ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

TÄTIGKEITSBERICHT
2023

ULD – SCHLESWIG-HOLSTEINS ZENTRUM FÜR DATENSCHUTZ UND INFORMATIONSZUGANG

Tätigkeitsbericht 2023
des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

BERICHTSZEITRAUM: 2022

REDAKTIONSSCHLUSS: 31.12.2022

LANDTAGSDRUCKSACHE 20/620

(41. TÄTIGKEITSBERICHT DER LANDESBEAUFTRAGTEN FÜR DATENSCHUTZ –

UMFASST DEN TÄTIGKEITSBERICHT DER LANDESBEAUFTRAGTEN FÜR INFORMATIONSZUGANG)

Dr. h. c. Marit Hansen

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

Leiterin des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein

Impressum

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstraße 98

24103 Kiel

Mail: mail@datenschutzzentrum.de

Web: https://www.datenschutzzentrum.de

Satz und Lektorat: Gunna Westphal, Kiel

Umschlaggestaltung: Martin Papp, Eyekey Design, Kiel

Titelfoto: ULD, Kiel

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

Inhaltsverzeichnis

01

KERNPUNKTE

Datenschutz und Informationsfreiheit im Koalitionsvertrag

Zahlen und Fakten

Evaluierung der Datenschutzgesetze

Vorsitz der Konferenz der Informationsfreiheit „by Design“

1 Datenschutz und Informationsfreiheit

Nachdem es in den vergangenen Jahren eine hohe Anzahl von Fragen, Beschwerden und Datenschutzfällen rund um Corona gegeben hatte, ist dies im Jahr 2022 etwas zurückgegangen und andere Themen sind in den Vordergrund getreten. Das hängt sicherlich auch damit zusammen, dass die Menschen von weiteren Großkrisen betroffen sind, die von jeder und jedem Aufmerksamkeit fordern, und von Politik und Gesellschaft ein umsichtiges Handeln erwartet wird. Dennoch bleibt es dabei, dass die Verarbeitung von Daten und die Beherrschung der damit verbundenen Risiken zentral für unsere Gesellschaft ist und hier unsere Grundrechte prägend sein müssen.

Im Bereich der Digitalisierung sind in diesem Jahrzehnt wichtige Entwicklungen zu erwarten. Auf europäischer Ebene ist es ein ganzes Bündel von Rechtsakten (Tz. 2.3), die sich im Gesetzgebungsverfahren befinden oder bereits verabschiedet sind und verschiedene Aspekte von Daten und Verarbeitung betreffen, z. B. das Datengesetz (Data Act), der Daten-Governance-Rechtsakt (Data Governance Act) oder das Gesetz über künstliche Intelligenz (AI Act). Insbesondere mächtige Anwendungen der künstlichen Intelligenz wie das Programm „Chat GPT", das ganz anders als herkömmliche Suchmaschinen funktioniert und als Ausgabe nicht Links auf möglicherweise passende Ergebnisse anzeigt, sondern einen ausformulierten – aber nicht unbedingt inhaltlich korrekten – Antworttext generiert, stellen unseren Umgang mit Daten und Wissen vor Herausforderungen (Tz. 2.6).

Ähnliche Entwicklungen gibt es im Grafikbereich – die auf Knopfdruck für uns generierte Sammlung von Bildern mit Datenschutzbezug lieferte uns Inspiration für das Titelbild dieses Berichts. Auch das Zusammenwachsen von virtueller, erweiterter und physischer Realität in einem „Metaverse" und die damit verbundenen Datenverarbeitungen werden neue Fragen für Individuen und Gesellschaft aufwerfen (Tz. 2.6). Dies alles versuchen wir frühzeitig im Blick zu haben, um auf eine faire Gestaltung und, wo nötig, sinnvolle Regulierungen hinzuwirken.

Auch wenn sich diese Vorboten der kommenden Entwicklungen noch nicht in den typischen Fällen von Beschwerden, Datenpannen und Beratungen niederschlagen, gibt es aus dem Jahr 2022 genügend wichtige, interessante und manchmal auch spannende Punkte, über die ich Sie mit diesem Bericht informiere. Damit können Sie einen Einblick in die Arbeit meines Teams, den Mitarbeitenden im Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD), gewinnen. Ich wünsche Ihnen viel Spaß beim Lesen!

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

1.1 Datenschutz und Informationsfreiheit im Koalitionsvertrag

Datenschutz und Informationsfreiheit sind eng mit der Digitalisierung verwoben. Digitalisierung ist natürlich ein globales Thema, weil die technischen Entwicklungen und darauf aufbauenden Angebote von irgendwo auf der Welt stammen und auch irgendwo genutzt werden können. Der Fortschritt der Digitalisierung wirkt sich auf die Chancen und Risiken der konkreten Datenverarbeitungen auf der ganzen Welt – und auch in Schleswig-Holstein – aus. Oft gibt es unmittelbare Bezüge zu Datenschutz oder Informationsfreiheit.

Ein Bundesland wie Schleswig-Holstein ist der Digitalisierung mit ihrem grenzenlosen Charakter aber nicht ausgeliefert, sondern kann und muss eigene Entscheidungen treffen – z. B. über die Digitalisierung der Verwaltung – und mitgestalten. Die neue Regierung hat ihr Gestaltungsprogramm im Koalitionsvertrag zwischen den regierenden Parteien – CDU und BÜNDNIS 90/DIE GRÜNEN – festgelegt. Dort kann man lesen, wie die Regierungskoalition die Digitalisierung im Land gestalten will.

Der Koalitionsvertrag würdigt die Wichtigkeit eines effektiven und modernen Datenschutzes, der die Menschenwürde schützt und auch überindividuelle Risiken in den Blick nimmt. Zahlreiche Projekte werden angesprochen, die auch Datenschutzbezug haben.

Aus dem Koalitionsvertrag 2022-2027 zum Datenschutz (Seite 216):

Neben klaren rechtlichen Vorgaben bedarf es der Durchsetzung durch gut ausgestattete, unabhängige Aufsichtsstrukturen, denen auch eine wichtige Beratungsfunktion zukommt.

[...] Wir setzen uns für eine europaweit einheitliche Anwendung der DSGVO ein und werden landesrechtliche Regelungen gegebenenfalls überarbeiten. Unser Ziel ist es, bestehende Möglichkeiten der DSGVO besser zu nutzen, beispielsweise, um die datenbasierte Forschung im Gesundheitsbereich zu verbessern.

[...] Für neue datengetriebene Geschäftsmodelle brauchen wir neue Datentreuhändermodelle, Lizenzen und innovative Datenschutzlösungen durch Technik (privacy by design, privacy by default). Die Forschung für Technologien zur Anonymisierung großer Datenbestände werden wir unterstützen. Ebenso sind durchgehende Ende-zu-Ende-Verschlüsselungen und überprüfbare Open-Source-Software wichtige Bausteine, um Transparenz herzustellen, digitale Souveränität zu stärken und die informationelle Selbstbestimmung zu garantieren.

In allen genannten Bereichen verfügt das ULD mit seinem Team über eine vieljährige Expertise.

Wichtig bei diesen Themen ist, dass sie nicht zu eng, etwa als rein juristische oder rein technische Angelegenheiten, eingestuft werden. Hier ist es im Sinne von praktikablen, nachhaltigen und rechtssicheren Konzepten vonnöten, Kompetenzen verschiedener Disziplinen einfließen zu lassen.

Der Koalitionsvertrag geht zudem auf Open Data und die verstärkte Bereitstellung öffentlicher Daten ein. Hier stellen sich weitere Fragen, zu denen das Team im ULD ebenfalls sein Know-how anbieten kann: sowohl aus Datenschutz- als auch aus Informationsfreiheitssicht.

Aus dem Koalitionsvertrag 2022-2027 zu Open Data (Seite 214):

Wir starten deshalb eine Landesdatenbereitstellungs- und -nutzungsoffensive, die neben dem Aufbau eines Kompetenzzentrums für Datenmanagement, in dem wir unser Daten-Know-how bündeln wollen, einen weiteren Kern unserer künftigen Landesdatenstrategie bilden wird.

In der Verwaltung erschaffen wir eine Datenkompetenz (Data Literacy) mit einer Kultur des Datenteilens und Datennutzens. Dazu werden wir in den Ressorts die Funktion einer oder eines Datenbereitstellungsnutzungsbeauftragten einführen und das Thema Datennutzung als verpflichtende Standardfortbildung etablieren. [...]

Der Koalitionsvertrag 2022-2027 ist abrufbar unter dem folgenden Link:

https://www.cdu-sh.de/sites/www.cdu-sh.de/files/koalitionsvertrag_2022-2027_.pdf

Kurzlink: *https://uldsh.de/tb41-1-1*

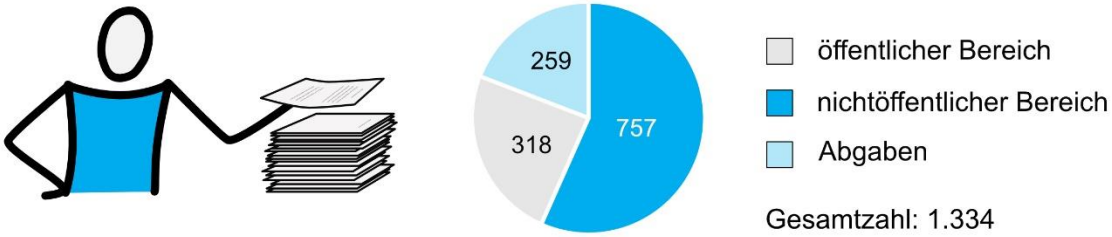
Was ist zu tun?

Sowohl in Gesetzgebungsvorhaben als auch bei der Umsetzung der Ideen des Koalitionsvertrags sowie anderen strategischen Planungen von Digitalisierungsprojekten sollte die Expertise des ULD weiterhin genutzt werden.

1.2 Zahlen und Fakten zum Jahr 2022

Im Vorjahr hatten wir berichtet, dass sich die Anzahl der Beschwerden im Großen und Ganzen eingependelt habe, aber die Datenpannenmeldungen stark gestiegen seien (40. TB, Tz. 1.2). Für das Jahr 2022 hat sich die Zahl der Beschwerden nicht weiter erhöht. Auch der Spitzenwert der Datenpannenmeldungen aus dem Jahr 2021 wurde nicht wieder erreicht. Dies liegt nach unserer Beobachtung daran, dass im Jahr 2021 zahlreiche Verantwortliche von gleichartigen Angriffen und Problemen in Bezug auf die von ihnen eingesetzte Technik betroffen waren und es daher zu Massenmeldungen in ähnlichen Konstellationen kam (40. TB, Tz. 6.3.3). Im Folgenden sind die genauen Zahlen dargestellt:

Insgesamt wurden in eigener Zuständigkeit 1.075 (Vorjahr: 1.181) Beschwerden bearbeitet, davon richteten sich **mehr als zwei Drittel der Beschwerden gegen Unternehmen** und andere nichtöffentliche Stellen (757; Vorjahr: 820), der Rest gegen Behörden (318; Vorjahr: 361). Dazu kamen 498 (Vorjahr: 712) Beratungen für den öffentlichen und den nichtöffentlichen Bereich. Die Abnahme der Zahl von Beratungen hängt insbesondere mit dem Rückgang der vielfältigen Nachfragen zur coronabezogenen Verarbeitung personenbezogener Daten zusammen, da hier die Verantwortlichen oft unsicher über die geltenden Regelungen und darüber, wie sie zu verstehen und in der eigenen Verarbeitung umzusetzen sind, waren.



Zahl der bearbeiteten Beschwerden im Jahr 2022

2022 erreichten uns 1.334 schriftliche **Beschwerden** (Vorjahr: 1.464), von denen 259 (Vorjahr: 283) nicht in unserer Zuständigkeit (öffentliche und nichtöffentliche Stellen in Schleswig-Holstein mit Ausnahme bestimmter Bereiche in Bundeszuständigkeit, z. B. Telekommunikation) lagen und an die zuständigen Behörden abgegeben werden mussten.

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

Die Zahl von 498 (Vorjahr: 649) **gemeldeten Verletzungen des Schutzes personenbezogener Daten** nach Artikel 33 DSGVO, § 41 LDSG

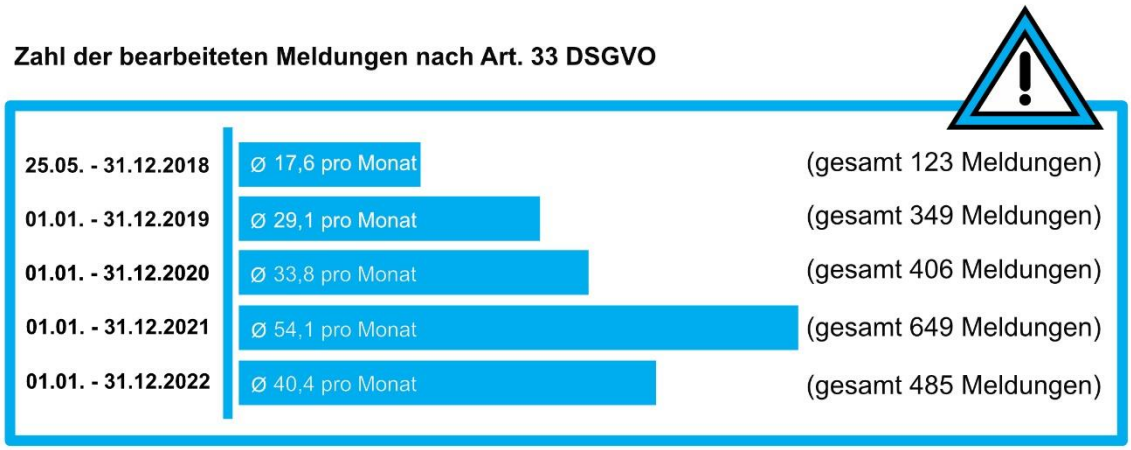
oder § 65 BDSG in Verbindung mit § 500 StPO (Datenpannen) ist im Vergleich zum Vorjahr deutlich gesunken, liegt jedoch dennoch um mehr als 20 Prozent höher als im Jahr 2020 (406), obwohl keine mit den Sicherheitsbedrohungen im Jahr 2021 vergleichbaren Massenphänomene zu verzeichnen waren.

Insgesamt ist zu merken, dass vielen Verantwortlichen ihre Pflicht zur Datenpannenmeldung bekannt ist. Dennoch gibt es eine Dunkelziffer von Datenpannen, bei denen die Verantwortlichen der Meldepflicht nicht nachgekommen sind. Manchmal erfahren wir durch Beschwerden von solchen Verletzungen des Schutzes personenbezogener Daten.

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

- 21 Warnungen (Vorjahr: 60),
- 30 Verwarnungen (Vorjahr: 51),
- eine Anordnung zur Änderung oder Einschränkung der Verarbeitung (Vorjahr: vier),
- zwei Geldbußen (Vorjahr: drei).

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



1.3 Evaluierungen der neueren Gesetze zu Datenschutz und Informationsfreiheit

Im vergangenen Tätigkeitsbericht (40. TB, Tz. 1.4) hatten wir bereits auf die **Evaluierungsklauseln in einigen Gesetzen zu Datenschutz und Informationsfreiheit** hingewiesen und von der Evaluierung zum Bundesdatenschutzgesetz im Jahr 2021 berichtet, die auf die Evaluierung der DSGVO im Jahr 2020 (39. TB, Tz. 1.4) folgte.

Evaluierungen sind nützlich, um Anpassungsbedarfe zu identifizieren und nötige oder gewünschte Änderungen umzusetzen. Ebenso wie die Gesetzgebung selbst bedarf dies einer ausreichenden Vorbereitung, einer Sorgfalt bei der Identifikation und Bewertung von etwaigen Kritikpunkten und vor allem eines Weitblicks bei der Formulierung und Diskussion der Änderungsvorschläge. Das Parlament als Gesetzgeber spielt dabei eine wichtige Rolle. Das ist zurzeit, nach der Bundestagswahl im Jahr 2021, auf Bundesebene zu merken, wo nun – im Jahr 2023 – die Frage entschieden werden muss, welche Änderungen das BDSG erfahren soll.

In diesem Zusammenhang sei auf die gemeinsame Stellungnahme der Datenschutzaufsichtsbehörden des Bundes und der Länder verwiesen,

die unter dem folgenden Link zur Verfügung steht:

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

Kurzlink: *https://uldsh.de/tb41-1-3a*

Im Abschlussbericht des Bundesministeriums des Innern und für Heimat, das für die Evaluierung zuständig war, heißt es zwar, dass „die überwiegende Zahl der Regelungen des BDSG als sachgerecht, praktikabel und normenklar angesehen werden kann". Jedoch sollen zu einigen Regelungen **Klarstellungen**, Umformulierungen oder Anpassungen **geprüft** werden.

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/tb41-1-3b*

Während das Bundesdatenschutzgesetz vereinfacht gesagt die Datenschutzregelungen für die Wirtschaft und für Bundesbehörden enthält, richtet sich das **Landesdatenschutzgesetz Schleswig-Holstein** (LDSG) an den öffentlichen Bereich im Land. Das LDSG enthält eine Pflicht zur Evaluierung, die bisher aussteht. Vor der Landtagswahl hatte zwar das Ministerium für Inneres, Ländliche Räume, Integration und Gleichstellung (MILIG) eine **Befragung** durchgeführt, mit der Einschätzungen der maßgeblichen Rechtsanwender gesammelt wurden. Die Evaluierung muss jedoch noch durchgeführt werden. Da im LDSG und BDSG einige Regelungen vollständig oder nahezu wortgleich formuliert sind, sollten dabei die Planungen auf Bundesebene für Änderungen im BDSG verfolgt werden, um zu entscheiden, inwieweit dies in ähnlicher Form in einer LDSG-Novellierung ihren Niederschlag finden soll.

Auf die Evaluationsklausel im **Informationszugangsgesetz Schleswig-Holstein** (IZG-SH) hatten wir bereits mehrfach hingewiesen (u. a. 40. TB, Tz. 1.4). Eigentlich hätte eine Evaluierung zum Jahr 2020 durchgeführt werden sollen, doch nach unserer Kenntnis gibt es dazu noch keinen Bericht, zu dem wir dann eine Stellungnahme abgeben würden.

> **§ 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.

Im Berichtsjahr wurde das IZG-SH geändert und im Zuge dessen die Regelung des § 14 IZG-SH über „Die oder der Landesbeauftragte für Informationszugang", in der unsere Aufgaben und Befugnisse festgelegt werden, neu gefasst (Tz. 12.4). Damit wurde mit einem Fehlverweis in das 2018 geänderte Landesdatenschutzgesetz aufgeräumt. Wir sind im Vorfeld zu den geplanten Änderungen angehört worden und haben eine Stellungnahme abgegeben.

Unabhängig von dieser Änderung ist gesetzlich festgelegt, die Evaluierung des IZG-SH in dieser Legislaturperiode durchzuführen. Auch für den Fall, dass die 2020er Evaluierung nicht mehr nachgeholt würde, ist zu empfehlen, frühzeitig ein Konzept für die kommende Evaluierung zu erstellen, für die im Jahr 2025 dem Landtag ein Bericht vorzulegen ist. Sollten nämlich für den Zweck der Evaluierung bestimmte Kennzahlen der Rechtsanwendenden – der öffentlichen Stellen im Land – erhoben werden, sollte sichergestellt sein, dass dies auch ohne großen Aufwand leistbar ist. Eine Erhebung von Anfragezahlen mag noch einfach sein und sich aus der Aktensystematik ergeben, aber falls im Rahmen der Evaluation Fragen zu über die Zeit verfügbaren Ressourcen, zu pro Anfrage notwendigen Aufwänden oder zu bestimmten Kategorien von Themen gestellt würden, wäre dies im Nachhinein nur sehr aufwendig ermittelbar. Wüsste eine informationspflichtige Stelle aber, welche Kennzahlen oder Kategorisierungen eine Rolle spielen sollen, könnten diese Informationen gleich im Zuge der Bearbeitung eines Antrags auf Informationszugang erhoben werden.

Geprüft werden sollte auch, inwieweit eine Orientierung an bereits stattgefundenen Evaluierungen auf Basis anderer Informationszugangs- oder Transparenzgesetze sinnvoll erscheint.

Eine weitere Aufgabe für den schleswig-holsteinischen Gesetzgeber in der aktuellen Legislaturperiode könnte die Verbesserung der bestehenden Gesetze in puncto der Übereinstimmung mit **europarechtlichen Vorgaben zum Datenschutz und zur dort eingeführten Terminologie** sein. Andernfalls besteht nämlich das Problem von Schutzlücken oder von Regelungslücken.

Ein besonderes Augenmerk ist vonnöten, wenn **Öffnungs- oder Spezifikationsklauseln der DSGVO** genutzt werden oder es sich um **Gesetzgebungsverfahren zur Umsetzung der EU-Richtlinie 2016/680 im Bereich Justiz und Inneres** handelt. Wir hatten zwar schon häufiger auf dieses Problem allgemein (40. TB, Tz. 1.4) und in unseren Stellungnahmen zu den spezifischen Gesetzgebungsverfahren hingewiesen, doch wurde dies nicht immer umgesetzt.

Um Beispiele zu nennen: Der Begriff **„Verarbeitung“** ist nunmehr zum Oberbegriff für alle Arten der Verarbeitung geworden, doch im Landesrecht wird „Verarbeitung“ teilweise noch auf derselben Ebene wie die Begriffe „Erhebung“, „Nutzung“ und „Übermittlung“ verwendet, die mittlerweile der „Verarbeitung“ untergeordnet sind. Was soll aber in diesen Fällen mit „Verarbeitung“ gemeint sein: jede Art von Verarbeitung, wie europarechtlich definiert, oder die enger definierte „Verarbeitung“, die nicht Erhebung, Nutzung und Übermittlung umfasst? Ebenfalls im Landesrecht zu finden sind Begriffe wie **„pseudonymisiert“** oder **„anonymisiert“**, die teilweise in anderen Definitionen verwendet werden, als dies nach der Datenschutzreform der Fall sein müsste.

Was ist zu tun?

Gesetzlich festgelegte Evaluierungen sind durchzuführen. In jedem Fall ist es sinnvoll, wenn Erfahrungen aus der Praxis der Rechtsanwendungen zu Verbesserungen der Gesetze beitragen können. Im Sinne der Rechtssicherheit sollten die Gesetze auf etwaige Schutzlücken und Regelungslücken überprüft werden. Die europarechtlichen Vorgaben zum Datenschutz sind auch in den Gesetzgebungsvorhaben in Schleswig-Holstein zu berücksichtigen.

1.4 2022: Vorsitz der Konferenz der Informationsfreiheitsbeauftragten

Im Berichtsjahr hatte die Landesbeauftragte für Datenschutz – oder vielmehr die **Landesbeauftragte für Informationszugang**, wie die Bezeichnung in § 14 IZG-SH lautet – den Vorsitz der Konferenz der Informationsfreiheitsbeauftragten (IFK) inne. Der Vorsitz wechselt jährlich, und da der Bund und fast alle Länder mittlerweile über ein Informationsfreiheits- oder Transparenzgesetz verfügen, kommt Schleswig-Holstein das nächste Mal vermutlich etwa im Jahr 2038 dran. Damit bot sich 2022 eine Gelegenheit, die anderen Beauftragten für Informationsfreiheit des Bundes und der Länder nach Schleswig-Holstein einzuladen und ihnen insbesondere die hiesigen Ansätze für Informationszugang und Transparenzportal sowie auch – durch eingeladene Vortragende – die Informationsfreiheitskulturen in Dänemark, Schweden und Norwegen näherzubringen (Tz. 12.1).

Wie angekündigt (40. TB, Tz. 1.5) haben wir uns im Jahr 2022 verstärkt technischen und organisatorischen Maßnahmen und Gestaltungsoptionen im Sinne der Informationsfreiheit „by Design“ gewidmet. Bei der Bearbeitung des Themas haben wir schnell gemerkt, dass es nicht nur um den Informationszugang auf Antrag, sondern auch um andere Arten der Datenherausgabe geht, die in einer grundrechtskonformen und praktikablen Art und Weise zu gestalten sind.

Aus dem Koalitionsvertrag 2022-2027 (Seite 216):

Insgesamt streben wir – gerade mit Blick auf nicht personenbeziehbare – einen besseren Zugang zu Daten an, um diese im Sinne des Gemeinwohls zu nutzen und zu ermöglichen, dass insbesondere Start-ups sowie KMU innovative digitale Anwendungen auf den Markt bringen.

Dabei ist uns klar, dass zwar organisatorische und technische Maßnahmen die Bearbeitung zu Informationsfreiheitsanträgen oder Bereitstellung von Informationen unterstützen können, aber eine vollständige Automatisierung – quasi eine überschnelle Informationsfreiheit „by Knopfdruck" ohne jegliche Prüfung von rechtlich normierten Ausschlussgründen – zu vermeiden ist. Zu diesen Ausschlussgründen gehört nicht nur das Recht auf Datenschutz, sondern es müssen auch Risiken berücksichtigt werden, wenn Geschäftsgeheimnisse oder bedeutsame Schutzgüter der öffentlichen Sicherheit betroffen sind. Doch selbst wenn menschliches Fachwissen und Risikobewusstsein weiterhin eingebracht werden müssen, kann der Aufwand für eine rechtskonforme Datenherausgabe signifikant verringert werden.

