aufgrund der Zweifel an der Erforderlichkeit und der Gewichtung der schutzwürdigen Interessen der betroffenen Personen die Überwachung in diesem Bereich nicht gerechtfertigt.

Besucherinnen und Besucher von Fitnessstudios haben grundsätzlich ein Interesse daran, unbeobachtet ihre Freizeit zu gestalten und sich sportlich zu betätigen bzw. sich auch nur in den Räumlichkeiten aufzuhalten und mit anderen zu treffen, ohne dass ihr Verhalten von Videokameras aufgezeichnet wird. Auch die Beschäftigten haben ein Interesse daran, dass ihr Verhalten am Arbeitsplatz während der Arbeitszeit nicht dauerhaft überwacht wird. Wer ununterbrochen bei der Arbeit gefilmt wird, muss davon ausgehen, dass jede seiner Verhaltensweisen kontrolliert und rekonstruiert werden kann. Gestik und beispielsweise Mimik bei der Arbeit oder bei der Kommunikation mit Vorgesetzten und Kollegen können mit der Videoüberwachung stets dokumentiert und gegebenenfalls zu einer Leistungsbewertung des Mitarbeiters genutzt

werden. Dieses greift in einem nicht zu rechtfertigenden Maß in das schutzwürdige Interesse der Beschäftigten daran ein, dass sie ihre Tätigkeit ohne dauerhafte Überwachung ausführen können.

Zwar haben Fitnessstudiobetreiber ein berechtigtes Interesse daran, ihre Studios vor unbefugter Benutzung durch Dritte, vor Diebstahl und Sachbeschädigung zu schützen. Hierbei könnte aber eine Videoüberwachung, die rund um die Uhr betrieben wird, nur die letzte Lösung sein. Zuvor sind andere, gleich geeignete Maßnahmen in der Praxis zu prüfen. Hierzu kann auch ein verstärkter Personaleinsatz gehören, der in der Regel zuverlässiger vor Gefahren oder Schäden schützt als eine Videokamera. Sofern das Ziel nur durch Videoüberwachung erreicht werden kann, ist sie eng auf den verfolgten Zweck zu beschränken. Dies gilt zunächst räumlich für die Auswahl des zu überwachenden Bereichs. Zeitlich sind ebenfalls oft Einschränkungen möglich, sodass vielfach beispielsweise auf eine Überwachung während der Öffnungszeiten des Studios ganz verzichtet werden kann.

Auch die Dauer der Speicherung von Videoaufnahmen ist sorgfältig zu prüfen. Nach der DSGVO sind personenbezogene Daten unverzüglich zu löschen, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind. Die Erforderlichkeit der Speicherung selbst sowie einer bestimmten Speicherdauer ist für jeden Erfassungsbereich, d. h. für jede Videokamera, gesondert zu begründen. Hieraus kann folgen, dass **für unterschiedliche Kameras unterschiedlich zulässige Speicherfristen** bestehen. Die Datenschutzkonferenz und der Europäische Datenschutzausschuss haben sich darauf verständigt, dass – sofern die Voraussetzungen für eine Speicherung vorliegen – eine **Speicherung personenbezogener Daten für 72 Stunden regelmäßig für erforderlich gehalten werden kann**, sodass sie keiner gesonderten Begründung bedarf. Bei der Festlegung auf diese Speicherdauer hatten die Gremien auch besonderen Umständen wie Wochenenden und Feiertagen Rechnung getragen. Eine darüber hinausgehende Speicherung der personenbezogenen Daten ist damit nicht ausgeschlossen. Sie bedarf aber einer tragfähigen Begründung.

5.13.3 Webcam auf dem Marktplatz

Im Berichtszeitraum erreichte uns eine Beschwerde über eine Webcam, die auf den Marktplatz einer Kleinstadt in Schleswig-Holstein ausgerichtet war. Auf diesem Platz findet einmal pro Woche ein Wochenmarkt statt und auch zu den übrigen Zeiten herrscht dort reger Betrieb. Es konnte daher nicht ausgeschlossen werden, dass Personen oder Fahrzeuge von den Internetnutzenden, die die Webcam-Bilder betrachten, erkannt werden konnten. Als besonders problematisch erachteten wir eine Rückspulfunktion, die auf der Webseite enthalten war. Mit dieser ließen sich auch die aufgezeichneten Aufnahmen der letzten Stunden abrufen.

Der Verantwortliche hat auf unser Einschreiten sofort reagiert und die Webcam zunächst außer Betrieb genommen. Anschließend hat er sein Konzept für die Webcam überarbeitet und uns schließlich das Ergebnis präsentiert.

Die neu gestaltete Webcam stellt einen gelungenen Ausgleich des Interesses der Stadt, sich im Internet zu präsentieren, mit den Persönlichkeitsrechten der Besucherinnen und Besucher sowie Anwohnerinnen und Anwohner des Marktplatzes dar. Auf die **Rückspulfunktion** hat der Verantwortliche **komplett verzichtet**. Auf den Liveaufnahmen, die nun zu sehen sind, sind alle sich bewegenden Personen und Fahrzeuge stark **verpixelt** dargestellt, um einer Identifizierung vorzubeugen. Bestimmte Bereiche des Marktplatzes sind dauerhaft verpixelt dargestellt.

Was ist zu tun?

Das Beispiel zeigt, dass auch belebte Orte im Internet präsentiert werden können, ohne Personen erkennbar abzubilden. Dazu kann eine geeignete Festlegung des aufgenommenen Bildausschnitts gehören. Zudem bieten technische Lösungen eine Verpixelung oder Verunschärfung von Personen oder Objekten an.

06

KERNPUNKTE

Künstliche Intelligenz im Land – mit Datenschutz
Digitalisierungsgesetz
Ergebnisse aus Prüfungen kommunaler Rechenzentren
Erkenntnisse aus Datenpannenmeldungen

6 Systemdatenschutz

6.1 Landesebene

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

Die Zusammenarbeit mit dem zentralen IT-Management des Landes (ZIT SH) gestaltet sich gut. Wie in den Vorjahren (vgl. 39. TB, Tz. 6.1.1) wird das ULD als Gast in der Konferenz der IT-Beauftragten (ITBK) und den Koordinierungsrunden der IT-anwendenden Behörden über aktuelle und geplante IT-Projekte informiert. Schwerpunkte in diesem Jahr waren neben der Bereitstellung von zusätzlichen IT-Kapazitäten im Rahmen der Coronakrise einzelne Anwendungen und Funktionalitäten, die ausgebaut wurden, u. a. Softphones an Wechselarbeitsplätzen (sogenannte Shared Decks) und mobilen Arbeitsplätzen (siehe auch Tz. 6.1.2) und die Weiterarbeit am zentralen Lizenzmanagementtool des Landes, das die aktuell installierte Software auf den Arbeitsplatz-PCs bzw. Laptops und die dazugehörigen Lizenzen ermittelt und verwaltet.

Beteiligt wurden wir zudem im Rahmen von Stellungnahmen und Anhörungen zu Verordnungsentwürfen (u. a. zur Umsetzung des Online-Zugangs-Gesetzes, OZG) und zu Nutzungsvereinbarungen für IT-Verfahren.

An einem weiteren Projekt des ZIT SH ist das ULD beratend schon in der Anforderungs- und Entwicklungsphase beteiligt: dem Projekt zur Implementierung des Nachfolgers von Ham.s.ter, dem Inventarisierungstool für IT-Systeme. Es handelt sich dabei nicht nur um eine haushaltstechnische Verwaltungssoftware für das IT-Vermögen des Landes, sondern beinhaltet Schnittstellen, wie etwa zu Tools des IT-Managements einschließlich eines Ticketsystems bei Dataport, mit dem Austausch und Reparaturen organisiert werden. Mit diesem Tool werden ebenso die zentralen IT-Systeme wie auch PCs, Laptops, Tablets und Mobiltelefone, die Beschäftigten persönlich zugeordnet werden, verwaltet. Da derartige Zuordnungen zu Beschäftigten zu dokumentieren sind, werden auch deren personenbezogene Daten verarbeitet, was beispielsweise **Fragen der Zugriffsrechte, der Protokollierung und der Löschung** dieser Daten aufwirft. Derzeit werden im Projekt die Anforderungen der Ressorts betrachtet und zusammengestellt, bevor 2022 die Umsetzung beginnt.

6.1.2 Künstliche Intelligenz in Schleswig-Holstein – mit Datenschutz

Anwendungen der sogenannten künstlichen Intelligenz (KI) sind nicht nur in der Wirtschaft, sondern auch in Behörden angekommen und werden **verstärkt für komplexe und verantwortungsvolle Aufgaben** eingesetzt. So übernehmen beispielsweise Chatbots 24 Stunden am Tag an der Schnittstelle Bürger – Verwaltung die Aufgabe automatisierter Serviceberater. Aber auch verwaltungsintern können KI-Anwendungen, z. B. in Akten- und Vorgangsbearbeitungssystemen, steuernd und koordinativ die Arbeit der Sachbearbeitung unterstützen.

KI-Anwendungen werden typischerweise in einer Lernphase trainiert: Darin werden sie mit dem notwendigen Wissen „gefüttert“ – häufig in Form von ausgesuchten und aufbereiteten Beispielen. In dieser Lernphase benötigen KI-Systeme sehr viele Daten.

Personenbezogene Daten sind durch die Verarbeitung von KI-Systemen besonderen Risiken für die Grundrechte und Grundfreiheiten ausgesetzt. Die DSGVO liefert dafür das entsprechende Grundgerüst. Neben den allgemeinen Grundsätzen finden sich auch spezifische Regelungen für Anwendungen mit automatisierter Entscheidungsfindung, beispielsweise die Einschränkung der Verarbeitung von besonders sensiblen Daten oder die Verhinderung von diskriminierenden Auswirkungen auf betroffene Personen.

Diese Anforderungen müssen in den **unterschiedlichen Lebenszyklen** (u. a. Aufbereitung der Trainingsdaten, Training, Echtbetrieb) von komplexen KI-Anwendungen umgesetzt werden. Das **„Positionspapier KI“** der Konferenz der unabhängigen Datenschutzaufsichtsbehörden (39. TB, Tz. 10.2) definiert die grundsätzlichen Anforderungen an ein KI-System und gibt somit Entwickelnden und Verantwortlichen einen roten Faden an die Hand:

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

Kurzlink: *https://uldsh.de/tb40-6-1-2*

In der Praxis zeigt sich, dass KI-Anwendungen diese Anforderungen nicht immer erfüllen. Das kann sich beispielsweise darin äußern, dass die KI-Anwendung einen Personenbezug herstellt, obwohl die Trainingsdaten vermeintlich keinen Personenbezug enthielten. Nicht nachvollziehbare und damit kaum kontrollierbare Fehler sind ein anderes Beispiel. Die Ursachen können vielfältig sein: von einer ungenauen Zieldefinition im Design über ungeeignete Algorithmen in der Entwicklung bis zu einer unzureichenden oder ungeeigneten Datenbasis in den Trainings- oder Validierungsphasen. Aus diesem Grund ist es wichtig, dass die Akteure bei Entwicklung und Einsatz von KI-Anwendungen voneinander lernen, eine „gemeinsame Sprache“ zur **Identifikation von Problemfeldern** entwickeln und bei der Entwicklung einer KI-Anwendung nicht nur ihren eigenen Spezialbereich sehen. Dies bedingt eine **interdisziplinäre Zusammenarbeit**. Dazu gehört auch die Expertise Datenschutz.

In Schleswig-Holstein geht der **KI-Transfer-Hub**, der im Zuge der KI-Strategie der Landesregierung entstanden ist, diesen Weg. Ziel ist der Austausch von Wissen über KI-basierte Technologien, indem der KI-Transfer-Hub als Knotenpunkt Wissenschaft und Wirtschaft in Schleswig-Holstein dient. In einem Impulsvortrag konnte das ULD im Herbst 2021 die Datenschutzperspektive auf KI-Anwendungen verdeutlichen. Dabei stand neben dem rechtlichen Rahmen vor allem die Verwendung von Daten im Mittelpunkt – sowohl die offensichtlich personenbezogenen Daten als auch solche Daten, die vermeintlich keinen Personenbezug aufweisen. Die Diskussion im Anschluss des Vortrags zeigte das große Interesse zur Zusammenarbeit auf beiden Seiten, aber auch, dass im Schnittbereich zwischen Datenschutzexpertise und Wissenschaft und Wirtschaft im Bereich der künstlichen Intelligenz ein vermehrter Austausch notwendig ist.

Dies gilt in ähnlicher Weise für die Bereitstellung von KI-Verarbeitungskapazitäten, wie dies beispielsweise durch den Dienstleister Dataport erfolgt. Denn auch die praktische Seite bei der Umsetzung der oben dargestellten Anforderungen bei der Entwicklung und dem Einsatz von KI-Verfahren ist wichtig. Große Anbieter von Cloud-Service-Diensten bieten entsprechende Dienstleistungen an, z. B. spezielle KI-Modelle für Bilderkennungsverfahren, die ein Anwender mit eigenen Bildern trainieren und dann das trainierte Modell für eigene Anwendungen einsetzen kann. Da insbesondere in der Trainingsphase größere Verarbeitungskapazitäten im Hinblick auf Speicherplatz und Rechnerleistung notwendig sind als in der Anwendungsphase, hat die Nutzung von Cloud-Diensten Vorteile, da diese kurzfristig skalierbar und bedarfsangepasst verfügbar sind. Aber auch „fertige KI-Dienstleistungen“ wie KI-basierte Übersetzungsdienste werden so angeboten. In diesem Zusammenhang spricht man von „KI-Software-as-a-Service“ (oder „Artificial Intelligence-as-a-Service“, AIaaS). Für klassische Verwaltungen, aber auch für Behörden mit einem Fokus auf der Verarbeitung großer Datenmengen, beispielsweise im Umweltbereich, liegt die Nutzung von Angeboten solcher Dienstleister nahe, da sie meist keine eigene Entwicklungs- und Betriebskapazitäten für KI-Techniken haben. Werden dabei personenbezogene Daten verarbeitet, ist dies in der Regel als Auftragsverarbeitung auszugestalten. Schwierigkeiten bereiten dabei Cloud-Dienstleistungen, bei denen die Anforderungen des Datenschutzrechts nicht umgesetzt werden, beispielsweise weil die Anbieter außerhalb des EU-Rechtsrahmens agieren.

6.1.3 Verpasster Telefonanruf – kein Anschluss unter dieser Nummer?

Zunehmend werden klassische interne Telefonanlagen durch sogenannte Unified-Communications-Anlagen ersetzt, die neben der klassischen Übertragung von Sprachdaten auch Chats und Videotelefonie bereitstellen können. Außerdem unterstützen sie die Nutzenden durch Adressbücher, Rufumleitungen oder Ansage- und Anrufbeantwortungsfunktionen. Bedienung und Konfiguration können sowohl über Endgeräte (meist

klassische Telefonapparate) als auch per Webbrowser in einem Webfrontend erfolgen.

Als technische Basis für Unified-Communications-Anlagen dienen Netzverbindungen auf IP-Ebene: Die Sprachübertragung zwischen Telefonanlage und Endgerät erfolgt intern über Voice-over-IP-Verbindungen. Die Nutzenden können für die Steuerung mittels Webbrowser und die Verwendung der Chatfunktion über ihre Arbeitsplatz-PCs bzw. Laptops auf die Telefonanlage zugreifen.

Die Verbindung von Arbeitsplatz-PCs und Laptops mit der Telefonanlage eröffnet die Möglichkeit, anstelle eines klassischen Endgeräts (Hardware) ein sogenanntes **Softphone** einzusetzen, d. h. eine Software auf dem Arbeitsplatz-PC bzw. Laptop, die Telefonfunktionalität bereitstellt und die über Kopfhörer und Mikrofon die Sprachaus- und -eingabe erlaubt. Über Kamera und Bildschirm ist zusätzlich Videotelefonie möglich. Im Prinzip ist dies die Bereitstellung typischer Funktionen eines Smartphones (Telefonie, Sprach- und Videoverbindungen innerhalb von Messenging-Apps) auf Arbeitsplatz-PCs bzw. Laptops – mit dem Unterschied, dass die Kopplung an eine Firmen- oder Behördentelefonanlage erfolgt und nicht an die Netze und Anlagen der Telefonbetreiber, Mobilfunkbetreiber oder Anbieter von Messenging-Apps.

Mit solchen Softphones werden klassische Endgeräte für Telefonie nicht mehr gebraucht und auch Videotelefonie ist möglich. Typische Einsatzbereiche sind Büroarbeitsplätze, die von mehreren Personen mit eigenen Laptops genutzt werden (Shared Desk), oder das mobile Arbeiten, das dann ohne ein gesondertes Mobiltelefon auskommt, weil eine Telefonverbindung über die (Daten-)Netzverbindung des Laptops an das Firmen- bzw. Behördennetz und die interne Telefonanlage hergestellt wird. Auch das Land betreibt seit einigen Jahren für wesentliche Teile der Sprachtelefonie eine solche Unified-Communications-Anlage. Neu hinzu kommen Softphones, die in verschiedenen Ressorts eingesetzt werden.

Unterschiede zwischen den klassischen Telefonapparaten und Softphones gibt es beim Umgang mit nicht zustande gekommenen **Anrufen in Abwesenheit** (verpasste Anrufe): In der Telefonanlage des Landes lässt sich für jede Rufnummer einzeln konfigurieren, ob verpasste Anrufe protokolliert werden sollen und auf dem Endgerät bereitgestellt werden. Ebenso können in den klassischen Telefonapparaten erfolgreich ein- und ausgehende Telefonate gespeichert werden. Dies ist mit dem Anrufjournal auf privaten Festnetz- oder Mobilgeräten vergleichbar. Anders als diese Endgeräte, die typischerweise dauerhaft eingeschaltet sind, werden Laptops auch ausgeschaltet oder sind zeitweise nicht mit einem Netz verbunden. In dieser Zeit können keine Anrufe in Abwesenheit registriert werden; die Telefonanlage des Landes erlaubt derzeit auch keine individuelle Bereitstellung von Listen verpasster Anrufe für Softphones.

Call Detail Record

Datensatz aus Telefonanlagen, die Details zu erfolgreichen und erfolglosen Telefonverbindungen enthalten. Typischerweise werden die Telefonnummern der teilnehmenden Anschlüsse, Zeitpunkt und Dauer des Gespräches erfasst. Diese Daten werden beispielsweise bei der Erstellung von Einzelverbindungsnachweisen verwendet. Sie werden auch als Verbindungsdaten bezeichnet.

Um Anrufversuche in Abwesenheit auch bei Softphones mitzuspeichern, wurde vorgeschlagen, auf der zentralen Telefonanlage („Call Manager“), die alle Telefonate (erfolgreiche Verbindungen und erfolglose Anrufversuche) technisch umsetzt, eine Zusatzfunktionalität zu aktivieren: Die Telefonanlage ermöglicht die Protokollierung sämtlicher erfolgreicher Telefonverbindungen und aller Anrufversuche in sogenannten **„Call Detail Records“**. Diese Protokollierung ist derzeit deaktiviert. Würde man diese Protokollierung aktivieren und die entstehenden Protokolldaten nach erfolglosen Anrufversuchen filtern, könnte man den Nutzenden der Softphones eine Liste der Anrufversuche in einem separaten System (z. B. als Webseite) anzeigen. Ebenso könnten erfolgreiche ein- und ausgehende Telefonate aus den Call Detail Records ermittelt und bereitgestellt werden.

Das Wissen um erfolglose Anrufversuche ist im Fall von bekannten Kommunikationspartnern mitunter hilfreich, um einen Rückruf initiieren zu können. Bei Anrufversuchen von unbekannten Nummern stellt sich die Frage, ob hier wirklich Rückrufe erfolgen sollen, ob also diese Funktion erforderlich ist, die mit der Speicherung von Daten Dritter einhergeht.

Während eine Filterung der Call Detail Records und die Bereitstellung der jeweils relevanten Daten für jede einzelne Rufnummer technisch möglich ist, lässt sich die dazu notwendige Voraussetzung, die Call Detail Records überhaupt zu erfassen, in der jetzigen Implementierung **nur für alle Anschlüsse gleichermaßen aktivieren oder für alle Anschlüsse deaktivieren**. Auf

dieser Grundlage wäre aus technischer Sicht also zunächst eine Erfassung sämtlicher Telefonate der Telefonanlage als Call Detail Records mit anschließender Übertragung in ein Zweitsystem notwendig, woraufhin dann die Daten zu erfolglosen Anrufversuchen selektiv für die relevanten Anschlüsse bereitgestellt werden können.

Diese Umsetzung würde jedoch Probleme aufwerfen: Die Telefonanlage des Landes wird nicht nur von der Staatskanzlei und den Ministerien, sondern auch vom **Landtag, vom Landesrechnungshof, Gerichten** und weiteren öffentlichen Stellen genutzt, deren **Vertraulichkeitsanforderungen** generell dagegensprechen, dass die Verbindungsdaten über ihre Telefonate und Anrufversuche zentral gespeichert werden. Hinzu kommen sensible Telefongespräche, bei denen allein die Tatsache eines Anrufs oder Anrufversuchs vertraulich sein kann, z. B. im Bereich der Personalvertretungen oder im Rahmen der Aufgaben der Beauftragten für Schwerbehinderung, Korruptionsprävention, Gleichstellung, Datenschutz usw.). Auch die erlaubte Nutzung für ausgehende Privatgespräche wäre betroffen; eingehende Privatgespräche ließen sich ohnehin nicht ausschließen. In diesem Umfeld sind nach unserer Ansicht die **Regelungen des Telekommunikationsgesetzes anwendbar**, die der Speicherung dieser Verbindungsdaten sehr enge Grenzen setzt (z. B. zu Abrechnungszwecken, die hier aber nicht relevant sind).