Passend zum Vorsitz der IFK haben wir im Jahr 2022 unsere Sommerakademie zum Thema „Informationsfreiheit by Design" ausgerichtet (Tz. 13).

Was ist zu tun?

Wir werden unsere Arbeiten zur Informationsfreiheit „by Design" fortsetzen und unsere Erkenntnisse auch in die Beratungs- und Schulungspraxis in Schleswig-Holstein einfließen lassen.

1.5 2023: Vorsitz der Datenschutzkonferenz

Im Jahr 2022 war die Landesbeauftragte für Datenschutz die Vorsitzende der Konferenz der Informationsfreiheitsbeauftragten (Tz. 1.4). Im Jahr 2023 ist sie nun die Vorsitzende der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, kurz: Datenschutzkonferenz oder DSK. Die Aufgabe der Datenschutzkonferenz ist es, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Dies geschieht namentlich durch Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen.

Im Jahr 2023 werden der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ebenso wie die anderen Landesbeauftragten für Datenschutz mehrfach auf unsere Einladung zu Sitzungen und Besprechungen nach Schleswig-Holstein kommen. Zusätzlich werden wir uns regelmäßig in Videokonferenzen austauschen und die aktuellen Themen besprechen. Dies dient auch der Kohärenz der Auffassungen der Datenschutzaufsichtsbehörden in Deutschland und ist zudem wichtig, um mit einer Stimme im Europäischen Datenschutzausschuss aufzutreten, dort zu einheitlichen Auslegungen der Kernkonzepte der DSGVO mitzuarbeiten und an verbindlichen Beschlüssen in Streitigkeiten über grenzüberschreitende Verarbeitungsaktivitäten mitzuwirken.

Aus dem Koalitionsvertrag 2022-2027 zum Datenschutz (Seite 216):

Auch und gerade im Sinne der Aufsichtsbehörden und ihrer öffentlichen Rezeption setzen wir uns für eine stärkere Kohärenz der Beschlüsse der Datenschutzaufsichtsbehörden auf Bundes- und Landesebene ein.

02

KERNPUNKTE

Koalitionsvertrag 2021-2025 auf Bundesebene

Die Europäische Datenstrategie

Forschungsdaten

Trends dieses Jahrzehnts

2 Datenschutz und Informationsfreiheit – global und national

Datenschutz und Informationsfreiheit sind selbstverständlich nicht nur Landesthemen, sondern werden von Entwicklungen auf nationaler, europäischer und internationaler Ebene beeinflusst. Diese Entwicklungen gilt es im Blick zu haben. Ein Ausschnitt der wichtigen Themen im Jahr 2022 wird im Folgenden vorgestellt.

2.1 Die Roadmap für Deutschland: der Koalitionsvertrag 2021-2025

Der Koalitionsvertrag auf Bundesebene stammt zwar schon aus dem Jahr 2021, doch er ist natürlich auch im Berichtsjahr relevant gewesen, um das Programm der Bundesregierung und der Koalitionspartner in Fragen von Datenschutz und Informationsfreiheit zu verstehen und dort aktiv werden zu können, wo Bezugspunkte bestehen. Während konkrete Projekte für Bundesbehörden in der Zuständigkeit des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit liegen, gibt es auch Stellen im Koalitionsvertrag, die sich auf Angelegenheiten in unserer Zuständigkeit beziehen oder anderweitig Auswirkungen auf die Bürgerinnen und Bürger in Schleswig-Holstein haben.

Besonders spannend sind für uns die Aussagen, in denen **digitale Bürgerrechte** verortet sind, beispielsweise im Abschnitt „Digitale Bürgerrechte und IT-Sicherheit“:

> **Aus dem Koalitionsvertrag 2021-2025 auf Bundesebene (Seite 16):**
>
> Wir stärken digitale Bürgerrechte und IT-Sicherheit. Sie zu gewährleisten ist staatliche Pflicht. Wir führen ein Recht auf Verschlüsselung, ein wirksames Schwachstellenmanagement, mit dem Ziel, Sicherheitslücken zu schließen, und die Vorgaben „security by design/default“ ein. Auch der Staat muss verpflichtend die Möglichkeit echter verschlüsselter Kommunikation anbieten. Hersteller haften für Schäden, die fahrlässig durch IT-Sicherheitslücken in ihren Produkten verursacht werden.

Diese Passagen klingen aus Datenschutzsicht vielversprechend. Ein Manko mag allerdings in der Tatsache liegen, dass diese Ideen in ähnlichen Worten schon im vorherigen Koalitionsvertrag 2018-2021 zwischen CDU, CSU und SPD festgelegt waren. Und auch in dem Koalitionsvertrag davor – für die Jahre 2013-2017 ebenfalls zwischen CDU, CSU und SPD – wurden sie ausgehandelt. **Seit den Snowden-Enthüllungen im Jahr 2013** (35. TB, Tz. 2.1) ist das Bewusstsein für die Wichtigkeit von vertrauenswürdiger Sicherheit für Bürgerinnen und Bürger, Unternehmen und Verwaltung in der Bundespolitik prinzipiell vorhanden, wie die Koalitionsverträge seit jenem Jahr zeigen. Bei den Konsequenzen daraus und der Umsetzung der Ankündigungen in den Koalitionsverträgen ist man **über die ersten Schritte bisher jedoch nicht hinausgekommen**. Wird sich dies nun ändern?

Aber schauen wir weiter: Auch zu Fragen der Überwachung oder zu anonymen und pseudonymen Nutzungen legt sich der Koalitionsvertrag erfreulich klar fest:

> **Aus dem Koalitionsvertrag 2021-2025 auf Bundesebene (Seite 17 f.):**
>
> Allgemeine Überwachungspflichten, Maßnahmen zum Scannen privater Kommunikation und eine Identifizierungspflicht lehnen wir ab. Anonyme und pseudonyme Online-Nutzung werden wir wahren.

Der Koalitionsvertrag betont die Gewährleistung des Rechts auf Anonymität:

Aus dem Koalitionsvertrag 2021-2025 auf Bundesebene (Seite 109):

Das Recht auf Anonymität sowohl im öffentlichen Raum als auch im Internet ist zu gewährleisten.

Außerdem werden Anonymisierungstechniken in den Blick genommen:

Aus dem Koalitionsvertrag 2021-2025 auf Bundesebene (Seite 17):

Wir fördern Anonymisierungstechniken, schaffen Rechtssicherheit durch Standards und führen die Strafbarkeit rechtswidriger Deanonymisierung ein.

In der Tat besteht hier **Bedarf an Entwicklungen und an Standards**, um den Personenbezug in Daten zu erkennen und irreversibel (oder im Fall der Pseudonymisierung: reversibel) beseitigen zu können. Die folgenden Fragen werden dabei eine wichtige Rolle spielen (siehe auch unser Policy Paper im Forum Privatheit, Tz. 8.1):

- Eine wirkliche Anonymisierung von personenbezogenen Daten geht zwangsläufig mit einem **Informationsverlust** einher. Wie lässt sich erreichen, dass die anonymisierten Daten noch die notwendigen Informationen für den jeweiligen Zweck enthalten?
- Wie soll mit der Situation umgegangen werden, dass sich ein **vermeintlich anonymisierter Datenbestand** als doch personenbezogen herausstellt? Was bedeutet dies in Bezug auf schon erfolgte oder weiterhin geplante Datennutzungen – und vor allem für die betroffenen Personen?
- Wie lässt sich das **Risiko** realistisch abschätzen, das mit der Verarbeitung der (vermeintlich?) anonymisierten Daten verbunden ist? Welche risikoeindämmenden Maßnahmen können, sollten oder müssen **vorausschauend** getroffen oder zumindest vorbereitet werden?
- Wie ließe sich eine **Strafbarkeit rechtswidriger Re-Identifizierung ohne unerwünschte Nebenwirkungen** einführen? Schließlich dürfen Verantwortliche, die die Qualität von Anonymisierung in den eigenen Verarbeitungen überprüfen, und Forschende, die gerade im Sinne der Entwicklung verbesserter Datenschutzgarantien Angriffe auf die Anonymisierung von Daten untersuchen, nicht kriminalisiert werden. Auch muss vermieden werden, dass eine solche Regelung den notwendigen Fortschritt bei Anonymisierungsmethoden konterkariert, wenn die Verantwortlichen das Unter-Strafe-Stellen einer Re-Identifizierung als ausreichenden Schutz ansähen.

Mit diesen Fragen werden auch wir uns genauer beschäftigen, u. a. im Rahmen des Projekts AnoMed (Tz. 8.5). Vorarbeiten sind bereits auf unserer Webseite zu finden (40. TB, Tz. 8.3):

https://uldsh.de/pseudoAnon

Kurzlink: *https://uldsh.de/tb41-2-1a*

Koalitionsvertrag 2021-2025:

https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf

Kurzlink: *https://uldsh.de/tb41-2-1b*

Was ist zu tun?

Die Ziele im Koalitionsvertrag zu digitalen Bürgerrechten sollten ernst genommen und vor allem auf eine sinnvolle Art und Weise in die Praxis umgesetzt werden. Dabei unterstützen wir gern.

In Bezug auf Anonymisierung ist in besonderem Maße dafür Sorge zu tragen, dass unzureichende Schnellschüsse bei Standards und der Gesetzgebung vermieden werden, damit nicht diejenigen benachteiligt werden, die eine „echte" Anonymisierung entsprechend den Anforderungen des Datenschutzrechts vornehmen.

2.2 Beschäftigtendatenschutz – jetzt aber wirklich

Im Koalitionsvertrag 2021-2025 wird es – wieder einmal – versprochen, aber derartige Anläufe gab es schon viele: **Regelungen zum Beschäftigtendatenschutz**. Im Januar 2022 hatte die beim Bundesministerium für Arbeit und Soziales zur Fortentwicklung des Beschäftigtendatenschutzes eingerichtete unabhängige und interdisziplinäre Expertenkommission Thesen und Empfehlungen vorgelegt (40. TB, Tz. 2.6). Auch die Landesbeauftragte für Datenschutz Schleswig-Holstein war vom Bundesarbeitsminister in diesen Beirat berufen worden und wirkte inhaltlich mit (39. TB, Tz. 2.4). Wir haben uns außerdem mit dem Thema des Beschäftigtendatenschutzes in einem Projekt zu „Datenschutz in digitalen Arbeitswelten" beschäftigt (Tz. 8.2).

Aus dem Koalitionsvertrag 2021-2025 auf Bundesebene (Seite 17):

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

Die Fragen des Ob und Wie eines Beschäftigtendatenschutzgesetzes konnten im Jahr 2022 auf Bundesebene noch nicht abschließend geklärt werden. So liegt auch **noch kein Gesetzentwur**f vor. In dieser Situation hat die Datenschutzkonferenz im April 2022 den Gesetzgeber aufgefordert, gesetzliche Regelungen in einem eigenständigen Beschäftigtendatenschutzgesetz zumindest für die folgenden Bereiche im Beschäftigtenkontext zu schaffen:

- Einsatz algorithmischer Systeme einschließlich künstlicher Intelligenz,
- Grenzen der Verhaltens- und Leistungskontrolle,
- Ergänzungen zu den Rahmenbedingungen der Einwilligung,
- Regelungen über Datenverarbeitungen auf Grundlage von Kollektivvereinbarungen,
- Regelungen zum Verhältnis zwischen § 22 und § 26 BDSG sowie zu Artikel 6 und 9 DSGVO,
- Beweisverwertungsverbote,
- Datenverarbeitung bei Bewerbungs- und Auswahlverfahren.

Die Datenschutzkonferenz hält die bisherige Regelung des § 26 BDSG angesichts der heutigen Entwicklungen für nicht mehr hinreichend praktikabel, normenklar und sachgerecht. Die daraus erwachsenden Interpretationsspielräume führen in der Praxis zu Unklarheiten für Arbeitgeber, Beschäftigte, Bewerberinnen und Bewerber sowie Personalvertretungen.

Thesen und Empfehlungen der Expertenkommission sind zu finden unter:

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

Kurzlink: *https://uldsh.de/tb41-2-2a*

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 2022: **„Die Zeit für ein Beschäftigtendatenschutzgesetz ist ‚Jetzt'!":**

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

Kurzlink: *https://uldsh.de/tb41-2-2b*

Was ist zu tun?

Zusammen mit den anderen Mitgliedern der Datenschutzkonferenz werden wir die Entwicklungen zur Fortentwicklung des Beschäftigtendatenschutzes begleiten. Das umfasst nicht nur die Kommentierung des erwarteten Gesetzentwurfs, sondern auch die Beschäftigung mit Problemen und fairen Lösungen in der betrieblichen oder behördlichen Praxis.

2.3 Die Europäische Datenstrategie – und der Datenschutz?

Aus der Europäischen Datenstrategie:

„Die EU schafft einen Binnenmarkt für Daten, in dem

- Daten innerhalb der EU und branchenübergreifend zum Vorteil aller weitergegeben werden können,
- europäische Vorschriften, insbesondere zum Schutz der Privatsphäre und zum Datenschutz, sowie das Wettbewerbsrecht in vollem Umfang eingehalten werden,
- die Regeln für Datenzugang und Datennutzung gerecht, praktikabel und eindeutig sind."

Der Startschuss ist längst gefallen: Die Europäische Datenstrategie setzt auf **EU-weite und branchenübergreifende Datenweitergaben** zum Nutzen von Unternehmen, Forschenden und öffentlichen Verwaltungen. Steht das nicht im Widerspruch zum Datenschutz, der doch erst vor kurzem EU-weit reformiert wurde? Sieht man sich die vorgeschlagenen Regelungen an, wird darin betont, dass selbstverständlich alle Verarbeitungen **gemäß den Vorgaben der europäischen Datenschutzanforderungen** umgesetzt werden.

Auf Anfrage der EU-Kommission vom Februar 2022 haben sich der Europäische Datenschutzausschuss (EDSA, auf Englisch: EDPB), in dem die Datenschutzaufsichtsbehörden aller EU-Mitgliedstaaten vertreten sind, zusammen mit dem Europäischen Datenschutzbeauftragten (EDSB) auf eine Rückmeldung zu dem Entwurf eines Datengesetzes (Data Act) verständigt und dies Anfang Mai 2022 als gemeinsame Stellungnahme vorgelegt. Begrüßt wird, dass der Gesetzgeber mit dem Entwurf zum Datengesetz die Datenschutzgesetzgebung im Prinzip unberührt lässt. Im Detail kann man der Stellungnahme jedoch viele Fragen und Hinweise entnehmen, wo noch Klärungsbedarf besteht – denn bei den neuen Vorschlägen zu Datenzugang und Datennutzung sollen personenbezogene Daten – selbst sensible Daten wie z. B. aus dem Gesundheitsbereich – umfasst sein. Deutlich wird bei der näheren Betrachtung, dass es essenziell sein wird, das Zusammenspiel der bereits vorhandenen und der geplanten Rechtsakte mit Bezug zu

(auch personenbezogenen) Daten zu betrachten, um die **Chancen, die Risiken und notwendigen oder empfehlenswerten Maßnahmen zur Risikobeherrschung** zu verstehen.

Da gleichzeitig an **vielen gesetzgeberischen Baustellen** gearbeitet wird, ist dies keineswegs trivial: Neben dem **Datengesetz (Data Act)**, das im Entwurf vorliegt, spielen die bereits in Kraft getretenen Gesetze wie der **Daten-Governance-Rechtsakt (Data Governance Act)**, das **Gesetz über digitale Märkte (Digital Markets Act)** und das **Gesetz über digitale Dienste (Digital Services Act)** eine Rolle für Fragen der Datennutzung; sie werden im Laufe der nächsten Monate (Ende 2023/Anfang 2024) wirksam werden. Wie mittlerweile immer, wenn es um große Datenmengen geht, werden Methoden der künstlichen Intelligenz bei der Auswertung zum Einsatz kommen, sodass zusätzlich das **Gesetz über künstliche Intelligenz (AI Act)** für die Umsetzung der Europäischen Datenstrategie Relevanz entfalten wird, das im Entwurf vorliegt und noch zwischen Kommission, Rat und Parlament verhandelt werden muss.

Ein Augenmerk der Datenschutzaufsichtsbehörden wird künftig auf den **Datenräumen** liegen, in denen europäische Daten aus Schlüsselsektoren – wie Mobilität oder Gesundheit – zusammengeführt werden. Auch die angekündigten **Maßnahmen zur Stärkung der Nutzenden**, wonach sie mit Rechten, Werkzeugen und Kompetenzen ausgestattet werden sollen, um die Kontrolle über ihre Daten zu behalten, müssen im Hinblick auf ihre Wirksamkeit und etwaige unerwünschte Nebenwirkungen untersucht werden.

Auch aus informationstechnischer Sicht – man denke an Datenschutz „by Design" – gibt es wertvolle Beiträge für ein faires und vor allem datenschutzkonformes Datenteilen. Dies war Mittelpunkt der Diskussion im Jahr 2022 in der **„Ad-Hoc Working Group on Data Protection Engineering"** der Agentur der Europäischen Union für Cybersicherheit (ENISA), an der die Landesbeauftragte für Datenschutz Schleswig-Holstein ebenso wie Vertreter von Datenschutzaufsichtsbehörden aus anderen EU-Staaten sowie Forschenden im Bereich der datenschutzgerechten Systemgestaltung mitwirkt. Der Bericht „Engineering Personal Data Sharing – Emerging Use Cases and Technologies" ist Anfang 2023 veröffentlicht worden:

https://www.enisa.europa.eu/publications/engineering-personal-data-sharing

Kurzlink: *https://uldsh.de/tb41-2-3a*

Europäischer Datenschutzbeauftragter (EDSB): Stellungnahme des EDSB zur Europäischen Datenstrategie, 16. Juni 2020:

https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_de.pdf

Kurzlink: *https://uldsh.de/tb41-2-3b*

EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), angenommen am 4. Mai 2022 (in englischer Sprache):

https://edpb.europa.eu/system/files/2022-05/edpb-edps_joint_opinion_22022_on_data_act_proposal_en.pdf

Kurzlink: *https://uldsh.de/tb41-2-3c*

Was ist zu tun?

Der Gesetzgeber ist aufgefordert, die ehrgeizige Aufgabe zur Umsetzung der Europäischen Datenstrategie im Einklang mit den europäischen Grundrechten und den Datenschutzanforderungen zu erfüllen. Dies gilt auch für die Umsetzung der europäischen Vorgaben auf nationaler Ebene. Dabei sollte der Sachverstand der Datenschutzaufsichtsbehörden einfließen.

2.4 Wissenschaftliche Forschung – selbstverständlich mit Datenschutz

Verhindert der Datenschutz die wissenschaftliche Forschung mit Daten? Natürlich nicht! Die Datenschutz-Grundverordnung sieht mit ihrem Artikel 89 sogar eine Privilegierung der Verarbeitung von personenbezogenen Daten zu wissenschaftlichen oder historischen Forschungszwecken vor. Achtung: Damit ist nicht die Auswertung personenbezogener Daten von Kundinnen und Kunden globaler Konzerne zu eigenen Geschäftszwecken gemeint!

Selbstverständlich müssen die nötigen Garantien zur Einhaltung der Datenschutzanforderungen vorhanden sein.

Art. 89 Abs. 1 Satz 1-2 DSGVO

(1) Die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken unterliegt geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung. Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird.

Die Datenschutzkonferenz hat sich im Jahr 2022 ausgiebig mit Datenschutz im Forschungsbereich beschäftigt und dazu mehrere Entschließungen verfasst. In der ersten Entschließung vom 23. März 2022 ging es um allgemeine Aspekte im Wechselspiel zwischen Forschung und Datenschutz. Dies war der Auftakt für die Arbeit der **Taskforce Forschungsdaten** (Tz. 4.5.1), die sich insbesondere mit länderübergreifenden Datenschutzfragen der Verbundforschung beschäftigt. Die Forschung in Deutschland bezieht sich in den seltensten Fällen auf ein Bundesland – und schon kann schnell die Situation entstehen, dass den Forschenden nicht mehr klar ist, welche Datenschutzregeln für welche Daten gelten und wer die zuständige Ansprechstelle ist. Ganz besonders deutlich wird dies im medizinischen Bereich angesichts der verschiedenen Landeskrankenhausgesetze (für Schleswig-Holstein siehe 39. TB, Tz. 4.5.6).

Die Datenschutzaufsichtsbehörden stehen **gesetzlichen Harmonisierungen** und der **Standardisierung von geeigneten und angemessenen Maßnahmen** zum Schutz der Rechte und Freiheiten der betroffenen Personen offen gegenüber. Die weitere Arbeit an diesen Themen wird ohnehin den europäischen Kontext berücksichtigen müssen (Tz. 2.3).

Die generellen Festlegungen der Datenschutzkonferenz können den folgenden Dokumenten entnommen werden:

Entschließung Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 23. März 2022: **„Wissenschaftliche Forschung – selbstverständlich mit Datenschutz“:**

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

Kurzlink: *https://uldsh.de/tb41-2-4a*

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 24. November 2022: **„Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung“:**

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

Kurzlink: *https://uldsh.de/tb41-2-4b*

Was ist zu tun?

Im Forschungsbereich besteht weiterhin Bedarf an einem konstruktiven Austausch zwischen Gesetzgebung, Praxis und Datenschutz. Die begonnenen Initiativen für Verbesserungen der Forschung mit Datenschutz sollen fortgesetzt werden.

2.5 Alles im Fluss – Umgang mit ständigen Veränderungen

Panta rhei (altgriechisch: πάντα ῥεῖ) – alles fließt! Diese alte Erkenntnis, die dem griechischen Philosophen Heraklit zugeschrieben wird, gilt in gewissem Sinne immer und für alle Lebenssachverhalte. Doch die Geschwindigkeit, in der sich Verarbeitungssysteme ändern, ist in der vergangenen Zeit immer höher geworden. Um im Beispiel zu bleiben: Es ist schon längst nicht mehr die Fließgeschwindigkeit eines gemächlich vor sich hin plätschernden Baches, sondern eher die eines reißenden Stromes oder gar des wirbeligen Soges eines Strudels.

Eine hohe Geschwindigkeit muss nicht schlecht sein: Schon weil immer wieder Schwachstellen in den Verarbeitungssystemen gefunden werden, soll es beim Ausbessern (Patchen) von **Sicherheitslücken** keine Verzögerungen geben. Gerade wenn es um das Treffen von Maßnahmen geht, um das IT-System gegen Angriffe zu schützen oder im Fall einer **Datenpanne** für Abmilderungen der Auswirkungen etwaiger Schäden für betroffene Personen zu sorgen, ist **Eile geboten**.

Doch auch unabhängig von diesen Fällen kommen neue Versionen der Soft- und Hardware auf den Markt, ändern sich die Vereinbarungen (wie ein Vertrag oder ein Addendum) oder werden neue Geschäftsmodelle eingeführt. Ob die **Änderungen aus Datenschutzsicht zu Verbesserungen oder zu Verschlechterungen** führen oder dieser Bereich gar nicht betroffen ist, lässt sich zumeist nicht so schnell und schon gar nicht auf einen Blick zuverlässig herausfinden – weder vom Verantwortlichen noch von den Aufsichtsbehörden.

Im Jahr 2022 wurde dies beispielsweise im **Fall der Facebook-Fanpages** deutlich: Für unseren im Jahr 2011 begonnenen Rechtsstreit erhielten wir nun endlich von der letzten gerichtlichen Instanz – dem Schleswig-Holsteinischen Oberverwaltungsgericht – die Gründe des ergangenen Urteils vom 25.11.2021 (Tz. 7.1 sowie 40. TB, Tz. 7.3). Das Urteil bezog sich auf die Gegebenheiten von 2011, sowohl was die technische Realisierung als auch die damalige Rechtslage betrifft. War das Urteil nun lediglich ein Erfolg von historischer Relevanz und womöglich nur akademischem Wert? Oder ließen sich die Urteilsgründe auch auf die heutige Situation übertragen?

Zur Klärung dieser Frage galt es, gemeinsam mit den anderen Teilnehmenden der von uns geleiteten Taskforce Facebook-Fanpages das Urteil und die Gründe genau zu analysieren und **in die Gegenwart zu übertragen** (Tz. 7.1). Die Ergebnisse stellten wir in Form eines Kurzgutachtens zur Verfügung. Doch auch dieses Kurzgutachten musste noch einmal **angepasst** werden, weil die Firma Meta (wie die vormalige Firma Facebook nun heißt) insbesondere die Vereinbarungen zum Angebot der Pages (wie die Fanpages nun heißen) und die Verarbeitung der Cookie-Daten geändert hatte.

Solche **„Moving Targets"** sind nicht die Ausnahme, sondern die Regel. Ähnliches war auch im Fall von Microsoft 365 festzustellen, als die Firma nach Veröffentlichung der über viele Monate erarbeiteten Berichte der DSK (Tz. 6.2.3) Änderungen für Europa ankündigte, die noch nicht Bestandteil der Ausarbeitungen sein konnten, aber nun in Bezug auf die datenschutzrechtlichen Auswirkungen betrachtet werden müssen. Dabei kann die Bewegung durchaus in Richtung „mehr Datenschutz" laufen, aber es gibt auch

Fälle, in denen die Veränderungen dazu führen, dass sich die Entscheidungen von Aufsichtsbehörden oder Gerichten auf einen völlig veralteten Stand beziehen und zur **Durchsetzung** einer datenschutzgerechten Verarbeitung personenbezogener Daten das **„Hase-und-Igel-Spiel"** erneut beginnt.

Veränderungen gehören zu den Punkten, die im Rahmen eines **Datenschutzmanagementsystems** beim Verantwortlichen identifiziert und bewertet werden müssen. Es wäre naiv zu glauben, dass die Datenschutzaufsichtsbehörden es leisten könnten, alle Auswirkungen aller Änderungen von allen (oder zumindest allen verbreiteten) informationstechnischen Systemen, die eine Rolle bei der Verarbeitung personenbezogener Daten spielen könnten, kurzfristig zu prüfen und zu beurteilen. In diesem Bereich müssen Regeln und Abläufe entwickelt werden, die es den Verantwortlichen erlauben, ihrer **Rechenschaftspflicht** nachzukommen. Ein wichtiger Bestandteil ist dabei die korrekte Information über Auswirkungen von Änderungen durch die Hersteller der Produkte, Dienste und Anwendungen sowie durch Dienstleister.

2.6 Trends dieses Jahrzehnts – was auf uns zukommt …

Zu unseren Aufgaben gehört es, **maßgebliche Entwicklungen** zu verfolgen, die sich auf den Schutz personenbezogener Daten auswirken.

> **Art. 57 Abs. 1 Buchst. i DSGVO**
>
> (1) Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet
>
> […]
>
> (i) maßgebliche Entwicklungen verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken; […]

Das ist eine spannende Aufgabe, bei der wir zumindest versuchen, sowohl die **Konzepte und Umsetzungen für Datenschutz „by Design" und „by Default"** als auch die **Herausforderungen und neue Risiken durch den technischen Fortschritt** oder durch Geschäftspraktiken im Blick zu haben. Je früher wir Probleme oder Lösungen antizipieren und dies in unsere Stellungnahmen und Beratungen aufnehmen können, desto größer ist der Effekt im Sinne einer grundrechtskonformen Gestaltung und Garantien für die Rechte und Freiheiten der Menschen. Aus diesem Grund soll an dieser Stelle ein kurzer Abriss über das gegeben werden, was wir in diesem Jahrzehnt erwarten.

Bei der Sammlung der folgenden Punkte zum technischen Fortschritt in diesem Jahrzehnt hat der Chatbot ChatGPT „mitgeholfen" – und wie zu erwarten war, nennt er (oder sie oder es?) die künstliche Intelligenz an erster Stelle:

- **Künstliche Intelligenz und Machine Learning:** Die KI-Technologien werden in immer mehr Verarbeitungen von Daten Einzug halten. Gerade bei der Verarbeitung von großen Datenmengen und bei dem Feststellen von Mustern ist die KI dem Menschen überlegen. Doch ob die Qualität der Ergebnisse wirklich immer weiter steigt oder sich stattdessen auch Fehler oder den Daten innewohnende Verzerrungen verfestigen, ist für viele Anwendungsbereiche offen. Auch ist zu klären, ob die aktuellen Datenschutzregeln – z. B. im Bereich der automatisierten Einzelentscheidungen – ausreichen. ChatGPT schreibt, dass die Entwicklung dazu führen könne, dass KI-Systeme komplexere Aufgaben und Prozesse automatisieren und eine höhere Genauigkeit und Zuverlässigkeit erreichen.
- **Robotik und Automatisierung:** Besonders im Bereich der Service-Roboter und der selbstfahrenden Fahrzeuge ist eine Weiterentwicklung zu erwarten, sodass sich auch die Einsatzbereiche ausweiten werden. Aus Datenschutzsicht muss besonders hingeschaut werden, welche Daten der Umgebung die Roboter und automatisierten Geräte (einschließlich der Fahrzeuge) auf welche Weise verarbeiten.

- **Internet der Dinge (IoT):** Das Internet der Dinge wird sich ebenfalls ausweiten, indem mehr Geräte und Systeme miteinander vernetzt werden und Daten in Echtzeit ausgetauscht werden. Beispiele sind Smart Homes und Smart Cities – und auch solche Verarbeitungen von Daten durch Sensoren oder Geräte im Internet gehören auf den Prüfstand der Datenschutzaufsicht, wenn ein Personenbezug gegeben ist.
- **Quantentechnologien:** Die Entwicklung im Quantencomputing und in der Quantenkommunikation wird zu Fragen in Bezug auf Informationssicherheit führen, weil die heutigen Annahmen und Einstufungen als Stand der Technik nicht mehr gelten. ChatGPT sieht optimistisch die Möglichkeit, dass die Rechenleistung und die Sicherheit erheblich verbessert werden.
- **Biotechnologie und Gentechnik:** Die Fortschritte in diesen Bereichen werden vermutlich zu neuen Möglichkeiten für die Medizin, die Landwirtschaft und die Umwelt führen, schreibt ChatGPT. Über die Risiken sagt er an dieser Stelle nichts – aber man kann den Chatbot direkt danach fragen, dann verfasst er auch zu dieser Aufgabenstellung einen Text.

Einen anderen Trend hat ChatGPT an dieser Stelle weggelassen – die **Entwicklung des „Metaverse"** oder vielleicht verschiedener Metaversen, in denen Menschen in virtuellen Welten interagieren, spielen oder arbeiten. Durch die Möglichkeiten der **„Augmented Reality"** (erweiterten Realität, z. B. mit besonderen Datenbrillen oder Datenanzügen) bleiben die Metaversen nicht auf eine reine Online-Erfahrung beschränkt. Die verschiedenen Entwicklungen der letzten Jahre könnten daher im Metaverse zusammenwachsen. Aus Datenschutzsicht stellen sich wieder viele Fragen, wenn die körperlichen und oft nicht bewusst steuerbaren Signale wie Pupillenveränderung oder Mimik von der Technik interpretiert werden und nicht nur zum Bewegen in der virtuellen Welt, sondern auch für ein **Profiling** der Interessen oder des Verhaltens ausgewertet werden. Das Geschäftsmodell der Finanzierung per individualisierter Werbung erhielte damit eine ganz neue Qualität von persönlichen Daten. Das Risiko einer Manipulation darf jedenfalls nicht auf die leichte Schulter genommen werden.

Was ChatGPT über sich selbst schreibt:

„Ich bin ChatGPT, ein KI-Modell, das von OpenAI trainiert wurde, um Texte zu generieren und Fragen zu beantworten. Ich funktioniere auf der Grundlage von maschinellem Lernen und Transformer-Netzwerken. Ich wurde mit einer großen Menge an Texten trainiert, um Trends und Muster in der Sprache zu erkennen und auf Eingaben zu reagieren. Wenn ich eine Frage erhalte, analysiere ich sie und generiere eine Antwort basierend auf den Mustern, die ich während des Trainings gelernt habe."

Schreibt das nächste Jahr ChatGPT diesen Bericht? Nein, sicherlich nicht. Der **Chatbot** ist zwar recht eloquent, aber er **nimmt es mit Fakten nicht so genau** oder argumentiert mit „erfundenen" zusätzlichen Aspekten, die mit der Aufgabenstellung oder dem Sachverhalt gar nichts zu tun haben. Als Leserin oder Leser ist es manchmal gar nicht einfach festzustellen, welche Stellen Quatsch und welche ganz brauchbar sind. Werden wir **künftig Beschwerden oder Stellungnahmen** erhalten, die mit **ChatGPT** verfasst wurden? Ja, davon müssen wir ausgehen. Wenn die Absender sich nur sprachlich haben helfen lassen und sie gewährleisten, dass die Darstellungen korrekt sind, ist daran nichts auszusetzen.

Was ist zu tun?

Politik, Gesellschaft, die Datenschutzaufsichtsbehörden und wir alle müssen die Entwicklungen mitverfolgen, möglichst verstehen, was sie für Konsequenzen haben können, und einen risikoadäquaten Umgang damit finden. Dazu kann auch gehören, dass wir rechtliche oder gesellschaftliche Regeln diskutieren und festlegen müssen.

03

KERNPUNKTE

Datenschutzgremium

Service für Abgeordnete zu Datenschutz und Informationsfreiheit

3 Landtag

Im Jahr 2022 wurde in Schleswig-Holstein ein neuer Landtag gewählt: Neue Abgeordnete kamen ins Parlament mit seinen Ausschüssen und anderen Gremien. So nahm auch das Datenschutzgremium seine Arbeit in neuer Besetzung auf, das in Schleswig-Holstein für die Belange des Datenschutzes in parlamentarischen Fragen zuständig ist (Tz. 3.1). Zusätzlich wird an dieser Stelle auf den Beratungsservice der Landesbeauftragten für Datenschutz und ihr Team für die Parlamentarier und ihre Teams hingewiesen (Tz. 3.2).

3.1 Datenschutzgremium

Die Landesbeauftragte für Datenschutz und ihre Dienststelle sind zwar für Datenschutz in Schleswig-Holstein zuständig, aber im Landesdatenschutzgesetz (LDSG) werden auch Grenzen der Zuständigkeiten aufgezeigt. Dazu gehört die Verarbeitung personenbezogener Daten, die in **Wahrnehmung parlamentarischer Aufgaben** geschieht.

> **§ 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.

Anstelle der Landesbeauftragten für Datenschutz tritt in diesbezüglichen Datenschutzfragen das **Datenschutzgremium des Schleswig-Holsteinischen Landtages**, das sich in seinen regelmäßigen Sitzungen mit Beschwerden, Hinweisen sowie aktuellen Themen beschäftigt. Mitglieder des Datenschutzgremiums sind Repräsentantinnen und Repräsentanten jeder im Landtag vertretenen Fraktion oder Gruppe. Die Landesbeauftragte für Datenschutz nimmt als Gast bei den Sitzungen teil.

Das LDSG sieht vor, dass der Landtag eine Datenschutzordnung beschließt. Die bisherige Datenschutzordnung stammt aus dem Jahr 1998, also aus der Zeit der ersten europäischen Datenschutzreform mit der Datenschutzrichtlinie 95/46/EG, und ist noch nicht vollständig an die neueren Gegebenheiten, wie sie beispielsweise in der jüngsten europäischen Datenschutzreform mit der DSGVO geformt wurden, angepasst. Somit gehört die Arbeit an der Novellierung der Datenschutzordnung zu den Aufgaben, mit denen sich das Datenschutzgremium beschäftigten wird. Die Landesbeauftragte für Datenschutz hat für die Erarbeitung ihre Unterstützung angeboten.

Webseite des Datenschutzgremiums:

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

Kurzlink: *https://uldsh.de/tb41-3-1*

3.2 Service für Abgeordnete in Fragen zu Datenschutz und Informationsfreiheit

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

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

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

§ 62 Abs. 1 Nr. 3 LDSG

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

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

Was ist zu tun?

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

04

KERNPUNKTE

Grundsteuerreform

Transparenz für Zeugen im OWi-Verfahren

Handelsregister im Internet

Pflicht von Datenschutzbeauftragten in Arztpraxen

Datenpannen im Medizinbereich

Datenschutz und Sozialarbeit

4 Datenschutz in der Verwaltung

4.1 Allgemeine Verwaltung

4.1.1 Umgang mit Solarkatastern

Mehrere Kommunen in Schleswig-Holstein veröffentlichen Solarkataster. Über deren Internetauftritte wird mittels einer Adressensuche die Auswahl eines konkreten Grundstücks ermöglicht. Die Darstellung der Dächer erfolgt für die Solarkataster in einer von vier festgelegten Farben, die das **Solarpotenzial** kennzeichnen (sehr gute, gute, mäßige, schlechte Eignung für Solaranlage). Betroffene Hauseigentümer können der farblichen Darstellung widersprechen, worauf die Kommunen in ihren Internetauftritten hinweisen. Als Rechtsgrundlage für die Veröffentlichung dienen Solarpotenzialkatastersatzungen.

Das ULD erhielt eine Anfrage, ob neben der farblichen Darstellung der Dachflächen auch die Bereitstellung einer technischen Einrichtung mit datenschutzrechtlichen Regelungen vereinbar ist, die sämtlichen Nutzerinnen und Nutzern des Solarkatasters eine Berechnung von Potenzialwerten zu bestimmten Dachflächen ermöglicht.

In der Vergangenheit hat das ULD die Veröffentlichung der farblichen Darstellungen der Dächer in den Solarkatastern nicht beanstandet. Für die Möglichkeit der Berechnung von Potenzialwerten für Solarflächen wurde allerdings eine vorherige Identifikation gefordert, um einen Datenabruf nur für berechtigte Personen (Hauseigentümer) anzubieten.

Vergleichbare Berechnungen von Potenzialwerten für die Errichtung von Solaranlagen unter Einbindung von Dienstleistern, welche die Berechnungsproramme zur Verfügung stellen, gibt es inzwischen auch in anderen Bundesländern. Über verschiedene Webauftritte sind bereits mehrere Solarkataster für ganze Bundesländer abrufbar. Brandenburg, Thüringen, Bremen, NRW und Rheinland-Pfalz ermöglichen etwa für jeden Nutzenden ohne Identifikation eine Berechnung von Potenzialwerten für beliebige Gebäude. Für jedes Gebäude können dort beliebige Parameter eingegeben werden, wie z. B. Anzahl der Personen im Hausstand, Stromverbrauch, private oder gewerbliche Nutzung für einen Schnellcheck oder Angaben zur Ermittlung eines Darlehensangebots. Hamburg veröffentlicht zu allen Gebäuden u. a. nähere Angaben zur Dachfläche, zu dem für Fotovoltaik geeigneten Flächenanteil und zum Wärme- und Stromertrag.

Unter Zugrundelegung der Vorgaben der DSGVO halten wir nunmehr sowohl die Veröffentlichung der farblich markierten Dachflächen als auch die Bereitstellung der Möglichkeit, Berechnungen von Potenzialwerten ohne vorherige Identifikation der Nutzerinnen und Nutzer vorzunehmen, für zulässig, wobei die nachfolgenden Punkte von Bedeutung sind:

- Rechtsgrundlage für die Veröffentlichung der Katasterdaten mit den Umrissen der Gebäude/Dächer ist Art. 6 Abs. 1 Buchst. e DSGVO in Verbindung mit § 3 Abs. 1 LDSG in Verbindung mit der jeweiligen Solarkatastersatzung.
- Betroffenen Personen steht ein Widerspruchsrecht gegen die farbliche Darstellung ihrer Dächer nach Art. 21 Abs. 1 DSGVO zu, worauf die Kommunen deutlich hinweisen müssen.
- Ergebnisse zur Berechnung von Potenzialwerten für Solarflächen bestimmter Dächer sind personenbezogene Daten der jeweiligen Grundstückseigentümer, soweit es sich bei letzteren um natürliche Personen handelt. Ausreichend ist die Zuordnung einer Berechnung zu einem konkreten Grundstück bzw. Dach.
- Öffentliche Stellen, welche Solarkataster veröffentlichen, sind nicht nach den Vorgaben des Art. 32 DSGVO verpflich-

tet, Nutzende vorab zu identifizieren, die für ein beliebiges Grundstück bzw. Dach eine Berechnung von Potenzialwerten für Solarflächen vornehmen lassen möchten. Maßgeblich ist dabei eine Abwägung der Kriterien gemäß Art. 32 Abs. 1 DSGVO, wobei im Ergebnis nur eine geringe Eintrittswahrscheinlichkeit und eine geringe Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen besteht und die Umstände der Verarbeitung keine andere Bewertung erfordern.

- Die Berechnung ermöglicht zwar einen tieferen Einblick in die Nutzbarkeit der Dachflächen für eine Solaranlage. Konkrete Berechnungsergebnisse sind allerdings individuell, da einzugebende Parameter nicht jedem beliebigen Nutzenden bekannt sein werden und von fremden Personen nur geschätzt werden könnten (z. B. durchschnittlicher Stromverbrauch, Einbeziehung eines Elektrofahrzeugs in die Berechnung, Auswahl der Option, eine Kreditberechnung mit weiteren Parametern durchzuführen, usw.). Die Berechnung erfolgt damit zwar zu einer konkreten Dachfläche, bildet aber nicht die für den Hauseigentümer maßgebliche Situation bzw. gewollte Planung ab, was die Sensibilität des Berechnungsergebnisses schmälert. Der Nutzerin und dem Nutzer wird ein Simulationstool bereitgestellt, um zu einer fremden Person unter Eingabe von frei wählbaren Daten ein beliebiges Berechnungsergebnis zu erstellen. Dabei entsprechen die Größen der Dächer und deren Einfärbungen häufig den Dächern vergleichbarer Gebäude in der Umgebung.
- Für die Einbindung eines Dienstleisters, welcher ein Programm zur Berechnung der Potenzialwerte bereitstellt, kommt eine Auftragsverarbeitung in Betracht. Zur Annahme der Auftragsverarbeitung ist ohne Bedeutung, dass der Auftraggeber keinen Zugang zu den Berechnungsergebnissen erhält.
- Nutzerinnen und Nutzer erheben mit Eingabe der Daten und der Erstellung des Berechnungsergebnisses personenbezogene Daten des Gebäudeeigentümers, selbst wenn diese Daten nicht die tatsächliche Situation des Eigentümers abbilden. Erfolgt durch diesen Nutzerkreis keine Weiterverarbeitung, etwa in Form der Veröffentlichung des Berechnungsergebnisses oder durch eine Verwendung der Daten für wirtschaftliche Zwecke, könnte die Ausnahmeregel nach Art. 2 Abs. 2 Buchst. c DSGVO eingreifen. Demnach würden die Nutzerin und der Nutzer die Berechnungen nur für persönliche Zwecke verarbeiten, was eine Anwendung der DSGVO ausschließt.

Unabhängig davon bliebe auch der Betrieb eines Solarkatasters zulässig, welches Berechnungen von Potenzialwerten zu bestimmten Dachflächen nur einem eingeschränkten Nutzerkreis (z. B. Hauseigentümern) ermöglicht.

Was ist zu tun?

Die Bereitstellung von Solarkatastern und Berechnungstools für Potenzialwerte bietet Hauseigentümerinnen und Hauseigentümern ein hilfreiches Informationsangebot zur Prüfung von Möglichkeiten einer umweltfreundlichen Energiegewinnung. Dabei sind die öffentlichen Stellen vor allem gehalten, die Grundlagen der Datenverarbeitung zu normieren – etwa in einer Satzung, betroffene Personen bezüglich eines Widerspruchsrechts zu informieren und im Falle der Einbindung eines technischen Dienstleisters weitere technische, organisatorische und vertragliche Vorgaben zu erfüllen.

4.1.2 Grundsteuerreform 2022 und Datenschutz

Der Bund verabschiedete ein **Gesetzespaket zur Reform der Grundsteuer**. Für den Zeitraum ab dem Kalenderjahr 2025 sind in diesem Zusammenhang neue Bemessungsgrundlagen für die Grundsteuer zu ermitteln.

Nach den Veröffentlichungen des Bundesfinanzministeriums ist eine Feststellungserklärung zur Ermittlung des Grundsteuerwerts auf den 1. Januar 2022 erforderlich, wobei folgende Angaben zu Wohngrundstücken zu erheben sind: Lage des Grundstücks, Grundstücksfläche, Bodenrichtwert, Gebäudeart, Wohnfläche und Baujahr des Gebäudes:

https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Steuern/Steuerarten/Grundsteuer-und-Grunderwerbsteuer/reform-der-grundsteuer.html

Kurzlink: *https://uldsh.de/tb41-4-1-2a*

Sind die Datenerhebungen der Finanzverwaltung rechtmäßig? Werden bei der Datenverarbeitung die Regeln der Datensicherheit eingehalten? All dies waren Fragen, die Bürgerinnen und Bürger auch an das ULD stellten.

Der Vollzug der Steuergesetze erfolgt in erster Linie durch die Länderbehörden, zu denen auch die Finanzämter zählen. Deren datenschutzrechtliche Kontrolle obliegt dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), soweit die Finanzämter personenbezogene Daten im Anwendungsbereich der Abgabenordnung (AO) verarbeiten (§ 32h Abs. 1 AO).

§ 32h Abs. 1 AO

Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nach § 8 des Bundesdatenschutzgesetzes ist zuständig für die Aufsicht über die Finanzbehörden hinsichtlich der Verarbeitung personenbezogener Daten im Anwendungsbereich dieses Gesetzes. Die §§ 13 bis 16 des Bundesdatenschutzgesetzes gelten entsprechend.

Die Beantwortung von Fragen in Bezug auf die Grundsteuererklärung obliegt dabei dem BfDI. Näheres hat das ULD unter folgendem Link veröffentlicht:

https://www.datenschutzzentrum.de/artikel/1411-Grundsteuerreform-2022-Zustaendigkeit-des-BfDI.html

Kurzlink: *https://uldsh.de/tb41-4-1-2b*

Was ist zu tun?

Bürgerinnen und Bürger können sich bei datenschutzrechtlichen Fragen in Bezug auf die Grundsteuerreform an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden.

4.1.3 Keine Verwendung privater E-Mail-Adressen für dienstliche Zwecke

Im Rahmen einer Beschwerde wurde vorgetragen, dass Mitglieder eines Gemeinderates private E-Mail-Adressen für dienstliche Zwecke verwenden würden.

In dem daraufhin eingeleiteten Verfahren ergab sich, dass die privaten E-Mail-Adressen u. a. für den Empfang von Nachrichten und Einladungen

zu Sitzungen der Ausschüsse und der Gemeindevertretung genutzt wurden. Eine Nutzung der privaten E-Mail-Adressen für den Empfang bzw. Versand von Protokollen der Sitzungen o. Ä. konnte nicht abschließend ermittelt werden, war jedoch angesichts der Gesamtumstände nicht gänzlich auszuschließen.

Das ULD legte seine rechtliche Einschätzung dar und führte dazu aus, dass personenbezogene Daten nach Art. 5 Abs. 1 Buchst. f DSGVO in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung. Ausgehend von diesem Grundsatz sind gemäß Art. 24 Abs. 1, Art. 32 Abs. 1 DSGVO die für die Rechte und Freiheiten natürlicher Personen geeigneten technischen und organisatorischen Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Auf das eingeleitete Verfahren reagierend, wurde von der Nutzung der privaten E-Mail-Adressen Abstand genommen. Zukünftig werden gesonderte, für die Arbeit eines Gemeinderats eingerichtete E-Mail-Adressen verwendet. Für den Einsatz dieser dienstlichen E-Mail-Accounts ist die Gemeinde imstande, einheitliche Sicherheitsvorgaben nicht nur zu fordern, sondern auch durchzusetzen und zu kontrollieren. Dienstliche Kommunikation, welche nicht für die Öffentlichkeit bestimmt ist, kann unter Beachtung der datenschutzrechtlichen Vorgaben dann über die dienstlichen E-Mail-Accounts erfolgen.

Was ist zu tun?

Die Nutzung privater E-Mail-Adressen durch Gemeinderäte entspricht nicht den zuvor genannten Anforderungen nach Art. 5 Abs. 1 Buchst. f DSGVO. Dies gilt vor allem dann, wenn Daten verarbeitet werden, die nicht für die Öffentlichkeit bestimmt sind. Insbesondere bestehen oftmals keine hinreichenden technisch-organisatorischen Maßnahmen, durch die sichergestellt ist, dass Dritte (z. B. Familienmitglieder) keine unbefugte Kenntnis von den personenbezogenen Daten erlangen können, die im Rahmen der E-Mail-Kommunikation verarbeitet werden.

4.1.4 Abfrage und Dokumentation des Impf- und Genesenenstatus auf Grundlage des Hausrechts?

Das ULD erhielt Anfragen und Beschwerden bezüglich des Umstandes, dass einige Behörden in Schleswig-Holstein den Zugang zu ihren Räumlichkeiten für Besucher von einer 3G-Kontrolle abhängig machen. Die Landesvorschriften zur Corona-Bekämpfung in Schleswig-Holstein enthalten keine entsprechende Kontrollobliegenheit. Die Behörden betrachteten das Hausrecht als Grundlage für die Erhebung und Speicherung von Angaben der Besucher zu deren Impf- oder Genesenenstatus im Zusammenhang mit Covid-19. Teilweise seien die Daten durch die Behörden im Rahmen der Kontrollen notiert worden oder es habe eine automatisierte Kontrolle durch Auslesen des QR-Codes aus den Bescheinigungen stattgefunden. In anderen Fällen habe die Behörde eine bloße manuelle Sichtkontrolle bezüglich mitgeführter Dokumente durchgeführt, ohne dass eine automatisierte Verarbeitung oder eine sonstige listenmäßige Erfassung erfolgte.

Bei den Angaben zum Genesenen- und Impfstatus handelt es sich um **Gesundheitsdaten**. Deren Verarbeitung darf nur auf Grundlage einer Einwilligung der betroffenen Personen oder in bestimmten gesetzlich geregelten Ausnahmefällen erfolgen. Ein hier maßgeblicher Ausnahmefall bestünde etwa dann, wenn die Erhebung

und Speicherung der Gesundheitsdaten Gegenstand einer gesetzlichen Vorschrift ist. Die hier zu prüfende Vorgabe nach Art. 9 Abs. 2 Buchst. g DSGVO („Recht eines Mitgliedstaats") wird bei isolierter Berufung auf das Hausrecht jedoch nicht erfüllt.

Art. 9 Abs. 2 Buchst. g DSGVO

Die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich.