Um eine nicht erforderliche und unzulässige Speicherung der Verbindungdaten auszuschließen, wären zumindest Ausnahmen von Dienststellen und Rufnummern von der Verarbeitung zu schaffen sowie Möglichkeiten zu einer sehr frühzeitigen Filterung und Löschung der verbleibenden Daten (z. B. im Hinblick auf erfolgreiche Telefonate) zu implementieren. Aus rechtlicher Sicht wären vorab die Rechtsgrundlagen für die Verarbeitung der Daten und Fragen der Mitbestimmung zu klären.

Eine Bereitstellung der Funktion „verpasste Anrufe“ ist somit prinzipiell auch bei Softphones möglich, erfordert aber die oben beschriebenen Einschränkungen und die Implementierung von Konfigurationsmöglichkeiten. Das Land hat nach unseren Hinweisen auf die Aktivierung einer solchen Funktion, die alle Verbindungen umfassen würde, verzichtet.

Was ist zu tun?

Bei der Beschaffung zentraler Systeme ist darauf zu achten, dass die teilnehmenden Dienststellen unterschiedliche Anforderungen haben – auch mitunter erst Jahre nach einer Beschaffung. Zentrale Systeme sollten daher umfangreiche Mandatierungs- und Konfigurationsmöglichkeiten erlauben.

6.1.4 Digitalisierungsgesetz mit KI und E-Government

Im September 2021 wurde in den Landtag ein Digitalisierungsgesetz eingebracht, das verschiedene Aspekte der Digitalisierung in Schleswig-Holstein regeln soll. Für den Datenschutz relevante Punkte sind u. a. **Regelungen zum E-Government und zum Einsatz von KI**.

Im Bereich des E-Governments gibt es beispielsweise Regelungsvorschläge zur Nutzung der OZG-Serviceportale durch Behörden, zur elektronischen Aktenbearbeitung, zum Austausch elektronischer Akten zwischen Behörden sowie zur Zustellung von Verwaltungsakten mittels elektronischer Portale. Für Behörden der Landesverwaltung wird die Nutzung von zentral bereitgestellten Basisdiensten (u. a. E-Akten-Verfahren, Landesportal, Kommunikationsschnittstellen, Formulardiensten, Bezahlverfahren) verpflichtend.

Aus Sicht des Datenschutzes ist es daher wichtig, dass diese verpflichtenden Basisdienste alle Anforderungen **aller beteiligten Stellen** erfüllen können oder sich ansonsten entsprechend ergänzen lassen. Spezifische Bedarfe können sich etwa aus rechtlichen Verpflichtungen, insbesondere im Fall einer besonderen Vertrauensstellung, ergeben. In einer solchen Situation könnten sich beteiligte Stellen nicht mit Aussagen wie „Wir setzen diese Anforderung nicht um, weil der Basisdienst dies nicht leistet.“ herausreden – Pflichtanforderungen sind umzusetzen. Es sind

daher entsprechende Ergänzungen, Anpassungen oder Konfigurationsmöglichkeiten vorzusehen (siehe auch Tz. 6.1.3 oder TB. 37, Tz. 6.3.4).

Bei dem Digitalisierungsgesetzentwurf handelt es sich um einen Entwurf für ein Mantelgesetz, das mehrere einzelne Gesetze betrifft. Im durch das Digitalisierungsgesetz als neue Rechtsnorm vorgeschlagenen IT-Einsatz-Gesetz (ITEG) will die Landesregierung erstmalig einen rechtlichen Rahmen für sich selbstständig weiterentwickelnde, datenbasierte Informationstechnologien – umgangssprachlich künstliche Intelligenz – schaffen. Dies ist angesichts des Interesses am Einsatz von sich selbstständig weiterentwickelnden Systemen und den damit verbundenen Risiken für die Rechte und Freiheiten betroffener Personen zu begrüßen. Nicht vergessen werden darf dabei, dass die Datenschutzgesetze, z. B. die DSGVO in Artikel 22, **Bedingungen an automatisierte Entscheidungen** knüpfen. So haben „betroffene Personen das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden“ (Art. 22 Abs. 1 DSGVO).

Vor dem Hintergrund hat das ULD in seinen Stellungnahmen angeregt, der Überprüfbarkeit und der Nachvollziehbarkeit sowie den Datenschutzgrundsätzen der DSGVO eine besondere Bedeutung im Gesetz zu verleihen.

Zudem haben wir eine **klarstellende Regelung** dazu angeregt, dass Daten von Beschäftigten nicht automatisiert zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden dürfen und dass der Einsatz solcher Technologien nicht zur massenweisen Identifikation von Personen – auch jenseits von dem im Gesetzentwurf genannten Verbot der Nutzung biometrischer Merkmale – zulässig ist. Wichtig ist auch, dass die sich selbstständig weiterentwickelnden, datenbasierten Informationstechnologien nicht zur Umkehr von Maßnahmen zum Schutz personenbezogener Daten wie z. B. Verschlüsselung, Anonymisierung und Pseudonymisierung verwendet werden dürfen.

Nicht allen Anregungen des ULD wurde im Rahmen der ersten Anhörung gefolgt. Anfang 2022 werden sich die Abgeordneten des Schleswig-Holsteinischen Landtages mit dem Digitalisierungsgesetz weiter befassen.

Was ist zu tun?

Unsere Anregungen zur Verbesserung des Gesetzentwurfs sollten aufgenommen werden.

6.2 Deutschlandweite und internationale Zusammenarbeit der Datenschutzbeauftragten

6.2.1 Neues aus dem AK Technik

Der AK Technik, der Arbeitskreis Technik der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, beschäftigte sich im Jahr 2021 mit zahlreichen Detailfragen zur Koordinierung einer einheitlichen Bewertung von Sachverhalten. Zu den Schwerpunkten gehörte die Betrachtung der typischen Datenverarbeitungsschritte und Datenströme bei der Nutzung von Apps zur **Kontaktdatennachverfolgung** im Rahmen der COVID-19-Bekämpfung. Hierzu wurde eine **Orientierungshilfe** erstellt:

https://www.datenschutzkonferenz-online.de/media/oh/20210429_DSK_OH_Kontaktnachverfolgung.pdf

Kurzlink: *https://uldsh.de/tb40-6-2-1a*

Ein weiterer Fokus lag auf der Erstellung einer zweiten Version der Orientierungshilfe zu „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“. Knackpunkt hier war die Frage, ob und **unter welchen Umständen ein E-Mail-Versand ohne Ende-zu-Ende-Verschlüsselung** – beispielsweise bei

Zustimmung in die Nutzung einer mit Sicherheitsrisiken verbundenen Datenverarbeitungstechnik durch die empfangende Person – zulässig sein kann. Dies war abzugrenzen von einer Einwilligung in die Weitergabe von Daten (vergleichbar einer Schweigepflichtentbindungserklärung), die im Hinblick auf Berufsgeheimnisse (z. B. ärztliche Schweigepflicht oder anwaltliches Mandantengeheimnis) möglich ist.

Die aktuelle Version der **Orientierungshilfe** ist abrufbar unter

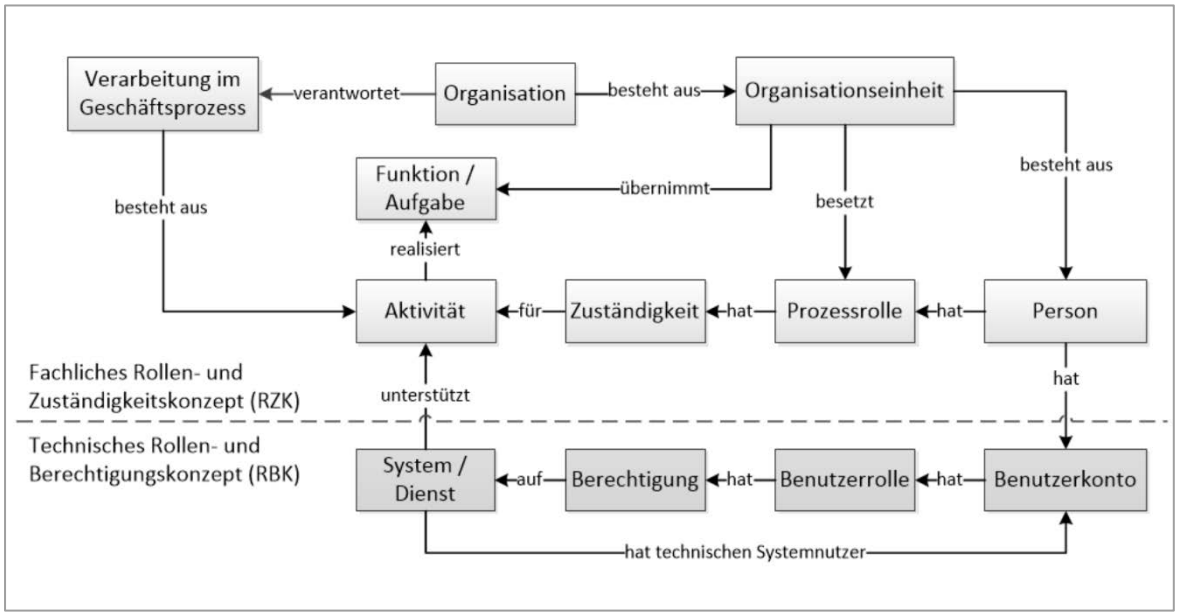
https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf

Kurzlink: *https://uldsh.de/tb40-6-2-1b*

In Arbeit sind derzeit eine Orientierungshilfe zur Nutzung von Telefax (siehe auch Tz. 10.2) sowie Zuarbeiten zu einer Veröffentlichung des Europäischen Datenschutzausschusses zur **Anonymisierung und Pseudonymisierung**. Die genaue Betrachtung von Anonymisierungsverfahren ist relevant, weil anonyme Daten nicht in den Regelungsbereich der DSGVO fallen. Die Anonymisierung von Daten (anstelle beispielsweise einer Löschung) erfolgt häufig gerade zu dem Zweck, die dann anonymisierten Daten außerhalb des Regelungsbereichs der DSGVO zu verarbeiten. Daher ist es wichtig, dass eine Anonymisierung technisch korrekt vorgenommen wird, um eine Personenbeziehbarkeit auch sicher ausschließen zu können (siehe auch Tz. 8.3). Pseudonymisierte Daten hingegen bleiben weiterhin im Regelungsrahmen der DSGVO.

6.2.2 Neuer Baustein „Zugriffe regeln“ im Standard-Datenschutzmodell

Der AK Technik der Datenschutzkonferenz verabschiedete auf der Sitzung am 27.10.2021 einen weiteren Baustein für das Standard-Datenschutzmodell (SDM) in der Version V2.0b. Es handelt sich um den **Baustein „Zugriff auf Daten, Systeme und Prozesse regeln“**. Mit diesem Baustein können das Gewährleistungsziel der Nichtverkettung bzw. der Grundsatz der Zweckbindung umgesetzt werden.



Kontext für die Vergabe der Prozess- und Benutzerrollen

Dieser Baustein ist mit 23 Seiten der umfangreichste aus der bislang insgesamt neun Bausteine umfassenden Reihe von SDM-Schutzmaßnahmen. Der Baustein listet Maßnahmen auf, um die Zweckbindung einer Verarbeitungstätigkeit auch bei komplexen Organisationsformen und modernen IT-Komponenten sicherzustellen.

Ausgangspunkt sind die zu gestaltenden Prozesse und Rollen einer Verarbeitungstätigkeit (Geschäftsprozess, Fachverfahren), Endpunkt ist die Konfiguration der technischen Zugriffsrechte an Daten, Dateien, Verzeichnissen, IT-Systemen und Prozessen. Der Baustein empfiehlt, einerseits die fachlichen Rollen und Zuständigkeiten in einem „Rollen- und Zuständigkeitskonzept“ (RZK) festzulegen und zu regeln sowie andererseits die technischen Rollen und deren Berechtigungen in einem „Rollen und Berechtigungskonzept“ (RBK) zuzuordnen (siehe Abbildung). Zur Differenzierung von Verantwortlichkeiten, die datenschutzrechtlich zentral bei der Leitung einer Organisation liegen, und den verschiedenen Zuständigkeiten der Beschäftigten einer Organisation wird die Nutzung der **RASCI-Systematik** nahegelegt.

Dieser Baustein kann von der Webseite des ULD oder aus dem zentralen SDM-Archiv des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern abgerufen werden:

https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Kurzlink: *https://uldsh.de/tb40-6-2-2*

RASCI

Durchführungsverantwortung (**R**esponsible): Person ist zuständig für die eigentliche Durchführung der Aktivität.

Gesamtverantwortung (**A**ccountable): Person ist verantwortlich im Sinne von „genehmigen“, „freigeben“ oder „unterschreiben“.

Unterstützung (**S**upport): Person hat eine unterstützende Rolle oder stellt Verarbeitungsmittel zur Verfügung.

Konsultation (**C**onsulted): Person hat relevante Informationen für die Umsetzung der Aktivität und soll/muss deshalb befragt werden.

Informationsrecht (**I**nformed): Person, die Informationen über den Verlauf bzw. das Ergebnis der Aktivität erhält oder die Berechtigung besitzt, Auskunft zu erhalten.

6.2.3 Office 365 – aktuelle Entwicklungen der Arbeitsgruppe

Schon seit längerer Zeit wird diskutiert, ob ein datenschutzgerechter Einsatz von Microsoft Office 365 in den verschiedenen Ausprägungen des Dienstes möglich ist. Verschiedene Arbeitskreise der Datenschutzkonferenz haben sich mit dem Thema beschäftigt. Um zu einer gemeinsamen und einheitlichen datenschutzrechtlichen Bewertung zu gelangen, wurde eine Arbeitsgruppe unter Federführung der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg und des Bayerischen Landesamts für Datenschutzaufsicht gegründet, die Gespräche mit dem Hersteller Microsoft aufgenommen hat.

In den seit Ende 2020 geführten Gesprächen wurden datenschutzrechtliche Problemstellungen erörtert, die sich aus den Nutzungsbedingungen für Microsoft-Produkte (Product Terms) sowie aus dem „Datenschutznachtrag für Produkte und Services“ („Data Protection Addendum“, DPA) sowie aus der grundsätzlichen Vertragsstruktur mit öffentlichen oder nichtöffentlichen Stellen ergeben. Insbesondere sollen Unklarheiten hinsichtlich der Art, des Umfangs und des Zwecks der Verarbeitung personenbezogener Daten und die eigene Verantwortlichkeit Microsofts im Rahmen der **Verarbeitung für berechtigte Geschäftszwecke** geklärt werden. Dies betrifft z. B. die Frage, ob und unter welchen Bedingungen eine Nutzung personenbezogener Daten für die Verbesserung von Funktionen oder Services als legitime Geschäftstätigkeit bewertet werden kann. Darüber hinaus muss sich die Arbeitsgruppe mit den **gegebenenfalls notwendigen Nachbesserungen und Anpassungen auf Grundlage der Schrems-II-Entscheidung** des EuGHs (Tz. 2.2) beschäftigen. Bei der Analyse durch die Arbeitsgruppe

fließt auch ein, dass sich die rechtlichen Anforderungen öffentlicher und nichtöffentlicher Stellen unterscheiden können.

Parallel zu den Gesprächen der Arbeitsgruppe wurde im Rahmen eines Pilotprojekts in Baden-Württemberg die Nutzung von Microsoft Office 365 an Schulen untersucht. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg hat sich dabei gegen eine Nutzung in Schulen ausgesprochen, da ein zu hohes Risiko der Verletzung von Rechten und Freiheiten von Lehrkräften, Lernenden und Eltern erkannt wurde. Insbesondere wurde die Sammlung und Übertragung von Telemetriedaten als problematisch eingestuft.

Die Arbeitsgruppe der DSK treibt eine Klärung der offenen Fragen voran, damit schnellstmöglich eine Bewertung bezüglich eines datenschutzgerechten Einsatzes möglich ist.

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

6.3.1 Prüfung des kommunalen Rechenzentrums Kommun.IT Zweckverband SH

Mit einem erfreulichen Ergebnis endete ein **größeres Prüfungsverfahren** beim kommunalen Rechenzentrum Kommun.IT Zweckverband SH in Elmshorn.

Kommun.IT wurde im Jahr 2008 durch einen öffentlich-rechtlichen Vertrag zwischen der Stadt Quickborn und dem Kreis Pinneberg gegründet. Im Laufe der Jahre traten mit Stand 2019 weitere Kommunen dem Zweckverband bei:

- das Amt Rantzau,
- die Gemeinde Kronshagen,
- die Stadt Barmstedt,
- das Amt Achterwehr,
- das Amt Horst-Herzhorn,
- das Amt Hürup,
- der Kreis Nordfriesland,
- der Kreis Schleswig-Flensburg,
- das Amt Kaltenkirchen,
- das Amt Mittelangeln,
- die Gemeinde Harrislee,
- die Stadt Wedel,
- das Amt Langballig und
- das Amt Südtondern.

Seitdem ist Kommun.IT um weitere Kommunen gewachsen, deren Datenverarbeitung in das Rechenzentrum von Kommun.IT migriert wurde. Kommun.IT beschäftigte mit Stand 2019 ca. 120 Mitarbeiterinnen und Mitarbeiter z. B. an den Standorten Elmshorn, Kronshagen und Husum. Die Beschäftigten betreuten zu dieser Zeit insgesamt ca. 4.000 Arbeitsplätze der angeschlossenen Kommunen.

Gegenstand der Datenschutzüberprüfung war der ordnungsgemäße und datenschutzkonforme Betrieb des Rechenzentrums. Im Rahmen der mehrtägigen Prüfung wurden Schwerpunkte auf die folgenden Bereiche gelegt:

- Zuständigkeiten und Aufgabenabgrenzung zwischen Kommun.IT und den angeschlossenen Kommunen,
- Umsetzung von Datenschutzmanagement und Datenschutzaufgaben,
- infrastrukturelle Sicherheit der personenbezogenen Datenverarbeitung,
- Schutz der technischen Komponenten für den Betrieb des Rechenzentrums und
- Dokumentation für die Nachvollziehbarkeit des Schutzes personenbezogener Daten.

An den in den Räumlichkeiten von Kommun.IT stattfindenden Prüfterminen nahmen die Geschäftsführung von Kommun.IT sowie zuständige Beschäftigte des Zweckverbands teil, die Dokumente als Nachweis der Rechtskonformität zur Verfügung stellten, auf die Fragen des Prüfteams des ULD Antworten gaben und dabei auch Sachverhalte mit eigenen Präsentationen veranschaulichten oder direkt auf den überprüften Systemen zeigten.

Im Rahmen der Prüfung wurden zunächst einige Abweichungen von datenschutzrechtlichen Anforderungen festgestellt, sodass Verbesserungsbedarf bestand. Dazu gehörten z. B.

- fehlende übergreifende Datenschutzprozesse,
- nicht angemessene Ausführung der Dienstleistung „Datenschutzbeauftragter“ für Kommunen, wo Aufgaben nach Art. 39 DSGVO nicht vollständig umgesetzt wurden,
- zu weitgehende Befugnisse im Rechtemanagement der Administratoren bei der Administration von IT-Komponenten des Rechenzentrums,
- Mängel in der Netzsicherheit durch fehlende Absicherung der Netzanschlussdosen bei den angeschlossenen Kommunen und nicht transparente Netzstrukturen,
- Mängel bezüglich der Nachvollziehbarkeit administrativer Aktivitäten, insbesondere im Bereich des Rechtemanagements und der Administration von IT-Komponenten,
- unzureichende Vertragslage im Rahmen der Auftragsverarbeitung mit mehreren Dienstleistern,
- Mängel in der Dokumentation über den Aufbau und den Betrieb des Rechenzentrums sowie der personenbezogenen Datenverarbeitungsvorgänge.

Noch während der Prüfung leitete die Geschäftsführung Maßnahmen zur Abhilfe der identifizierten Punkte ein. In einer umfassenden Stellungnahme zum Prüfbericht wurden weitere Schritte zur Beseitigung der festgestellten Mängel dargestellt.

Die abschließende Nachprüfung konnte bei Kommun.IT aufgrund der Corona-Beschränkungen erst eineinhalb Jahre später im Oktober 2021 stattfinden. Diese Zeit hatte die Geschäftsführung genutzt, um die Mängel weitgehend zu beseitigen. Die Umsetzung der Prüfpunkte konnte durch Vorlage einer ordnungsgemäßen Dokumentation nachgewiesen werden. Nur noch hinsichtlich weniger Punkte bestand Optimierungsbedarf. Hervorzuheben ist die Umsetzung des IT-Grundschutzstandards des Bundesamts für Sicherheit in der Informationstechnik. Für 2025 wird nunmehr eine ISO-27001-Grundschutzzertifizierung angestrebt, auch eine Datenschutzzertifizierung wird in Erwägung gezogen.

Zusammenfassend lässt sich sagen, dass nicht nur die Verantwortlichen von Kommun.IT die in der Prüfung festgestellten Sachverhalte mit Nachdruck bearbeitet, sondern auch die Trägerverantwortlichen von Kommun.IT **unterstützend strategische Entscheidungen zur Verbesserung der Informationssicherheit und des Datenschutzes getroffen** haben. Die Datenschutzprüfung beim IT-Zweckverband Kommun.IT wurde mithin mit positivem Ergebnis abgeschlossen.

6.3.2 Prüfung in einem weiteren kommunalen Rechenzentrum

Bereits im Jahr 2019 führte das ULD in einem weiteren kommunalen Rechenzentrum eine umfassende datenschutzrechtliche Prüfung durch. Im letzten Tätigkeitsbericht 2021 berichteten wir über die gravierenden Mängel im Rechenzentrum (siehe 39. TB, Tz. 4.1.10). Das Prüfverfahren ist leider **nach drei Jahren** immer noch **nicht abgeschlossen**. Es stellt sich chronologisch wie folgt dar:

- Nach den ersten Prüfungstagen im Januar 2019 wurde das Rechenzentrum angewiesen, einige bestehende Mängel umgehend abzustellen. Gleichzeitig wurden die Träger des Rechenzentrums mit einer Warnung nach Art. 58 Abs. 2 Buchst. a DSGVO über die Mängel informiert.
- Nach Abschluss der Prüfung im Frühjahr 2019 erhielten die Träger und das Rechenzentrum im Rahmen eines Anhörungsverfahrens Gelegenheit zur Stellungnahme. Dabei wurde dem ULD mitgeteilt, dass die bestehenden Mängel auf Grundlage einer Projektplanung behoben werden sollen.
- Die im Projektplan dokumentierten Maßnahmen wurden vom Rechenzentrum jedoch nicht wie angekündigt umgesetzt.
- Das ULD sprach daraufhin mehrere Verwarnungen aus und ordnete gegenüber dem Rechenzentrum und seinen Trägern an, die Mängel bis zum 24.03.2020 zu beheben. Die Frist zur Mängelbehebung wurde auf Bitten der Verpflichteten bis Ende April 2020 verlängert. Gegen die Bescheide erhoben das Rechenzentrum und die Träger Klage beim Verwaltungsgericht.
- Dem ULD wurde im Folgenden zugesagt, die notwendigen Maßnahmen zur Mängel-

beseitigung bis Ende November 2020 umzusetzen und das IT-Sicherheitskonzept bis zum 31.12.2020 zu finalisieren.

- Die geforderten Statusberichte über den Umsetzungsstand der Mängelbeseitigung ließen jedoch auch nach den Zusagen des Rechenzentrums und der Träger keine belastbaren Fortschritte über den Umsetzungsstand der Mängelbeseitigung erkennen, sodass das ULD im September 2020 den Status der Umsetzung der Maßnahmen im Rahmen einer Nachprüfung vor Ort kontrollierte. Die Stichprobenprüfung des Istzustands der Datenverarbeitung ergab, dass das Rechenzentrum in Bezug auf die in der Prüfung vom Frühjahr 2019 festgestellten Mängel keine wesentlichen Fortschritte vorweisen konnte. Bei der Nachprüfung wurde festgestellt, dass eine Auditierbarkeit der Umsetzung der technischen und organisatorischen Maßnahmen bis Ende November 2020 nicht erreichbar war.
- Eine erneute Nachprüfung des ULD bei dem Rechenzentrum im September 2021 führte zu dem Resultat, dass die festgestellten Mängel noch immer nicht vollständig beseitigt waren. Das ULD teilte den Verantwortlichen mit, dass der Weiterbetrieb des Rechenzentrums ohne kurzfristige Behebung der Sicherheitsmängel nicht vertretbar ist.

Im Ergebnis bleibt festzustellen, dass die Verantwortlichen der Träger und das Rechenzentrum seit 2019 die Vorschriften der DSGVO bezüglich der Datenverarbeitung im Rechenzentrum nicht vollständig einhalten.

Was ist zu tun?

Die bisherigen Bemühungen der Träger und des Rechenzentrums waren nicht ausreichend, um die bestehenden Mängel vollständig zu beseitigen. Erschwerend ist zu berücksichtigen, dass die ersten Prüffeststellungen bereits im Frühjahr 2019 getroffen wurden. Es besteht für die Verantwortlichen die Obliegenheit, umgehend die nötigen Schritte zu veranlassen.

6.3.3 Erkenntnisse aus Datenpannenmeldungen

Im Berichtsjahr 2021 sind aus technischer Sicht zwei Sicherheitsvorfälle im Rahmen der Meldungen von Verletzungen des Schutzes personenbezogener Daten (Artikel 33 DSGVO) besonders hervorzuheben. Im März 2021 sorgte die Hackergruppierung „Hafnium“ für Aufsehen, indem sie mithilfe eines sogenannten **Zero-Day-Exploits** unbekannte Schwachstellen in Microsoft Exchange-Servern ausnutzte, wodurch Inhalte aus sämtlichen Postfächern ausgelesen, beliebige Dateien abgelegt und sogar eigener Code ausgeführt werden konnte. Im Juli 2021 konnte die Hackergruppe „REvil“ den Softwareanbieter Kaseya infiltrieren. Dadurch konnten die Angreifer einen **Erpressungstrojaner,** getarnt als Update, zu der von Kaseya erstellten Software an die Kaseya-Kunden ausliefern. Da diese Kunden häufig selbst als IT-Dienstleister auftreten, wurden diese „Updates“ mit Schadcode auch an deren Kunden weiterverteilt. In der Folge wurden bei den Opfern die Server und die freigegebenen Ordner verschlüsselt. Dieser Angriff betraf also nicht nur eine einzelne Firma, sondern deren Kunden und wiederum deren Kunden – also eine ganze Lieferkette. Er wird daher auch als **Supply-Chain-Attacke** bezeichnet.

Gemeinsam ist beiden Sicherheitsvorfällen, dass sie mit technischen oder organisatorischen Maßnahmen **nicht hundertprozentig zu verhindern** sind. Eine unbekannte Sicherheitslücke in einer Software kann nicht durch einen Patch oder gezielte anderweitige Gegenmaßnahmen geschlossen werden, da das Wissen darüber nicht mal dem Hersteller offenkundig ist. Einem durch Schadsoftware verseuchtes Software-Update, das direkt aus der Quelle des Herstellers übermittelt wird, ist ebenfalls schwer beizukommen: Generell wird ja solchen Software-Updates vertraut, da sie explizit vom Server des Herstellers kommen. Selbst etwaige Warnungen einer Antivirussoftware werden in solchen Fällen zumeist ignoriert, weil – wie bei Kaseya – eine Fernwartungssoftware (hier: Remote-Netzwerkmanagement) durchaus Strukturen aufweisen

kann, die einer Schadsoftware ähneln, was zu Fehlalarmierungen führen kann.

Allerdings konnten betroffene Unternehmen oder Behörden, die ein ausgereiftes IT-Sicherheitsmanagement betrieben, einen größeren Datenschutzschaden vermeiden. Ein wichtiger Punkt war dabei die zeitnahe **Installation von Sicherheitspatches**. Heutzutage können die Zeiten zwischen der Bereitstellung eines Sicherheitspatches und dem massenweisen Angriff auf ungeschützte Systeme sehr kurz sein. Dies erfordert ein kontinuierliches Lesen von Warnmeldungen der Hersteller und IT-Sicherheitsorganisationen (z. B. der CERT-Newsletter des BSI) und eine schnelle Reaktion – mitunter ist es nach dem Wochenende bereits zu spät.

Zero-Day-Exploit

Ein **Exploit** bezeichnet die Ausnutzung einer Schwachstelle eines IT-Systems, meist in Form einer Datei, eines Datenpakets oder eines Netzzugriffs, mit der das IT-System angegriffen wird. Häufig werden erkannte Schwachstellen von zunächst dem Hersteller gemeldet, der Gegenmaßnahmen in Form eines Sicherheitspatches entwickelt und bereitstellt. Das Ausnutzen der Schwachstellen durch einen Exploit ist dann bei den noch ungeschützten Systemen möglich.

Ein **Zero-Day-Exploit** ist ein Exploit, der bereits vor der Meldung einer Sicherheitslücke an den Hersteller oder vor der Bereitstellung eines Patches im Umlauf ist und Sicherheitslücken aktiv ausnutzt. Die Zeit, die Betreibern zum Absichern ihrer Systeme verbleibt, hat sich auf null Tage verkürzt.

Im Falle eines wohldurchdachten IT-Sicherheitsmanagements ließen sich verdächtige Aktivitäten auf den Systemen und ungewöhnlicher Datenverkehr zeitnah erkennen, entsprechende Alarmierungswege auslösen und Gegenmaßnahmen einleiten. Zwar konnten die Angreifer teilweise die genannten Sicherheitslücken ausnutzen und unbefugt auf Systeme zugreifen; ein Datenabfluss oder größere Schäden an den Systemen ließen sich aber vielfach einschränken oder sogar verhindern.

Wichtig: Sofern ein unautorisierter Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, bleibt eine Meldung nach Artikel 33 DSGVO an die Datenschutzaufsichtsbehörde obligatorisch.

Die weniger stark betroffenen Unternehmen und Behörden in beiden Fällen zeichnete aus, dass ihr **IT-Sicherheitsmanagement** umfangreiche Konzepte zur Überwachung der Systeme und des Netzverkehrs beinhalteten. Der Einsatz professioneller Sicherheits- und Incident-Response-Software, das aussagekräftige Protokollieren und das Monitoring des Netzverkehrs konnten bei einigen Opfern der Angriffe einen größeren Schaden verhindern. Die alleinige Umsetzung dieser Maßnahmen ist dabei aber nicht ausreichend, zeichneten sich doch häufig Schwächen im zeitnahen Sichten, Auswerten und Reagieren ab. Die besten Warnmeldungen helfen nicht weiter, wenn sie nicht bemerkt werden oder man falsch oder zu spät reagiert.

Das IT-Sicherheitsmanagement muss also neben den technischen auch die organisatorischen Maßnahmen beinhalten, die beispielsweise die **Zeitintervalle zur Kontrolle der Protokolldaten und Sichtung der Systemmeldungen** definieren. Zusätzlich sollten mögliche Reaktionen auf Warn- und Alarmmeldungen sowie **Meldewege** und Verantwortliche festgelegt werden, um adäquat auf Vorfälle reagieren zu können. Häufig können dadurch größere Schäden der Systeme vermieden, insbesondere aber auch die nachteiligen Auswirkungen für die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen vermindert werden.

Was ist zu tun?

Das IT-Sicherheitsmanagement von Verantwortlichen und deren Dienstleistern ist so auszustatten und zu organisieren, dass eine zeitnahe und effektive Reaktion gewährleistet ist. Durch eine gehärtete und robuste Systemgestaltung lassen sich mögliche Angriffswege vorab weitgehend versperren.

6.3.4 Elektronische Akten

Viele Verwaltungen setzen bereits Verfahren zur Führung elektronischer Akten (E-Akten-Systeme) ein oder rollen solche Verfahren innerhalb der Dienststellen in ihren Fachbereichen aus. Das Land beispielsweise hat vor einigen Jahren das Verfahren VIS-Kompakt beschafft und stellt dies sukzessive den Ressorts und den nachgeordneten Behörden zur Verfügung. Auch im Justizressort werden elektronische Gerichtsakten eingeführt.

Andere Verwaltungen planen die Einführung elektronischer Akten oder befinden sich in der Umsetzungsphase. Besonders für diese Verwaltungen können Erkenntnisse relevant sein, die aus Beratungen und Meldungen von Datenschutzverletzungen gewonnen wurden.

Ein Schwerpunkt solcher Meldungen von Datenschutzverletzungen betrifft Zugriffsrechte auf Dokumente und Dateien, die entweder gar nicht oder falsch gesetzt wurden. **Mangelhafte Zugriffsrechte** können zur Folge haben, dass Beschäftigte über ihre Zuständigkeitsgrenzen hinweg unbefugt Zugriff auf Daten anderer Organisationseinheiten nehmen können. Möglichkeiten unbefugter Kenntnisnahmen sind insbesondere dann ein großes Problem, wenn es sich um Zugriffe auf besonders schützenswerte personenbezogene Daten handelt, etwa Daten der Personalverwaltung, der Personalvertretung oder Daten, die einem besonderen Berufs- und Amtsgeheimnis unterliegen. Bei solchen Verarbeitungen, die voraussichtlich ein hohes Risiko mit sich bringen, ist eine Datenschutz-Folgenabschätzung (Artikel 35 DSGVO) durchzuführen.

Die Verarbeitung sensibler Daten ist aber nicht das einzige Kriterium, das die Notwendigkeit einer Datenschutz-Folgenabschätzung auslösen kann. Ein weiteres Kriterium ist die Breite der Anwendung und die Durchdringung einer (größeren) Verwaltung: Werden in Fachämtern dezentrale Papierregistraturen, Speicherungen in Fachverfahren oder elektronische Aktensysteme durch ein zentrales, verwaltungsweites System abgelöst, werden in dem neuen System an dieser Stelle wesentlich mehr Daten verarbeitet. Betroffen sind dann auch sämtliche Personen, die mit der Verwaltung in Kontakt treten. Ebenso steigt die Anzahl der Beschäftigten, die dieses Verfahren nutzen und bei einer Fehlkonfiguration möglicherweise unbefugten Zugriff nehmen könnten. Daneben stellen sich in E-Akten-Systemen neue Fragen im Vergleich zu Papier- oder Dateiablagen, etwa nach **Protokollierung lesender Zugriffe oder Löschungen**. Außerdem gehen mit der Implementierung von E-Akten-Systemen auch organisatorische Veränderungen einher, etwa die Notwendigkeit, Papiereingänge zu digitalisieren oder **Anschlüsse des E-Akten-Systems an digitale Ein- und Ausgangskanäle** bereitzustellen.

Anders als in Papierregistraturen fällt die **Überschreitung von Aussonderungs- und Löschfristen** nicht unmittelbar durch überquellende Regale auf. Datenschutzrechtlich ist hingegen klar, dass Daten nicht mehr aufbewahrt werden dürfen, wenn sie nicht mehr zur Aufgabenerfüllung erforderlich sind und keine Aufbewahrungsfristen einzuhalten sind. Im Bereich der Verwaltungen sind diese Daten den Archiven auf Kommunal- bzw. Landesebene anzubieten und, sofern sie nicht in diese Archive übernommen werden, zu löschen. Auch diese Verarbeitungsschritte sind bereits bei der Einführung von E-Akten-Systemen zu berücksichtigen – es empfiehlt sich eine Kontaktaufnahme mit dem zuständigen Archiv.

Mit der Implementierung von Maßnahmen bei der Einführung eines Verfahrens ist die Arbeit noch nicht getan: Im Rahmen des Datenschutzmanagements (Art. 32 Abs. 1 Buchst. d DSGVO) sind die **Regelungen**, die Durchsetzung und die Änderungen von Zugriffsrechten **permanent zu überwachen**. Auch hier zeigen Meldungen von Datenschutzverletzungen, dass solche Überprüfungen entweder gar nicht oder mit sehr großen zeitlichen Abständen erfolgen. Zu überprüfen sind die Aspekte SOLL und IST:

- Sollen die Zugriffsrechte weiterhin so, wie sie konzeptioniert wurden, umgesetzt werden oder haben sich Änderungen in der Organisation ergeben (d. h., ist das SOLL weiterhin angemessen)?
- Sind die Berechtigungen und Protokollierungen tatsächlich technisch so umgesetzt, wie sie geplant wurden (IST = SOLL)?

Da die Einführung eines Verfahrens zur elektronischen Aktenführung tiefgreifende Veränderungen der Verwaltungsarbeit zur Folge haben kann, ist ein genauer Blick auf **Datenschutzrisiken** und die **Implementierung von Datenschutzmaßnahmen** erforderlich.

Was ist zu tun?

Sowohl die Planung als auch die Implementierung und der laufende Betrieb von E-Akten-Verfahren erfordern datenschutzrechtliche Sorgfalt.

6.3.5 Prüfung von Videokonferenzsystemen

Dataport ist IT-Dienstleister für mehrere Länder. Daher bieten sich gemeinsame Datenschutzprüfungen durch die Aufsichtsbehörden betroffener Dataport-Trägerländer an.

Im Spätsommer 2021 begann eine **gemeinsame Prüfung von Videokonferenzsystemen**, die Dataport für die zentralen IT-Stellen der Länder (in Schleswig-Holstein das ZIT SH) sowie weitere Behörden anbietet. Beteiligt sind die Datenschutzaufsichtsbehörden in den Ländern Hamburg, Bremen, Sachsen-Anhalt und Schleswig-Holstein.

In einem ersten Schritt wird die vorhandene Dokumentation auf Konsistenz geprüft. Als Prüfmaßstab wird dabei die Orientierungshilfe „Videokonferenzsysteme“ verwendet. Sie ist zusammen mit einer Checkliste unter folgenden Links abrufbar:

https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf

Kurzlink: *https://uldsh.de/tb40-6-3-5a*

https://www.datenschutzkonferenz-online.de/media/oh/20201111_checkliste_oh_videokonferenzsysteme.pdf

Kurzlink: *https://uldsh.de/tb40-6-3-5b*

Die Prüfung erstreckt sich nicht nur auf die funktionelle Ebene, sondern auch auf die technische Realisierung, die Dataport mit eigenen Mitteln und direkt beauftragten Auftragsverarbeitern erbringt. Anders als bei den zahlreichen Anbietern von Videokonferenzdiensten, die diese „as a Service“ anbieten, ist hier auch eine Prüfung der technischen Realisierung, also auch jenseits des Lesens von Verträgen und Funktionsbeschreibungen, möglich. Dies erhöht den **Prüfaufwand**, aber auch die **Prüftiefe**. Durch gemeinsame Prüfungen der Aufsichtsbehörden lässt sich einerseits die Arbeitslast verteilen und andererseits ein gemeinsames Verständnis der Sachverhalte mit einer einheitlichen Beurteilung schaffen.

07

KERNPUNKTE

Gemeinsame Medienprüfung
Mängel bei Websites und Apps
Zehn Jahre Rechtsstreit wegen Facebook-Fanpages

7 Neue Medien

7.1 Gemeinsame Branchenprüfung im Bereich Medien

Die Datenschutzaufsichtsbehörden mehrerer deutscher Länder haben die **Webseiten von Medienunternehmen** in Bezug auf den Einsatz von **Cookies** und die Einbindung von **Drittdiensten** untersucht (39. TB, Tz. 7.3). Insgesamt wurden auf Basis eines gemeinsamen Prüfkatalogs 49 Webangebote in elf Ländern geprüft. Schwerpunkt dabei war das Nutzertracking zu Werbezwecken. Auch das ULD hat sich an dieser Prüfung beteiligt. Für die koordinierte Untersuchung verschickten die Behörden aus Baden-Württemberg, Brandenburg, Bremen, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, dem Saarland, Sachsen und Schleswig-Holstein ab Mitte August 2020 einen gemeinsam erarbeiteten Fragebogen an Medienunternehmen in ihrer jeweiligen Zuständigkeit. Geprüft wurden nicht sämtliche Webseiten der Unternehmen, sondern deren reichweitenstärksten Angebote. Bereits vor Versendung der Fragebögen waren die ausgewählten Webseiten technisch gesichert und analysiert worden. So war ein Abgleich zwischen den Antworten der Medienunternehmen und der tatsächlichen technischen Ausgestaltung der Seiten möglich. Auf den meisten der geprüften Medienwebseiten wurde eine hohe Anzahl von Cookies und Drittdiensten verwendet, die überwiegend dem Nutzertracking und der Werbefinanzierung dienen. Die Webseiten fragen zwar in der Regel differenzierte Einwilligungen der Nutzenden für die Verwendung von Cookies und Drittdiensten ab. In der Mehrheit der Fälle waren diese Einwilligungen allerdings nicht wirksam.

Im Rahmen der Prüfung wurden vor allem die folgenden Mängel festgestellt:

- **Falsche Reihenfolge:** Häufig werden einwilligungsbedürftige Drittdienste bereits beim Öffnen der Webseiten eingebunden und Cookies gesetzt – also noch vor der Einwilligungsabfrage.
- **Fehlende Informationen:** Auf der ersten Ebene der Einwilligungsbanner werden nur unzureichende oder falsche Informationen über das Nutzertracking gegeben.
- **Unzureichender Einwilligungsumfang:** Selbst wenn Nutzende die Möglichkeit wahrnehmen, bereits auf der ersten Ebene des Einwilligungsbanners alles abzulehnen, bleiben zahlreiche Cookies und Drittdienste aktiv, die eine Einwilligung erfordern.
- **Keine einfache Möglichkeit der Ablehnung:** Während bei allen Einwilligungsbannern auf der ersten Ebene eine Schaltfläche vorhanden ist, mit der eine Zustimmung zu sämtlichen Cookies und Drittdiensten erteilt werden kann, fehlt auf dieser Ebene häufig eine ebenso einfache Möglichkeit, das einwilligungsbedürftige Nutzertracking in Gänze abzulehnen oder das Banner ohne Entscheidung schließen zu können.
- **Manipulation der Nutzenden:** Die Ausgestaltung der Einwilligungsbanner weist zahlreiche Formen des Nudging auf. Das bedeutet, dass Nutzende unterschwellig zur Abgabe einer Einwilligung gedrängt werden, indem die Schaltfläche für die Zustimmung beispielsweise durch eine farbliche Hervorhebung deutlich auffälliger als die Schaltfläche zum Ablehnen gestaltet ist oder indem die Verweigerung der Einwilligung unnötig verkompliziert wird.

Cookie-Banner / Einwilligungsbanner

Für die Praxis, beim Besuch einer Webseite prominent durch ein vorgeschaltetes Element, häufig in Form einer Banderole oder eines Banners, Einwilligungen für die Verarbeitung von Cookies einzuholen, hat sich der Begriff Cookie-Banner, auch Consent-Banner oder Einwilligungsbanner genannt, etabliert.

Wichtig: Wer keine einwilligungsbedürftigen Datenverarbeitungen durchführen möchte, benötigt ein solches Banner nicht.

Im Rahmen der Zusammenarbeit wurden **einheitliche Bewertungsmaßstäbe** unter allen an der Prüfung beteiligten und weiteren Aufsichts-

behörden abgestimmt. Unter den beteiligten Aufsichtsbehörden besteht Einigkeit dahin gehend, dass Einwilligungen, die mittels Cookie-Banner eingeholt werden, nur dann als wirksam anzusehen sind, wenn die **Möglichkeit zum Erteilen und zum Ablehnen einer Einwilligung gleichwertig** gestaltet sind. Dies bedeutet, dass es aus Sicht der Nutzer nicht aufwendiger oder komplizierter sein darf, die Einwilligung abzulehnen, als sie zu erteilen. Schaltflächen, die z. B. mit „Einstellungen bearbeiten“ gekennzeichnet sind und dann in weitere (Unter-)Menüs führen, können zusätzlich durchaus sinnvoll sein, leisten aber allein nicht die erforderliche Gleichwertigkeit.