Hinsichtlich des „Rechts eines Mitgliedstaats" ist zwar kein Parlamentsgesetz notwendig, was sich aus Erwägungsgrund 41 zur DSGVO ergibt. Allerdings müsste das Hausrecht zumindest im Kontext mit einer Befugnisnorm angewendet werden, etwa einer landesrechtlichen Bestimmung zur Corona-Bekämpfung. Unbestritten können Behörden hinsichtlich des Zutritts zu ihren Gebäuden und Räumen im Einzelfall ein Hausrecht ausüben. Möchten diese allerdings darüber hinaus Gesundheitsdaten automatisiert oder in Listen manuell erfassen, benötigen diese nach den Vorgaben der DSGVO eine klare rechtliche Regelung, welche u. a. hinreichend bestimmt den Verarbeitungszweck normiert und eine Verarbeitung der sensiblen Gesundheitsdaten legitimiert.

Eine solche rechtliche Regelung ist in Schleswig-Holstein nicht vorhanden. Das Bundesland Berlin hatte für entsprechende Kontrollen eine Vorschrift geschaffen (§ 10 Abs. 1 Satz 1 und 2 der Vierten SARS-CoV-2-Infektionsschutzmaßnahmenverordnung – für Besucherinnen und Besucher von Dienstgebäuden des Landes Berlin). Im Übrigen haben die Gesetz- und Verordnungsgeber auf Bundes- und Landesebene hinsichtlich normierter Kontrollregelungen abschließende Vorgaben entwickelt.

§ 10 Abs. 1 der Vierten Verordnung über erforderliche Maßnahmen zum Schutz der Bevölkerung vor Infektionen mit dem Coronavirus SARS-CoV-2

(1) Der Zugang zu den Dienstgebäuden des Landes Berlin ist für Besucherinnen und Besucher bzw. Kundinnen und Kunden nur unter der 3G-Bedingung möglich. Der Nachweis ist beim Betreten der jeweiligen Behörde unaufgefordert vorzulegen. Die Behörde hat die Besucherinnen und Besucher in barrierefrei zugänglicher Form über die behördlichen Zugangsregelungen zu informieren und auf Testangebote nach § 6 hinzuweisen. Die Behörde kann im Einzelfall von der Einhaltung der 3G-Bedingung absehen, sofern das Aufsuchen des Dienstgebäudes durch die Person zur Verfolgung oder Verhütung von Straftaten oder zur Abwehr einer Gefahr erforderlich ist oder zur Inanspruchnahme von Beratungsangeboten oder Stellung von Anträgen erfolgt und ansonsten eine unbillige Härte entstehen würde; in diesem Fall hat die Person eine FFP2-Maske zu tragen.

[...]

Die bloße manuelle Sichtkontrolle ohne Dokumentation/ohne beabsichtigte Dokumentation des Ergebnisses der Sichtkontrolle in einer Liste erfüllt nicht den Tatbestand einer nicht automatisierten Verarbeitung in einem Dateisystem, Art. 3 Abs. 1, 4 Nr. 6 DSGVO. Der sachliche Anwendungsbereich der DSGVO ist hingegen eröffnet, wenn die Kontrolle etwa mithilfe einer App (z. B. CovPassCheck-App) erfolgt, da dann bereits eine automatisierte Verarbeitung durchgeführt wird.

Die aktuelle Rechtsprechung zur Thematik bezieht sich überwiegend auf den Zugang von Mandatsträgern zu kommunalen Sitzungen. Dabei wird die bloße Berufung auf das Hausrecht als ausreichend betrachtet, um die Anordnung einer 3G-Kontrolle zu rechtfertigen. Eine weitere

Legitimation, etwa in einer Bestimmung zur Corona-Bekämpfung, wird teilweise als nicht erforderlich erachtet. Leider enthalten die Entscheidungen keinerlei Ausführungen zu den Bestimmungen der DSGVO. Eine auf das Hausrecht gestützte Anordnung muss aber gerade mit höherrangigem Recht und daher auch mit der DSGVO vereinbar sein.

Was ist zu tun?

Eine Sichtkontrolle ohne Dokumentation des Kontrollergebnisses im Rahmen von Stichproben bei den Besucherinnen und Besuchern erscheint noch zulässig, da insoweit die Vorgaben der DSGVO keine Anwendung finden. Hingegen bedarf jede automatisierte Erfassung oder manuelle Dokumentation von Angaben zum Impf- oder Genesenenstatus einer spezifischen Rechtsgrundlage, sodass dann allein die Berufung auf ein Hausrecht nicht ausreicht.

4.1.5 Kurabgabe – Angabe der Mieter

Dem ULD wurde mitgeteilt, dass eine kommunale Einrichtung Vermieter aufgefordert habe, personenbezogene Daten von ihren Mietern, bei denen es sich um Dauermieter handelte, zu erheben und diese der kommunalen Einrichtung zu übermitteln. Hintergrund war eine etwaige Erhebung einer Kurabgabe gegenüber den Mietern. Der betreffende Vermieter fragte das ULD, ob es zulässig sei, dass der Vermieter die personenbezogenen Daten von dem Mieter erhebe und an die Verwaltung übermittele.

Maßgebend ist, ob für diese Verarbeitung personenbezogener Daten eine Rechtsgrundlage vorliegt. Als mögliche Rechtsgrundlage kann im Einzelfall § 10 Abs. 4 des Kommunalabgabengesetzes des Landes Schleswig-Holstein (KAG) in Verbindung mit der betreffenden kommunalen Kursatzung in Betracht kommen.

Dabei sind jedoch die allgemeinen Grundsätze zur Verarbeitung personenbezogener Daten, z. B. die **Grundsätze der Erforderlichkeit und der Datensparsamkeit**, zu berücksichtigen. Ergeben sich konkrete Anhaltspunkte dafür, dass die Daten nicht auf eine Rechtsgrundlage gestützt werden können, dürfen die Daten nicht übermittelt werden.

§ 10 Abs. 4 Kommunalabgabengesetz

Kurabgabesatzungen können aus sozialen, kulturellen oder sonstigen wichtigen Gründen Ermäßigungen und die teilweise oder vollständige Befreiung für Personen oder Personengruppen von der Kurabgabepflicht vorsehen. Insbesondere kann die Anerkennung von Kurabgaben, die in anderen Gemeinden entrichtet wurden, bestimmt werden.

In dem konkreten Fall verhielt es sich so, dass sich aus der betreffenden Kurabgabensatzung ergab, dass Dauermieter nicht von dem abgabepflichtigen Personenkreis erfasst waren. Die Datenverarbeitung wäre vor diesem Hintergrund aus Sicht des ULD nicht erforderlich und daher nicht zulässig gewesen.

Was ist zu tun?

Die Verwaltung sollte gegenüber den Vermietern die konkrete Rechtsgrundlage benennen, auf die die Verarbeitung der personenbezogenen Daten gestützt werden darf. Sieht die jeweilige, datenschutzkonform ausgestaltete Kurabgabensatzung die geforderte Verarbeitung nicht vor, ist davon Abstand zu nehmen.

4.1.6 Auskunftsansprüche nach Artikel 15 DSGVO gegenüber Arbeitgebern

Im Rahmen einer Beschwerde wurde vorgetragen, dass ein nach Art. 15 Abs. 1 DSGVO gegenüber dem ehemaligen Arbeitgeber geltend gemachter Auskunftsanspruch nicht erfüllt worden sei.

> **Art. 15 Abs. 1 DSGVO**
>
> Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; […]

Der Beschwerdeführer vertrat die Auffassung, er habe einen umfassenden Anspruch gegenüber dem ehemaligen Arbeitgeber, der sämtliche personenbezogene Daten von ihm betrifft, die bei diesem noch gespeichert sind. Dies umfasse neben der E-Mail-Korrespondenz, Schriftsätzen und internen Vermerken auch Metadaten, wie etwa Protokolleinträge in informationstechnischen Systemen.

Unter Berücksichtigung der einschlägigen Rechtsprechung kam das ULD im Rahmen des daraufhin eingeleiteten Verfahrens zunächst zu der Einschätzung, dass sich der Auskunftsanspruch gemäß Art. 15 Abs. 1 DSGVO z. B. auch auf Telefonvermerke oder vertragliche Unterlagen bezieht, welche personenbezogene Daten der betroffenen Person enthalten. Nicht erfasst sind hingegen beispielsweise Unterlagen zu separaten rechtlichen Bewertungen oder Analysen.

Zum anderen war zu berücksichtigen, dass ein gegenüber dem ehemaligen Arbeitgeber geltend gemachter Auskunftsanspruch, der explizit auch jeglichen Systemeintrag und jedes digital gespeicherte Protokolldatum umfassen soll, von der Rechtsprechung vielfach u. a. aus dem Grunde abgelehnt wird, dass der damit für den Arbeitgeber verbundene Aufwand unverhältnismäßig sei und sich die Geltendmachung des Anspruchs insoweit als treuwidrig erweise. So wird beispielsweise die Ansicht vertreten, dass der Aufwand, nach personenbezogenen Daten der betroffenen Person in sämtlichen Servern, Datenbanken, Webanwendungen, E-Mail-Postfächern, Verzeichnisstrukturen, Speichermedien und diversen anderen Endgeräten des Verantwortlichen nebst aller Vorgesetzten und Kollegen zu suchen, als in einem groben Missverhältnis zum Leistungsinteresse der betroffenen Person stehend anzusehen ist.

Diese Erwägungen sind insbesondere im Hinblick auf gegebenenfalls von einem Beschwerdeführer erwähnte Mittel der Kommunikation zu prüfen. In diesem Zusammenhang kann im Einzelfall nicht nur ein erheblicher „Suchaufwand" für den Arbeitgeber bestehen, sondern vor allem aufgrund eines etwaigen Personenbezugs Dritter ein erheblicher Prüf- und Bearbeitungsaufwand (Schwärzen).

Dem Beschwerdeführer wurde mitgeteilt, dass sich das ULD dieser vielfach in der Rechtsprechung geäußerten Ansicht anschließt.

Was ist zu tun?

Soweit es um personenbezogene Daten geht, die im Kontext zu der Arbeitsleistung des (ehemaligen) Beschäftigten stehen und die bei dem (ehemaligen) Arbeitgeber gespeichert werden, unterliegen diese dann nicht dem Auskunftsanspruch, wenn damit für den (ehemaligen) Arbeitgeber ein unverhältnismäßiger Aufwand abverlangt werden würde. Der (ehemalige) Arbeitgeber hat diese Gründe im Einzelnen darzulegen.

4.1.7 Elektronische Akteneinsicht im Bußgeldverfahren

Einsicht in die Bußgeldakte wird mittlerweile häufig in elektronischer Form gewährt. Dafür wird die Akte digital für die Auskunftssuchenden in einem Akteneinsichtsportal bereitgestellt. Mit bestimmten Zugangsdaten können die berechtigten Personen dann auf die Daten zugreifen.

In einem Fall wurden wir durch eine Beschwerde darauf aufmerksam gemacht, dass die Datensicherheit bei einem solchen Verfahren der digitalen Akteneinsicht nicht ausreichend gewährleistet war. Die Zugangsdaten für die im Akteneinsichtsportal eingestellte Bußgeldakte waren dem Beschwerdeführer von der Bußgeldbehörde des Kreises per unverschlüsselter E-Mail zugeschickt worden. Für den Zugriff auf die Akte musste der Nutzende im Portal seinen Vornamen, Nachnamen und seine E-Mail-Adresse angeben. Die Richtigkeit der Angaben wurde dabei nicht überprüft. In dem der Beschwerde zugrunde liegenden Fall hat der Beschwerdeführer Fantasienamen eingegeben.

Dieses Verfahren haben wir als unzureichend bewertet. Es öffnet an mehreren Stellen Einfallstore für Zugriffe durch Unbefugte. Dies beginnt bei der **Zusendung der Zugangsdaten in einer E-Mail**. Wem die E-Mail-Adresse gehört und welche Personen Zugriff auf diese E-Mail-Adresse haben, dürfte der Behörde in der Regel nicht bekannt sein. Damit wäre es möglich, dass sich ein Dritter als Betroffener eines Ordnungswidrigkeitenverfahrens ausgibt, bei der Behörde Akteneinsicht beantragt und sich die Zugangsdaten an eine E-Mail-Adresse schicken lässt, auf die er Zugriff hat. Bei einem Versand per Post hat es die Behörde dagegen in der Hand, das Risiko einer Fehladressierung zu minimieren. Meist ist die Postanschrift ohnehin im Ordnungswidrigkeitenverfahren ermittelt worden. In Zweifelsfällen kann die Richtigkeit durch eine Auskunft aus dem Melderegister geklärt werden. Zudem kann das Schreiben direkt an den Antragsteller adressiert werden. Dadurch kann die Ordnungswidrigkeitenbehörde dem Risiko einer Öffnung durch haushaltsangehörige Personen entgegenwirken.

Eine weitere Sicherheitslücke bestand beim **Download der Akte**. Hier war es möglich, mit falschen Angaben die Daten abzurufen. Schließlich bestand ein Risiko auch auf dem Übertragungsweg der E-Mail, da die Übertragung nicht Ende-zu-Ende-verschlüsselt erfolgte.

Alle drei genannten Stellen müssen in einer Gesamtschau betrachtet werden. Wenn die Zugangsdaten an eine verifizierte Adresse verschickt werden, ist es nicht mehr zwingend erforderlich, dass vor dem eigentlichen Zugriff auf die Akte eine Identitätsprüfung erfolgt. Ist aber schon beim Versand der Zugangsdaten nicht gesichert, dass der Empfänger tatsächlich der Einsichtsberechtigte ist, wäre eine **Identitätsprüfung** beim Zugriff immerhin eine Möglichkeit, das Risiko zu verringern.

Es handelt sich dabei nicht nur um geringfügige Risiken. § 32 f Abs. 4 Satz 1 der Strafprozessordnung schreibt vor, dass bei der Einsicht in elektronische Akten durch technische und organisatorische Maßnahmen gewährleistet sein muss, dass Dritte im Rahmen der Akteneinsicht keine Kenntnis vom Akteninhalt nehmen können.

Nachdem wir den Kreis auf die Sicherheitsrisiken hingewiesen haben, hat er das Verfahren der Akteneinsicht geändert. Die Zugangsdaten werden fortan nicht mehr per E-Mail versendet, sondern per Post.

Was ist zu tun?

Personenbezogene Daten sind bei elektronischer Akteneinsicht in gleicher Weise zu schützen wie bei der Einsicht in eine Papierakte. Durch technische und organisatorische Maßnahmen muss sichergestellt werden, dass nur die berechtigten Personen Einsicht erhalten können.

4.2 Polizei und Verfassungsschutz

4.2.1 Allgemeine Entwicklungen

Die Datenverarbeitung durch die Polizei ist durch eine hohe Dynamik gekennzeichnet. Zwar waren landespolitisch im Berichtszeitraum, bedingt durch die Landtagswahl, weniger Rechtssetzungsvorhaben zu verzeichnen als in den Vorjahren. Doch ein Blick in den schleswig-holsteinischen **Koalitionsvertrag** zeigt, dass die neue Landesregierung sich für die neue Legislaturperiode viel vorgenommen hat (siehe auch Tz. 1.1). So soll der Einsatz von Bodycams durch die Polizei auch in Wohnungen ermöglicht werden. Auch die Anschaffung von Dashcams für Streifenwagen der Polizei soll geprüft werden. Zudem soll die notwendige Technik für die automatische Kennzeichenerfassung zur Verfolgung von Straftaten beschafft werden. Zur Auswertung großer Datenmengen bei der Polizei soll auch der Einsatz von künstlicher Intelligenz fortentwickelt werden.

Die größte Veränderung der polizeilichen Datenverarbeitung entsteht jedoch im Verbund der Polizeibehörden des Bundes und der Länder. Unter der Bezeichnung **„Programm P20“** wird die gesamte Datenverarbeitung der Polizei neu aufgestellt. Die Grundlage für die Datenverarbeitung soll künftig ein gemeinsames **Datenhaus** der Polizei bilden. Dort sollen alle Daten der Länder- sowie der Bundespolizeien gespeichert werden. Das Programm verfolgt dabei das Ziel der Einmalspeicherung. Jedes Datum soll im Datenhaus nur einmal gespeichert werden und für alle Behörden und Anwendungen im Rahmen der gesetzlichen Verwendungsmöglichkeiten zur Verfügung stehen. Gleichzeitig sollen die von den Polizeibehörden genutzten Systeme, wie Vorgangs- und Fallbearbeitungssysteme, vereinheitlicht werden. Hinzu kommen Basisdienste, teilweise auch mit dem Ziel einer Verbesserung des Datenschutzes oder der Datensicherheit, und einzelne Anwendungen zur Datennutzung. Ziel des Gesamtvorhabens ist es, die polizeiliche Fall- und Sachbearbeitung und somit auch Ermittlungen zu vereinfachen, Informationen schneller miteinander abgleichen, verifizieren und austauschen zu können. Die Polizei soll dadurch effizienter zusammenarbeiten und zielgerichteter agieren können.

Im Zusammenhang mit diesem Vorhaben stellen sich eine ganze Reihe datenschutzrechtlicher Fragen. Diese werden gemeinsam mit den Datenschutzbeauftragten des Bundes und weiterer Länder in einer Arbeitsgruppe behandelt. Die Arbeitsgruppe steht in einem direkten Austausch mit den Verantwortlichen für das Programm P20. Zugleich sind wir hierzu regelmäßig im direkten Kontakt mit dem Innenministerium des Landes Schleswig-Holstein.

Eine wichtige Rolle für die polizeiliche Datenverarbeitung sowie für den Bereich des Verfassungsschutzes spielt – wie schon immer – das

Bundesverfassungsgericht. Im Berichtszeitraum wurde eine Verfassungsbeschwerde gegen die Regelungen in Hessen und Hamburg zum Einsatz von **Auswertesoftware bei der Polizei** vor dem Bundesverfassungsgericht verhandelt. Die in Kürze erwartete Entscheidung wird sicherlich richtungsweisend auch für das Programm P20 sein.

In einem anderen Bereich hat das Bundesverfassungsgericht im Berichtszeitraum deutlichen Nachbesserungsbedarf aufgezeigt: Mit Urteil vom 26. April 2022 – 1 BvR 1619/17 – hat das Bundesverfassungsgericht zahlreiche Vorschriften des Bayerischen Verfassungsschutzgesetzes für unvereinbar mit dem Grundgesetz erklärt. Diese Entscheidung hat umfassenden Reformbedarf für das Bayerische Verfassungsschutzgesetz ausgelöst. Auch das **Verfassungsschutzgesetz** Schleswig-Holstein bedarf vor dem Hintergrund dieser Entscheidung einer Überprüfung. Wir begrüßen daher, dass im Koalitionsvertrag eine Reformierung des Verfassungsschutzgesetzes angekündigt ist.

Was ist zu tun?

Die genannten Vorhaben haben teilweise erhebliche Auswirkungen auf die Datenschutzrechte der Bürgerinnen und Bürger. Sowohl bei der Rechtssetzung als auch bei der Umsetzung in der Praxis sollte das ULD frühzeitig einbezogen werden.

4.2.2 Durchgeführte Prüfungen (SIS II und ATD/RED)

Die Koordinierungsgruppe des SIS II (SIS II SCG) hat beschlossen, dass die Datenschutzaufsichtsbehörden der Mitgliedstaaten eine gemeinsame Kontrolle der Personenausschreibungen zur verdeckten oder gezielten Kontrolle nach Artikel 36 des Beschlusses (EU) 2007/533/JI des Rates (SIS-II-Beschluss) vornehmen.

Die SIS II SCG ist ein Gremium, das den Schutz personenbezogener Daten im Informationssystem SIS II überwacht. Die Gruppe besteht aus Vertretern der nationalen Aufsichtsbehörden der Mitgliedstaaten sowie dem Europäischen Datenschutzbeauftragten.

Für Schleswig-Holstein hat sich das ULD an der Prüfung der polizeilichen Ausschreibungen beteiligt. Ausschreibungen nach Artikel 36 SIS-II-Beschluss werden hier zentral durch das Landeskriminalamt (LKA) eingestellt. Geprüft wurde u. a., ob die erforderlichen gerichtlichen Beschlüsse nach nationalem Recht vorhanden waren sowie ob die materiellen Voraussetzungen für eine Ausschreibung im SIS vorgelegen haben.

Was ist das Schengener Informationssystem (SIS II)?

Das SIS II ermöglicht es den zuständigen Behörden der Schengener Mitgliedstaaten, Ausschreibungen zu Personen oder Gegenständen vorzunehmen. Dazu zählen beispielsweise Einreiseverweigerungen von Personen, die den Schengenraum nicht betreten dürfen, Fahndungen nach Personen, die mittels Europäischem Haftbefehl gesucht werden, die Suche nach vermissten Personen oder die Fahndung nach verlorenen oder gestohlenen Gegenständen (z. B. Reisepässe oder Autos). Eine SIS-II-Ausschreibung beinhaltet Informationen zu einer bestimmten Person oder eines Gegenstandes sowie klare Anweisungen, was zu tun ist, wenn die Person oder der Gegenstand gefunden wird.

Zum Stichtag der Prüfung gab es nur wenige aktive Ausschreibungen. Alle geprüften Ausschreibungen waren datenschutzrechtlich nicht zu beanstanden.

Ebenfalls beim LKA wurden die **Antiterrordatei (ATD)** sowie die **Rechtsextremismusdatei (RED)** geprüft. Dabei handelt es sich um sogenannte Pflichtprüfungen. Gemäß § 10 Abs. 2 ATDG und § 11 Abs. 2 RED-G besteht für die Datenschutzaufsichtsbehörden eine Verpflichtung zur regelmäßigen Prüfung der jeweiligen Dateien in bestimmten Abständen.

Im Vorwege wurde eine Stichprobe festgelegt. Sie bestand aus 34 Personendatensätzen in der ATD sowie 67 Personendatensätzen in der RED. Die geprüften Personendatensätze waren datenschutzrechtlich nicht zu beanstanden. In einem Fall konnte im Rahmen der Vor-Ort-Prüfung zunächst nicht geklärt werden, ob der korrekte Speichergrund angegeben war. Die Speicherung wäre aber auch aus einem anderen Grund rechtmäßig gewesen. Nach LKA-interner Prüfung wurde der Speichergrund dann tatsächlich korrigiert.

Was sind die Antiterrordatei (ATD) und die Rechtsextremismusdatei (RED)?

Als Verbunddateien sind die ATD wie die RED bundesweit nutzbare Datenbestände, in denen Erkenntnisse von Polizei und Nachrichtendiensten zur Terrorismusbekämpfung bzw. zur Bekämpfung des gewaltbereiten Rechtsextremismus zusammengeführt werden. Gespeichert werden bestimmte Informationen zu Ziel- und Randpersonen (mutmaßlichen Unterstützern, Kontaktpersonen usw.) aus dem Bereich des internationalen Terrorismus (ATD) bzw. des Rechtsextremismus (RED).

4.2.3 Transparenz für Zeugen im Ordnungswidrigkeitenverfahren

Im Berichtszeitraum ging eine Beschwerde gegen eine Verkehrsordnungswidrigkeitenbehörde ein. Der Beschwerdeführer hatte ein wiederholt falsch parkendes Fahrzeug der zuständigen Ordnungsbehörde über eine App gemeldet. Im Rahmen des OWi-Verfahrens wurde dem Fahrzeughalter der Name des Beschwerdeführers als Zeuge mitgeteilt. Der Beschwerdeführer sah in der Übermittlung seiner personenbezogenen Daten an den Fahrzeughalter einen Verstoß gegen datenschutzrechtliche Vorschriften. Insbesondere sei er vorab weder über die geplante Weitergabe informiert worden, noch habe man seine Erlaubnis eingeholt.

Für das OWi-Verfahren finden die Regelungen des Gesetzes über Ordnungswidrigkeiten (OWiG) sowie sinngemäß die der Strafprozessordnung (StPO) Anwendung. Danach sind dem Empfänger eines Bußgeldbescheides die Beweismittel zu benennen. Dazu gehört auch die Benennung von Zeugen (in diesem Fall der Anzeigende). Der Empfänger des Bußgeldbescheides soll die Beweiskraft des gegen ihn erhobenen Vorwurfs überprüfen können und in der Lage sein, die Erfolgsaussichten eines Einspruchs gegen den Bußgeldbescheid einzuschätzen.

Die Erforderlichkeit beachten!

Anzeigende oder Hinweisgeber dürfen nur als Zeugen im Bußgeldverfahren benannt werden, wenn dies erforderlich ist, um das Verfahren rechtssicher abzuschließen. Entsendet eine Behörde aufgrund eines Hinweises beispielsweise eigenes Personal, das dann vor Ort selbst Zeuge des Verstoßes wird, so ist die Benennung des ursprünglichen Hinweisgebers als Zeuge in der Regel nicht mehr erforderlich und damit unzulässig.

Dies ist seit Jahrzehnten gelebte Praxis und auch gerichtlich so bestätigt. Vielen Anzeigenden ist dies jedoch nicht bewusst – so auch im vorliegenden Fall. Und die Zahl betroffener Anzeigender nimmt zu. Zum einen ist es heute viel einfacher, eine Ordnungswidrigkeit anzuzeigen, da

viele ein Smartphone besitzen und entsprechende Apps die Übersendung an die Ordnungsbehörde/Polizei übernehmen. Zum anderen hat die mediale Aufmerksamkeit der DSGVO dazu geführt, dass viele Bürgerinnen und Bürger sich an die Bekanntmachungs- und Informationspflichten der DSGVO gewöhnt haben und – irrtümlicherweise – davon ausgehen, dass diese auch bei einer OWi-Anzeige zur Anwendung kommen. Über die (stillschweigende) Weitergabe ihrer Daten an die angezeigte Person sind viele Anzeigende deshalb überrascht.