Die beteiligten Landesdatenschutzbehörden haben damit begonnen, auf die Unternehmen in ihrem jeweiligen Zuständigkeitsbereich einzuwirken, um datenschutzkonforme Zustände herzustellen. Mitunter wurden die Prozesse und insbesondere das Einwilligungsmanagement der geprüften Webseiten bereits angepasst. Falls nötig wurden und werden aufsichtsbehördliche Maßnahmen ergriffen.

Die dazu ehörige Pressemitteilung ist unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/artikel/1377-Laenderuebergreifende-Datenschutz-Pruefung-von-Medien-Webseiten-Nachbesserungen-noetig.html

Kurzlink: *https://uldsh.de/tb40-7-1*

Was ist zu tun?

Betreiber von Webseiten, deren Angebot mit einer Verarbeitung personenbezogener Daten beispielsweise zum Nutzertracking verbunden ist, müssen vielfach nachbessern, um die Anforderungen des Datenschutzrechts zu erfüllen.

Wo es sich anbietet, werden die Aufsichtsbehörden weiterhin gemeinsame Prüfungen durchführen.

7.2 Immer wieder Mängel bei Cookies, Pflichtinformationen auf Webseiten und Drittstaatentransfers

Uns erreichen kontinuierlich Kontrollanregungen und Beschwerden bezüglich der Verwendung von Cookies auf Webseiten sowie den Pflichtangaben nach Artikel 13 DSGVO. Häufig wird auch ein mangelhaftes Impressum moniert. Für Letzteres sind allerdings nicht wir, sondern (sofern das Impressum nicht als Teil der Pflichtinformationen aus Artikel 13 DSGVO anzusehen ist) die **Medienanstalt Hamburg/Schleswig-Holstein** (MA HSH) zuständig:

https://www.ma-hsh.de/

Die Beschwerden richten sich in einer Vielzahl der Fälle insbesondere dagegen, dass durch Webseiten Cookies gesetzt würden, ohne dass dies auf einer hinreichenden Rechtsgrundlage basieren würde, weil keine vorherige ausdrückliche und freiwillige Einwilligung eingeholt wird oder auch eine Übermittlung in einen Drittstaat stattfindet. Ein weiterer Großteil der Beschwerden richtet sich dagegen, dass die Informationspflichten nach Artikel 13 DSGVO nicht eingehalten würden, meistens weil sie unvollständig seien.

1. Zur Verwendung von Cookies

Bezüglich der Nutzung von Cookies und anderen Tracking-Technologien hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder im Jahr 2019 eine **„Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien“** veröffentlicht.

https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

Kurzlink: *https://uldsh.de/tb40-7-2a*

Zum damaligen Zeitpunkt hatte der deutsche Gesetzgeber es jahrelang versäumt, die **ePrivacy-Richtlinie** (Richtlinie 2009/136/EG) in

nationales Recht umzusetzen, wonach die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, grundsätzlich nur nach einer vorherigen Einwilligung zulässig ist, wenn nicht eine der in der Richtlinie genannten Ausnahmen greift. Die in der – nach wie vor geltenden – Richtlinie genannten **Ausnahmen** sind:

- technische Speicherung oder Zugang zum **alleinigen Zweck, die Durchführung** der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz **zu ermöglichen**, sowie
- wenn dies **unbedingt erforderlich ist**, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer **ausdrücklich gewünscht** wurde, diesen Dienst zur Verfügung stellen kann.

Das bedeutet: Nur in diesen Fällen bedarf es keiner vorherigen Einwilligung.

Weil der Gesetzgeber in Deutschland zum Zeitpunkt der Geltungserlangung der DSGVO nicht für klare gesetzliche Vorgaben gesorgt hatte, entschieden sich die Aufsichtsbehörden, die oben genannte Orientierungshilfe zu veröffentlichen. Wo keine Vereinbarkeit mit europäischem Recht gegeben war, konnten zwar die nationalen Vorgaben des Telemediengesetzes (TMG) keine Anwendung finden, jedoch galten nunmehr die Regelungen der DSGVO auch für den Bereich von Cookies. Eine direkte Anwendung der ePrivacy-Richtlinie schied aus rechtsstaatlichen Gründen aus. Eine Auslegung der nationalen Vorschriften im Sinne der ePrivacy-Richtlinie vermochten die Aufsichtsbehörden nicht vorzunehmen, da die Regelung im TMG und die Vorgaben in der ePrivacy-Richtlinie diametral verschieden waren.

Mit dem **Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG)** und insbesondere dessen § 25 hat sich die Rechtslage zum 1. Dezember 2021 erneut geändert, wenn auch im Ergebnis nicht wesentlich: Der Gesetzgeber hat zehn Jahre nach der Umsetzungsfrist eine nahezu wortidentische Umsetzung der ePrivacy-Richtlinie und deren Art. 5 Abs. 3 vorgenommen. Daraus ergibt sich, dass die allgemeinen Regeln der DSGVO für die Prozesse des Setzens und Auslesens von Informationen aus Endgeräten nicht mehr greifen, da es spezielleres Recht, nämlich **§ 25 TTDSG**, gibt, das als Umsetzung der ePrivacy-Richtlinie vorrangig anzuwenden ist. Die nachgelagerte Verarbeitung unterfällt jedoch nach wie vor den allgemeinen Regelungen der DSGVO.

Die Vorgaben an eine wirksame Einwilligung ergeben sich – weiterhin – aus der DSGVO. Die ePrivacy-Richtlinie verweist insofern auf das allgemeine Datenschutzrecht und damit nunmehr auf die DSGVO. Dazu gehört insbesondere, dass es für eine Einwilligung einer **eindeutig bestätigenden Handlung** bedarf, wie auch im Urteil des Europäischen Gerichtshofs (EuGH) in der Rechtssache C-673/17 („Planet 49“) sowie der darauf aufbauenden Entscheidung des Bundesgerichtshofs vom 28.05.2020 unter dem Aktenzeichen I ZR 7/16 bestätigt wurde.

Weitere Informationen zur Einwilligung ergeben sich aus den **Leitlinien 05/2020 zur Einwilligung** gemäß Verordnung 2016/679, Version 1.1, des Europäischen Datenschutzausschusses, angenommen am 4. Mai 2020:

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_de

Kurzlink: *https://uldsh.de/tb40-7-2b*

Die Aufsichtsbehörden der Länder haben daher Ende 2021 die **„Orientierungshilfe für Anbieter von Telemedien“ (Stand: Dezember 2021)** überarbeitet, um Rechtsanwendern Klarheit über die Anwendung der neuen Vorgaben zu verschaffen. Die Orientierungshilfe kann hier abgerufen werden:

https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf

Kurzlink: *https://uldsh.de/tb40-7-2c*

Im Grundsatz bleibt es bei der Konstellation, dass der Zugriff auf Endgeräte und damit – als prominentestes Beispiel – der Einsatz von Cookies grundsätzlich nur nach vorheriger wirksamer Einwilligung zulässig ist, wenn nicht eine der gesetzlichen Ausnahmen greift.

Das **Merkmal „unbedingt erforderlich“**, auf das es im Rahmen der Ausnahme aus § 25 Abs. 2 Nr. 2 TTDSG ankommt, ist eng zu verstehen. In der Gesetzesbegründung wird von einer technischen Erforderlichkeit ausgegangen. Eine Ausnahme von der Einwilligungsbedürftigkeit kann somit nicht dadurch begründet werden, dass das Speichern von oder der Zugriff auf Informationen im Endgerät wirtschaftlich für das Geschäftsmodell erforderlich ist, in das der Telemediendienst eingebunden ist.

Cookie-Banner sollten nur zum Einsatz kommen, wenn auch tatsächlich einwilligungsbedürftige Datenverarbeitungen stattfinden.

Werden **Consent-Management-Plattformen** verwendet, bedeutet dies nicht automatisch, dass damit rechtskonforme Einwilligungen eingeholt werden, da mitunter zahlreiche Konfigurationsmöglichkeiten gegeben sind. Die Verantwortlichkeit für die Rechtskonformität verbleibt zudem bei den Webseitenbetreibern. Diese haben sicherzustellen, dass einwilligungsbedürftige Datenverarbeitungen beim Besuch ihrer Webseiten erst nach einer wirksamen Einwilligung durchgeführt werden.

Consent-Management-Plattformen

Unter dem Begriff „Consent-Management-Plattform“ werden Dienste verstanden, die Webseiten-Betreiber auf ihren Webseiten einbinden und nutzen können, um damit Einwilligungen für einwilligungsbedürftige Datenverarbeitungsvorgänge, häufig mittels Cookies, einzuholen. Diese Plattformen sind weitestgehend ähnlich gestaltet, dennoch können sie von den Webseiten-Betreibern konfiguriert und auf ihre Bedürfnisse und Datenverarbeitungen angepasst werden.

2. Zu den Pflichtinformationen nach Artikel 13 DSGVO

Gemäß Art. 13 Abs. 1 und 2 DSGVO müssen die Verantwortlichen im Falle der Erhebung personenbezogener Daten bei betroffenen Personen Informationen über die Datenverarbeitung bereitstellen. Diese Informationspflichten entstehen auch bei der Ansteuerung eines Webauftritts durch Webseitenbesucher. In Webauftritten werden diese Pflichtinformationen häufig in „Datenschutzhinweisen“ oder „Datenschutzerklärungen“ aufgeführt.

Zu den Inhalten der **Informationspflichten** hat das ULD eine Informationsbroschüre veröffentlicht:

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

Kurzlink: *https://uldsh.de/tb40-7-2d*

Immer wieder finden sich generische **Datenschutzerklärungen**, die die tatsächlich auf den Webseiten stattfindenden Verarbeitungen **nicht wahrheitsgetreu** abbilden. Wenn Webseitenbetreiber bei der Abfassung der Datenschutzerklärungen auf Dienstleister zurückgreifen, die vorformulierte Datenschutzerklärungen anbieten, muss sichergestellt sein, dass diese auch auf die konkrete Webseite und die damit im Zusammenhang stehenden Datenverarbeitungen passen. Weder dürfen Verarbeitungen fehlen noch sollten Verarbeitungen genannt werden, die gar nicht stattfinden.

3. Zur Übermittlung personenbezogener Daten in einen Drittstaat

Durch das Urteil des EuGH in der Rechtssache C-311/18 (Schrems II), wurde der Privacy-Shield-Beschluss der Europäischen Kommission 2016/1250 für ungültig erklärt (39. TB, Tz. 2.5).

Nach Art. 46 DSGVO gilt, dass, falls kein derartiger Beschluss der Europäischen Kommission nach Art. 45 Abs. 3 DSGVO vorliegt, ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln darf, sofern der Verantwortliche bzw. der Auftragsverarbeiter **geeignete Garantien** vorgesehen hat und sofern den betroffenen Personen **durchsetzbare Rechte und wirksame Rechtsbehelfe** zur Verfügung stehen. Weitere Informationen dazu hat der Europäische Datenschutzausschuss bereitgestellt:

https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_de

Kurzlink: *https://uldsh.de/tb40-7-2e*

Sofern durch Webseitenbetreiber Drittstaatentransfers veranlasst werden, z. B. weil Dienste auf der Webseite eingebunden werden, die einen Datenfluss in einen Drittstaat zur direkten Folge haben, müssen Webseitenbetreiber die Vorgaben zu Drittstaatentransfers berücksichtigen und vorab prüfen, ob ein solcher Transfer zulässig ist.

Für die Prüfung etwa notwendiger ergänzender Maßnahmen können Verantwortliche und Auftragsverarbeiter die **„Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“** nutzen.

https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de

Kurzlink: *https://uldsh.de/tb40-7-2f*

Mit Durchführungsbeschluss vom 4. Juni 2021 hat die Europäische Kommission **neue Standardvertragsklauseln** erlassen (Tz. 2.2), die eine rechtskonforme Übermittlung personenbezogener Daten in Drittländer ermöglichen sollen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder weist – wie auch der Europäische Datenschutzausschuss – darauf hin, dass auch bei Verwendung der neuen EU-Standardvertragsklauseln eine **Prüfung der Rechtslage im Drittland und der Notwendigkeit zusätzlicher ergänzender Maßnahmen erforderlich** ist.

https://www.datenschutzkonferenz-online.de/media/pm/2021_pm_neue_scc.pdf

Kurzlink: *https://uldsh.de/tb40-7-2g*

Was ist zu tun?

1. Einwilligungsbedürftige Datenverarbeitungsvorgänge dürfen nicht ohne vorherige wirksame Einwilligung der betroffenen Personen durchgeführt werden.
2. Wenn Maßnahmen zur Einholung von Einwilligungen eingesetzt werden, müssen diese auch wirksam funktionieren, d. h., erst nach einer wirksamen Einwilligung darf eine darauf gestützte Datenverarbeitung stattfinden und nicht vorher.
3. Die Übermittlung personenbezogener Daten in einen Drittstaat darf nur im Einklang mit den Art. 44 ff. DSGVO erfolgen.

7.3 Facebook-Fanpages – Zehn Jahre Rechtsstreit

Mit Urteil vom 25.11.2021 hat ein zehn Jahre währender Rechtsstreit nunmehr ein (vorläufiges) Ende gefunden. Das Schleswig-Holsteinische Oberverwaltungsgericht (OVG Schleswig) hat entschieden, dass mit dem **Betrieb einer Facebook-Fanpage** durch die Wirtschaftsakademie Schleswig-Holstein GmbH zum maßgeblichen Zeitpunkt im Dezember 2011 ein **schwerwiegender Verstoß gegen datenschutzrechtliche Vorschriften** einherging.

Im Dezember 2011 hatte das ULD gegenüber der Wirtschaftsakademie angeordnet, die von ihr betriebene Facebook-Fanpage wegen datenschutzrechtlicher Verstöße zu deaktivieren. Nachdem der Rechtsweg bis zum Bundesverwaltungsgericht beschritten worden war, hatte dieses einige Vorlagefragen an den EuGH gestellt, die dieser mit Entscheidung vom 5. Juni 2018 dahin gehend beantwortet hatte, dass **Betreiber einer Facebook-Fanpage gemeinsam mit Facebook als Verantwortliche anzusehen** sind. Damit war klar, dass Fanpage-Betreiber Adressaten einer aufsichtsbehördlichen Maßnahme bezüglich ihrer Fanpage sein können, eben weil sie dafür auch datenschutzrechtlich verantwortlich sind und nicht bloß ein Angebot von Facebook nutzen können, ohne dafür die Verantwortung zu tragen.

Ob die Maßnahme, die auf die Deaktivierung der Fanpage gerichtet war, in der Sache auch Bestand haben kann, war keine Frage, die vom EuGH entschieden werden konnte, weshalb das Verfahren dann zunächst zurück zum Bundesverwaltungsgericht und nun zum OVG Schleswig gegeben wurde, das nun entschieden hat, dass die **Deaktivierungsanordnung rechtmäßig** erfolgte. Das OVG Schleswig hat einen schwerwiegenden Verstoß in der Verwendung der personenbezogenen Daten von im Facebook-Netzwerk registrierten und angemeldeten Personen erkannt. Diese Datenverwendung sei weder gesetzlich erlaubt, noch hätten die Nutzenden in diese eingewilligt. Außerdem seien die betroffenen Personen nicht hinreichend über

sämtliche Datenerhebungs- und -verwendungsvorgänge, die durch den Besuch einer Fanpage angestoßen würden, informiert worden.

https://uldsh.de/pmovg2021

Zum Zeitpunkt der Abfassung dieses Tätigkeitsberichts liegen die Urteilsgründe noch nicht vor.

Erste Informationen finden sich hier: *https://www.datenschutzzentrum.de/artikel/1384-Urteil_OVG.html*

Kurzlink: *https://uldsh.de/tb40-7-3a*

Wir werden die **Urteilsgründe und weitere Informationen** unter dem folgenden Link veröffentlichen:

https://www.datenschutzzentrum.de/facebook/

Kurzlink: *https://uldsh.de/tb40-7-3b*

08

KERNPUNKTE

Forum Privatheit
Digitale Arbeitswelten
IuK-Forschung

8 Modellprojekte und Studien

Das Unabhängige Landeszentrum für Datenschutz hat als Behörde der Landesbeauftragten für Datenschutz seine Aktivitäten in Initiativen im Bereich drittmittelfinanzierter Projekte und Studien fortgesetzt. Damit ist das ULD weiterhin im Bereich der Kooperation mit der Wissenschaft aktiv und erhält die Möglichkeit, proaktiv an der Erforschung datenschutzspezifischer Fragen und der Gestaltung einschlägiger Technologien und Lösungen mitzuwirken. Im Berichtszeitraum wurden Projekte von der Europäischen Kommission und dem Bundesministerium für Bildung und Forschung (BMBF) gefördert.

Im Jahr 2021 beteiligte sich das ULD an Projekten zu aktuellen Themen in den Bereichen Privatheit und selbstbestimmtes Leben (Tz. 8.1), Datenschutz in digitalen Arbeitswelten (Tz. 8.2) sowie Datenschutz in der Technikforschung (Tz. 8.3) und setzt sein Engagement für Datenschutz, Transparenz- und Einwilligungsmanagement fort (Tz. 8.4).

8.1 Privatheit, Demokratie und Selbstbestimmung – Fortsetzung des Forum Privatheit

Die Digitalisierung lässt sich nicht aufhalten, aber gestalten – und das ist auch dringend notwendig. Dafür reicht es nicht aus, dass hier und da ein paar Forschende an Hochschulen ihre Gedanken und Ideen aufschreiben. Vielmehr braucht man für die wichtigen Fragen unserer Zeit eine interdisziplinäre Kooperation, und das nicht nur, aber auch im Bereich Datenschutz und Privatheit.

Im März 2021 ging unsere Mitarbeit im **Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt** zu Ende, ein interdisziplinäres Projekt, das insgesamt über sieben Jahre gelaufen ist. Unsere Arbeit zu wissenschaftlichen und gesellschaftspolitischen Herausforderungen hat viele Aspekte rund um Privatheit und Datenschutz berührt. Die Ergebnisse sind in Veröffentlichungen für Akteure im politischen Bereich (Policy Paper) und für Forschung, Anwendung und Nutzende (White Paper oder Forschungsberichte) dokumentiert.

Über die letzten vier Jahre haben die Projektpartner Schwerpunkte auf besondere Fokusthemen gelegt:

- 2017: Fortentwicklung des Datenschutzes
- 2018: Zukunft der Datenökonomie
- 2019: Inklusion und Exklusion
- 2020: Selbstbestimmung und Privatheit – Gestaltungsoptionen für einen europäischen Weg

Die Abschlussarbeiten Anfang 2021 beschäftigten sich insbesondere mit ganzheitlich gestalteten Lösungen für einen weiter gedachten Datenschutz „by Design“ (siehe Tz. 2.4). Das letzte Projektjahr war außerdem von der Diskussion zu Wirkungen und Auswirkungen der Instrumente zur Pandemiebekämpfung geprägt. In diesem Zusammenhang wurde auch mit einem Team von Expertinnen und Experten zusammengearbeitet, die von der Nationalen Akademie der Wissenschaften Leopoldina eingeladen wurden. Die aus zahlreichen Gesprächen entstandene Publikation „Ansatzpunkte für eine Stärkung digitaler Pandemiebekämpfung“ (Diskussion Nr. 25, 2021) ist unter dem folgenden Link abrufbar:

https://www.leopoldina.org/publikationen/detailansicht/publication/ansatzpunkte-fuer-eine-staerkung-digitaler-pandemiebekaempfung-2021/

Kurzlink: *https://uldsh.de/tb40-8-1a*

Nach Abschluss unserer Mitwirkung im Forum Privatheit geht die Arbeit im Nachfolgeprojekt **„PRIDS – Privatheit, Demokratie und Selbstbestimmung im Zeitalter von Künstlicher Intelligenz und Globalisierung“** weiter. In dem PRIDS-Projekt beschäftigen wir uns u. a. mit Effekten der künstlichen Intelligenz und deren Beherrschbarkeit (Tz. 6.1.2), mit Risiken für die Rechte und Freiheiten natürlicher Personen in den verschiedenen Konstellationen, mit möglichen gesellschaftlichen Folgen der Digitalisierung sowie mit dem Thema Überwachungsgesamtrechnung (Tz. 2.3).

Die Ergebnisse werden weiterhin über die bekannte Webseite des Forum Privatheit bereitgestellt:

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

Kurzlink: *https://uldsh.de/tb40-8-1b*

Was ist zu tun?

Für die großen Herausforderungen, die mit der zunehmenden Digitalisierung für Einzelpersonen und unsere Gesellschaft verbunden sind, braucht es eine verstärkte interdisziplinäre Zusammenarbeit.

8.2 Projekt EMPRI-DEVOPS – Datenschutz in digitalen Arbeitswelten

Das Projekt **„Employee Privacy in Software Development and Operations“ (EMPRI-DEVOPS)** (39. TB, Tz. 8.2) beschäftigt sich mit dem datenschutzkonformen Einsatz von Softwaretools in der Arbeitswelt. Projektziel ist die datenschutzkonforme Gestaltung von Softwareprodukten, die typischerweise im Kontext der agilen Softwareprogrammierung und der Systemadministration zum Einsatz kommen. Lehren aus diesem speziellen Anwendungsfeld lassen sich jedoch auf den Einsatz anderer Kooperationstools und Office-Umgebungen verallgemeinern.