Mit der Umsetzung der *„EU-Richtlinie 2016/680 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr"* in nationales Recht sind jedoch auch im Bereich der Gefahrenabwehr und Strafverfolgung (einschließlich der Verfolgung von Ordnungswidrigkeiten) erweiterte Transparenzvorschriften erlassen worden. Für das OWi-Verfahren gelten damit neben dem OWiG und der StPO die Regelungen des dritten Teils des Landesdatenschutzgesetzes (LDSG). Bezüglich der Transparenz im OWi-Verfahren sind u. a. **§ 22 Nr. 1 LDSG und § 31 LDSG** zu beachten.

Nach dem Grundsatz aus **§ 22 Nr. 1 LDSG** müssen personenbezogene Daten *„auf rechtmäßige Weise und nach Treu und Glauben"* verarbeitet werden. Dies bedeutet, dass die Datenverarbeitung für die betroffenen Personen grundsätzlich nachvollziehbar und im Allgemeinen erwartbar sein sollte (Grundsatz der Transparenz).

§ 31 LDSG regelt im Sinne dieses Grundsatzes, welche Informationen zur Datenverarbeitung bekannt zu geben sind. Während nach der DSGVO solche Informationen dem einzelnen Betroffenen im Hinblick auf die konkrete Datenverarbeitung mitzuteilen sind, reicht es nach **§ 31 LDSG** aus, dass der Verantwortliche Informationen zur Datenverarbeitung *„in allgemeiner Form und für jedermann zugänglich"* zur Verfügung stellt. In der Regel kann dem durch eine Veröffentlichung auf der Homepage entsprochen werden. Zu den Informationen nach **§ 31 LDSG** gehört es u. a., die *„Zwecke"* zu benennen, zu denen personenbezogenen Daten verarbeitet werden.

Es wäre durchaus möglich und damit auch geboten, auf allgemeine Weise und für jedermann zugänglich darauf hinzuweisen, für welche Zwecke die personenbezogenen Daten von Anzeigenden verwendet werden.

Im vorliegenden Fall hat der verantwortliche Kreis auf seiner Homepage allgemeine Informationen zum Datenschutz veröffentlicht. Diese Informationen sind sogar einzeln für jeden Aufgabenbereich der Kreisverwaltung abrufbar. Darunter findet man auch den Bereich der „allgemeinen Ordnungswidrigkeiten". Leider sind diese Informationen nicht leicht zu finden, selbst wenn man danach sucht. Außerdem verweisen die Datenschutzhinweise in Bezug auf Ordnungswidrigkeiten nicht auf **§ 31 LDSG**, sondern fälschlicherweise auf die DSGVO. Des Weiteren beziehen sich die Angaben nur auf die Verarbeitung der personenbezogenen Daten der Betroffenen des OWi-Verfahrens. Auf die Verarbeitung der Daten von Anzeigenden, Hinweisgebern oder Zeugen wird nicht eingegangen.

Dies ist leider kein Einzelfall. Bisher hat kaum eine Ordnungs- oder Sicherheitsbehörde Informationen nach **§ 31 LDSG** veröffentlicht, und wenn doch, liegt der Schwerpunkt auf der Verarbeitung der personenbezogenen Daten der Betroffenen des OWi-Verfahrens. Meist muss man lange suchen, um überhaupt Informationen zu finden. Für Anzeigende, Hinweisgeber oder Zeugen bleiben die Zwecke, für die ihre Daten verarbeitet werden, damit intransparent und kaum nachvollziehbar.

Was ist zu tun?

Behörden, die personenbezogene Daten nach dem dritten Abschnitt des LDSG verarbeiten, sollten prüfen, ob sie ihrer Transparenzpflicht nach § 31 LDSG nachkommen. Dies schließt den Umgang mit den Daten von Anzeigenden und Hinweisgebern ein. Außerdem sollten diese Informationen leicht zugänglich und schnell auffindbar sein.

4.3 Justiz

4.3.1 Handelsregister im Internet

In den Handelsregistereinträgen zu Unternehmen befindet sich regelmäßig auch eine Vielzahl personenbezogener Daten. Dazu gehören Angaben über Geschäftsführer oder Gesellschafter von Unternehmen, private Wohnanschriften, Unterschriften oder Personalausweiskopien. Teilweise ist die Angabe dieser Daten im Handelsregister gesetzlich vorgeschrieben. Teilweise geht der tatsächliche Inhalt der Handelsregister über das gesetzlich Geforderte hinaus.

Das Handelsregister war immer schon öffentlich. Die Publizität des Handelsregisters soll Vertrauen im Rechtsverkehr schaffen. Seit 2007 wird das Handelsregister in elektronischer Form geführt und ist über das gemeinsame Justizportal der Länder abrufbar. Bislang waren die Abrufe jedoch kostenpflichtig und nur registrierten Nutzerinnen und Nutzern möglich.

Mit Inkrafttreten des Gesetzes zur Umsetzung der **Digitalisierungsrichtlinie** zum 1. August 2022 ist der Abruf der Registerinhalte sowie der durch die Registergerichte eingestellten Dokumente kostenfrei und ohne Registrierung möglich. Diese Gesetzesänderung hat der Bundesgesetzgeber vorgenommen, um die EU-Digitalisierungsrichtlinie umzusetzen.

Faktisch führt der Wegfall der Zugangsbeschränkungen zum Handelsregister dazu, dass sich die Reichweite der abrufbaren Daten bzw. die Zahl der Personen, die auf das Portal zugreift, deutlich erhöht. Gleichzeitig ist unter den betroffenen Personen, die im Handelsregister eingetragen sind, eine große Besorgnis vor einem Missbrauch ihrer Daten entstanden. Dies hat sich in vielen Beschwerden gezeigt, die uns im Berichtszeitraum erreicht haben. Die Sorge ist nicht unberechtigt, und der öffentlichen Berichterstattung ist zu entnehmen, dass auf Bundesebene an verschiedenen Stellen bereits an Änderungen gearbeitet wird, um die Risiken für die betroffenen Personen wieder zu minimieren.

Für die Eintragungen im Handelsregister sind die Registergerichte verantwortlich. Die Eintragungen beruhen auf Dokumenten wie z. B. Gesellschaftsverträgen. Letztere werden meist von den beurkundenden Notaren zum Handelsregister eingereicht. Das Registergericht stellt die eingereichten Dokumente zum Abruf im Handelsregister bereit. Oftmals enthalten solche Dokumente mehr Informationen als die im Gesetz vorgesehenen Pflichtangaben für das Handelsregister.

Um in zukünftigen Fällen die Veröffentlichung von nicht eintragungspflichtigen personenbezogenen Daten zu vermeiden, sollten Notarinnen und Notare daher bereits bei der Erstellung, spätestens bei der Einreichung von Dokumenten zum Handelsregister darauf achten, dass sie nur die notwendigen Daten enthalten. Hierfür können auch geschwärzte Dokumente beim Handelsregister eingereicht werden.

Sind überschüssige personenbezogene Daten bereits im Handelsregister eingetragen, haben die betroffenen Personen nach der Datenschutz-

Grundverordnung grundsätzlich einen Anspruch auf Löschung. Ein solcher Anspruch kommt für die nicht eintragungspflichtigen personenbezogenen Daten in Betracht. Der Anspruch ist gegenüber dem jeweils zuständigen Registergericht geltend zu machen.

Praktisch umgesetzt werden kann der Löschungsanspruch in der Weise, dass die ursprünglichen Dokumente für die Veröffentlichung durch geschwärzte Dokumente ersetzt werden. Die geschwärzten Dokumente müssten von den betroffenen Personen neu beim Registergericht eingereicht werden.

Dieses Verfahren ist seit Ende des Jahres 2022 in § 9 Abs. 7 der Handelsregisterverordnung (HRV) vorgesehen.

In der Begründung zur Änderung der HRV wird dazu folgende Erläuterung gegeben:

BR-Drucksache 560/22, Seite 29:

„Einmal in den Registerordner eingestellte Dokumente können im Sinne der Registerwahrheit grundsätzlich nicht verändert oder ausgetauscht werden. In Ausnahmefällen kann jedoch von diesem Grundsatz abgewichen werden. Dies soll durch den neuen Absatz 7 klargestellt werden. Sind beispielsweise in dem ursprünglich eingereichten Dokument teilweise Angaben enthalten, die nicht in den Registerordner gehören, muss die Möglichkeit bestehen, dieses Dokument nicht mehr zu beauskunften. In diesem Fall ist ein neu eingereichtes Dokument in den Registerordner einzustellen, welches lediglich die für den Rechtsverkehr erforderlichen Angaben enthält."

4.4 Soziales

4.4.1 Nur eine Datenpanne? Bei Fehlverhalten droht Beschäftigten ein Bußgeld!

Wiederholt schilderten im letzten Jahr Jobcenter, dass Mitarbeiterinnen und Mitarbeiter zu privaten Zwecken auf **Kundendaten (Sozialdaten)** in den zentralen Systemen der **Bundesagentur für Arbeit (BA)** zugegriffen haben, ohne dass hierfür ein dienstliches Erfordernis bestanden habe. Mal wollte ein Beschäftigter etwas über die Ex-Frau erfahren, ein anderes Mal herausfinden, ob eine attraktive Antragstellerin als neue Partnerin infrage kommt. Die Neugier war größer als die Angst vor dem Verbot. Dieses Fehlverhalten der Beschäftigten wird als Mitarbeiterexzess bezeichnet.

Keine Frage, solche privaten Recherchen stellen einen **gravierenden Verstoß gegen das Sozialgeheimnis** und eine Datenschutzverletzung dar. Zuständige Aufsichtsbehörde für die Datenpannenmeldungen ist in diesen Fällen der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Das Jobcenter muss darlegen, welche technischen und organisatorischen Maßnahmen getroffen wurden, um derartige unbefugte Zugriffe zu verhindern.

Aber auch den Beschäftigten, die gegen das Sozialgeheimnis verstoßen, drohen Konsequenzen – in manchen Fällen sogar die Kündigung. Damit aber nicht genug. Die Beschäftigten müssen zudem mit einem hohen Bußgeld rechnen. Als zuständige Behörde prüfen wir bei entsprechenden Hinweisen der Jobcenter die Einleitung eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten.

Was ist zu tun?

Sozialleistungsträger dürfen nicht alleine darauf vertrauen, dass Mitarbeiterinnen und Mitarbeiter ausschließlich auf Sozialdaten zugreifen, wenn dies dienstlich erforderlich ist. Neben organisatorischen Vorgaben müssen auch technische Vorkehrungen getroffen werden, damit Beschäftigte gar nicht die Möglichkeit haben, auf Sozialdaten zuzugreifen, die sie nichts angehen. Besonders wichtig sind das Rollen- und Berechtigungskonzept und regelmäßige Kontrollen der zu protokollierenden Zugriffe. Beschäftigte müssen geschult und auf die Konsequenzen von Fehlverhalten hingewiesen werden.

4.4.2 Hackerangriff in einer Jugendhilfeeinrichtung

Hacker machen vor niemandem halt. Auch nicht vor Jugendhilfeeinrichtungen. In diesem Fall verschlüsselten die Hacker mit einer Malware eine Netzwerkfestplatte. Die Einrichtung konnte nicht mehr auf die Daten ihrer Mitarbeitenden und auf die besonders sensiblen Daten der betreuten Jugendlichen und deren Familien zugreifen. Über 160 Personen waren betroffen.

Ärgerlich war, dass der Infektionsweg nicht ermittelt werden konnte. So konnte man nur vermuten, wie die Hacker auf die IT zugreifen konnten. Vielleicht hing es damit zusammen, dass Beschäftigten im Homeoffice der direkte Zugriff auf das System ermöglicht wurde?

Zudem konnte nicht mit Sicherheit ausgeschlossen werden, dass die Hacker die Daten nur verschlüsselten oder womöglich sogar kopierten. Die Einrichtung ging auf Nummer sicher und meldete uns diese Datenschutzverletzung.

4.4.3 Datenschutz bei der „Arztsuche“ der KVSH verbessert

Die Kassenärztliche Vereinigung Schleswig-Holstein (KVSH) bietet auf ihrer Homepage für Patienten die Möglichkeit einer „Arztsuche“ an. Wer den Namen einer Ärztin oder eines Arztes in die Suchmaske eingibt, dem wird die aktuelle Anschrift der Praxis angezeigt. Bei einer Eingabe eines Ortes werden die in diesem Ort tätigen Ärztinnen und Ärzte sowie Psychotherapeutinnen und Psychotherapeuten angezeigt.

Bei der Nutzung dieser Suchfunktion erfolgte bislang eine automatisierte Einbindung von Google Maps. Bei einem Suchergebnis wurde automatisch eine Karte von Google Maps mit dem Standort der Praxis eingeblendet. Um diesen Service zu ermöglichen, wurden zumindest die IP-Adressen der Nutzenden automatisiert und ohne Einflussmöglichkeit der Patientinnen und Patienten an die Firma **Google** übertragen. Eine Befugnis für diese Datenübermittlung war nicht zu erkennen.

Unsere Nachfrage nahm die KVSH sofort zum Anlass, die „arztsuche.kvsh.de“ neu aufzusetzen. Zukünftig werden Patientinnen und Patienten gefragt, ob eine Google-Karte angezeigt werden soll, verbunden mit dem Hinweis, dass bei Zustimmung Daten an Google übermittelt werden. Die Suchergebnisse, also die Praxisnamen und -anschriften, können zukünftig aber auch ohne die Google-Karte angezeigt werden.

Was ist zu tun?

Wenn externe Dienste von Anbietern wie Google in das Informationsangebot einer Homepage eingebunden werden, muss die verantwortliche Stelle prüfen, ob, in welchem Umfang und mit welcher Befugnis personenbezogene oder personenbeziehbare Daten an diesen externen Dienstleister übermittelt werden. Für die Übermittlung dieser Daten wird immer eine Befugnis, z. B. die Einwilligung der Betroffenen, benötigt.

4.5 Schutz des Patientengeheimnisses

4.5.1 Taskforce Forschungsdaten – Sachstand

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat im November 2021 die Taskforce Forschungsdaten unter der gemeinsamen Leitung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit eingerichtet. Das Arbeitsgremium soll als **einheitlicher Ansprechpartner für die Technologie- und Methodenplattform für die vernetzte medizinische Forschung (TMF)** dienen und sich mit länderübergreifenden Datenschutzfragen der Verbundforschung befassen. Das ULD ist Mitglied der Taskforce Forschungsdaten und beteiligt sich an den maßgeblichen Erörterungen.

Im Jahr 2022 nahm die Taskforce Forschungsdaten ihre Arbeit auf. Dabei sind insbesondere folgende Themen Gegenstand der Erörterung:

- aktuelle Entwicklungen zu Gesetzgebungsverfahren,
- Verarbeitung personenbezogener Daten im Rahmen von Forschungsprojekten,
- Fragen zu Einwilligungslösungen,
- Anonymisierung von personenbezogenen Daten,
- Erarbeitung von Veröffentlichungen der DSK.

Zuletzt erbrachte die Taskforce Forschungsdaten Vorarbeiten für die **Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung**. Die Petersberger Erklärung skizziert das Spannungsverhältnis, einerseits die Verarbeitung von Gesundheitsdaten zu im öffentlichen Interesse liegenden wissenschaftlichen Forschungszwecken zu ermöglichen und ihre Vorzüge nutzbar zu machen. Andererseits ist den damit verbundenen Risiken für die allgemeinen Persönlichkeitsrechte konsequent zu begegnen, um den betroffenen Personen einen angemessenen Grundrechtsschutz zu gewähren.

Die entsprechende Entschließung der DSK beinhaltet Empfehlungen für den Gesetzgeber und Forschungsstellen, welche auf den bestehenden Gesetzgebungsbedarf und Handlungspflichten von Verantwortlichen bei der Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung eingehen.

Die Petersberger Erklärung ist unter folgendem Link abrufbar:

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

Kurzlink: *https://uldsh.de/tb41-4-5-1*

4.5.2 Pflicht zur Benennung von Datenschutzbeauftragten in Arztpraxen

Wann muss in einer Arztpraxis eine Datenschutzbeauftragte bzw. ein Datenschutzbeauftragter benannt werden?

Die Pflicht zur Benennung einer bzw. eines Datenschutzbeauftragten besteht immer dann, wenn entweder in der Regel **mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder eine umfangreiche Verarbeitung besonderer Kategorien von Daten (Gesundheitsdaten) erfolgt**. Nur wann ist eine Verarbeitung von Patientendaten umfangreich? Dies hat der Gesetzgeber nicht abschließend definiert.

In dem Erwägungsgrund 91 zur DSGVO findet sich der Hinweis, dass, wenn die Datenverarbeitung durch eine einzelne Ärztin oder einen einzelnen Arzt erfolgt, davon ausgegangen werden kann, dass keine umfangreiche Verarbeitung von Patientendaten erfolgt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu ergänzend in einem Beschluss vom 26.04.2018 ausgeführt, dass von einer umfangreichen Verarbeitung von Patientendaten ausgegangen werden kann, wenn hiermit in der Arztpraxis mindestens zehn Personen beschäftigt sind.

Wir haben diese Fragestellung anlässlich unserer Sommerakademie 2022 in einem Workshop mit Ärzten, anderen Aufsichtsbehörden und weiteren Fachleuten diskutiert und vertreten folgende Einschätzung:

- Sind in einer Arztpraxis mindestens 20 Personen mit der Verarbeitung von personenbezogenen Daten von Patientinnen und Patienten und/oder Beschäftigten beschäftigt, muss eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter benannt werden.
- Sind in einer Arztpraxis zwischen 10 und 19 Personen mit der Verarbeitung von Patientendaten beschäftigt, muss von der jeweiligen Arztpraxis geprüft und entschieden werden, ob die Verarbeitung umfangreich ist. Hierbei ist u. a. die Anzahl der Patientenfälle sowie der Inhalt und der Umfang der Patientenunterlagen (auch von bereits abgeschlossenen bzw. archivierten Patientenfällen) einzubeziehen. Diese Prüfung und Entscheidung sind von der Arztpraxis zu dokumentieren.
- Sind in einer Arztpraxis weniger als zehn Personen mit der Verarbeitung von Patientendaten beschäftigt, besteht nicht pauschal eine Pflicht zur Benennung einer bzw. eines Datenschutzbeauftragten. Aber auch in diesen Fällen ist zu prüfen, ob nicht gleichwohl eine umfangreiche Verarbeitung von Patientendaten erfolgt.

Unabhängig davon haben wir für jede Arztpraxis folgenden Rat: Das **Patientengeheimnis** ist für jede einzelne Patientin bzw. jeden einzelnen Patienten zu gewährleisten. Eine Datenschutzbeauftragte bzw. ein Datenschutzbeauftragter hilft dabei, die Verarbeitung von Patientendaten rechtmäßig und sicher zu gestalten, und das bereits ab der ersten Patientenakte. Warum sollte man also auf diese Hilfe verzichten?

Was ist zu tun?

Jede Arztpraxis muss als verantwortliche Stelle prüfen und entscheiden, ob sie die Voraussetzungen für die Pflicht zur Benennung einer Datenschutzbeauftragten bzw. eines Datenschutzbeauftragten erfüllt. Arztpraxen, die keine Datenschutzbeauftragte bzw. keinen Datenschutzbeauftragten benennen, müssen gleichwohl die Anforderungen des Datenschutzes und der ärztlichen Schweigepflicht beachten.

4.5.3 Artikel 15 DSGVO kontra § 630g BGB – ist eine Patientenauskunft kostenpflichtig?

Patientinnen und Patienten haben den Anspruch, von ihren Ärzten eine Kopie der Patientenakte zu bekommen. Aber müssen sie dafür auch bezahlen? Wir sagen weiterhin Nein! Nicht für die erste Kopie.

Gemäß § 630g Abs. 2 Satz 2 Bürgerliches Gesetzbuch (BGB) und § 10 Abs. 2 Satz 2 der Berufsordnung der Ärztekammer Schleswig-Holstein können Ärztinnen und Ärzte von den Patientinnen und Patienten die Erstattung der für die Anfertigung von Kopien entstandenen Kosten verlangen. Hingegen sieht Art. 15 Abs. 3 DSGVO vor, dass Verantwortliche, zu denen auch die Arztpraxen, Krankenhäuser usw. gehören, die erste Kopie kostenfrei aushändigen müssen. Was gilt?

In unserem 39. Tätigkeitsbericht (Tz. 4.5.3) haben wir darauf hingewiesen, dass nach unserer Einschätzung die (erste) Auskunft kostenfrei zu erteilen ist, wenn betroffene Personen ihr Auskunftsersuchen auf Artikel 15 DSGVO stützen, und auf ein entsprechendes Urteil des Landgerichtes Dresden hingewiesen. Nun hat sich auch der Bundesgerichtshof (BGH) mit der Frage beschäftigt, wie Artikel 15 DSGVO auszulegen ist. Das Verfahren wurde jedoch ausgesetzt und mit Beschluss vom 29.03.2022 (VI ZR 1352/20) dem Europäischen Gerichtshof (EuGH) zur Vorabentscheidung vorgelegt. Die Antwort aus Brüssel steht noch aus. So viel sei aber schon verraten, dem Beschluss des BGH ist nicht zu entnehmen, dass der BGH eine andere Einschätzung vertritt als wir. Das lässt darauf hoffen, dass auch der EuGH die Rechte der Patientinnen und Patienten stärken wird.

Was ist zu tun?

Weiterhin gilt, dass Patientinnen und Patienten in Schleswig-Holstein die erste Kopie der Patientenunterlagen kostenfrei zu überlassen ist, wenn das Auskunftsersuchen auf Artikel 15 DSGVO gestützt wird.

4.6 Datenpannen im Medizinbereich

4.6.1 Wenn das Auto aufgebrochen wird …

Nicht nur in Büroräume wird eingebrochen. Im letzten Jahr wurden uns wiederholt Autoaufbrüche und der **Diebstahl von Unterlagen mit sensibelsten Klientendaten** gemeldet. Waren es zuvor häufig private Pkw von Beschäftigten, die nach Feierabend in Wohngegenden aufgebrochen wurden, waren zuletzt vermehrt dienstliche Pkw während der Dienstzeit betroffen.

Auch bei der Betreuung vor Ort werden von Pflegediensten und Beratungsstellen Daten ihrer Klientinnen und Klienten verarbeitet. So müssen z. B. die Pflegetätigkeiten zeitnah dokumentiert oder Notizen über Beratungsgespräche angefertigt werden. Die Beschäftigten verwenden hierfür mobile Datenträger wie z. B. Laptops oder Papierakten.

In einem Fall wurden Papierunterlagen in einem Rucksack transportiert, der im Fußraum hinter dem Fahrersitz verstaut wurde, als die Beschäftigte zu einem Klientengespräch ging. Das Auto wurde mitten am Tag, zwischen 13.00 und 14.30 Uhr, aufgebrochen und der Rucksack gestohlen. In einem anderen Fall wurde ein Rucksack mit einem Laptop gestohlen. Die

Beschäftigte hielt nur kurz beim Bäcker an, um sich etwas zu kaufen. Die Zeit reichte dem Dieb, um die Autoscheibe einzuschlagen und den Laptop zu stehlen.

In beiden Fällen hatten die Beschäftigten dienstliche Vorgaben nicht beachtet. Eigentlich sollten die Datenträger nie unbeaufsichtigt bleiben und – wenn überhaupt – nur im Kofferraum, also nicht sichtbar für Dritte, transportiert werden. Generell gilt, dass nur die Datenträger mitgenommen werden, die auch wirklich benötigt werden.

Was ist zu tun?

Die Verwendung bzw. der Transport von mobilen Datenträgern außerhalb von Büroräumen birgt zusätzliche Risiken. Die verantwortliche Stelle muss ausreichende technische und organisatorische Maßnahmen treffen, um den Schutz der Daten vor Diebstahl und unbeabsichtigtem Verlust zu schützen. Digitale Datenträger sind zu verschlüsseln.

4.6.2 Wasserrohrbruch – 600 Patientenakten vernichtet

Was für ein Schlamassel! Ein Wasserrohrbruch im Archiv eines Krankenhauses durchnässte die dort aufbewahrten Papierakten. Auch die beauftragte Fachfirma konnte nicht alle Akten trocknen. 600 Patientenakten waren nicht zu retten. Wichtige Patientendaten wie Vorbefunde, Diagnosen und Aufzeichnungen der Ärztinnen und Ärzte waren verloren.

Das Krankenhaus kündigte in seiner Datenpannenmeldung an, dass alle noch vorhandenen Papierakten in ein externes Archiv verlagert und digitalisiert werden sollen.

Was ist zu tun?

Archivräume müssen nicht nur dahin gehend gesichert werden, dass Unbefugte keinen Zugang haben. Es müssen auch technische und organisatorische Maßnahmen getroffen werden, damit eine unbeabsichtigte Zerstörung oder unbeabsichtigte Schädigung der Daten verhindert wird (Grundsatz der Integrität und Vertraulichkeit der Datenverarbeitung).

4.6.3 Krankenhausseelsorge mal anders – fehlerhafte Videoübertragung

Manchmal steckt auch bei der Krankenhausseelsorge der Teufel im Detail.

In einem Krankenhaus können Patientinnen und Patienten und Angehörige in einem „Raum der Stille“ abseits des zum Teil hektischen Klinikgeschehens ihren ganz persönlichen Gedanken nachgehen. In diesem Raum werden zu bestimmten Zeiten auch Gottesdienste abgehalten. Da nicht alle Patientinnen und Patienten aufgrund ihrer gesundheitlichen Situation an diesen Gottesdiensten teilnehmen können, wurde eine

Kamera in diesem Raum installiert, damit Patientinnen und Patienten per Liveübertragung die Gottesdienste auf den TV-Apparaten in ihren Patientenzimmern verfolgen können. Außerhalb einer Liveübertragung sollte die Kamera keine Bilder übertragen.

Leider lief die Kamera jedoch auch außerhalb der Zeiten von Gottesdiensten. Die Technik war nicht richtig eingestellt. Über mehrere Monate wurde so das Geschehen in diesem „Raum der Stille" auf die Bildschirmgeräte in den Patientenzimmern übertragen, auch wenn Patientinnen und Patienten und Angehörige eigentlich dachten, einen Moment der Stille für sich zu haben.

Was ist zu tun?

Das Krankenhaus muss verbindlich festlegen, in welchen Zeiten eine Liveübertragung aus dem „Raum der Stille" erfolgt, dies technisch fehlerfrei umsetzen und Betroffene hierauf mit einer entsprechenden Beschilderung hinweisen.

Wir haben detaillierte Informationen zur Zulässigkeit einer Videoüberwachung und Muster für die Hinweisbeschilderung unter folgendem Link veröffentlicht:

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

Kurzlink: *https://uldsh.de/tb41-4-6-3*

4.6.4 Ein Hauch von Hollywood – YouTube im Krankenhaus

Tue Gutes und rede darüber. Noch besser, man dreht einen Film. Nur blöd, wenn dabei Patientinnen und Patienten ungewollt zu Statisten werden.

Wenn Ärztinnen und Ärzte Behandlungsmethoden verbessern, ist es durchaus sinnvoll, hierüber auch medial zu berichten. In diesem Fall wurde hierfür eine Medienagentur beauftragt. Diese bekam die Erlaubnis, in dem Krankenhaus einen Film zu drehen.

Das Krankenhaus wurde zum Drehort. Hauptsächlich wurden Ärztinnen und Ärzte interviewt oder bei ihrer Tätigkeit in Behandlungsräumen gezeigt. Aber auch die Operation einer Patientin wurde gefilmt. In einer Szene waren sogar die Daten dieser Patientin sichtbar. Der Film wurde u. a. auf YouTube online gestellt. Das Krankenhaus konnte jedoch nicht darlegen, dass die Patientin zuvor aufgeklärt und ihre Einwilligung erteilt hatte. Eine klare Datenschutzverletzung!

Was ist zu tun?

Verantwortliche dürfen externen Personen nur dann Zugang zu Patientendaten gewähren, wenn hierfür eine ausreichende und dokumentierte Befugnis, z. B. eine Einwilligung der Patientin oder des Patienten, vorliegt. Gleiches gilt für die Veröffentlichung von Patientendaten. Das Krankenhaus kündigte an, bestehende Verfahrensanweisungen zu ergänzen und die Beschäftigten gerade im Hinblick auf die strengen Anforderungen des Datenschutzes bei der Anfertigung von Bild- und Tonaufnahmen zu schulen.

4.6.5 Offener Datenmüllcontainer in der Psychiatrie

„Ein Datenmüllcontainer auf dem Ambulanzflur war mit einem Schloss versehen, dieses stand jedoch offen. Der Datenmüllcontainer war also über mehrere Tage frei zugänglich (er ist schon deutlich gefüllt).“ Kurz und deutlich war die interne Mittteilung einer Mitarbeiterin.

In dem Datenmüllcontainer befanden sich Daten von Patientinnen und Patienten sowie von Mitarbeiterinnen und Mitarbeitern. Der Container wurde sofort verschlossen und in einen abschließbaren Raum geschoben, zu dem nur Mitarbeiterinnen und Mitarbeiter Zutritt haben. Dass dieser Datenmüllcontainer nicht verschlossen war, lag daran, dass der für die Schlosscodierung verantwortliche Mitarbeiter seine Aufgabe nicht wahrgenommen hatte. Sicherheitshalber wurden alle Datenmüllcontainer kontrolliert. Ob aber zuvor Daten aus dem Container entwendet wurden, konnte nicht geklärt werden.

Was ist zu tun?

Datenmüll in einem Krankenhaus kann sensibelste Patientendaten enthalten. Für das Sammeln und Vernichten dieses Datenmülls sind daher verbindliche technische und organisatorische Maßnahmen zu treffen, um sicherzustellen, dass Unbefugte keinen Zugang zu diesen Daten haben.

4.6.6 Fotos und Videos von (verstorbenen) Patientinnen und Patienten per WhatsApp geteilt

Was muss die Mitarbeiterin eines Krankenhauses gedacht haben, als sie per WhatsApp Fotos und Videos von Patientinnen und Patienten erhielt? Absenderin war die ehemalige Lebenspartnerin eines Mitarbeiters aus dem Patiententransportdienst. Dieser Mitarbeiter hatte mit seinem Handy u. a. Aufnahmen von lebenden wie verstorbenen Patientinnen und Patienten gemacht und auch nicht davor zurückgeschreckt, Fußzettel von Verstorbenen zu fotografieren. Das Krankenhaus erstattete Strafanzeige. Der betroffene Mitarbeiter wurde sofort vom Dienst freigestellt und inzwischen entlassen.

Die Aufklärung dieser Datenschutzverletzung gestaltete sich äußerst schwierig. Nicht jedes Foto bzw. nicht jede Videoaufnahme war Patienten zuzuordnen. Nicht immer waren Gesichter zu

erkennen. Der Mitarbeiter verweigerte die Aussage. Zum Zeitpunkt der Datenpannenmeldung war daher nicht bekannt, wie viele Aufnahmen gemacht und an wen diese verschickt wurden. Betroffene Personen konnten nicht informiert werden. Eine Strafanzeige wurde gestellt, die Staatsanwaltschaft ermittelt.

Was ist zu tun?

In Krankenhäusern und Arztpraxen werden sensibelste Gesundheitsdaten von Patientinnen und Patienten verarbeitet, die der ärztlichen Schweigepflicht unterliegen. Es müssen organisatorische Maßnahmen zum Schutz der Integrität und Vertraulichkeit dieser Daten getroffen werden. Beschäftigte sind zu schulen und auf die möglichen personal- und strafrechtlichen Folgen bei Fehlverhalten hinzuweisen.

4.7 Bildung

4.7.1 Datenschutz und Sozialarbeit in Schulen – die neue Broschüre

Die Schulen erhalten bei der Erfüllung ihres Bildungs- und Erziehungsauftrags von Schulsozialarbeiterinnen und Schulsozialarbeitern Unterstützung. Im Rahmen dieser Unterstützung verarbeiten die in der Sozialarbeit tätigen Personen auch sensible personenbezogene Daten von Schulkindern, zu deren familiären Hintergrund und den bestehenden Konfliktsituationen im schulischen Bereich. Jene Datenverarbeitung zählt nicht zum datenschutzrechtlichen Verantwortungsbereich der Schulen.

Vielmehr sind die Schulsozialarbeiterinnen und Schulsozialarbeiter zwar in die schulische Organisation integriert. Datenschutzrechtlich sind die Schulsozialarbeiterinnen und Schulsozialarbeiter jedoch dem jeweiligen Anstellungsträger zuzuordnen, der auch die grundsätzlichen organisatorischen und technischen Maßnahmen für die sichere Verarbeitung der personenbezogenen Daten durch die Schulsozialarbeiterinnen und Schulsozialarbeiter treffen muss.

Die Broschüre gibt Antworten auf grundsätzliche Fragen zum Datenschutz und zur Datensicherheit, informiert den angesprochenen Personenkreis über die Rechte betroffener Personen und geht auf spezifische Fragestellungen ein. Zu letzteren zählen insbesondere:

- Stellung der Sozialarbeiterinnen und Sozialarbeiter aus Datenschutzsicht,
- anwendbare Rechtsvorschriften,
- Zusammenarbeit mit Schulleitung und Lehrkräften,
- Teilnahme an Konferenzen,
- Datenübermittlungen zwischen der Schulleitung, den Lehrkräften und den Sozialarbeiterinnen und Sozialarbeitern,
- Verdacht auf Kindeswohlgefährdung,
- Datenübermittlung an Polizei, Staatsanwaltschaft und Gerichte,
- Zusammenarbeit mit dem Jugendamt,
- Datenübermittlung an nichtöffentliche Stellen,
- Schulwechsel eines Schulkindes,
- Schulwechsel einer Sozialarbeiterin oder eines Sozialarbeiters.

Mit der Broschüre soll eine praktische Hilfestellung für den Bereich der Sozialarbeit in Schulen gegeben werden. Ein Abruf ist unter folgendem Link möglich:

https://www.datenschutzzentrum.de/uploads/schulen/dokumente/Handreichung-Schulsozialarbeit.pdf

Kurzlink: *https://uldsh.de/tb41-4-7-1a*

Eine Pressemitteilung des ULD zur Thematik finden Sie unter:

https://www.datenschutzzentrum.de/artikel/1400-Datenschutz-und-Sozialarbeit-in-Schulen-Praxiswissen-in-neuer-Broschuere-des-ULD.html

Kurzlink: *https://uldsh.de/tb41-4-7-1b*

4.7.2 Fotoaufnahmen als Gedächtnisstütze für Lehrkräfte

Wie präge ich mir die Namen von Schulkindern ein? Kann ich die Namen sicher bestimmten Schulkindern zuordnen? Dies fragte sich eine Lehrkraft bei der Übernahme von Schulklassen einer öffentlichen Grundschule in Schleswig-Holstein.

Zur besseren Orientierung fotografierte die Lehrkraft daraufhin die Schulkinder. Dabei verwendete die Lehrkraft ein privates Smartphone. Die Schule meldete den Sachverhalt an das ULD und sorgte für eine Löschung der angefertigten Aufnahmen. Schließlich erfolgte eine Sensibilisierung der Lehrkraft. Die Anfertigung der Fotoaufnahmen war nicht erforderlich, eine Einholung von wirksamen Einwilligungserklärungen hätte bei Schulkindern der Grundschule eine Mitwirkung der Eltern erfordert, und im Übrigen verstößt der Einsatz eines privaten Endgeräts ohne ausreichende technische und organisatorische Vorkehrungen gegen die Vorgaben der Datensicherheit.

Zur Aufgabenerfüllung war es für die Lehrkraft nicht erforderlich, Fotoaufnahmen der Schulkinder anzufertigen. Es mag sein, dass bei der Übernahme von mehreren neuen Schulklassen anfangs eine Unterscheidung der Schulkinder und das Einprägen von Namen anfangs eine Herausforderung darstellen kann. Dies rechtfertigt allerdings nicht die Herstellung einer privaten Fotodatenbank. Es wäre auch nicht nachvollziehbar und zu rechtfertigen, wenn jede Lehrkraft – ausgehend vom jeweils bestehenden Erinnerungsvermögen – von Schulkindern Fotoaufnahmen anfertigt.

Darüber hinaus wäre bei Schulkindern im Grundschulalter nicht pauschal von einer Fähigkeit auszugehen, die Tragweite einer Einwilligungserklärung zur Aufnahme und Speicherung eines Fotos zu übersehen. Es würde sich zudem nicht um freiwillige Erklärungen handeln, wenn die Schulkinder allgemein in der Gruppe befragt werden und so noch ein gewisser Antwortdruck erzeugt wird. Für die Anfertigung von Fotoaufnahmen – vorausgesetzt es würde losgelöst vom vorliegenden Sachverhalt überhaupt ein zulässiger Verarbeitungszweck vorliegen – müsste eine **Einwilligung der Eltern** vorliegen.

Die Verwendung eines privaten Endgeräts zur Aufnahme von Schulkindern verstieß gegen geltendes Schulrecht. Die Verwendung von privaten Endgeräten ist grundsätzlich unzulässig.

§ 30 Abs. 2 Satz 1 und 2 Schulgesetz

Die Daten der Schulverwaltung dürfen grundsätzlich nur mit Datenverarbeitungsgeräten des Schulträgers oder des Regionalen Berufsbildungszentrums verarbeitet werden. Ausnahmen hiervon regelt das für Bildung zuständige Ministerium durch Verordnung.

Ausnahmen von diesem Grundsatz bedürfen der Genehmigung der Schulleitung. Eine solche Genehmigung war nicht ersichtlich.

§ 14 Abs. 1 Schul-Datenschutzverordnung

Der Einsatz eines privaten informationstechnischen Geräts darf abweichend von § 30 Abs. 2 Satz 1 SchulG ausnahmsweise erfolgen, wenn kein dienstlich bereitgestelltes informationstechnisches Gerät zur Verfügung steht und soweit hierfür zuvor eine schriftliche Genehmigung der Schulleiterin oder des Schulleiters erteilt worden und diese nicht nach Absatz 7 erloschen ist. Verantwortliche bleibt auch in diesem Fall die jeweilige Schule.

Was ist zu tun?

Die Schule hat nach Kenntnis von dem Vorgang das ULD informiert und hinreichende Maßnahmen ergriffen, um ein wiederholtes Fehlverhalten auszuschließen. Es ist zu empfehlen, dass Schulen bei regelmäßigen internen Besprechungen der Schulleitung mit den Lehrkräften die Thematik der Anfertigung von Fotos und der Verwendung von privaten Endgeräten erörtern.

4.7.3 Anfertigung von Fotos durch Lehrkraft für Schulprojekt

Zur Gestaltung einer Danksagung für Praktikumsbetriebe hatte eine Lehrkraft die Idee, auch Fotos der Schulkinder beizufügen. Hierzu fotografierte die Lehrkraft die Schulkinder und stellte Ausdrucke der Aufnahmen her. Auf Beschwerden der Eltern hin erfuhr das ULD, dass keine wirksamen Einwilligungserklärungen für die Aufnahme der Fotos vorliegen und hinsichtlich der Abgabe der Erklärungen eine Beteiligung der Eltern nicht erfolgte. Die Schulleitung kontaktierte daraufhin die Lehrkraft, worauf letztere für die Vernichtung verbliebener Ausdrucke Sorge trug.

Die Schulleitung sensibilisierte im Folgenden die Lehrerschaft in einer internen Besprechung hinsichtlich der Anforderungen an die Zulässigkeit von Fotos der Schulkinder. Nach weiterer interner Aufklärung des Sachverhalts stellte sich schließlich heraus, dass die Lehrkraft die Aufnahmen entgegen der gesetzlichen Bestimmungen und im Widerspruch zu einer zunächst getätigten Aussage gegenüber der Schulleitung mit einem privaten Endgerät angefertigt hatte. Die Schulleitung hat dies gegenüber der Lehrkraft geahndet. Ferner wurde sichergestellt, dass die Fotoaufnahmen nunmehr von dem privaten Endgerät gelöscht werden.

Für den Einsatz privater Endgeräte ist eine Genehmigung der Schulleitung notwendig, was gesetzlich in der Schul-Datenschutzverordnung normiert ist.

> **§ 14 Abs. 2 Schul-Datenschutzverordnung**
>
> Die Genehmigung […] ist der Lehrkraft auf Antrag zu erteilen, wenn […]

Voraussetzungen einer Genehmigung sind insbesondere Zusicherungen der Lehrkraft zur rein dienstlichen Verwendung der Daten und dazu, dass keine Offenlegung gegenüber Dritten erfolgt, dass die Datenverarbeitung nur auf dem speziell von der Genehmigung erfassten Gerät erfolgt und die Sicherheitsanforderungen nach der DSGVO eingehalten werden. Ferner sind dem ULD und der Schulleitung zu ermöglichen, dass diese ihren Kontrollaufgaben nachkommen können. Die Lehrkraft muss die verwendeten informationstechnischen Geräte und Programme genau bezeichnen und ist verpflichtet, unverzüglich mitzuteilen, wenn die Datensicherheitsanforderungen nicht eingehalten werden können. Näheres ergibt sich aus § 14 Abs. 2 Schul-Datenschutzverordnung.

Was ist zu tun?

Schulleitungen müssen darauf hinwirken, dass die Lehrkräfte ihre Pflichten nach dem Datenschutzrecht und insbesondere der Schul-Datenschutzverordnung kennen und einhalten. Für einen Informationsaustausch bieten sich regelmäßige Besprechungen in den Schulen an.

05

KERNPUNKTE

Vorabübermittlung von Impf- und Genesenennachweisen

Übermittlung des Impfstatus ans Gesundheitsamt

Datenpannen in der Wirtschaft

Videoüberwachung im Fitnessstudio

5 Datenschutz in der Wirtschaft

5.1 Datenverarbeitung in Corona-Testzentren

Mehrere Beschwerden, die beim ULD eingingen, bezogen sich auf die Datenverarbeitung in Corona-Testzentren. So wurde u. a. moniert, dass betroffene Personen nicht ausreichend über die Verarbeitung ihrer Daten informiert worden seien. Weiterhin wurde dem ULD mitgeteilt, dass ein Testergebnis ohne zuvor erfolgten Test übermittelt wurde.

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 setzt der Verantwortliche gemäß Artikel 24 DSGVO geeignete technische und organisatorische Maßnahmen um. Weiterhin müssen bei der Verarbeitung personenbezogener Daten auch die Informationspflichten aus Artikel 13 DSGVO beachtet werden. Demnach teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung die in Art. 13 Abs. 1 und 2 DSGVO genannten Informationen mit. Diese beinhalten u. a. Angaben zum Zweck der Verarbeitung und der Speicherdauer sowie zu den bestehenden Betroffenenrechten.

In den vorliegenden Fällen wurden nach erfolgter Anhörung durch das ULD seitens der Verantwortlichen konkrete Maßnahmen umgesetzt, um die monierten Missstände zu beseitigen und eine datenschutzkonforme Verarbeitung der Daten zu gewährleisten. Es wurden hierzu u. a. die Informationsschreiben für die betroffenen Personen angepasst. Die Übermittlung eines Testergebnisses ohne zuvor erfolgten Test erfolgte in einem Einzelfall aufgrund des Bedienfehlers des Mitarbeiters eines Testzentrums. Hierbei bekam der Kunde seine eigenen Daten übermittelt, ohne dass es zur Offenlegung der Daten gegenüber unberechtigten Dritten kam. In diesem Fall wurde durch den Verantwortlichen eine zusätzliche Checkbox in der verwendeten Software zur Verarbeitung der Daten implementiert. Weiterhin erfolgte eine erneute **Sensibilisierung der Mitarbeiter** hinsichtlich der datenschutzrechtlichen Bestimmungen im Umgang mit den **Kundendaten**.

Das ULD erteilte in den Fällen, in denen datenschutzrechtliche Verstöße festgestellt wurden, gegenüber den Verantwortlichen Hinweise zur datenschutzkonformen Anpassung der Verarbeitungsvorgänge gemäß Art. 58 Abs. 1 Buchst. d DSGVO.

5.2 Zweckentfremdung von Kundendaten für politische Zwecke

Mehrere Beschwerden, die beim ULD eingingen, bezogen sich auf die Zweckentfremdung von Kundendaten, die seitens eines Verantwortlichen für Kundenkarten verarbeitet wurden. Die hierzu erhobenen Adressdaten nutzte das Unternehmen zweckwidrig dazu, um Werbung für ein Bürgerbegehren zu machen. Hierdurch sollten die Adressaten dazu bewegt werden, das Bürgerbegehren zu unterschreiben.

Einer der Grundsätze für die Verarbeitung personenbezogener Daten sieht vor, dass diese **für festgelegte, eindeutige und legitime Zwecke erhoben werden** und nicht in einer mit diesen

Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Die betroffenen Personen hatten im vorliegenden Fall ihre Adressdaten im Zusammenhang mit der Nutzung der Kundenkarte an den Verantwortlichen übermittelt. Darin erschöpfte sich der Zweck der Datenverarbeitung.

Art. 5 Abs. 1 Buchst. b DSGVO

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

Die Nutzung der **Adressdaten** zur Werbung für ein Bürgerbegehren stellt einen anderen Zweck dar, welcher zudem mit dem Zweck der Verwendung einer Kundenkarte in keinem inneren Zusammenhang stand. Für die Verwendung der Adressdaten zur Übermittlung der Schreiben hinsichtlich des Bürgerbegehrens hätte es demnach einer gesonderten Rechtsgrundlage bedurft. Der Verantwortliche gab dem ULD gegenüber an, dass er die Schreiben aufgrund seines berechtigten Interesses nach Art. 6 Abs. 1 Buchst. f DSGVO an die Nutzerinnen und Nutzer der Kundenkarte versandt hätte.

Er sei davon ausgegangen, dass für den angeschriebenen Personenkreis ein Interesse an dem Bürgerbegehren bestehe, da der Inhalt des Begehrens sich auf diesen auswirke.

Art. 6 Abs. 1 Buchst. f DSGVO

Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Dieser Wertung folgte das ULD nicht. Es liegt nicht im Erwartungshorizont der Nutzerinnen und Nutzer von Kundenkarten, dass diese unter den angegebenen Adressdaten wegen eines Bürgerbegehrens angeschrieben werden. Ferner geht es bei der Prüfung von Art. 6 Abs. 1 Buchst. f DSGVO zunächst um die Prüfung eines berechtigten Interesses des Verantwortlichen. Hinsichtlich des betroffenen Personenkreises ist hingegen zu untersuchen, ob und welche Interessen einer Verarbeitung entgegenstehen können. Daher konnte nicht pauschal darauf verwiesen werden, man nehme an, das Bürgerbegehren könnte für den angeschriebenen Personenkreis interessant sein.

Das ULD stellte folglich einen datenschutzrechtlichen Verstoß fest und erteilte dem Unternehmen Maßgaben, in welchem Rahmen personenbezogene Daten der Kundinnen und Kunden verarbeitet werden dürfen und dass der Grundsatz der Zweckbindung der Datenverarbeitung einzuhalten ist.

5.3 Tauchsport und Gesundheitsdaten zum Coronavirus

Das ULD wurde darauf aufmerksam gemacht, dass ein Verein im Rahmen des Trainings einer Tauchsportgruppe Corona-Daten der Mitglieder abfragte. Hierzu wurde den Mitgliedern vorab ein Fragebogen übermittelt, 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 und kürzlich erfolgter Reisen in ein Risikogebiet gestellt. Die Beantwortung der Fragen sollte vor jedem Training erfolgen. Die Mitglieder wurden darauf hingewiesen, dass ohne die Beantwortung der Fragen eine Teilnahme am Training nicht möglich sei. Die Fragebögen wurden für vier Wochen durch den Verein gespeichert.

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 Kunden vorgelegen hätte. Im vorliegenden Fall **wurde jedoch die Teilnahme am Tauchtraining an die Angaben der Mitglieder zum aktuellen Gesundheitszustand gekoppelt**, was keine freie Willensbekundung darstellt. Es lag demnach keine Rechtsgrundlage zur Verarbeitung der Gesundheitsdaten vor.

Anzuzweifeln waren auch die Erforderlichkeit und Eignung der Gesundheitsfragen. So bestand das Risiko, dass keine wahrheitsgemäße Beantwortung der Fragen erfolgt, wenn seitens der Mitglieder ein starkes Interesse an der Teilnahme am Tauchtraining vorliegt. Die Abfrage der Gesundheitsdaten stellte demnach kein geeignetes Mittel dar, um die anderen Teilnehmer vor einer möglichen Corona-Infektion zu schützen.

Das ULD verfügte neben der Löschung der erhobenen Gesundheitsdaten, dass eine Abfrage der Gesundheitsdaten seitens des Vereins nicht mehr durchgeführt wird. Abschließend wurde ein Hinweis nach Art. 58 Abs. 1 Buchst. d DSGVO erteilt und darauf hingewiesen, dass es zur Verarbeitung von Gesundheitsdaten einer Rechtsgrundlage bedarf, die sich nur aus Art. 9 Abs. 2 DSGVO ergeben kann.

5.4 Vorabübermittlung von Impf- und Genesenennachweisen bei Buchung einer Ferienwohnung

Gegenstand einer Beschwerde war die Vorabübermittlung von Impf- und Genesenennachweisen bei der Buchung einer Ferienwohnung. Der Gast wurde hierbei dazu aufgefordert, diese Nachweise vorab per E-Mail an den Vermieter zu übermitteln. Zudem wurde dem Gast mitgeteilt, dass ohne ein vorheriges Übersenden der Nachweise der Antritt der Reise nicht möglich wäre.

Bei Informationen hinsichtlich des Impf- und Genesenenstatus einer Person handelt es sich um Gesundheitsdaten im Sinne des Art. 4 Nr. 15 Datenschutz-Grundverordnung (DSGVO). Diese Daten unterliegen einem erhöhten Schutzbedarf.

Vorgaben hinsichtlich des Test-, Genesenen- und Impfstatus von Personen fanden sich in der jeweils gültigen **Corona-Bekämpfungsverordnung des Landes Schleswig-Holstein (Corona-BekämpfVO)**. Demnach galt für bestimmte Einrichtungen, dass eine Beherbergung von Personen nur zulässig war, wenn diese geimpft oder genesen waren. Demnach musste durch den Verantwortlichen gewährleistet werden, dass diese Vorgaben eingehalten werden. Die Corona-BekämpfVO sah 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 ergab sich jedoch keine Verpflichtung, sich diese Nachweise in irgendeiner Form vorab übermitteln zu lassen. Zur Erfüllung der Vorgaben aus der Corona-BekämpfVO reichte die kurze Einsichtnahme in die entsprechenden Nachweise aus. Zudem konnte der Umstand vermerkt werden, dass kontrolliert wurde. Eine Rechtsgrundlage zur Verarbeitung dieser Daten konnte sich nur aus Art. 6 Abs. 1 in Verbindung mit Art. 9 DSGVO (und gegebenenfalls weiteren landesrechtlichen Regelungen) ergeben.