In einem früheren Tätigkeitsbericht haben wir bereits darauf hingewiesen, dass bei Auswahl, Konfiguration und Betrieb von Softwareprodukten die Risiken ermittelt und berücksichtigt werden sollten (38. TB, Tz. 8.2). Eine umfassende Erhebung und Bewertung von Risiken für eine Verarbeitung kann im Rahmen einer Datenschutz-Folgenabschätzung (DSFA) geschehen. Ein Schritt einer DSFA ist es, die Risikoquellen zu identifizieren – in der Informatik spricht man hier vom Angreifermodell. Erfolgt die DSFA für den Einsatz von Software in Beschäftigungsverhältnissen, ist auch an das Unternehmen selbst bzw. dessen Leitung und die Vorgesetzten als Risiko zu denken. Diese können etwa übermäßig anfallende Metadaten oder systembedingt vorhandene Zugriffs- und Kontrollmöglichkeiten erheben, auswerten und so missbräuchlich verwenden. Solche „Angreifer“ können zudem aus dem Kollegium stammen, wenn ihnen der Zugriff auf entsprechende Daten möglich ist. Derartige Risiken potenzieren sich, wenn diese Informationen über lange Zeiträume kontinuierlich verfügbar sind und sich so komplette detaillierte Profile über Tätigkeiten – und damit Verhalten oder Leistung – von Beschäftigten erstellen lassen. Sofern solche Risiken nicht systemseitig ausgeschlossen werden können, ist ihnen durch geeignete technische und organisatorische Maßnahmen zu begegnen.

Die technischen Partner im Projekt haben exemplarisch für die **Versionskontrolle** mittels des weitverbreiteten Versionskontrollsystems Git Lösungen dafür erarbeitet, **Zeitstempel zentral zu kürzen oder zumindest deren Darstellung lokal zu vergröbern**. Statt sekundengenauer Angaben wären diese dann beispielsweise nur noch taggenau ablesbar.

Dieser Ansatz lässt sich für andere Anwendungsfälle verallgemeinern: Ist lediglich eine Reihenfolge von Beiträgen oder Eingängen relevant, könnten Zeitstempel durch Sequenz- oder Tagebuchnummern ersetzt werden. Ist zur weiteren Bearbeitung nur eine fachliche Zugehörigkeit von früheren Bearbeitenden relevant und sind auch Rückfragen bei konkreten Einzelpersonen die Ausnahme, könnten namentliche Kennungen durch Abteilungsnamen oder Teambezeichnungen ersetzt werden. Liegt die zu verwendende Software in geeigneter Lizenz vor, bestünde bei großen Arbeitgebern die Möglichkeit, vergleichbare Anpassungen für im Informationsgehalt überschießende Metadaten selbst vorzunehmen oder dies bei den Entwicklungsteams für künftige Versionen zu beauftragen. Gerade öffentliche Arbeitgeber könnten so eine Vorbildfunktion einnehmen, indem beim Beschäftigtendatenschutz (siehe auch Tz. 2.6) schon bei grundlegenden Verarbeitungen auf Prinzipien wie Datenminimierung geachtet wird.

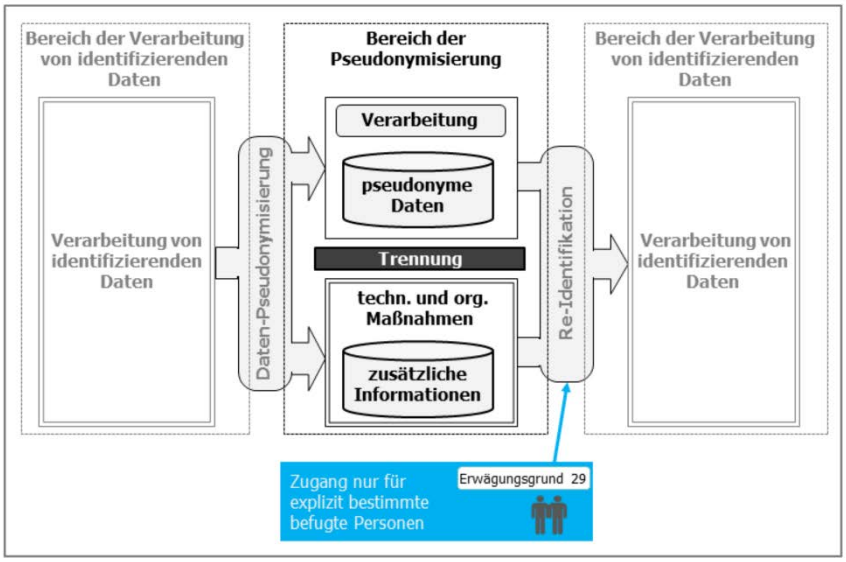
Für eine realistische Folgenabschätzung im Zusammenhang von Softwareeinsatz am Arbeitsplatz genügt es nicht, nur solche Daten zu betrachten, die offensichtlich personenbezogen

sind, wie Stamm- oder Profildaten von Beschäftigten. Vielmehr sind alle Anwendungsdaten zu betrachten, die **unmittelbar oder über eine Verkettung einen Personenbezug zu einzelnen Beschäftigten** aufweisen. Entstehen die Metadaten und Informationen über die Nutzung nicht unternehmensintern, sondern bei einem Austausch mit externen Stellen, müssen auch diese Daten in den Blick genommen werden. Wird etwa in Projekten unternehmensübergreifend mit einer Software zum Informationsaustausch gearbeitet, bestünden vergleichbare Auswertungsoptionen bei allen Zugriffsberechtigten – und das können neben dem Betreiber einer solchen Infrastruktur auch alle beteiligten Stellen sein.

Wo technische Abhilfemaßnahmen nicht zur Verfügung stehen, können flankierende organisatorische Maßnahmen helfen, unzulässige Zugriffe für Leistungs- und Verhaltenskontrollen zu verhindern. Das können beispielsweise Betriebsvereinbarungen oder hilfsweise Selbstverpflichtungen der Arbeitgeber und entsprechende Weisungen und Schulung der Beschäftigten sein.

8.3 Projekt PANELFIT – Datenschutz und Ethik in der europäischen IuK-Forschung

Das von der EU-Kommission geförderte Projekt **„Participatory Approaches to a New Ethical and Legal Framework for ICT“ (PANELFIT)** (39. TB, Tz. 8.3) zielt darauf ab, dass Neuerungen durch die DSGVO schnell und vollständig von allen europäischen Akteuren im Bereich der Forschung zu Informations- und Kommunikationstechnologien (IuK) aufgegriffen und umgesetzt werden können. Ein Schwerpunkt der Tätigkeit des ULD-Teams im Projekt war eine Ausarbeitung zu Identifizierung und Identifizierbarkeit von Personen. Dies ist ebenso relevant für die Bestimmung eines **Personenbezugs** wie für die Bewertung der Effektivität von Schutzmaßnahmen wie **Anonymisierung und Pseudonymisierung**. Zu der Arbeit gehörte zunächst, eine Übersicht von technischen Verfahren zu erstellen, die für eine Anonymisierung zum Einsatz kommen können, und sie zu kategorisieren. Außerdem wurden die rechtlichen Normen der DSGVO analysiert.



Pseudonymisierung nach der DSGVO im Schaubild

Da das Projekt PANELFIT vor allem auf datenintensive Forschung im IuK-Bereich abzielt, bestand eine Herausforderung darin, diese Grundsätze und Regelungen der DSGVO einem Publikum mit primär naturwissenschaftlich-technischem Hintergrund zugänglich zu machen. Besonderes Augenmerk galt präzisen, aufeinander aufbauenden und kompatiblen Definitionen aller wichtigen Konzepte im Sinne einer Terminologie oder sogar Ontologie.

Exemplarisch sei hier etwa die klarstellende Herausarbeitung der Unterschiede zwischen einer Pseudonymisierung im Sinne der DSGVO, die bestimmten Anforderungen genügen muss, und den im üblichen Sprachgebrauch allgemein als Pseudonymisierung bezeichneten Verarbeitungen genannt. Zu den Anforderungen der DSGVO an eine Pseudonymisierung gehört insbesondere, dass die von den identifizierenden Informationen getrennten Daten nur in einem gesicherten Umfeld verarbeitet werden dürfen und dass die Trennung der zur Re-Identifikation erforderlichen „zusätzlichen Informationen" gewährleistet ist. Ausschließlich zuständige Personen dürfen Zugriff auf letztgenannte Daten haben (siehe Abbildung).

Der Personenbezug der pseudonymisierten Daten bleibt bestehen. Regelmäßig sind die pseudonymisierten Daten weiterhin mit angemessenen technischen und organisatorischen Maßnahmen zu schützen, wobei das zu gewährleistende Schutzniveau im Vergleich mit dem der ursprünglichen nichtpseudonymisierten Daten aber zumeist als niedriger einzustufen ist.

Ein weiterer Schwerpunkt in der Projektarbeit lag auf dem **Prinzip von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen** („Data Protection by Design and by Default", DPbDD). Zusätzlich zu der Analyse des Gesetzestextes wurden die Prozesse zur Implementierung von DPbDD in jeder der identifizierten Phasen einer Verarbeitungstätigkeit analysiert. Dies hilft den praxisorientierten Adressaten des Projekts, das Prinzip von DPbDD effizient umzusetzen.

Schließlich hat das ULD-Team im PANELFIT-Projekt zu einer vergleichenden Länderstudie zu **Datenschutz im Forschungsbereich** sowie zu Cybersecurity beigetragen. Die im Berichtsjahr erarbeiteten Beiträge zu Identifizierbarkeit und DPbDD sowie diejenigen des Vorjahres (GDPR in a Nutshell, Principles, Documentation of Processing, DPIA (Datenschutz-Folgenabschätzung), siehe 39. TB, Tz. 8.3) wurden nach einem zweistufigen Reviewprozess in eine konsolidierte Fassung überführt und werden als Kapitel für die PANELFIT-Leitfäden verwendet. Diese werden derzeit in mehrere Sprachen übersetzt und sollen sowohl in gedruckter Form als auch online vom Projekt publiziert werden.

Die im Projekt erstellten Texte und das gewonnene Wissen werden vom ULD in die Datenschutz-Community getragen, etwa mit dem Ziel, zu einem gemeinsamen Verständnis der Konzepte von Pseudonymisierung und Anonymisierung in Europa beizutragen.

Die Studie zur Identifizierbarkeit sowie die weiteren Projektergebnisse sind unter den folgenden Links verfügbar:

https://uldsh.de/pseudoAnon

https://www.panelfit.eu/outcomes/

Was ist zu tun?

In Forschungsprojekten, die auf einer umfangreichen Datenverarbeitung beruhen, sollte das Verständnis zum Datenschutz verbessert werden. Einen Beitrag zu der dafür notwendigen „Übersetzung" der Anforderungen aus der DSGVO will das Projekt PANELFIT leisten. Es gilt, diese Aufbereitung für die Praxis fortzusetzen.

8.4 Projekt TRAPEZE – Transparenz- und Einwilligungsmanagement für das semantische Netz

Das Projekt **„TRAnsparency, Privacy and security for European citiZEns" (TRAPEZE)** wird von der EU-Kommission gefördert und widmet sich der Entwicklung von Lösungen für Datenschutz und Transparenz in der „Data Economy" (39. TB, Tz. 8.4). Auf europäischer Ebene werden zurzeit die Weichen dafür gestellt, dass Daten für Forschungszwecke und Wirtschaft verstärkt verfügbar sein sollen. Gleichzeitig wird die Geltung der DSGVO nicht infrage gestellt – Datenschutz bleibt also auch weiterhin ein wichtiger Eckpfeiler. Mit dem geplanten europäischen „Data Governance Act" (DGA) sollen Möglichkeiten geschaffen werden, Dienste zur

gemeinsamen Datennutzung einzurichten. Betroffene Personen können ihre eigenen Daten im Rahmen von „Datenaltruismus“ für „Zwecke von allgemeinem Interesse“ zur Verfügung stellen.

Im Entwurf des Data Governance Acts wird Datenaltruismus definiert. Betroffene Personen sollen eine Einwilligung erteilen können zur Verarbeitung ihrer Daten für Zwecke von allgemeinem Interesse, etwa für wissenschaftliche Forschung oder die Verbesserung öffentlicher Dienstleistungen.

Mit den Regelungen des DGA deutet sich in Teilen ein Richtungswechsel an: Gegenwärtig wird in Deutschland nach überwiegender Rechtsauffassung angenommen, dass eine Einwilligung im Datenschutz nur selbst (höchstpersönlich) oder durch einen gesetzlichen Vertreter erteilt werden könne. Das wird aus dem höchstpersönlichen Charakter des Rechts auf informationelle Selbstbestimmung abgeleitet. Aus den eher strikten und umfassenden Bedingungen an die Bestimmtheit einer informierten Einwilligung resultieren Hürden etwa für die Verwendung bereits vorhandener Daten für Sekundärzwecke. Diese Sekundärzwecke betreffen nicht nur eine wirtschaftliche Auswertung personenbezogener Daten, sondern können etwa bei Forschung allgemein anerkannter Interessen oder anderen Zwecken, die die jeweils betroffene Person unterstützen möchte, liegen.

Im TRAPEZE-Projekt spielt das Verständnis der Einwilligung und der Ansätze, eine Einwilligung nicht nur höchstpersönlich erteilen zu können, eine wesentliche Rolle. Beispielsweise könnten Stellvertreter, Treuhänder oder Informationstechnik zum Einsatz kommen, um ein **Einwilligungsmanagement** zu gewährleisten oder zu unterstützen. Sinnvoll ist hierbei eine europäische Harmonisierung. Dabei sind die wesentlichen Kernpunkte der Einwilligung vorab zu bestimmen und verständlich mitzuteilen, namentlich die Kategorien von Empfängern, Daten, Zwecken und Verarbeitungsarten. Schließlich müssen auch besondere Modalitäten und Beschränkungen bestimmt werden können – etwa eine Einschränkung auf Weitergaben und Verarbeitungen im Anwendungsbereich der DSGVO.

Bausteine für eine mögliche Umsetzung einer technisch unterstützten Einwilligung unter Kontrolle der betroffenen Person werden u. a. im TRAPEZE-Projekt entwickelt. Sowohl für automatische als auch menschliche Entscheidungen über die Verarbeitung anvertrauter Daten ist eine maschinenlesbare Abbildung der geplanten oder zu gestattenden Verarbeitung nötig (Policy). Die Grundlagen für ein derartiges Policy-Vokabular wurden bereits im Vorgängerprojekt SPECIAL unter dem Dach des W3C gelegt (dazu 39. TB, Tz. 8.4) und werden gegenwärtig im TRAPEZE-Projekt weiterentwickelt. So wäre es damit möglich, **Einwilligungen für Sekundärnutzungen sinnvoll zu bedingen oder zu begrenzen**. Diese Informationen zu Reichweite und Grenzen der Einwilligung könnten direkt mit den jeweiligen personenbezogenen Daten verarbeitet oder übermittelt werden. Dies wäre nicht zuletzt ein Mehrwert u. a. für das von der EU eingeführte Konzept des **Datenaltruismus**.

Daneben stehen weitere Forschungsbereiche des Projekts wie die Erarbeitung einer **Benutzungsoberfläche**, die alle datenschutzrelevanten Aspekte klar und verständlich darzustellen vermag. Wünschenswert wäre es, den Nutzenden zu ersparen, sich für jede Plattform erneut in die jeweilige Darstellungsweise einzuarbeiten. Dies ließe sich beispielsweise mit einer annähernden Vereinheitlichung entsprechender Benutzungsoberflächen oder mit einer **standardisierten maschinenlesbaren Policy** erreichen, sodass die Nutzenden eine beabsichtigte Verarbeitung in der gewohnten Umgebung einer eigenen App anzeigen oder computerunterstützt für sich selbst auswerten können.

Insgesamt bleibt es spannend. Die gegenwärtig in Europa entwickelten Lösungen zum Datenschutz durch Technikgestaltung können relevante Beiträge leisten, um eine europäische „Data Economy“ auch für personenbezogene Daten sicher, vertrauenswürdig und fair zu gestalten. Zugleich sind die Gesetzgeber auf europäischer und nationaler Ebene gefragt, den Einsatz solcher Lösungen rechtssicher zu regeln und damit die nötigen Leitplanken für die weiteren Entwicklungen – auch im Sinne des Gemeinwohls – zu geben.

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

09

KERNPUNKTE

Leitung Arbeitskreis Zertifizierung
Prüfkriterienkatalog
Eigene Zertifizierung des ULD

9 Zertifizierung und Akkreditierung

Seit Mai 2018 sind die Regelungen der DSGVO zu Akkreditierung und Zertifizierung in Kraft getreten, doch noch fehlt es an Akkreditierungen von Zertifizierungsstellen in Europa. Inzwischen wurden aber die notwendigen Voraussetzungen beim Europäischen Datenschutzausschuss geschaffen, sodass erste Verfahren zur Genehmigung von Kriterienkatalogen als Voraussetzung für Akkreditierungen gestartet wurden. Die notwendigen Prozesse begleiten wir als Leitung des Arbeitskreises Zertifizierung der deutschen Aufsichtsbehörden (Tz. 9.1). Insbesondere wurde ein Prüfkriterienkatalog verabschiedet, der es Antragstellern und Aufsichtsbehörden erlaubt, einheitliche Maßstäbe an Kriterienkataloge bzw. Zertifizierungsprogramme anzulegen (Tz. 9.2). Auch die europäische Ebene (siehe auch Kap. 11) spielt für das einheitliche Verständnis einer Zertifizierung nach der DSGVO eine wesentliche Rolle (Tz. 9.3). All dies berücksichtigen wir für die Möglichkeit, ein eigenes Zertifizierungsverfahren anzubieten (Tz. 9.4).

9.1 Leitung des AK Zertifizierung

Schon seit einigen Jahren leitet das ULD den Arbeitskreis (AK) Zertifizierung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK). Nachdem im Jahr 2020 die deutschen Akkreditierungskriterien finalisiert und veröffentlicht wurden (39. TB, Tz. 9.3), begannen 2021 **die ersten echten Genehmigungsverfahren für Kriterienkataloge** als Vorbereitung von Akkreditierungen. Um einen einheitlichen Bewertungsmaßstab in Deutschland zu erreichen, wurde insbesondere ein Prüfkriterienpapier entwickelt (Tz. 9.2).

Auch im Berichtsjahr arbeitete der AK Zertifizierung eng mit der Deutschen Akkreditierungsstelle GmbH (DAkkS) zusammen. Während die Aufsichtsbehörden die Genehmigung von Kriterienkatalogen vornehmen, betreibt die DAkkS das eigentliche Akkreditierungsverfahren in Kooperation mit den Datenschutzaufsichtsbehörden.

Fünf Sitzungen des AK Zertifizierung wurden von uns organisiert, die pandemiebedingt als Videokonferenzen stattfanden. Zu den Schwerpunktthemen gehörten die laufenden Genehmigungsverfahren von Kriterienkatalogen in mehreren Bundesländern.

Was ist zu tun?

Auch 2022 wird das ULD die Leitung des AK Zertifizierung fortsetzen. Neben dem Abgleich mit europäischen Entwicklungen werden die laufenden Genehmigungs- und Akkreditierungsverfahren Hauptthema sein.

9.2 Prüfkriterienkatalog

Im Frühjahr 2021 hat die DSK das Papier **„Anforderungen an datenschutzrechtliche Zertifizierungsprogramme – Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6)“** verabschiedet, das der Unterarbeitskreis Prüfkriterien des AK Zertifizierung entwickelt hat. Dieses Papier erweitert die europäischen Vorgaben für Zertifizierungsprogramme und war notwendig, um eine einheitliche Bewertung in Deutschland sicherzustellen. Auch potenzielle Zertifizierungsstellen können

sich für ihre Anträge an diesem Papier orientieren.

Maßgebliche Quellen für das Papier waren die Vorgaben aus Artikel 43 DSGVO, die Leitlinien des EDSA, die Normen ISO/IEC 17065 und ISO/IEC 17067 und das Ergänzungspapier der DSK gemäß Art. 43 Abs. 3 i. V. m. DIN EN ISO/IEC 17065 für Zertifizierungsstellen, die im Rahmen der Akkreditierung durch die DAkkS im Einvernehmen mit den zuständigen unabhängigen Datenschutzaufsichtsbehörden geprüft werden. Zentraler Teil ist das Kapitel 2, in dem für wichtige Normen der DSGVO die Erwartungen an ein Zertifizierungsprogramm beschrieben werden. Drei Bereiche werden jeweils dargestellt:

- die gesetzlichen Tatbestandsmerkmale,
- in den Zertifizierungskriterien die zu behandelnden Prüfthemen und deren Umsetzung durch die Kunden der Zertifizierungsstelle und
- die Art und Weise der Prüfung der Umsetzung durch die Zertifizierungsstelle.

Das Papier ist unter dem folgenden Link abrufbar:

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

Kurzlink: *https://uldsh.de/tb40-9-2*

Was ist zu tun?

Bis zur ersten DSK-Sitzung im Frühjahr 2022 soll eine Evaluation des Papiers erfolgen. Diese wird vom Unterarbeitskreis Prüfkriterien vorbereitet. Zusätzlich werden auch weitere Normen der DSGVO in das Kapitel 2 nach dem vorgestellten Muster aufgenommen.

9.3 Akkreditierung und Zertifizierung in der europäischen Expert Subgroup

Auf europäischer Ebene werden Akkreditierung und Zertifizierung in der „Compliance, e-Government und Health Expert Subgroup“ (CEH Expert Subgroup) behandelt, in der wir mitwirken. Hierbei handelt es sich quasi um eine parallele Arbeitsgruppe zu unserem nationalen AK Zertifizierung, die zahlreiche Dokumente, Grundsatzentscheidungen und insbesondere Stellunnahmen zu Kriterien vorbereitet. Unter anderem wurde im Berichtszeitraum die Leitlinie **„Guidance on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation)“** entwickelt, die wiederum Einfluss auf das Prüfkriterienpapier in Deutschland hatte (siehe Tz. 9.2). Auch konnten wir uns in die Bewertung von ersten Zertifizierungskriterien anderer Mitgliedstaaten einbringen und darüber wichtige Erkenntnisse für die Verfahren der Antragsteller in Deutschland gewinnen.