Wie auch schon im vergangenen Jahr zeigte sich in solchen Fällen, dass die Aufforderung zur Vorabübermittlung der Nachweise aus Unwissenheit und fehlenden Vorgaben zur praktischen Umsetzung der Corona-BekämpfVO erfolgte.

Schließlich änderten sich während der Bearbeitung der Beschwerde die Vorgaben der Corona-BekämpfVO dahin gehend, dass selbst die Kontrolle der Impf- und Genesenennachweise nicht mehr erforderlich war.

Der Verantwortliche wurde vom ULD auf die Unrechtmäßigkeit der Vorabübermittlung der Nachweise hingewiesen. Der Vermieter der

Ferienwohnung wurde angehalten, von der Praxis einer Vorabübersendung von Unterlagen zum Test-, Genesenen- und Impfstatus künftig abzusehen. Für eine entsprechende Anforderung fehlte eine Rechtsgrundlage. Ferner bestand nun auch keine Kontrollverpflichtung mehr.

Weiterhin wurde mitgeteilt, dass bei einem gegebenenfalls erneuten Inkrafttreten von Kontrollpflichten die datenschutzrechtlichen Bestimmungen sowie die Vorgaben der jeweils gültigen Corona-Bekämpfungsverordnung des Landes Schleswig-Holstein eingehalten werden müssen.

5.5 Einsichtnahme in Impfnachweise bei Kinobesuch

Ende des Jahres 2021 erreichten uns mehrere Beschwerden, die sich auf die Einsichtnahme sowie das Fotografieren von Impfnachweisen beim Besuch eines Kinos bezogen.

Vorgaben hinsichtlich des Test-, Genesenen- und Impfstatus von Personen fanden sich in der jeweils gültigen Corona-Bekämpfungsverordnung des Landes Schleswig-Holstein (Corona-BekämpfVO). Demnach galt für Freizeit- und Kultureinrichtungen, dass nur Besucherinnen und Besucher in die Einrichtung eingelassen werden dürfen, wenn diese im Sinne von § 2 Nummer 2, 4 oder 6 COVID-19-Schutzmaßnahmen-Ausnahmenverordnung (SchAusnahmV) geimpft, genesen oder getestet waren. Demnach mussten die Einrichtungen gewährleisten, dass diese Vorgaben eingehalten wurden. Aus der Corona-BekämpfVO ergab sich jedoch **keine Verpflichtung, diese Nachweise in irgendeiner Form zu speichern**.

Eine Gewährleistung, dass nur Personen mit den entsprechenden Nachweisen die Räumlichkeiten betreten, war datensparsam durch eine bloße Sichtkontrolle in die mitgeführten Unterlagen möglich. Das Abfotografieren und Speichern der Unterlagen war zur Einhaltung der Kontrollverpflichtung nicht erforderlich.

In den vorliegenden Sachverhalten wurden seitens des ULD Hinweise nach Art. 58 Abs. 1 Buchst. d DSGVO erteilt und Erläuterungen gegeben, dass für Freizeit- und Kultureinrichtungen keine Verpflichtung bestand, die Nachweise zu speichern. Zudem wurde die Löschung der bisher erhobenen Daten verfügt.

Aus den Rückmeldungen der Verantwortlichen ergab sich im Übrigen, dass in einigen Fällen die Nachweise nicht abfotografiert worden sind, sondern lediglich eine Überprüfung des Impfstatus mittels der **CovPassCheck-App** erfolgte.

5.6 Verwendung von Bildern der Töchter auf Webseite

Das ULD erreichte die Beschwerde einer Mutter, die sich auf die Verwendung von Bildern ihrer Töchter auf einer Webseite bezog. Die Webseite wurde von dem Vater der Kinder betrieben, der mittels dieser Webseite seine Sicht der Dinge auf die vorangegangene Trennung und den darauf folgenden Sorgerechtsstreit darstellen wollte. Das alleinige Sorgerecht wurde hier zuvor der Mutter zugesprochen.

Gemäß Art. 6 Abs. 1 DSGVO ist die Verarbeitung von personenbezogenen Daten nur rechtmäßig, wenn mindestens eine der in der genannten Norm aufgeführten Bedingungen erfüllt ist. Es bedarf also einer Rechtsgrundlage zur Verarbeitung personenbezogener Daten. **Kinder verdienen hinsichtlich ihrer personenbezogenen Daten besonderen Schutz**, da diese sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind.

Für bestimmte Dienste der Informationsgesellschaft sieht die DSGVO vor, dass **für Kinder, die das 16. Lebensjahr noch nicht vollendet haben, eine Einwilligung des gesetzlichen Vertreters zur Verarbeitung der personen-**

bezogenen Daten des Kindes vorliegen muss. Eine Einwilligung des Kindes alleine ist nicht ausreichend. Diese Bestimmung zur Altersgrenze kann eine Richtschnur auch für Sachverhalte bieten, in denen nicht ein spezifischer Dienst im Fokus steht. Bei Kindern unter 16 Jahren ist daher grundsätzlich zu prüfen, ob für die Abgabe von Einwilligungserklärungen die nötige Einsichtsfähigkeit gegeben ist.

Das Alter der Töchter betrug zum Zeitpunkt der Beschwerde vier und sechs Jahre. Demnach war zur Verarbeitung ihrer personenbezogenen Daten die Einwilligung des gesetzlichen Vertreters notwendig. Da das alleinige Sorgerecht der Mutter zugesprochen wurde, war hier für die Veröffentlichung der Bilder auf der Webseite deren Einwilligung erforderlich. Diese lag jedoch nicht vor.

Der Vater wurde seitens des ULD angeschrieben und zur Löschung aller Bilder, auf denen die Töchter auf der Webseite zu sehen waren, aufgefordert. Dieser zeigte sich jedoch nicht sehr kooperativ und bestritt, der Betreiber der Webseite zu sein, wollte diesen gegenüber dem ULD aber auch nicht nennen. Es lagen jedoch ausreichend Anhaltspunkte dafür vor, dass der Vater auch der Betreiber der Webseite war. Als nach wiederholter Aufforderung keine Löschung der Bilder von der Webseite erfolgte, wurde die Löschung der Bilder unter Androhung eines Zwangsgelds angeordnet.

Daraufhin deaktivierte der Vater den Webauftritt. Das aufsichtsbehördliche Verfahren wurde mit einer Warnung an den Vater abgeschlossen, zukünftig ohne vorhandene Rechtsgrundlage (Einwilligung der Sorgeberechtigten) Bilder der Töchter zu veröffentlichen.

5.7 Übermittlung des Impfstatus von Beschäftigten an das Gesundheitsamt

Für Beschäftigte in Medizin und Pflege und weitere Personen, die in entsprechenden Einrichtungen tätig sind, gilt seit dem 16. März 2022 eine einrichtungsbezogene Impfpflicht. Das **Gesetz zur einrichtungsbezogenen Impfung** sieht nach dem § 20a Infektionsschutzgesetz (IfSG) vor, dass Personen, die in medizinischen und pflegerischen Einrichtungen tätig sind, über einen gültigen Nachweis einer Impfung oder Genesung verfügen und diesen bei der Einrichtungsleitung vorlegen müssen.

Wenn der Nachweis nicht bis zum Ablauf des 15. März 2022 vorgelegt wurde oder wenn Zweifel an der Echtheit oder inhaltlichen Richtigkeit des vorgelegten Nachweises bestehen, hat die Leitung der jeweiligen Einrichtung unverzüglich das zuständige Gesundheitsamt darüber zu benachrichtigen.

In einer Ende März eingereichten Beschwerde beklagte eine Beschäftigte einer entsprechenden Einrichtung, dass sie an das Gesundheitsamt gemeldet wurde. Es sei zwar richtig, dass sie keinen entsprechenden Nachweis vorgelegt habe, aufgrund einer längerfristigen Erkrankung sei derzeit jedoch nicht absehbar, wann sie ihre Arbeitsfähigkeit zurückerlange und wieder einer Beschäftigung in der Einrichtung nachgehen könne.

Nach den Regelungen des IfSG hat zwar die Leitung der jeweiligen Einrichtung unverzüglich das Gesundheitsamt darüber zu benachrichtigen, dass der erforderliche Nachweis nicht vorgelegt wurde, dieses bezieht sich allerdings lediglich auf die Personen, die in der entsprechenden Einrichtung „tätig" sind. Dabei ist es erforderlich, dass die Person **regelmäßig und nicht nur zeitlich vorübergehend** in der Einrichtung tätig ist, sodass beispielsweise auch regelmäßig dort tätige Handwerker, Auszubildende oder freie Mitarbeiter der Nachweispflicht unterfallen.

Da die Tätigkeit allerdings nicht gleichbedeutend mit einem Beschäftigungsverhältnis im sozialversicherungsrechtlichen Sinne ist und es nach dem Sinn und Zweck des § 20a IfSG auf die Ausübung der Tätigkeit und nicht auf das bloße Bestehen eines Beschäftigungsverhältnisses ankommt, sind Personen, die sich bei Ablauf der Frist im Mutterschutz, in Elternzeit, in vollständiger Freistellung wegen Pflegezeit befinden oder

einem Beschäftigungsverbot unterliegen, **erst bei ihrer Rückkehr vorlagepflichtig**. Das Gleiche gilt für Sonderurlaub, Krankschreibung oder Ruhen des Arbeitsverhältnisses wegen befristeter Erwerbsminderung.

Im Rahmen des durchgeführten Verfahrens räumte die Einrichtungsleitung die Übermittlung an das Gesundheitsamt ein. Nach ihrer Schilderung sei die Meldung nach bestem Wissen und Gewissen und sorgfältigem Studium des § 20a IfSG als auch sämtlicher damals veröffentlichter Leitlinien und Handreichungen des Gesundheitsministeriums zur Umsetzung der einrichtungsbezogenen Impfpflicht erfolgt.

Die hierzu erschienene Handreichung des Bundesministeriums für Gesundheit zur Impfprävention in Bezug auf einrichtungsbezogene Tätigkeiten, die auf die zu beachtende Unterscheidung zwischen „tätig" und „beschäftigt sein" hinweist, sei jedoch erst am 22. März 2022 erschienen, sodass sie zum Zeitpunkt des Inkrafttretens der einrichtungsbezogenen Impfpflicht und somit auch zum Zeitpunkt der Übermittlung der Daten an das Gesundheitsamt noch nicht vorlag.

Durch diese am 22. März 2022 erfolgte Klarstellung des Bundesministeriums hätte auch nach Auffassung der Einrichtungsleitung die Übermittlung der Daten der erkrankten Beschäftigten nicht stattfinden dürfen. Da die Einrichtungsleitung das Gesundheitsamt darüber hinaus bat, die fälschlicherweise übermittelten Daten umgehend zu löschen, konnte von weiteren Maßnahmen abgesehen werden.

5.8 Dokumentation der Übergabe einer fristlosen Kündigung

Fristlose Kündigungen sind für Beschäftigte wie für Arbeitgeber eine heikle Angelegenheit. Ein Beschäftigter beklagte sich beim ULD, dass ihm die fristlose Kündigung durch einen ihm bekannten Beschäftigten des Arbeitgebers persönlich überbracht worden sei und sowohl der Inhalt der Kündigung als auch die Übergabe von diesem fotografiert worden sei. Der Beschäftigte fühlte sich dadurch in seinem Recht auf Datenschutz verletzt.

Die Kenntnisnahme des Inhalts eines Kündigungsschreibens zu Zwecken des Nachweises der Übergabe war als erforderlich zur Beendigung des Beschäftigungsverhältnisses im Sinne des § 26 BDSG anzusehen. Bei anderen Übergabeformen, wie beispielsweise bei einem Einschreiben, könnte sowohl die Zustellung scheitern, wenn der Empfänger beim Zustellversuch nicht anwesend ist, oder der Inhalt des zugestellten Briefes kann nicht rechtssicher nachgewiesen werden.

Zu prüfen war in diesem Fall zudem, ob das Fotografieren des Inhalts und der Übergabe der fristlosen Kündigung als (noch) erforderlich erachtet werden konnte oder ob es sich dabei um eine nicht gerechtfertigte Verarbeitung personenbezogener Daten handelte, weil die Übergabe durch den Boten persönlich bezeugt werden könnte. Erforderlich ist eine Verarbeitung dann, wenn sie zur Erreichung des legitimen Zweckes der Verarbeitung notwendig ist und kein anderes gleich geeignetes milderes Mittel zur Verfügung steht. Der Nachweis durch eine Fotografie, dass gerade ein Schreiben mit dem Inhalt einer fristlosen Kündigung vom Boten übergeben wird, konnte als erforderlich beurteilt werden, weil sie die Übergabe gerade dieses Schreibens dokumentierte.

Darüber hinaus hatte der Arbeitgeber nachzuweisen, dass es sich bei dem Boten um einen Beschäftigten des Unternehmens, der mit Personalangelegenheiten betraut war, handelte und die Dokumentation der Übergabe des Kündigungsschreibens durch ein Diensttelefon erfolgt war.

Was ist zu tun?

Arbeitgeber müssen sicherstellen, dass nicht nur bei Begründung und Durchführung eines Beschäftigungsverhältnisses, sondern auch bei dessen Beendigung nur solche Daten verarbeitet werden, die zu diesen Zwecken erforderlich sind.

5.9 Auslesen von Impressumsangaben zum Zweck der Direktwerbung

Durch eine Beschwerde erlangte das ULD Kenntnis von einer Auskunft, in der ein Unternehmen der betroffenen Person mitteilte, dass die zum Zweck der Direktwerbung genutzten personenbezogenen Daten aus dem Impressum seiner Webseite entnommen wurden.

Die Daten in einem Impressum werden nicht freiwillig, sondern aufgrund der gesetzlichen Verpflichtung zur Anbieterkennzeichnung gemäß § 5 Telemediengesetz (TMG) bzw. § 55 Abs. 2 Rundfunkstaatsvertrag (RStV) veröffentlicht. Eine Interessenabwägung nach Art. 6 Abs. 1 Buchst. f DSGVO führt daher mangels Freiwilligkeit der Veröffentlichung regelmäßig dazu, dass eine werbliche Nutzung der so erhobenen Daten unzulässig ist.

Impressum

Impressums- oder auch Anbieterkennzeichnungspflicht bedeutet, dass der Anbieter eines Online-Angebots, das nicht ausschließlich privaten oder familiären Zwecken dient, leicht erkennbar, unmittelbar erreichbar und ständig verfügbar seinen vollständigen Namen und seine vollständige Anschrift im Angebot vorzuhalten hat. Für in Hamburg und Schleswig-Holstein betriebene Internetseiten kontrolliert die Medienanstalt Hamburg/Schleswig-Holstein die Einhaltung dieser Anforderungen.

Der Verantwortliche teilte hierzu mit, dass irrtümlich ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 Buchst. f DSGVO angenommen wurde, und bestätigte nach erfolgter eigener rechtlicher Prüfung unter Hinzuziehung eines eigenen Anwaltes, dass die Voraussetzungen für eine werbliche Nutzung der Daten ohne vorherige Einwilligung der betroffenen Person mangels bestehender Kundenbeziehung nicht vorlagen.

Nach seiner Angabe habe es sich bei der im Falle des Beschwerdeführers erfolgten Erhebung personenbezogener Daten aus dem Impressum jedoch um einen Ausnahmefall gehandelt. Der Verantwortliche bestätigte ausdrücklich, dass es keine weiteren Fälle dieser Art gegeben habe, und versicherte, dass sich ein solcher Vorgang nicht wiederholen werde.

Unter Berücksichtigung der erfolgten Zusicherung eines Einzelfalls, der ursprünglich innerhalb weniger Tage erfolgten Auskunft an den Beschwerdeführer und der inzwischen erfolgten Löschung der streitgegenständlichen Daten wurde dem Verantwortlichen unter Abwägung insbesondere der Art, Schwere und Dauer des Verstoßes, dem Grad der Fahrlässigkeit und den ergriffenen Maßnahmen zur Minderung des eventuell entstandenen Schadens eine Warnung dahin gehend erteilt, dass er im Falle einer werblichen Nutzung von personenbezogenen Daten aus einem Impressum gegen die Datenschutz-Grundverordnung verstößt.

5.10 Rückabwicklung bei EC-Kartenzahlung

Während der Coronapandemie kam es zu vielen Absagen von Veranstaltungen und Konzerttickets konnten zurückgegeben werden. Die Rückabwicklung der Ticketverkäufe führte dann zur Erstattung der Kaufpreise.

In einem Beschwerdefall hatte die Vorverkaufsstelle nach Absage einer Veranstaltung den per EC-Karte gezahlten Ticketpreis nur gegen Angabe des Namens, der Kontonummer, Anschrift, Telefonnummer und E-Mail-Adresse des Kunden erstatten wollen. Auch in diesem Fall war die Datenverarbeitung im Hinblick auf ihre Vereinbarkeit mit der Datenschutz-Grundverordnung zu prüfen.

Es wurde ein aufsichtsbehördliches Verfahren nach § 74 LVwG eingeleitet und das verantwortliche Unternehmen um eine Stellungnahme gebeten. Die Prüfung des Sachverhalts ergab, dass die Erhebung der Kontaktdaten für die Rückerstattung eines Tickets, das mit EC-Karte bezahlt wurde, nicht erforderlich ist. Bei diesen Informationen handelt es sich um personenbezogene Daten des Kontoinhabers, die nur dann verarbeitet werden dürfen, wenn diese Verarbeitung auf eine der in Artikel 6 DSGVO genannten Rechtsgrundlagen gestützt werden kann und dafür erforderlich ist. Eine solche Erforderlichkeit war für die Rückzahlung des Kaufpreises nicht gegeben. Die Rückzahlung kann dabei auf dem gleichen Zahlungsweg erfolgen wie die Kaufpreiszahlung.

Was ist zu tun?

Veranstalter haben bei Ticketverkäufen stets zu prüfen, welche personenbezogenen Daten im Falle einer Rückabwicklung erforderlich sind.

5.11 Veröffentlichung von Wohnungsfotos und Durchführung von Besichtigungen

Im Frühjahr des Jahres 2022 ging beim ULD eine Beschwerde eines Mieters ein, in der er beklagte, dass sein Vermieter ohne seine Zustimmung Wohnungsfotos zur Neuvermietung im Internet veröffentlichte und Wohnungsbesichtigungen in seiner Abwesenheit durchführte.

Er schilderte, dass der Vermieter nach der erfolgten Mietvertragskündigung eine Wohnungsvorabnahme durchgeführt habe. Da der Mieter zu diesem Zeitpunkt ortsabwesend war, habe er auf seine Nachbarin verwiesen, die einen Zweitschlüssel hatte und dem Vermieter die Wohnung zur Durchführung der Vorabnahme aufschließen durfte. Im Rahmen der Durchführung der Wohnungsvorabnahme wurden allerdings Fotos von der Wohnung angefertigt und ohne Zustimmung des derzeitigen Mieters im Internet hochgeladen.

Darüber hinaus habe der Vermieter die Nachbarin in acht Fällen gebeten, im Namen des Vermieters Wohnungsbesichtigungen mit Mietinteressenten durchzuführen, ohne dass der Mieter hiervon in Kenntnis gesetzt oder an einer Terminabstimmung beteiligt wurde.

Obwohl die Veröffentlichung von Wohnungsfotos eine schnellere Wiedervermietung fördern kann, rechtfertigt dies nicht, Aufnahmen von den privaten Lebensbedingungen ohne Wissen und Einverständnis des Mieters zu erstellen. Das Persönlichkeitsrecht überwiegt gegenüber dem Interesse des Vermieters, die Wohnung möglichst schnell und attraktiv im Internet zu präsentieren, sodass dieser ohne vorherige Einwilligung des Mieters keine Wohnungsfotos zum Zweck der Vermarktung erstellen darf.

Auch wenn ein Mieter grundsätzlich verpflichtet ist, möglichen Nachmietern die Besichtigung der Wohnung zu ermöglichen, so ist es dem Vermieter jedoch nicht gestattet, die Besichtigungen ohne Einverständnis des Mieters durchzuführen.

Art. 13 Abs. 1 Grundgesetz

Die Wohnung ist unverletzlich.

Im Rahmen des gegen den Vermieter eingeleiteten aufsichtsbehördlichen Verfahrens räumte dieser zunächst ein, dass ihm keine Einwilligung des Mieters zur Erstellung und Veröffentlichung von Wohnungsfotos oder zur Durchführung von Wohnungsbesichtigungen vorlag. Aufgrund des erfolgten Verweises auf die Nachbarin sei er jedoch davon ausgegangen, dass diese umfassend bevollmächtigt gewesen sei. Fragen, ob Fotos erstellt und sie zur Durchführung von Wohnungsbesichtigungen bereit sei, habe sie jeweils bejaht.

Zur Verhinderung vergleichbarer Fälle wies der Vermieter seine Beschäftigten an, zukünftig in jedem Fall vor dem Erstellen von Fotos oder der Weitergabe von Kontaktdaten an potenzielle Nachmieter von dem jeweiligen Mieter selbst eine schriftliche Einwilligung einzuholen. Darüber hinaus würden Wohnungsvorabnahmen und Wohnungsbesichtigungen nur noch im Beisein des Mieters selbst oder im Beisein einer Bevollmächtigten durchgeführt, sofern die Bevollmächtigte eine schriftliche Vollmacht vorlegen könne.

Was ist zu tun?

Vor der Erstellung von Wohnungsfotos zum Zweck der Vermarktung müssen stets die mietenden Personen um Einwilligung gebeten werden. Ohne eine Einwilligung dürfen Fotos grundsätzlich erst nach Auszug der Mietpartei erstellt und veröffentlicht werden.

5.12 Schnupperstunde im Vereinsvorstand

Eine Vielzahl der Schleswig-Holsteinerinnen und Schleswig-Holsteiner engagieren sich ehrenamtlich in Vereinen, was für den Zusammenhalt unserer Gesellschaft von sehr großer Bedeutung ist. Immer weniger sind allerdings bereit, einen Vorstandsposten zu übernehmen. Es reicht jedoch nicht, wenn alle nur mitmachen wollen, es braucht Menschen, bei denen die Fäden zusammenlaufen und die bereit sind, sich im Vorstand zu engagieren.

In einer beim ULD eingereichten Beschwerde berichtete ein Vereinsmitglied, dass ein anderes Mitglied vom bisherigen Vorstand als mögliche Nachfolgerin vorausgewählt und in die Tätigkeiten der Vorstandsarbeit eingeführt wurde. Eine ordentliche Wahl, wie es die Satzung vorschreibe, habe bisher jedoch noch nicht stattgefunden. Es wurde beklagt, dass die Betreffende im Rahmen ihrer „Einarbeitung" bereits jetzt die Möglichkeit hätte, auf diverse Vereinsunterlagen zuzugreifen, durch die sie Einblick in personenbezogene Daten einzelner Mitglieder hätte. Darüber hinaus würde sie an Besprechungen und Verhandlungen teilnehmen, in denen über persönliche Angelegenheiten einzelner Mitglieder verhandelt werde.

Verantwortliche sind im Rahmen der Beachtung der **Grundsätze der Integrität und Vertraulichkeit** verpflichtet, personenbezogene Daten in einer Art und Weise zu verarbeiten, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Offenlegung gegenüber Dritten und vor unbeabsichtigtem Verlust.

Zur Gewährleistung einer angemessenen Sicherheit haben Verantwortliche geeignete technische und organisatorische Maßnahmen umzusetzen. Ein Verein sollte die jeweiligen Aufgaben bestimmten Vorstandsmitgliedern durch die Satzung oder die Geschäftsordnung zugewiesen haben. Die Vorstandsmitglieder dürfen hierbei nur einen Zugriff auf die für die Erfüllung der ihnen übertragenen Aufgaben erforderlichen Daten erhalten.

Der Vorstand des Vereins teilte zu dem vorgetragenen Vorwurf mit, dass die Aufgabe der Betreffenden darin bestand, die Vorstandsarbeit vor ihrer möglichen Wahl als neue Vorsitzende kennenzulernen. Dies sei erforderlich, da neu gewählte Vorstandsmitglieder in der Vergangenheit die Vorstandsarbeit falsch eingeschätzt hätten und nach kurzer Zeit wieder vom Amt zurückgetreten seien.

Die rechtliche Grundlage für ihre Mitarbeit im Vorstand ergebe sich aus einer entsprechenden Regelung der Vereinssatzung, nach der der Vorstand berechtigt sei, Personen für bestimmte Angelegenheiten eine Vollmacht zu erteilen und ihnen Aufgaben zu übertragen. Im Rahmen der erfolgten Aufgabenübertragung habe die Vorstandsanwärterin u. a. auch eine Verschwiegenheitserklärung unterzeichnet.

Da der Vorstandsanwärterin nach Mitteilung des Vereinsvorstandes nur die zur Erfüllung der ihr übertragenen Aufgaben erforderlichen Daten zur Verfügung gestellt wurden und sie darüber hinaus zu keinem Zeitpunkt eine eigene Zugriffsmöglichkeit auf den vom Verein verwalteten Datenbestand erhalten habe, konnte von etwaigen Maßnahmen gegen den Verein abgesehen werden.