Die Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679 können über folgenden Link abgerufen werden:

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_de

Kurzlink: *https://uldsh.de/tb40-9-3a*

Die Leitlinie „Guidance on certification criteria assessment“ steht hier zur Verfügung:

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidance-certification-criteria-assessment_de

Kurzlink: *https://uldsh.de/tb40-9-3b*

Was ist zu tun?

Das Engagement in Europa für den Austausch zu Akkreditierungs- und Zertifizierungsvorgaben und kritischen Stellungnahmen ist fortzusetzen.

9.4 Planung eigener Zertifizierungen des ULD

Auch im Jahr 2021 haben uns einige Anfragen erreicht, ob in Zukunft Zertifizierungen, vergleichbar mit dem früheren Datenschutz-Gütesiegel Schleswig-Holstein des ULD, vorgenommen werden können. Erste Vorbereitungen für einen eigenen Zertifizierungskatalog basierend auf unseren Kriterien bis 2018 hatten wir zurückgestellt, da sich abzeichnete, dass noch Vorgaben von europäischer Seite fehlten und zunächst hierauf beruhende nationale Akkreditierungskriterien und Vorgaben für Prüfkriterien verabschiedet werden mussten. Diese Schritte sind nun abgeschlossen, sodass wir unsere ursprüngliche Planung wieder aufnehmen wollen.

Parallel beobachten wir die Stellungnahmeverfahren des Europäischen Datenschutzausschusses zu Kriterienkatalogen privater Anbieter. Wichtig ist uns, nicht in Konkurrenz zu privaten akkreditierten Anbietern zu treten, sondern aus unseren eigenen Kompetenzen ein **ergänzendes Angebot für öffentliche Stellen in Schleswig-Holstein** zu erarbeiten. Im Rahmen unserer gesetzlich geregelten Aufgaben in der DSGVO und dem LDSG müssen wir auch die Verhältnismäßigkeit und Effektivität des zu entwickelnden Angebots im Blick behalten. Private Antragsteller (auch von außerhalb von Schleswig-Holstein), die noch bis Mai 2018 das Datenschutz-Gütesiegel Schleswig-Holstein verliehen bekommen konnten, müssen wir dann an akkreditierte private Zertifizierungsstellen verweisen.

Was ist zu tun?

Für ein Zertifizierungsangebot muss ein Kriterienkatalog entwickelt werden, der den Vorgaben für einen deutschen Prüfkriterienkatalog sowie den europäischen Vorgaben entspricht. Dazu ist ein Zertifizierungsprogramm zu erstellen, das u. a. das Prüfungsverfahren beschreibt. Dabei sind die Entwicklungen in Deutschland und Europa zu beobachten und in diesem Zusammenhang kritisch zu hinterfragen, welches Zertifizierungsangebot tatsächlich mit den zur Verfügung stehenden Ressourcen realisierbar ist.

10

KERNPUNKTE

Anonymisierung und Schwärzung in Dokumenten

Die Faxen dicke

Impfzertifikate: prüfen, fälschen, stehlen

10 Aus dem IT-Labor

10.1 Anonymisierung und Schwärzung in Dokumenten

Die **fachgerechte Anonymisierung und Schwärzung von Dokumenten** beschäftigt das ULD weiterhin. Schon in vergangenen Tätigkeitsberichten haben wir auf die Tücken bei der Anonymisierung elektronischer Dateien hingewiesen (36. TB., Tz. 10.4 und 39. TB, Tz. 10.3). Mittlerweile zeigen sich die angesprochenen Risiken auch in der Praxis: Uns erreichen Meldungen nach Artikel 33 DSGVO über Datenschutzverletzungen durch ungenügend anonymisierte Unterlagen, bei denen im Zuge einer Offenlegung der Dokumente, beispielsweise durch eine Veröffentlichung, personenbezogene Daten unbefugt offenbart wurden.

Im Rahmen von Transparenzverpflichtungen wird die Offenlegung von Unterlagen, Gutachten, Verträgen usw. zunehmen, besonders im öffentlichen Bereich, der Anforderungen der Informationsfreiheits- und Transparenzgesetze erfüllen muss. Da hierbei Portale und Webseiten zum Einsatz kommen, sind diese Dokumente dann – anders als die frühere Auslage von Papierdokumenten in Amtsräumen z. B. in einem Zeitraum von zwei Wochen zur Einsichtnahme – weltweit und oft dauerhaft verfügbar. Selbst wenn ungenügend anonymisierte Dokumente entdeckt und von den Portalen entfernt werden, bleiben sie häufig dennoch **in Suchmaschinenergebnissen und Webarchiven verfügbar**. Daher ist eine besondere Sorgfalt bei der Anonymisierung geboten.

Dies kann leichter gelingen, wenn die Anonymisierung nicht erst im fertigen PDF-Dokument vorgenommen wird, sondern vor dessen Erstellung im zugrundeliegenden Textdokument stattfindet. In der Textverarbeitung oder Tabellenkalkulation können Schwärzungen durch schlichtes **Löschen** erfolgen und müssen nicht, wie im PDF-Format nötig, mit anderen Objekten überlagert und verschmolzen werden. Bereinigt man das Textdokument danach um die enthaltenen **Metadaten**, ist eine gute Ausgangsbasis für ein wirklich anonymisiertes PDF-Dokument geschaffen.

Bei der Beauftragung Dritter (z. B. zur Erstellung von Gutachten, Vertragsentwürfen o. ä.) kann man die Erstellung von **zwei Versionen zum Auftragsgegenstand** machen: eine Vollversion und eine zur Veröffentlichung geeignete Version, die um sensible Informationen bereinigt wurde. Zwar muss der Verantwortliche auch in dieser bereinigten Version überprüfen, ob sie tatsächlich zur Veröffentlichung geeignet ist – schließlich können noch Informationen enthalten sein, die aus Sicht des Auftragnehmers unkritisch sind – jedoch nicht vom Verantwortlichen so herausgegeben werden dürfen. Aber zumindest die Entfernung von Adress-, Autoren- und Metadaten aus einem Dokument kann Gegenstand des Auftrags sein. Die fertiggestellten Auftragsdokumente sollten zudem dem Verantwortlichen in einer weiterbearbeitbaren Form übergeben werden, also nicht ausschließlich im PDF-Format, sondern parallel in einem offenen Dateiformat. Da zum Zeitpunkt der Auftragsvergabe mögliche Offenlegungsgründe und „Schwärzungsbedürfnisse“ womöglich nicht vollständig bekannt sind, muss die auftraggebende Stelle die Möglichkeit haben, **Anonymisierungen und Schwärzungen hinreichend flexibel anzupassen**. Dies geschieht am besten im ursprünglichen Dokument und nicht in der finalen PDF-Version.

10.2 Die Faxen dicke?

Seit der Einführung im Bereich der deutschen Bundespost im Jahr 1979 hatte sich das Fax in geschäftlichen und behördlichen Kommunikationsprozessen einen festen Platz gesichert. Dies nicht zuletzt, weil auch manche Fristwahrung auf den allerletzten Drücker „vorab per Fax“ doch noch eingehalten werden konnte. Rechtlich war eine **Übermittlung von Willenserklärungen per Fax** seit Längerem akzeptiert. Nun mehren sich Berichte, dass es dabei wohl nicht bleiben wird (siehe auch Tz. 4.5.3).

Für Aufsehen sorgten im letzten Jahr nicht nur die Hinweise mancher Datenschutzaufsichtsbehörden, die zur Abkehr vom Fax mahnten. Auch ein erstes **Oberverwaltungsgericht** entschied, dass die Übermittlung personenbezogener Daten per Fax ohne gesonderte Sicherheitsvorkehrungen den Anforderungen der DSGVO nicht entspricht (OVG Lüneburg, Beschluss vom 22.07.2020 – 11 LA 104/19, https://openjur.de/u/2263419.html). Nicht nur die Rechtslage hat mit der DSGVO eine Auffrischung erhalten.

Der technische Fortschritt hat nämlich auch den Faxdienst nicht verschont, und damit ist nicht nur der sicherlich bemerkenswerte Umstieg von Thermo- zu Normalpapier gemeint. Relevante Veränderungen für die rechtliche Bewertung von Faxdiensten gab es an mehreren Stellen. So war das Telefonnetz, über das ein Fax übertragen wird, ursprünglich ein Verbund relaisgeschalteter Leitungen, woraus sich vergleichsweise wenige Möglichkeiten für Angreifende ergaben, auf Kommunikationsinhalte zuzugreifen. Inzwischen sind die **Telefonnetze allerdings auf IP-Technik** umgestellt, sodass sämtliche Herausforderungen der Systemsicherheit, mit denen sich Administrationen von Firmen- oder Behördennetzen heutzutage täglich konfrontiert sehen, auch diese betreffen. Diese Problematik betrifft gleichermaßen die Telefonie ohne Ende-zu-Ende-Verschlüsselung.

Auch auf Empfangsseite stehen nur noch selten Endgeräte, die Faxe tatsächlich auf Papier ausdrucken. Meist werden ankommende Faxe als Grafik in eine PDF-Datei eingebettet und dann per E-Mail weitergeleitet. Während beim Papierfax nicht ohne zusätzliche Maßnahmen sichergestellt werden kann, wer da nun eigentlich alles einen Blick draufwirft, und damit eine Vertraulichkeit nicht gegeben ist, bleiben auch beim E-Mail-Versand Probleme: Zwar gibt es einerseits mehr Möglichkeiten, Faxnachrichten zielgenau zu adressieren (persönliche Faxnachrichten anstelle eines Faxversands an ein Gerät, auf das eine Vielzahl von Personen Zugriff hat), doch durch die **Umsetzung als E-Mail** besteht in externen und internen Netzen die gleiche Problematik hinsichtlich der IT-Sicherheit wie bei E-Mails. Dies kann auch den Faxversand betreffen, wenn Mail-to-Fax-Gateways oder Webdienste zum Einsatz kommen. War ein Fax früher nach dem Ausdruck aus den übertragenden Systemen verschwunden, können nun **an vielen Stellen Kopien verbleiben**, die bei gezielten Angriffen oder den immer wieder bekannt werdenden Infektionen mit Ransomware (verschlüsselnde Erpressungs-Trojaner) ebenfalls betroffen sind.

Insgesamt betrachtet kann daher die Sicherheit von Fax im Vergleich zum Versand unverschlüsselter E-Mail nicht mehr als höher beurteilt werden.

Dass das Fax trotz der für aktuelle technische Verhältnisse miserablen Übertragungsqualität immer noch eingesetzt wird, liegt neben Gewöhnung auch daran, dass es sich um ein offen standardisiertes System handelt, das mit Endgeräten beliebiger Hersteller genutzt werden kann. Niemand ist gezwungen, ein bestimmtes Gerät oder eine bestimmte Software zu kaufen oder zu verwenden. Das Fax sollte daher durch einen ebenso **offen standardisierten und insbesondere herstellerunabhängigen digitalen Übertragungsweg mit sicherer Ende-zu-Ende-Verschlüsselung abgelöst** werden.

Was ist zu tun?

Die bisherige rechtliche Einordnung von Faxdiensten ist auf den Prüfstand zu stellen, da sich die technischen Realisierungen maßgeblich verändert haben und für die Kommunikationspartner nicht ersichtlich sind. Pauschal kann das Fax nicht mehr als sicherer als unverschlüsselte E-Mails betrachtet werden.

Personenbezogene Daten sollten ausschließlich so übermittelt werden, dass unbefugte Dritte darauf keinen Zugriff erlangen können. Dazu bietet sich eine Ende-zu-Ende-Verschlüsselung an.

10.3 Digitale Impfzertifikate: prüfen, fälschen, stehlen

Die Vorläufer des Impfpasses waren im 17. Jahrhundert „Bescheinigungen der Pestfreiheit“: Dokumente, deren vorrangiger Zweck es war, die Ein- und Durchreise von Personen in Zeiten großer Infektionsgefahren zu erleichtern. Das gelbe Impfbuch, wie wir es kennen, dient hingegen primär der Dokumentation der eigenen Impfhistorie, um Impflücken oder Doppelimpfungen auszuschließen. Mit der fortschreitenden Coronapandemie wird aus dem gelben Büchlein jedoch wieder das, was schon die „Bescheinigung der Pestfreiheit“ war: ein Garant für den Zugang zu vielen Bereichen des Alltags. Dieser Bedeutungszuwachs bringt jedoch Probleme mit sich. So war das **gelbe Impfbuch nie sonderlich manipulationssicher**, was in Zeiten von 2G-Beschränkungen (Nachweis, dass eine Person geimpft oder genesen ist) des öffentlichen Lebens für einige Menschen den Anreiz schafft, sich statt um eine Impfung lieber um die Fälschung des Impfstatus zu kümmern.

Gegen das schlichte Umheften der betreffenden Seiten eines Impfpasses ist wenig auszurichten. Abgesehen von der Papierfarbe lassen sich solche Manipulationen höchstens an malträtierten Heftklammern erkennen. Hier rächt sich, dass die Seiten des Impfpasses nicht individualisiert sind, wie es bspw. beim Reisepass der Fall ist, wo die Ausweisnummer in alle Einzelseiten eingestanzt ist. Überhaupt lässt der Impfpass **grundlegende Sicherheitsmerkmale** vermissen. So kann man gefälschte Impfpässe bei professionellen Fälscherbanden für wenig Geld bestellen, bei denen eine erfolgreiche Corona-Impfung samt gefälschter Chargen-Aufkleber bereits eingetragen ist. Für fachfremde Personen, zu denen man in diesem Fall das Personal für Türkontrollen und in der Gastronomie zählen muss, sind diese Ausweise nicht als Fälschung zu identifizieren. Gewiss fallen geübten Kontrolleuren Inkonsistenzen zwischen dem Ort der Impfung, den Chargennummern und den Datumsangaben auf. Derlei Plausibilitätsprüfungen können allerdings nur mit zusätzlichem Hintergrundwissen und der nötigen Akribie erfolgreich sein.

Spätestens, wenn aus einem manipulierten Impfpass ein digitales Impfzertifikat erstellt wurde, ist der Papierbetrug noch besser getarnt. Durch den Umstand, dass die impfenden Ärzte neben dem Impfpass nicht gleich auch ein digitales Zertifikat ausstellen, sind Betroffene in der Regel gezwungen, zu diesem Zweck in Apotheken vorstellig zu werden. Dort muss dann anhand weniger Indizien wie Stempel, Unterschrift und Chargen-Aufkleber die Echtheit des vorgelegten Papierdokuments geprüft werden. Vonnöten sind nicht nur **Sorgfalt und Integrität** der Apotheken-Mitarbeitenden, sondern auch eine **vertrauenswürdige Informationstechnik** der Apotheken. Diese setzen zum Verarbeiten der Zertifikatsdaten u. a. das Webportal des Deutschen Apothekerverbands (DAV) ein, das allerdings bis zum Sommer 2021 eklatante Sicherheitslücken aufwies. So gelang es beispielsweise, Fantasie-Apotheken in diesem Portal zu registrieren und technisch betrachtet echte Zertifikate für den längst verstorbenen Robert Koch zu erstellen. Nun sollte es bei hierarchisch aufgebauten digitalen Zertifikaten eigentlich möglich sein, Schwindler unter den Ausstellern zu ermitteln und deren Zertifikate gezielt zu sperren (revozieren). Da anfangs die digitalen Impfzertifikate jedoch keine Angaben über die konkrete Apotheke enthielten, war ein gezieltes Zurückziehen ausgeschlossen. Immerhin wurde zwischenzeitlich an dieser Front nachgebessert, aber es bleibt die Frage, warum solche groben Schnitzer überhaupt möglich waren.

Corona-Warn-App

App des RKI zur Kontaktverfolgung mittels Bluetooth-Entfernungsmessung. Die App kann seit einiger Zeit auch das Impfzertifikat von mehreren Personen speichern und ermöglicht das „Einchecken“ in bestimmte Orte, die einen QR-Code zur Kontaktverfolgung ausweisen.

CovPass-App

App des RKI zur Speicherung von Impfzertifikaten. Die CovPass-App kann die Zertifikate von mehr als einer Person verwalten, beispielsweise bei Familien.

CovPassCheck-App

App des RKI zur Prüfung der Gültigkeit von vorgezeigten digitalen Impfzertifikaten, z. B. für eine Einlasskontrolle. Die App speichert keine Zertifikate und kann offline verwendet werden. Zur Aktualisierung der Liste gesperrter Zertifikate ist eine periodische Netzverbindung notwendig.

Aber auch beim Einsatz der digitalen Zertifikate gibt es Fallstricke und Hürden. Besorgte Bürgerinnen und Bürger fragten sich, wie ein **unbefugtes Kopieren des QR-Codes beim Scannen** im Rahmen einer Überprüfung verhindert werden könne. Die unbefriedigende Antwortet lautet: in letzter Konsequenz gar nicht.

Zum Prüfen eines digitalen Impfzertifikats benötigt die Prüfperson die CovPassCheck-App des Robert Koch-Instituts (RKI). Kommt diese zum Einsatz, wird das Zertifikat gescannt, geprüft, aber nicht anderweitig gespeichert.

Ob die prüfende Person jedoch wirklich die korrekte App einsetzt, ist für die Betroffenen im Allgemeinen nicht zu ermitteln. So könnte die prüfende Person anstelle der CovPassCheck-App auch die CovPass-App einsetzen, die jedes gescannte Zertifikat speichert – und dabei optisch der Check-App ähnelt. Was für Familien mit mehreren Kindern praktisch ist, wird beim Gastwirt oder bei der Türsteherin schnell zum Zertifikate-Sammelalbum. Es ist also durchaus denkbar, dass digitale Impfzertifikate in den Händen unbefugter Dritter landen, ohne dass **wirksame Gegenmaßnahmen** vorstellbar wären.

Umso wichtiger ist es, dass Prüfende wirklich einen Abgleich des im Zertifikat hinterlegten Namens mit einem gültigen Ausweisdokument vornehmen. Der oftmals anzutreffende Blick mit Profi-Augen auf den vorgezeigten QR-Code reicht da nicht. Auf Basis des Status Ende 2021 ist zu fordern, dass die beiden Apps optisch voneinander unterscheidbar gemacht werden, sodass auf den ersten Blick erkennbar ist, ob hier eine **Check- oder Speicher-App** am Werke ist.

10.4 Filterlisten: Kontrollverlust durch DNS-, Werbe- und Inhaltsfilter

Wie sieht das heutige World Wide Web aus? Auf der einen Seite stehen Software- und Inhaltsschaffende, die zur Monetarisierung ihrer Dienstleistungen personenbezogene Daten sammeln und Werbung ausspielen. Auf der anderen Seite stehen die Nutzenden, unter denen sich viele von diesem Vorgehen unwohl oder belästigt fühlen. Als Konsequenz haben sich diverse **Formen der digitalen Gegenwehr durch Software-Tools** etabliert, die wiederum regelmäßig von den Werbetreibenden torpediert werden – ein **Katz-und-Maus-Spiel**. Mitunter geht nicht einmal die Hälfte aller Netzverbindungen eines durchschnittlichen Smartphones auf Aktivitäten der nutzenden Person zurück; der weitaus größte Teil des Datenverkehrs findet im Hintergrund und ohne inhaltlichen Mehrwert statt, wenn Apps mit Werbenetzwerken Informationen austauschen.

Als probates Mittel für die Nutzenden, solche Datenverbindungen wenigstens teilweise zu kontrollieren, haben sich **Filterprogramme** herausgestellt, die aufzubauende Datenverbindungen analysieren, bewerten und beeinflussen können. Dabei kann die Filterung auf dem jeweiligen Gerät erfolgen oder auf ein extern vorgeschaltetes Gerät ausgelagert werden. Die am weitesten verbreitete Variante stellen Werbeblocker im Browser dar. Als nachladbares Modul (Add-on) kontrollieren sie den Datenfluss und gleichen aufzurufende Webadressen mit Listen ab, auf denen Werbetreibende, Trackingdienste und Malware-Verteiler verzeichnet sind. Externe Geräte, die als Proxy den Datenverkehr filtern, setzen ebenfalls solche Listen ein.

Domain Name System (DNS)

Um den Aufruf von Webressourcen zu vereinfachen, übersetzt das Domain Name System die IP-Adressen, mit denen Computer untereinander kommunizieren, in verständliche Buchstabenkombinationen. Auf diese Weise kann z. B. die ULD-Webseite (www.datenschutzzentrum.de) erreicht werden. Im Hintergrund wird diese Zeichenfolge vom DNS in die IP-Adresse 213.178.69.184 übersetzt.

Technisch betrachtet findet hier zumeist eine **DNS-Filterung** statt: Wenn eine App Kontakt zu einer Domain aufnehmen möchte, wird eine sogenannte DNS-Abfrage erzeugt, um die passende IP-Adresse der Domain zu ermitteln. Dorthin werden die Datenpakete dann gesendet. Viele Filter setzen an dieser DNS-Abfrage an und ermitteln, nach welchen Domains gefragt wurde. Handelt es sich um eine als unerwünscht klassifizierte Domain, wird die Zieladresse als nicht erreichbar zurückgemeldet. Die anfragende App geht dann davon aus, dass keine Netzverbindung besteht. Legitime bzw. er-

wünschte Domains hingegen lässt der Filter passieren, sodass hier eine nahtlose DNS-Auflösung erfolgen kann.

Auf der Seite der Inhaltsschaffenden werden solche Bestrebungen natürlich bemerkt und es wird versucht, mit allerlei Maßnahmen das Vorhandensein eines Filters festzustellen. Das Ergebnis solcher Werbeblocker-Blocker sind weitere Filterlisten, die eben diese Maßnahmen erkennen. **Werbeblocker-Blocker-Blocker** – fast wie beim Wettrüsten.

Dabei ist der zugrundeliegende Konflikt oft nicht deutlich. Wer eine Webseite betreibt und Werbung schaltet, möchte zumeist seine Arbeit monetarisieren. „Webseite gegen Werberezeption“ lautet die vordergründige Formel. Tatsächlich ist der Preis, den die Lesenden zahlen, ein anderer: **„Webseite gegen personenbezogene Daten UND Werberezeption“**. Die personenbezogenen Daten, die zum Ausspielen der Werbung erhoben werden, machen das oberflächlich betrachtet faire Tauschgeschäft zu einem fragwürdigen Deal: Nutzende kennen den Wert ihrer Daten nicht. Neben Zeit und Aufmerksamkeit „zahlen“ sie also in Form von Nutzungsdaten in einer unbekannten Währung. Will man sich vor dem Abfließen von Nutzungsdaten schützen, kommt dies zumeist einer Blockade jeglicher Werbung gleich.

Aber die Technik eignet sich **nicht nur, um sich gegen Werbung und Nutzungsverfolgung zur Wehr zu setzen**. Es gibt spaßige Filter, die Webseitentexte mit Einhörnern umformulieren, und ernsthafte, die sogenannte Hate-Speech finden und die Beschimpfungen durch aufmunternde Worte ersetzen können. Ebenso existieren Filter, die geschlechtergerechte Ausdrücke in die Sprachästhetik des vergangenen Jahrhunderts zurückwandeln.

Das Risiko solcher Filter – seien es nun Werbe- oder Formulierungsfilter – liegt in deren **Redaktion**. Denn praktisch werden Filterlisten einmalig eingerichtet und **keiner regelmäßigen nennenswerten Prüfung unterzogen**. Oft werden auch schlicht die Standardlisten der eingesetzten Software beibehalten. Was dann genau der Filterung zum Opfer fällt, ist im Alltag nur mit Mühe zu rekonstruieren. De facto übereignen Nutzende mit der Einrichtung von Webfiltern die Darstellung der rezipierten Inhalte einer dritten Instanz. Das ist umso bedenklicher, je mehr die Filter neben dem Blockieren auch eine Ersetzung oder Adaption der Inhalte vornehmen. Niemand wird etwas dagegen haben, Beschimpfungen in freundliche Worte zu verwandeln. Eine Technik, die das kann, wäre jedoch prinzipiell auch in der Lage, **jedweden anderen Inhalt zu ersetzen und beliebige Bedeutungsveränderungen vorzunehmen**. Die Kontrolle der Filter- und Ersetzungslisten bedeutet somit die Kontrolle über sämtliche dargestellten Inhalte.

Webfilter bestimmen nicht nur darüber, was wir nicht sehen, sondern zunehmend auch über das, was wir sehen, lesen und aufnehmen. So entsteht ein neuer Aspekt der sogenannten Filterblase, in der Nutzende sich befinden. Diesmal sind es jedoch nicht nur multinationale Konzerne, die **mit undurchsichtigen Algorithmen Einfluss darauf nehmen, welche Inhalte wir zu Gesicht bekommen**. Die oftmals von vielen Beitragenden gemeinsam in Open-Source-Manier erstellten **Listen und Programme zum Filtern**, die bewusst und aktiv von den Nutzenden eingesetzt werden, prägen fortan deren Sicht auf die Online-Welt entscheidend mit. Dies alles bewirkt nicht nur einen Kontrollverlust für jede und jeden Einzelnen, sondern kann auch über die Beeinflussung von Meinungen oder Verstärkung extremer Positionen unserer demokratischer Gesellschaft Schaden zufügen.

11

KERNPUNKTE

Leitlinien aus Europa zu Targeting
Leitlinien aus Europa zu Datenpannen
Stand zur ePrivacy-Verordnung

11 Europa und Internationales

Für ein einheitliches Verständnis und eine einheitliche Anwendung der DSGVO ist eine Abstimmung unter den Aufsichtsbehörden der EU-Mitgliedstaaten notwendig. Dies geschieht im Europäischen Datenschutzausschuss (EDSA). Der EDSA veröffentlicht beispielsweise Guidelines (Leitlinien) und Empfehlungen, die in Arbeitsgruppen (Expert Subgroups) erarbeitet werden. Das ULD ist als Vertreter der Datenschutzaufsichtsbehörden der Länder Mitglied in der Key Provisions Expert Subgroup, die sich grundsätzlichen Fragen widmet. Als stellvertretender Ländervertreter arbeitet das ULD in der Technology Expert Subgroup mit, die sich mit Informations- und Kommunikationstechnologien beschäftigt. Ländervertreter haben insbesondere die Aufgabe, Auffassungen aus allen Bundesländern zu Auslegungsfragen einzuholen und Formulierungen abzustimmen. Auch an weiteren Unterarbeitsgruppen und zu spezifischen Themen (beispielsweise zu Zertifizierung, Tz. 9.3) beteiligt sich das ULD auf europäischer Ebene, soweit dies mit den zur Verfügung stehenden beschränkten Ressourcen möglich ist.

11.1 Guidelines aus Europa – Finalisierung zu Targeting in sozialen Medien

Die Arbeiten an den **„Leitlinien 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien“** sind abgeschlossen (39. TB, Tz. 11.2). Eine deutsche Version ist mittlerweile auf den Webseiten des EDSA abrufbar.

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_de

Kurzlink: *https://uldsh.de/tb40-11-1*

Targeting

Unter dem Begriff ‚Targeting‘ (auch Microtargeting) werden Dienste zur gezielten, meist werblichen Ansprache von Nutzenden in sozialen Netzwerken oder auf Webseiten verstanden.

Damit wird es natürlichen oder juristischen Personen, die in dem Dokument des EDSA als „Targeter“ bezeichnet werden, ermöglicht, spezifische Botschaften an die Nutzenden sozialer Medien oder Webseiten zu übermitteln, um kommerzielle, politische oder sonstige Interessen zu fördern. Je detaillierter das zugrunde liegende Profil über eine Person ist, desto passgenauer können Botschaften an die jeweiligen Nutzenden angepasst werden und desto höher ist die Wahrscheinlichkeit, dass die beworbenen Produkte oder Dienstleistungen tatsächlich nachgefragt werden.

Diese Dienste werden häufig zur werblichen Ansprache verwendet, um Nutzenden passgenaue Werbung anzuzeigen, aber auch im politischen Meinungskampf werden diese Dienste vermehrt genutzt.

Umfangreich eingesetzt und auch untersucht wurde Microtargeting unter anderem im Zusammenhang mit der Volksabstimmung zum Brexit. Detaillierte Informationen dazu finden sich z. B. auf der Webseite der Aufsichtsbehörde für Großbritannien, Information Comissioner‘s Office (ICO).

Link: *https://ico.org.uk/*

Im Rahmen einer öffentlichen Konsultation hatte der EDSA eine Vielzahl an Rückmeldungen insbesondere von Wirtschaftsunternehmen und -verbänden, Nichtregierungsorganisationen, Verbraucherschutzorganisationen sowie Akteuren der Wissenschaft erhalten. Nach Sichtung und Auswertung der Rückmeldungen wurden die Leitlinien final abgefasst. Dabei wurden die Rückmeldungen berücksichtigt und teilweise Änderungen am Text vorgenommen.

Die Leitlinien beleuchten vor dem Hintergrund der Entscheidungen des Europäischen Gerichtshofs zu Fragen der **gemeinsamen Verantwortlichkeit**, wie die Rollen der Akteure im Bereich des **Targeting** (auch „Micro-Targeting“ oder „gezielte Ansprache“ genannt) zu beurteilen sind und welche rechtlichen Konsequenzen sich daraus für die Beteiligten ergeben. Die Urteile in den Rechtssachen Wirtschaftsakademie (C-210/16),

Jehovan todistajat (C-25/17) und Fashion ID (C-40/17) sind hierbei von besonderer Bedeutung. Die Leitlinien fokussieren sich dabei maßgeblich auf die Social-Media-Anbieter und die sogenannten Targeter, d. h. diejenigen, die Social-Media-Dienste nutzen, um auf der Grundlage bestimmter Parameter oder Kriterien bestimmte (Werbe-)Botschaften gezielt an eine Gruppe von Social-Media-Nutzenden zu richten.

Nach einer Darstellung der verschiedenen **Targeting-Techniken (Targeting auf Grundlage bereitgestellter, beobachteter oder abgeleiteter Daten sowie einer Kombination dieser Daten)** wird anhand von Beispielen dargelegt, welche Rollen die jeweils Beteiligten einnehmen und welche damit einhergehenden Anforderungen eingehalten werden müssen, damit die Beteiligten datenschutzkonform handeln.

Da die Rolle des datenschutzrechtlich Verantwortlichen zentral für die DSGVO ist (siehe auch Tz. 11.4), muss klargestellt werden, **für welche Verarbeitungsschritte eine (gemeinsame) Verantwortlichkeit** besteht. Den Verantwortlichen treffen nämlich sämtliche Pflichten aus der DSGVO für von ihm (auch in gemeinsamer Verantwortung) verantwortete Datenverarbeitungen. Dies betrifft vor allem die Pflicht, die Rechtmäßigkeit der Verarbeitung sicherzustellen und dies auch nachweisen zu können.

Auch vor dem Hintergrund, dass aufgrund der ungleich größeren tatsächlichen Einwirkungs- und Gestaltungsmöglichkeiten des Social-Media-Anbieters dort auch ein wesentlich höherer Grad der Verantwortlichkeit gegeben ist, lässt das die **Verantwortlichkeit der Targeter** nicht entfallen. Dies ändert sich auch dann nicht, wenn kaum eine Möglichkeit für Targeter besteht, Bedingungen auszuhandeln oder Änderungen an Standardvereinbarungen vorzunehmen.

Gemeinsam Verantwortliche müssen in einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Verpflichtung gemäß der DSGVO erfüllt. Der EDSA ist der Ansicht, dass die **Vereinbarung zwischen den Targetern und den Anbietern sozialer Medien** alle Verarbeitungsvorgänge umfassen sollte, für die sie gemeinsam verantwortlich sind (d. h. die unter ihrer gemeinsamen Kontrolle stehen). Durch den Abschluss einer nur oberflächlichen und unvollständigen Vereinbarung würden die Targeter und die Social-Media-Anbieter gegen ihre Verpflichtungen aus Artikel 26 DSGVO verstoßen. Zur Erarbeitung einer umfassenden Vereinbarung müssen sowohl der Social-Media-Anbieter als auch der Targeter die durchgeführten spezifischen Datenverarbeitungsvorgänge kennen und **ausreichend detaillierte Informationen** darüber haben.

Ohne ausreichende Informationen über die Verarbeitung kann eine Bewertung über die Rechtskonformität nicht vorgenommen werden. Verantwortliche können so ihrer **Rechenschaftspflicht** nicht nachkommen.

Was ist zu tun?

Wer eine gezielte Ansprache (Targeting) von Nutzenden auf Social Media Plattformen betreiben möchte, muss sicherstellen, dass er die rechtlichen Vorgaben bei der Verarbeitung personenbezogener Daten zu diesen Zwecken einhält, da eine Verantwortlichkeit der Werbetreibenden (Targeter) in diesen Fällen gegeben ist. Die Leitlinien des EDSA zeigen anhand von Beispielen auf, wie die Rollen der Beteiligten zu sehen sind und welche Pflichten sich daraus ergeben.

11.2 Guidelines aus Europa – Data Breach Notifications

Täglich erhalten wir **Meldungen nach Artikel 33 DSGVO** über Verletzungen des Schutzes personenbezogener Daten (auch als Datenpannen bezeichnet).

Häufig wenden sich Verantwortliche an uns, weil **Unsicherheiten angesichts der Risikoeinschätzung** bestehen, ob ein eingetretener Vorfall beim Verantwortlichen die Meldepflicht nach Artikel 33 DSGVO an die Landesbeauftragte für Datenschutz auslöst.

Verletzung des Schutzes personenbezogener Daten (Datenpanne)

Eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich **nicht** zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

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

Auch ist einigen Verantwortlichen nicht klar, ob zusätzlich eine Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person nach Artikel 34 DSGVO notwendig ist.

Die Unsicherheit der Verantwortlichen in der **Abgrenzung sowohl bei der Meldung an die Aufsichtsbehörde als auch hinsichtlich der Benachrichtigung der betroffenen Personen** wurden in den anderen Mitgliedstaaten ähnlich wahrgenommen. Zwar existieren bereits Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten, die noch von dem Vorgängergremium des EDSA, der Artikel-29-Datenschutzgruppe, erstellt und vom EDSA übernommen wurden.

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-personal-data-breach-notification-under_de

Kurzlink: *https://uldsh.de/tb40-11-2a*

Es hat sich jedoch gezeigt, dass Bedarf an weiterer Orientierung besteht. Aus diesem Grund hat der EDSA im Jahr 2021 neue **Leitlinien mit diversen Fallbeispielen** veröffentlicht und einem Konsultationsverfahren zugeführt.

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_de

Kurzlink: *https://uldsh.de/tb40-11-2b*

Die Konsultationsfrist ist mittlerweile abgelaufen, die Rückmeldungen werden analysiert und bei Abfassung des finalen Dokuments berücksichtigt. Mit der Veröffentlichung einer endgültigen Version ist im ersten Quartal 2022 zu rechnen.

Was ist zu tun?

Im Fall von Verletzungen des Schutzes personenbezogener Daten müssen die datenschutzrechtlichen Anforderungen an eine Meldung an die Aufsichtsbehörde und gegebenenfalls an eine Benachrichtigung der betroffenen Personen erfüllt werden. Hilfestellung geben die Veröffentlichungen des Europäischen Datenschutzausschusses.

11.3 Stand zur ePrivacy-Verordnung

Eigentlich schon für 2018 geplant, aber noch immer nicht da: die ePrivacy-Verordnung. Auch unter der Ratspräsidentschaft Deutschlands hat es keine wesentliche Entwicklung in Bezug auf die geplante **Verordnung zum Schutz personenbezogener Daten in der elektronischen Kommunikation** (ePrivacy-Verordnung) gegeben, die dazu geführt hätten, dass ein seit langem herbeigesehntes Regelwerk für diesen so relevanten Bereich der Datenverarbeitung verabschiedet worden wäre.

Die Entwicklungen im Rahmen der Gesetzgebung veranlassten den EDSA jedoch dazu, seine Position zu einigen Punkten darzulegen. Daher veröffentlichte der EDSA im März 2021 eine **Erklärung** dazu:

https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-032021-eprivacy-regulation_de

Kurzlink: *https://uldsh.de/tb40-11-3*

So betont der EDSA erneut, dass es zügig einheitlicher Vorschriften für den Bereich der elektronischen Kommunikation bedarf. Eine Vielzahl der Beschwerden, die die mitgliedstaatlichen Aufsichtsbehörden erreichen, haben nämlich direkten oder unmittelbaren Bezug zu Verarbeitungen im Internet.

Der EDSA weist darauf hin, dass bei Webseiten die Bestimmungen über die Einwilligung nach der DSGVO gelten (siehe auch Tz. 7.2). Damit eine Einwilligung wirksam ist, muss sie insbesondere freiwillig sein. Aus diesem Grund vertritt der EDSA die Ansicht, dass unlautere Praktiken, die den Zugang zu Diensten und Funktionen von der Einwilligung einer Nutzerin oder eines Nutzers in die Speicherung von Informationen im eigenen Gerät oder dem Zugang zu bereits darin gespeicherten Informationen abhängig machen (sogenannte „Cookie Walls“), verhindert werden müssen.

Der EDSA ist der Ansicht, dass von Verantwortlichen verlangt werden kann**, faire Alternativen zu Angeboten mit Tracking und Profiling anzubieten**. Dies solle für alle Diensteanbieter gleichermaßen gelten, unabhängig von ihrem Tätigkeitsbereich oder ihrem derzeitigen Finanzierungsmodell.

Nach jetziger Rechtslage ist es nur in sehr begrenztem Umfang zulässig, eine **Verarbeitung personenbezogener Daten zur Reichweitenmessung** ohne vorherige Einwilligung durchzuführen. Der EDSA fordert daher, dass eine gesetzliche Regelung geschaffen wird, die vorgibt, welche Arten der Reichweitenmessung ohne vorherige Einwilligung zulässig sind. Dabei müsse aber sichergestellt sein, dass eine solche Regelung nur solche Verarbeitungen erlaubt, die für die Auswertung der Leistung des vom Nutzer angefragten Dienstes **zwingend erforderlich** sind, und sollte sich daher ausschließlich auf die Bereitstellung von Statistiken für den Dienstebetreiber beschränken. Eine Regelung, die in diese Richtung ging, fand sich zwischenzeitlich auch in Entwürfen zur Verordnung.

Eine Reichweitenmessung dürfe weder allein noch in Kombination mit anderen Tracking-Lösungen zu einem **gezielten Herausgreifen oder zu einem Profiling von Nutzenden** durch den Anbieter oder andere Verantwortliche führen.

Darüber hinaus dürfe ein solcher Dienst für Reichweitenmessung es nicht ermöglichen, Daten zum **Surfverhalten von Nutzenden über verschiedene Websites oder Anwendungen hinaus** zu sammeln. Außerdem sollte es einen **nutzungsfreundlichen Opt-out-Mechanismus** in Bezug auf jegliche diesbezügliche Datenerhebung geben.

Bis es soweit sein wird, dass eine Überarbeitung der ePrivacy-Richtlinie erfolgt ist, gilt die bisherige Richtlinie fort. Mit Inkrafttreten des **Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien** (TTDSG) am 1. Dezember 2021 hat der deutsche Gesetzgeber nun endlich die Vorgaben der ePrivacy-Richtlinie umgesetzt. § 25 TTDSG setzt die dortigen Vorgaben zu Cookies um (siehe Tz. 7.2).

11.4 Guidelines aus Europa – Verantwortlicher und Auftragsverarbeiter

Das ULD vertritt die Bundesländer in der sogenannten **Key Provisions Expert Subgroup** (KEYP ESG). Die Arbeitsgruppe befasst sich mit der Auslegung der Kernbegriffe und wesentlicher Regelungen der DSGVO und berät andere Arbeitsgruppen des EDSA zu den Grundsätzen.

Im Jahr 2021 hat die KEYP ESG die Arbeit an den **Leitlinien 7/2020 über Verantwortliche und Auftragsverarbeiter** abgeschlossen (siehe 38. TB, Tz. 11.1). Die Begriffe „Verantwortlicher", „gemeinsam Verantwortliche" und „Auftragsverarbeiter" spielen im Datenschutzrecht eine wesentliche Rolle, denn mit ihrer Hilfe wird bestimmt, wer für die Einhaltung der gesetzlichen Vorgaben bei einer Verarbeitung personenbezogener Daten verantwortlich ist.

Die Verantwortlichkeit kann nur so weit vertraglich festgelegt werden, wie auch tatsächlich über die Mittel und Zwecke der Verarbeitung entschieden wird. In den Leitlinien wird dargelegt, wie dies im Einzelnen bestimmt werden kann und wie sich ein Verantwortlicher und gemeinsam Verantwortliche von einem Auftragsverarbeiter unterscheiden.

Verantwortlicher

ist nach Art. 4 Nr. 7 DSGVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Die Leitlinien 7/2020 zu den Begriffen des Verantwortlichen und Auftragsverarbeiters sind unter dem folgendem Link abrufbar:

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_de

Kurzlink: *https://uldsh.de/tb40-11-4*

11.5 Guidelines aus Europa – Einschränkungen im Sinne des Artikel 23 DSGVO

Im Jahr 2021 wurden die Arbeiten an den Leitlinien zu den Einschränkungen nach Artikel 23 DSGVO abgeschlossen.

Die Mitgliedstaaten können aus bestimmten Gründen, wie beispielsweise der nationalen Sicherheit und wichtiger öffentlicher Interessen, die **Rechte der betroffenen Personen einschränken**, soweit trotz dieser Einschränkungen die wesentlichen Elemente der Grundrechte gewahrt bleiben. In den Leitlinien wird der Begriff der „Einschränkung" erläutert. Es wird beschrieben, unter welchen Bedingungen eine gesetzliche Regelung von Einschränkungen möglich erscheint.

Die Leitlinien 10/2020 zu den Einschränkungen nach Artikel 23 DSGVO stehen unter dem folgendem Link zur Verfügung:

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-102020-restrictions-under-article-23-gdpr_de

Kurzlink: *https://uldsh.de/tb40-11-5*

12

KERNPUNKTE

Viele IZG-Anträge zu Corona-Fragen

Befugnisse des ULD sollen erweitert werden

ULD übernimmt den Vorsitz der Konferenz der Informationsbeauftragten

12 Informationsfreiheit

Jede natürliche oder juristische Person hat ein Recht auf freien Zugang zu Informationen, über die insbesondere Behörden in Schleswig-Holstein verfügen. Wenn bei der Ausübung dieses Rechts Probleme auftreten, kann das ULD zur Vermittlung eingeschaltet werden. Aber auch informationspflichtige Stellen können sich beraten lassen, wenn Unklarheiten in Bezug auf die Umsetzung des Informationszugangsgesetzes Schleswig-Holstein (IZG-SH) bestehen. Im Berichtszeitraum haben wir eine **neue Broschüre zum Informationszugangsgesetz** herausgebracht, die sowohl in gedruckter Form als auch online beim ULD erhältlich ist.

12.1 Aktuelle Entwicklung bei der Anpassung des IZG-SH an LDSG und DSGVO

In der Vergangenheit haben wir mehrfach darauf hingewiesen, dass das IZG-SH an die geänderten Bedingungen des LDSG und der DSGVO angepasst werden muss. Insbesondere bestehen Unklarheiten, welche **Befugnisse das ULD** in Bezug auf Prüfungen von der Umsetzung des IZG-SH in öffentlichen Stellen hat, wenn Personen sich beschweren (vgl. TB 39, Tz. 12.1). Mit dem Digitalisierungsgesetz liegt nun auch ein Entwurf für einen geänderten § 14 IZG-SH vor, der sich an unseren schon vor einiger Zeit übermittelten Vorschlägen orientiert. Neben Auskunftspflichten und Betretungsrechten wird in diesem Entwurf beispielsweise geregelt, wann das ULD Beanstandungen aussprechen kann. Unsere Anmerkungen zu dem Entwurf bezogen sich insbesondere auf **Klarstellungen** in Bezug auf Unterrichtungspflichten gegenüber der zuständigen Rechts-, Dienst- oder Fachaufsichtsbehörde und auf eine **Klagemöglichkeit** des ULD.

Was ist zu tun?

Die längst überfällige Überarbeitung des § 14 IZG-SH muss zeitnah abgeschlossen werden.

12.2 IZG-SH und Corona

Viele Themen durchziehen die Eingaben nach dem IZG-SH, die uns erreichen. Die Coronapandemie war auch im Berichtsjahr das dominierende Thema in den zahlreichen Anfragen: Neben Fragen zu Prüfungsarten und Ausstattung in Laboren interessierten sich die Bürgerinnen und Bürger für **genauere Informationen zu Fallzahlen vor Ort** in der Gemeinde, in den Schulen oder auch in Seniorenheimen. Diese Anträge waren teilweise von den Behörden mit Verweis auf den Personenbezug dieser Informationen nach § 10 Satz 1 Nr. 1 IZG-SH abgelehnt worden. In den meisten Fällen haben wir die Behörden darauf hingewiesen, dass eine solche pauschale Ablehnung nicht zulässig ist. Dies liegt schon daran, dass jeweils zu prüfen ist, ob die schutzwürdigen privaten Interesse an der Geheimhaltung gegenüber dem öffentlichen Bekanntgabeinteresse überwiegen. Vorher muss jedoch zunächst festgestellt werden, ob überhaupt personenbezogene Daten vorliegen oder es sich um statistische Fallzahlen handelt, bei denen die Anonymität gewahrt bleibt. Wir gehen in der Regel davon aus, dass ab etwa 100 Personen eine ausreichende Anonymität gegeben sein kann, damit praktisch **kein Rückschluss auf Einzelpersonen möglich** ist. Dabei müssen jedoch weitere Faktoren beachtet werden, beispielsweise in Coronasachverhalten die Anzahl der tatsächlich infizierten Personen. Wenn sich z. B. unter 100 Personen 50 Infizierte befinden, ist eine Rückverfolgung eher wahrscheinlich und eine Personenbeziehbarkeit kann vorliegen.

Dies kann auch der Fall sein, wenn über weitere Angaben zu Zeitpunkten Rückschlüsse erleichtert werden. Ist aus den Daten erkennbar, dass z. B. eine Person an einem bestimmten Tag zusätzlich als infiziert eingetragen wurde, kann etwa bezogen auf eine Schule wieder durch Beobachtungen innerhalb eines Klassenverbandes eine Identifizierung der betroffenen Person denkbar sein.

In den meisten Fällen dürfte jedoch bei **Fallstatistiken** etwa zu Gemeinden **kein Personenbezug mehr** vorliegen. So kam es auch in den weit überwiegenden Fällen, in denen wir um Vermittlung gebeten wurden, dazu, dass die Daten doch herausgegeben wurden. Einige Gemeinden und Kreise sind sogar dazu übergegangen, diese Informationen aktiv auf ihren Webseiten bereitzustellen.

Weitere Anfragen mit Corona-Bezug betrafen u. a. Verträge mit CTS Eventim bei der Terminvergabe von Impfterminen und die Datenschutz-Folgenabschätzung für die Luca-App (Tz. 12.3).

Was ist zu tun?

Neben der Verfolgung der Anfragen von natürlichen und juristischen Personen sind auch die informationspflichtigen Stellen weiter zu sensibilisieren, dass „Datenschutz“ kein pauschaler Ablehnungsgrund ist und weitere Prüfungen vorgenommen werden müssen, um den Anspruch auf Informationszugang so weit wie möglich zu erfüllen.

12.3 Top 5 der Beschwerden von Petentinnen und Petenten

Vier der fünf häufigsten Beschwerdegründe, die wir im letzten Tätigkeitsbericht (39. TB, Tz. 12.2) aufgeführt haben, gehören auch im Berichtsjahr wieder zu den „Top 5“. Seltener als im Vorjahr wurde bei Ablehnungen auf einen vermeintlichen Missbrauch durch den Antragsteller verwiesen. Hingegen fehlten sehr oft gesetzlich geforderte **Abwägungen und Anhörungen** bzw. die Abfrage einer Zustimmung, sodass diese Problembereiche nunmehr deutlicher in den „Top 5“ formuliert werden.

1. Keine Antwort

Des Öfteren kommt es vor, dass von informationspflichtigen Stellen auf Anträge gar nicht geantwortet wird. Auch wenn die Kenntnisse bei den Behörden zum IZG-SH und den damit verbundenen Rechten auf Zugang zu Informationen nach unserer Beobachtung zunimmt, so gibt es immer noch Stellen, bei denen diesbezüglich Grundlagenarbeit geleistet werden muss. Insbesondere Anfragen per E-Mail, die großenteils über das Portal Fragdenstaat.de eingereicht werden, werden immer wieder ignoriert. Allerdings wird in der Regel auf unsere Aufklärung hin zeitnah das Gespräch gesucht und/oder die Informationen werden herausgegeben.

2. Kein Bescheid im Fall einer Ablehnung

Eng verwandt mit dem ersten Punkt ist, dass bei Ablehnungen kein ordentlicher Bescheid nach § 6 IZG-SH erlassen wird. Teilweise wird nur mit formloser E-Mail über die Nichtübermittlung der angefragten Informationen informiert, ohne auf die Rechtsschutzmöglichkeiten nach § 6 Abs. 4 IZG-SH hinzuweisen. Dies hat für die Behörde den zusätzlichen Nachteil, dass dann die Fristen für eine Klagemöglichkeit deutlich verlängert werden. Es zeigt sich aber insbesondere, dass nicht immer bei den informationspflichtigen Stellen erkannt wird, dass es sich bei Anträgen um solche nach dem IZG-SH handelt bzw. diese entsprechend auszulegen und zu bescheiden wären. Die Antragstellerin bzw. der Antragsteller ist nicht in der Pflicht, ausdrücklich auf das IZG-SH hinzuweisen. Es ist Aufgabe der Behörde, im Zweifel von einem Antrag im Sinne des IZG-SH auszugehen oder zumindest diesbezüglich noch einmal bei der Antragstellerin bzw. dem Antragsteller nachzufragen.

3. Gebühren

Die überwiegende Zahl der uns zur Kenntnis gelangten Verfahren wird von den Behörden kostenfrei durchgeführt. Gelegentlicher Streitpunkt waren aber auch in diesem Berichtszeitraum die

Gebühren, die angefragte Behörden den Antragstellerinnen und Antragstellern für die Auskunft auferlegten. Geregelt ist dieses in einer Kostenverordnung des Landes (GVOBl SH 2007, 225). Danach können für umfassende Auskünfte Gebühren bis 250,- Euro und für außergewöhnlich aufwendige Auskünfte Gebühren bis 500,- Euro erhoben werden. Für einfache Auskünfte mit einem Aufwand von einer halben bis dreiviertel Stunde gehen wir davon aus, dass keine Gebühren erhoben werden. Dabei ist zu beachten, dass das grundsätzliche Einarbeiten in den Themenbereich der Informationsfreiheit nicht zum anzusetzenden Verwaltungsaufwand hinzugerechnet werden darf. Dasselbe gilt für die Zeiten, in denen uns die Verwaltungsmitarbeitenden ihre Rückfragen zu den jeweiligen Sachverhalten stellen. Anfragende sollen nicht durch übermäßige Gebühren von ihrem Recht auf Informationszugang abgehalten werden.

4. Fehlende Abwägung

Bei den Ablehnungsgründen wurde besonders oft auf das Vorliegen personenbezogener Daten im Sinne des § 10 Satz 1 Nr. 1 IZG-SH oder von Betriebs- und Geschäftsgeheimnissen im Sinne des § 10 Satz 1 Nr. 3 IZG-SH verwiesen. Mehrfach ließen es die Behörden mit einem dürren Verweis auf das Gesetz bewenden, ohne eine wirkliche Begründung abzugeben. So fehlte die Bewertung, ob die schutzwürdigen privaten Interessen an der Geheimhaltung gegenüber dem öffentlichen Bekanntgabeinteresse überwogen. Auch fehlten mehrfach Aussagen darüber, ob zumindest Teile der begehrten Informationen hätten herausgegeben werden können.

5. Fehlende Anhörung / Bitte um Zustimmung

Informationspflichtige Stellen übersahen mehrfach die Pflicht zur Anhörung der Betroffenen nach § 10 Satz 3 IZG-SH, in der auch eine mögliche Zustimmung abgefragt werden kann.

Auf unsere Vermittlung hin wurden die notwendigen Abwägungen und Nachfragen bei den Betroffenen zur möglichen Einwilligung in die Weitergabe der Informationen nachgeholt. Manchmal ergaben sich hieraus doch Möglichkeiten, um zumindest teilweise den Anfragen auf Informationszugang zu entsprechen. Einen besonderen Schwerpunkt in diesem Bereich bildeten erneut Anfragen zur Einsicht in Bauakten, wobei gerade bei diesen meist nur schwerlich Informationen ohne Personenbezug abgetrennt werden können.

Was ist zu tun?

Die informationspflichtigen Stellen müssen sich über ihre Rechte und Pflichten bei der Bearbeitung von Anträgen nach dem IZG-SH bewusst sein. Hierzu stellt das ULD Informationsmaterial zur Verfügung, das regelmäßig weiterentwickelt wird. Eine neue Broschüre in der „Praxis-Reihe“ bietet Unterstützung. Auch stehen wir gerne für Fragen zur Verfügung.

12.4 Einige besondere Fälle

Einige besondere Verfahren gab es in diesem Jahr:

1. Herausgabe Eventim-Verträge

Beim Ministerium für Soziales Gesundheit, Jugend, Familien und Senioren Schleswig-Holstein war von mehreren Personen der Antrag gestellt worden, die Verträge mit der Firma CTS Eventim AG & Co. KGaA zu übermitteln. CTS Eventim war damit beauftragt worden, das System zur Vergabe von Impfterminen in Schleswig-Holstein zu entwickeln. Die Herausgabe der Verträge war jedoch verweigert worden. Als Begründung diente dabei der Verweis auf § 2 Abs. 4 Nr. 2 IZG-SH, da es sich um Informationen im Rahmen des Gesetzgebungsverfahrens bzw. dem Erlass von Rechtsverordnungen handele.

Dies konnten wir nicht nachvollziehen: § 2 Abs. 4 Nr. 2 IZG-SH betrifft zwar den Erlass von Rechtsverordnungen, zu denen auch die Verordnungen des Landes zur Bekämpfung des COVID 19-Virus mittels Testverfahren und Impfungen gehören. Zur geschützten Tätigkeit zählen insbesondere die Erstellung der Entwürfe sowie die Verfahren der Abstimmung der Entwürfe

mit anderen Ressorts bzw. anderen Ländern und dem Bund und den externen Interessenvertretern. Der hier erbetene Vertrag mit der Firma CTS Eventim stellte nach unserem Verständnis jedoch erst eine Folge aus dem Gesetzgebungsverfahren dar. Uns war nicht nachvollziehbar, weshalb der Vertrag unmittelbarer Teil des Gesetzgebungsverfahrens sein sollte. In den Verordnungen wurde die Firma nicht erwähnt.

Dies sah auch die Behörde ein, sodass sie im weiteren Verlauf von dieser Argumentation abrückte und die erbetenen Unterlagen – zumal der Petent Klage beim Verwaltungsgericht in Schleswig eingereicht hatte – zumindest teilweise übermittelte.

2. Luca-App

Die Luca-App war Gegenstand einer Anfrage beim IT-Verbund Schleswig-Holstein unter Einbindung von Dataport. Einige Informationen konnten auf unsere Vermittlung hin weitergegeben werden, nicht jedoch die angefragte Datenschutz-Folgenabschätzung. Begründet wurde dieses damit, dass eine solche nicht vorlag.

Tatsächlich bezieht sich das IZG-SH nur auf bei Behörden vorhandene Informationen. Eine Beschaffungspflicht von Informationen aufgrund einer Anfrage besteht nicht. Sollte eine Petentin bzw. ein Petent dabei zu der Vermutung kommen, dass dieses unrechtmäßig sei, so kann losgelöst vom IZG-SH eine Beschwerde bei uns eingereicht werden.

3. Protokolle Ministerpräsidentenkonferenzen

Ein weiterer Fall betraf die Herausgabe der Protokolle der Ministerpräsidentenkonferenzen anlässlich der Abstimmung von Corona-Maßnahmen durch die Staatskanzlei. Die angefragte Behörde verwies dabei darauf, dass lediglich die veröffentlichten Ergebnisprotokolle in Form von Beschlüssen vorliegen würden. In diesem Zusammenhang machten wir deutlich, dass grundsätzlich alle bei einer Behörde vorhandenen Unterlagen Gegenstand einer IZG-SH Anfrage sein können und somit auch weitergehende Protokolle bzw. Notizen erfasst sein können. Dabei können sich aus § 9 oder § 10 IZG-SH Ablehnungsgründe ergeben, beispielsweise bei nachteiligen Auswirkungen auf die Vertraulichkeit der Beratungen von informationspflichtigen Stellen, die Beziehungen zum Bund oder einem anderen Land oder wenn ein überwiegendes öffentliches Interesse am Funktionieren von Verwaltungsabläufen bezüglich interner Mitteilungen oder noch nicht abgeschlossener Schriftstücke usw. besteht. Dies muss jedoch begründet werden, wobei dies jeweils mit dem öffentlichen Bekanntgabeinteresse abgewogen werden muss. In diesem Fall bekräftigte die Behörde, dass nur die Ergebnisprotokolle vorhanden seien.

4. Anonymer Antrag

Der Antrag eines Petenten wurde zunächst nicht bearbeitet, da sich dieser nur per E-Mail über Fragdenstaat.de an eine informationspflichtige Stelle gewandt hatte. Diese verlangte eine ladungsfähige Adresse.

Wir vertreten jedoch die Ansicht, dass eine anonyme Antragstellung zulässig ist, da das IZG-SH keine weiteren Vorgaben hierzu macht und es sich um ein Recht für jede Person handelt. Die Übermittlung der Antwort ist über Fragdenstaat.de möglich. Sollten Gebühren erhoben werden, kann gegebenenfalls eine andere Bewertung erfolgen. Diese Ansicht ist jedoch auch nach Urteilen von Verwaltungsgerichten in anderen Bundesländern nicht unumstritten, sodass wir die Entwicklung aufmerksam weiterverfolgen.

Was ist zu tun?

Wir unterstützen Petentinnen und Petenten bei ihren Beschwerden gegenüber informationspflichtigen Stellen und erreichen in vielen Fällen, dass zeitnah zumindest erste Teile der gewünschten Informationen zur Verfügung gestellt werden.

12.5 Vorsitz der Konferenz der Informationsbeauftragten

Am 1. Januar 2022 übernimmt das ULD turnusgemäß von Sachsen-Anhalt den **Vorsitz der Konferenz der Informationsbeauftragten in Deutschland**. Zum üblichen Programm gehört dabei, zwei Sitzung des Arbeitskreises Informationsfreiheit (AKIF) und zwei Sitzungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) zu organisieren. Wir hoffen dabei, dass diese Sitzungen im Mai, Juni, September und November in Präsenz in Schleswig-Holstein stattfinden können, bereiten aber auch alternative Möglichkeiten vor.

Daneben planen wir, Akzente bei der Weiterentwicklung des Informationsfreiheitsrechts zu setzen. Dies betrifft die aktuellen Gesetzgebungsvorhaben in den Bereichen Informationsfreiheit sowie die Tendenz zu modernen Transparenzgesetzen, erweiterten Open-Data-Ansätzen und Integrationen von anderen Informationsrechten wie im Verbraucherrecht oder auch Umweltrecht. Ein Schwerpunkt soll auf dem Thema **Informationsfreiheit „by Design“** und praktischen Umsetzungsfragen liegen.

Was ist zu tun?

Neben der Durchführung der üblichen Arbeitskreissitzungen und Konferenzen der Informationsfreiheitsbeauftragten wollen wir wichtige Akzente setzen, beispielsweise zu Informationsfreiheit „by Design“.

13

KERNPUNKTE

DATENSCHUTZAKADEMIE

Vorschau: Sommerakademie 2022

13 DATENSCHUTZAKADEMIE Schleswig-Holstein

13.1 Die DATENSCHUTZAKADEMIE

Die DATENSCHUTZAKADEMIE Schleswig-Holstein ist für die Konzeption und Organisation der **Fortbildungsveranstaltungen zu den Themenbereichen Datenschutz und Informationsfreiheit** zuständig. So wird beispielweise den behördlichen und betrieblichen Datenschutzbeauftragten nötiges Fachwissen rund um die Datenschutz-Grundverordnung vermittelt.

Das Jahr 2021 war durch Corona und den damit einhergehenden Einschränkungen durch die Maßnahmen zur Bekämpfung der Ausbreitung des Coronavirus geprägt. Im Schulungsjahr 2021 konnte die DATENSCHUTZAKADEMIE daher nur eine sehr geringe Anzahl an Fortbildungsveranstaltungen anbieten.

Die alljährlich an einem Montag im Spätsommer stattfindende Sommerakademie der DATENSCHUTZAKADEMIE konnte pandemiebedingt auch in 2021 leider nicht stattfinden. So fiel ein zweites Mal hintereinander diese große Veranstaltung aus, bei der wir in den Jahren zuvor jeweils knapp 500 Teilnehmende begrüßen durften.

Die Vorbereitungen konzentrieren sich jetzt auf das Veranstaltungsjahr 2022 (siehe Tz. 13.2).

https://www.datenschutzzentrum.de/akademie/

13.2 Sommerakademie 2022 „Informationsfreiheit by Design – und der Datenschutz?!“

Nachdem die Sommerakademie der DATENSCHUTZAKADEMIE pandemiebedingt zwei Jahre lang pausieren musste, soll sie 2022 wieder durchstarten. Expertinnen und Experten zu Informationsfreiheit und Datenschutz sowie Interessierte aus dem gesamten Bundesgebiet und darüber hinaus werden am 12. September 2022 in Kiel erwartet.

Das Öffentlichkeitsprinzip behördlicher Informationen geht schon auf das 18. Jahrhundert in Schweden zurück. In Schleswig-Holstein besteht seit 2000 für jede und jeden das Recht, Auskunft über Informationen bei öffentlichen Stellen zu verlangen, ohne dass hierfür ein gesondertes Interesse nachgewiesen werden muss. Auf Bundesebene wurde 2006 das Informationsfreiheitsgesetz eingeführt.

Im Detail gibt es Unterschiede, aber in ihrer Zielrichtung stimmen die Gesetze überein: mehr Transparenz über das Behördenhandeln und damit Nachvollziehbarkeit von Entscheidungen. Für viele Behörden war dies in der Einführungszeit eine ungewohnte Form der Transparenz, die nicht immer ohne Streit ablief. Inzwischen werden die Gesetze zu modernen Transparenzgesetzen umgestaltet, die die öffentlichen Stellen verpflichten, proaktiv Informationen in Transparenzportalen zu veröffentlichen. Hierzu gehören zunehmend die sogenannten offenen Daten (Open Data), also staatlich erhobene Messwerte und Erhebungen, die frei etwa für Forschungsvorhaben genutzt werden können.

Unter dem **Thema „Informationsfreiheit by Design – und der Datenschutz?!"** wollen wir dem aktuellen Stand nachgehen und erkunden, wo noch Reibungspunkte sind. Welche Nutzung der vorhandenen Daten ist gewollt? Muss zwischen privaten Interessen und Interessen zu Zwecken des Gemeinwohls unterschieden werden?

Manchmal stehen die informationspflichtigen Stellen vor praktischen Problemen, wenn sie versuchen, den Ansprüchen der Bürgerinnen und Bürgern nachzukommen: Beispielsweise kann aus (vermeintlich) kleinen Anträgen ein großer Aufwand bei den angefragten Stellen resultieren. Informationen müssen herausgesucht, Anhörungen durchgeführt und Abwägungen vorgenommen werden. Oft bleibt das Gefühl der Ungewissheit, ob man etwa zu wenig oder gar zu viel weitergegeben hat.

Informationsfreiheit und Datenschutz sehen viele als zwei Seiten derselben Medaille. Dennoch kann es zu Problemen kommen, wenn auch direkt oder indirekt personenbezogene Daten abgefragt werden – wie es beispielsweise bei Bauanträgen der Fall ist. Transparenzgesetze dürfen nicht zum gläsernen Bürger führen, dessen Daten sich plötzlich im Internet wiederfinden. Die Weitergabe von Namen, Adressen usw. ist in der Regel zwar ausgeschlossen, doch wie sieht es mit indirekten Informationen aus? Geodaten, besondere Merkmale oder auch vermeintlich anonymisierte Profile können in der Gesamtschau über die an verschiedenen Orten veröffentlichten Daten doch wieder einzelne Personen identifizierbar machen – und dann?

Im Rahmen der Sommerakademie sollen daher effektive Möglichkeiten der Umsetzung der gesetzlichen Vorgaben diskutiert werden. Was ist handhabbar, was ist praxistauglich – auch in Belastungssituationen wie einer weltweiten Pandemie? Welche Lösungsansätze für mehr Transparenz zeigt die Forschung zu algorithmischen Systemen auf? Wie prüft man berechtigte öffentliche und private Interessen, die einer Auskunft ganz oder teilweise entgegenstehen können, und welche technischen und organisatorischen Schutzmaßnahmen sind praktikabel? All dies wollen wir **am 12. September 2022 in Kiel** mit den Teilnehmenden an der Sommerakademie diskutieren.

Index

F

G

H

I

J

K

L

M

N

O

P

ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

Schleswig-Holsteins
Zentrum für Datenschutz
und Informationszugang

https://www.datenschutzzentrum.de/tb/