5.13 Datenpannen in der Wirtschaft (Meldungen nach Artikel 33 DSGVO)

5.13.1 Erfolglose Fehlersuche – Fehlversand von Rechnungen

Ende des Jahres 2021 erreichten uns mehrere Beschwerden von Kundinnen und Kunden eines Unternehmens, bei dem diese Online-Geschenkgutscheine für Kinobesuche erworben hatten. Gemeinsam mit ihrer eigenen Rechnung waren ihnen die Kaufbelege von jeweils bis zu 45 weiteren Personen zugesandt worden, sodass die Sorge bestand, dass auch ihre personenbezogenen Daten anderen Kundinnen und Kunden gegenüber offengelegt worden waren. Bei den in den Rechnungen enthaltenen personenbezogenen Daten handelte es sich um den Namen, die Anschrift und die Kundennummer der Kundinnen und Kunden sowie deren Telefonnummer. Ebenfalls in den Rechnungen abgedruckt waren an die beschenkten Personen gerichtete Grußtexte, aus denen sich teilweise weitere personenbezogene Daten wie die Namen oder Spitznamen weiterer Familienmitglieder oder der beschenkten Personen und Informationen über den Anlass der Schenkung ergaben: In den bekannten Grußtexten waren dies beispielsweise ein Dank für die Hilfe bei einem Umzug, ein Geburtstag oder eine Eheschließung.

Aus dem übermittelten Schriftwechsel ergab sich, dass das Unternehmen über die Verletzung des Schutzes personenbezogener Daten benachrichtigt worden war, eine entsprechende Meldung des Verantwortlichen an die Landesbeauftragte für Datenschutz war jedoch nicht erfolgt.

Der Verantwortliche wurde zu dem geschilderten Sachverhalt angehört und teilte in einer Stellungnahme mit, dass es bei dem Versand der Rechnungen zu einem technischen Fehler gekommen sei, auf den das Unternehmen durch einen Kunden aufmerksam gemacht worden sei. Diesen Hinweis habe man zum Anlass genommen, die Fehlersuche zu beginnen. Da der technische Fehler trotz detaillierter Suche nicht verlässlich habe ausfindig gemacht werden können, sei der Rechnungsversand inzwischen eingestellt worden.

Aufgrund des langen Zeitraums von mindestens 21 Tagen, in dem ein fehlerhafter Versand immer wieder aufgetreten war, erfolgte eine genauere

Nachfrage. Es stellte sich heraus, dass der zuständige Dienstleister nach dem ersten Bekanntwerden des Fehlversands zunächst einen vermeintlichen Fehler auf dem Liveserver korrigiert hatte und damit der Überzeugung war, das Problem erfolgreich behoben zu haben. Der Fehlversand korrelierte zeitlich mit einer kurz zuvor durchgeführten Änderung am E-Mail-Versand, die zurückgenommen worden sei.

Zehn Tage später wurden weitere gleichartige Fälle bekannt, woraufhin durch eine erneute genauere Prüfung festgestellt wurde, dass der angenommene Fehler nicht ursächlich für den Fehlversand war. Die Prüfung ergab, dass das Problem grundsätzlich schon vorher existierte, jedoch aufgrund des geringen Bestellaufkommens zuvor nie zum Tragen kam. Der Fehler trat nur genau dann auf, wenn innerhalb einer Minute mehr als eine erfolgreich abgeschlossene Bestellung durchgeführt wurde. Dieser Umstand führte nach Angaben des Verantwortlichen auch dazu, dass der Fehler bei routinemäßigen Tests und auch im Produktivbetrieb des Shops bisher nicht aufgetreten war. Der Code des E-Mail-Rechnungsversands wurde verändert und der Rechnungsversand wieder aktiviert. Etwa zweieinhalb Stunden nach der Änderung wurden nach Angaben des Verantwortlichen vier weitere Rechnungsmails versendet, die jeweils nur eine korrekte Rechnung als Dateianhang hatten.

Wiederum neun Tage später wurden jedoch weitere Fälle des Fehlversands bekannt. In der Folge wurden die E-Mail-Anhänge komplett deaktiviert.

Eine Verletzung des Schutzes personenbezogener Daten lag nach Auffassung des Verantwortlichen nicht vor, da es sich bei den durch die Rechnungen offengelegten Daten um Daten eines normalen Schutzbedarfs handele, die typischerweise auch dem Telefonbuch und im Einzelnen auch anderen öffentlichen Medien zu entnehmen seien. Voraussichtlich führe die Verletzung des Schutzes personenbezogener Daten somit nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen; eine Meldepflicht habe daher nicht bestanden.

Dieser Einschätzung wurde nicht gefolgt, da weder mobile Telefonnummern noch vollständige Namen unter Angabe der Anschrift üblicherweise in Telefonbüchern vermerkt werden, sondern zumeist – wenn überhaupt ein Eintrag vorliegt – lediglich der Hausanschluss unter Anfügung eines Anfangsbuchstabens oder des Vornamens eines Familienmitgliedes, in der Regel eines Elternteils, sollte es sich um einen Familienanschluss handeln. Im Hinblick auf ein mögliches Risiko ist insbesondere zu beachten, dass tatsächlich einzelne Informationen den öffentlichen Medien zu entnehmen sind, die durch den vorliegenden Sachverhalt um Informationen ergänzt werden können. So wäre es möglich, anhand des Namens einer betroffenen Person deren Profil in den sozialen Medien aufzufinden oder durch Einspeichern der mobilen Telefonnummer ein möglicherweise bei einem Messengerdienst hinterlegtes Profilbild zu erlangen. Eine Kontaktaufnahme wäre problemlos möglich, da die Telefonnummer sowie die Anschrift durch die erfolgte Übermittlung bekannt waren. Bei Zusatzinformationen könnten diese ebenfalls genutzt werden, um etwa eine Bekanntschaft mit den in den Grußworten genannten Personen vorzugeben.

Neben der Verletzung des Schutzes personenbezogener Daten wurde die Rechtmäßigkeit der Erhebung der Telefonnummer geprüft. Hierzu teilte der Verantwortliche mit, dass diese zur Erfüllung des Vertrags erforderlich sei, da in seltenen Einzelfällen physische Gutscheine nicht aktiviert werden könnten, weil deren Barcodes nur teilweise, unvollständig oder gar nicht übermittelt wurden. Um in solchen Fällen eine schnelle Klärung herbeizuführen, könne der betroffene Kunde direkt kontaktiert und um Übermittlung des Barcodes gebeten werden, sodass eine manuelle Nachaktivierung erfolgen könne.

Diese Darstellung war als nicht schlüssig zu betrachten, da es sich bei den physischen Gutscheinen um Geschenkkarten oder -boxen handelt, die sich zu dem Zeitpunkt, zu dem ein Defekt oder das Fehlen des Barcodes bemerkt wird, üblicherweise nicht mehr im Besitz des Schenkenden befinden. Eine telefonische Kontaktaufnahme zu diesem würde eine Klärung somit nicht oder nur in seltenen Fällen ermöglichen. Zudem war nicht ersichtlich, wie dem Verantwortlichen ohne eine vorherige Kommunika-

tion durch die Person, die den Gutschein einlösen möchte, oder das Kinopersonal, das den Gutschein nicht einlösen kann, der Defekt oder das Fehlen des Barcodes zur Kenntnis gelangen könnte. Nach alldem war nicht ersichtlich, wie es zu einer ersten Kontaktaufnahme vonseiten des Unternehmens zur Lösung der beschriebenen Problematik kommen könnte.

Der Fehlversand der Anlagen zeigte auf, dass durch den Verantwortlichen keine geeigneten technischen und organisatorischen Maßnahmen getroffen worden waren, um eine angemessene Sicherheit der personenbezogenen Daten zu gewährleisten. Hierbei war insbesondere zu beanstanden, dass Korrekturen aufgrund von lediglich vermuteten Fehlerquellen erfolgten und ein geeignetes Testverfahren nicht vorhanden war, um die Wirksamkeit der ergriffenen Maßnahmen zu prüfen. Der Verantwortliche wurde diesbezüglich sowie aufgrund der Verarbeitung personenbezogener Daten ohne Rechtsgrundlage und der nicht erfolgten Meldung der Verletzung des Schutzes personenbezogener Daten verwarnt. Die Erhebung der Telefonnummern im Online-Shop wurde durch den Verantwortlichen eingestellt.

Was ist zu tun?

Getroffene technische und organisatorische Maßnahmen sind auf ihre Wirksamkeit hin zu prüfen.

5.13.2 Nichts passiert – oder doch?

Es ist der Albtraum für jedes Unternehmen: **Das IT-System wird angegriffen und verschlüsselt, zumeist unmittelbar mit der Anforderung einer Lösegeldzahlung verbunden**, die auf dem Bildschirm erscheint oder in Papierform den Drucker verlässt. Instruktionen dazu, wie das Unternehmen durch Zahlung einer bestimmten Summe eine Entschlüsselung erwirken kann, sind beigefügt, für Fragen steht in einigen Fällen sogar ein Chat-Support zur Verfügung. Da sich die Angreifer jedoch in der Regel nicht darauf verlassen wollen, dass sich das Unternehmen alleine aufgrund der Verschlüsselung auf eine Zahlung einlässt, wird **mit der Veröffentlichung von erbeuteten Daten gedroht**. Schließlich kann es sein, dass das Unternehmen so gut mit Back-ups aufgestellt ist, dass es die Forderung ignoriert – und dann wäre der betriebene Aufwand für die Erpresser umsonst, die die Angriffe schließlich als Geschäftsmodell betreiben.

Ob und in welchem Umfang tatsächlich ein Datenabfluss stattgefunden hat, ist oft nicht sicher festzustellen, da die entsprechenden Vorgänge technisch verschleiert werden. Dass auch eine intensive Untersuchung unter Hinzuziehung des Landeskriminalamtes und trotz Sichtung der von den Erpressern angegebenen Adresse, unter denen eine Veröffentlichung der erbeuteten Daten im **Darknet** erfolgen sollte, keine zuverlässige Aussage hierzu ermöglicht, zeigte sich im Fall eines im August 2021 erfolgreich angegriffenen Unternehmens. Hier war insbesondere aufgrund einer festgestellten verhältnismäßigen kurzen Zugriffsdauer davon ausgegangen worden, dass die Daten des Unternehmens nur lokal verschlüsselt wurden.

Als im Februar 2022 für ein anderes aufsichtsbehördliches Verfahren Einsicht in die Veröffentlichungsseite der Erpressergruppe im Darknet genommen wurde, stellte sich diese Einschätzung als falsch heraus. Hier wurden umfangreiche personenbezogene Daten von Beschäftigten des Unternehmens vorgefunden, darunter eine Geburtstagsliste, Kommunikation mit dem Jobcenter, Verdienstabrechnungen und eine Aufstellung der Krankheitstage. Das Auffinden der Daten erforderte dabei keine besonderen Kenntnisse oder eine gezielte Recherche; die agierende Erpressergruppe stellt die Namen der angegriffenen Unternehmen in übersichtlicher

Anordnung unter Nennung des Standorts sowie einer kurzen Beschreibung des jeweiligen Unternehmenszwecks dar, die erbeuteten Dateien sind unmittelbar über einen Link abrufbar. Der Verantwortliche wurde von der Veröffentlichung der Daten benachrichtigt und informierte seinerseits seine Beschäftigten über die neuen Erkenntnisse.

Der beschriebene Fall zeigt, dass ein Sicherheitsvorfall ernst zu nehmen ist. Auch wenn in der Folge eines erfolgreichen Angriffs keine veröffentlichten Daten vorgefunden werden, bedeutet dies nicht, dass keine Daten abgeflossen sind und keine Veröffentlichung zu einem späteren Zeitpunkt erfolgt oder die Daten für andere Zwecke genutzt werden (40. TB, Tz. 5.11.1). Insoweit war von einem hohen Risiko für die persönlichen Rechte und Freiheiten der Beschäftigten auszugehen. Dies erforderte eine ordnungsgemäße Benachrichtigung der Beschäftigten, die durch das Unternehmen nunmehr nachgeholt wurde.

Im Übrigen wird auch die Zahlung des geforderten Lösegeldes für die Entschlüsselung der Dateien keine Garantie dafür darstellen, dass erbeutete Daten vernichtet werden. Angesichts der kriminellen Energie, die durch das Vorgehen der Erpresser deutlich wird, dürfte dies nicht überraschen.

Was ist zu tun?

Eine nicht erfolgte Veröffentlichung von personenbezogenen Daten im Darknet im Zuge eines erfolgreichen Angriffs mit Verschlüsselungssoftware kann nicht dahin gehend bewertet werden, dass kein Abfluss erfolgt ist.

5.13.3 Datenpannen von nicht in der EU niedergelassenen Verantwortlichen

Auch Verantwortliche, die über keine Niederlassung in der Europäischen Union verfügen, können gemäß der Datenschutz-Grundverordnung verpflichtet sein, den EU-Aufsichtsbehörden Verletzungen des Schutzes personenbezogener Daten zu melden. Dies ist u. a. dann der Fall, wenn sie personenbezogene Daten von betroffenen Personen verarbeiten, die sich in der Europäischen Union befinden, oder wenn die Verarbeitung im Zusammenhang damit steht, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist.

Entsprechende Meldungen erfolgen jedoch nur in geringer Zahl und insbesondere aus Großbritannien – sicher zurückzuführen auf die örtliche Nähe sowie den Umstand, dass die Datenschutz-Grundverordnung dort bis zum Austritt aus der Europäischen Union Anwendung fand – und den Vereinigten Staaten von Amerika, wobei es sich hier überwiegend um größere Unternehmen handelt, die offenbar bereits zuvor über eine rechtliche Vertretung in Deutschland verfügten.

Aber auch Verantwortliche aus **Asien** kamen den gesetzlichen Vorgaben der Datenschutz-Grundverordnung nach: Im Jahr 2022 meldete ein Hotel aus Hongkong einen unrechtmäßigen Zugang zu personenbezogenen Daten von Gästen aus Deutschland durch einen IT-Vorfall, außerdem wurde eine Verletzung des Schutzes personenbezogener Daten in Form einer Offenlegung auf der Pinnwand eines Anbieters einer Spielplattform aus Shanghai gemeldet.

Unter den gemeldeten Sachverhalten befanden sich auch Verletzungen des Schutzes personenbezogener Daten, die ein hohes Risiko für die betroffenen Personen darstellten. So flossen bei einem Unternehmen aus **Großbritannien**, von

dem auch 17 Kundinnen und Kunden aus Schleswig-Holstein über den Online-Shop Waren erworben hatten, durch einen Angriff auf das Zahlungssystem Kreditkartendaten ab; die betroffenen Personen wurden über den Vorfall benachrichtigt.

Einen aktuellen politischen Hintergrund hatte ein unrechtmäßiger Zugriff auf eine Spendenplattform in den **Vereinigten Staaten von Amerika**: Hier beabsichtigten die Angreifer in Zusammenhang mit der Verschärfung des Abtreibungsrechts Spenderlisten von Abtreibungsgegnern zu erlangen, um diese im Internet zu veröffentlichen. Als ehrenamtlicher Helfer einer Entwicklungshilfeorganisation, die die Plattform für die Verwaltung ihrer Helfer nutzte, war eine Person in Schleswig-Holstein zwar nicht Ziel des Angriffs, jedoch war davon auszugehen, dass ihre personenbezogenen Daten dennoch an die Angreifer abgeflossen waren. Auch hier erfolgte eine Benachrichtigung der betroffenen Person.

Die Möglichkeiten der Landesbeauftragten für Datenschutz als Aufsichtsbehörde, ihre Aufgaben und Befugnisse außerhalb der Europäischen Union wahrzunehmen und auszuüben, sind beschränkt. Die Verantwortlichen, die Verletzungen des Schutzes personenbezogener Daten meldeten, kamen den gesetzlichen Vorgaben nach den vorliegenden Erkenntnissen jedoch bisher umfassend nach.

5.14 Videoüberwachung

5.14.1 Allgemeine Entwicklungen

Im Berichtszeitraum nahm die Anzahl von Beschwerden über Videoüberwachungsanlagen im Vergleich zum Vorjahr weiter zu. Häufig sehen die betroffenen Personen eine Kamera im öffentlichen Raum, eine Hinweisbeschilderung hingegen fehlt. Daraus resultiert für die betroffenen Personen eine gewisse Unsicherheit, da sie lediglich die Kamera wahrnehmen, nicht aber, wer diese zu welchem Zweck betreibt, ob Aufnahmen gespeichert werden und an wen sie sich mit weiteren Fragen wenden können. Die **nicht vorhandene Hinweisbeschilderung** ist daher Gegenstand vieler Beschwerden.

Ein Großteil der Beschwerden bezieht sich auf die Videoüberwachung durch Privatpersonen, oftmals im nachbarschaftlichen Kontext. Insbesondere wenn für Außenstehende nicht klar erkennbar ist, ob auch benachbarte Grundstücke oder öffentliche Flächen mit erfasst werden, wenden sich Betroffene häufig an uns. In solchen Konstellationen sind die Fronten zum Teil häufig schon so verhärtet, dass die Videoüberwachung nur einen Teilaspekt der nachbarschaftlichen Streitigkeit darstellt und ein Verweis auf den Zivilrechtsweg hilfreich sein kann.

Erfreulich ist der zu verzeichnende Anstieg an Beratungsanfragen im Vergleich zum Vorjahr. Daraus lässt sich schließen, dass Verantwortliche immer sensibler mit dem Thema Videoüberwachung umgehen und sich verstärkt über die rechtlichen Möglichkeiten informieren, bevor eine Videoüberwachungsanlage installiert wird. Dies ist dringend anzuraten, um nachträgliche Beschwerden, aber auch etwaig erforderliche kostenträchtige Änderungen an der Anlage zu vermeiden. Erste Ansprechpartnerinnen und Ansprechpartner sind hierfür die betrieblichen oder behördlichen Datenschutzbeauftragten. Als Datenschutzaufsichtsbehörde kann das ULD eine Beratung von Verantwortlichen nur eingeschränkt erbringen.

Leider zeigte sich auch im Berichtszeitraum ein Teil der Verantwortlichen wenig bis gar nicht kooperativ, selbst wenn bereits ein aufsichtsbehördliches Verfahren eingeleitet worden ist. Dies führte dazu, dass wir mehrere Verantwortliche zur Beantwortung von Fragen verpflichtet haben, die von uns im Rahmen der Sachverhaltsaufklärung gestellt wurden.

5.14.2 Videoüberwachung im Fitnessstudio – endlich abgebaut

Bei einer größeren Fitnessstudiokette konnten wir im Berichtszeitraum erreichen, dass alle Videokameras in Umkleiden, in Aufenthaltsbereichen und auf Trainingsflächen abgebaut wurden. Dieser Fall hat uns zuvor mehrere Jahre beschäftigt (u. a. 38. TB, Tz. 5.4.1, 37. TB, Tz. 5.5.6). Wir hatten die Unterlassung der Videoüberwachung in den Umkleide- und Aufenthaltsbereichen sowie auf den Trainingsflächen angeordnet. Der Verantwortliche hat gegen unsere Anordnung Klage vor dem Verwaltungsgericht in Schleswig erhoben. Als Begründung für die Videoüberwachung wurde u. a. angegeben, dass die Videoüberwachung in sämtlichen Bereichen für die Verhinderung und Verfolgung von Straftaten erforderlich sei. In der Vergangenheit sei es wiederholt zu Sachbeschädigungen und Diebstählen gekommen. Auf den Trainingsflächen und in den Aufenthaltsbereichen habe es Auseinandersetzungen mit dem Personal und unter den Kunden gegeben. Zudem sei auch in den Umkleidebereichen keine unzumutbare Beeinträchtigung der Kunden erkennbar, da einige Bereiche von der Videoüberwachung ausgenommen seien, insbesondere Duschen und WCs, und die Aufnahmen nur anlassbezogen, z. B. nach einem Aufbruch eines Spindes, eingesehen und ausgewertet werden würden. Einige der vorgetragenen Begründungen waren eher vage, andere wiederum waren konkreter. So legte der Verantwortliche auch eine Auflistung von Vorfällen vor, die sich in der Vergangenheit bereits ereignet hatten. Dazu gehörten u. a. auch Aufbrüche von Spinden sowie Auseinandersetzungen auf der Trainingsfläche.

Das Verwaltungsgericht Schleswig hat unsere Auffassung vollumfänglich bestätigt, nach der **die Videoüberwachung insbesondere in den Umkleidebereichen, aber auch auf den Trainingsflächen und in den Aufenthaltsbereichen unverhältnismäßig ist**. Die Videoüberwachung in den Umkleidebereichen berühre nach den Ausführungen des Gerichts die Intimsphäre der betroffenen Personen und sei geeignet, das Schamgefühl der Betroffenen zu verletzen. Ein solcher Eingriff könne nicht durch Sachbeschädigungen, wie z. B. Spindaufbrüche, gerechtfertigt werden. Im Bereich der Trainingsflächen sei der Eingriff zwar grundsätzlich weniger intensiv als in Umkleidebereichen, da die Sozialsphäre, nicht aber die Intimsphäre betroffen sei. Da sich die betroffenen Personen aber für einen langen Zeitraum im überwachten Bereich aufhalten und sich dem auch nicht entziehen können, entstünde ein permanenter Überwachungsdruck, sodass auch hier die schutzwürdigen Interessen der betroffenen Personen schwerer zu gewichten waren. Das Argument, dass die Aufnahmen nur im Bedarfsfall eingesehen werden, sei für die betroffenen Personen nicht ersichtlich und daher nicht geeignet, die Eingriffsintensität zu verringern. Für die Videoüberwachung des Aufenthaltsbereiches mit Sitzgelegenheiten sah das Verwaltungsgericht Schleswig ebenfalls kein berechtigtes Interesse. Hier führte es aus, dass nicht jeder Ort, an dem es einmal eine Auseinandersetzung gegeben haben mag, in der Folge überwachungsbedürftig sei.

Schleswig-Holsteinisches Verwaltungsgericht, Urteil vom 19. November 2019 – 8 A 835/17

Der Verantwortliche war mit dem Urteil nicht einverstanden und hat beim Oberverwaltungsgericht Antrag auf Zulassung der Berufung gestellt. Dieser wurde nunmehr im Berichtszeitraum abgelehnt. Daraufhin hat der Betreiber in allen seinen Studios in Deutschland vorhandene Kameras in Umkleiden, auf Trainingsflächen und in Aufenthaltsbereichen abgebaut.

Schleswig-Holsteinisches Oberverwaltungsgericht, Beschluss vom 13. Juli 2022 – 4 LA 11/20

Was ist zu tun?

Für die Betreiber von Fitnessstudios sollte die gerichtliche Bestätigung, dass die Videoüberwachung insbesondere in Umkleidebereichen, aber auch auf der Trainingsfläche und in Aufenthaltsbereichen als unzulässig angesehen wurde, ein Signal sein, genau zu prüfen, ob und in welchen Bereichen eine Videoüberwachung überhaupt rechtmäßig eingesetzt werden kann.

5.14.3 Videoüberwachung aus Fahrzeugen

Immer häufiger erreichen uns Hinweise auf fest in und an Fahrzeugen verbaute Videoüberwachungstechnik. Insbesondere (Elektro-)Fahrzeuge neueren Modells ermöglichen die **Videoüberwachung sowohl im fließenden als auch im ruhenden Verkehr**. Neben der grundlegenden Frage nach der Zulässigkeit einer solchen Datenverarbeitung ist aus datenschutzrechtlicher Sicht bei beiden Varianten besonders problematisch, dass die betroffenen Personen eine solche Videoüberwachung oftmals kaum erkennen können. Wenn die betroffenen Personen keine Kenntnis über eine Datenverarbeitung haben, können sie die Rechte, die ihnen nach der Datenschutz-Grundverordnung zustehen, nicht ausüben.

Die Videoüberwachung im fließenden Verkehr durch sogenannte **Dashcams** (im Dashboard eines Fahrzeugs verbaute Kamera) wirft einige datenschutzrechtliche Fragestellungen auf. Unzulässig ist in jedem Fall eine permanente und anlasslose Videoüberwachung des gesamten Verkehrsgeschehens. Diese Auffassung wurde auch durch den Bundesgerichtshof (BGH) bestätigt. Dieser hielt zwar die Verwertung von Aufnahmen einer Dashcam im Zivilprozess im Einzelfall für zulässig, betonte aber gleichzeitig, dass die anlasslose Anfertigung der Aufnahmen aus datenschutzrechtlicher Sicht in der Regel unzulässig sei. Die Frage der datenschutzrechtlichen Zulässigkeit und die Frage der prozessualen Verwertbarkeit sind unabhängig voneinander zu betrachten. Es liegt im Ermessen des jeweiligen Gerichts, ob unzulässig angefertigte Beweismittel in der Verhandlung zugelassen werden oder nicht.

Der BGH äußerte sich auch zu der Frage, ob und nach welchen Erwägungen der Betrieb von Dashcams im fließenden Straßenverkehr aus datenschutzrechtlicher Sicht denkbar sein könnte. Das Interesse an dem Betrieb der Dashcam könne laut BGH allenfalls dann überwiegen, wenn die Kamera bestimmte (technische) Datenschutzmechanismen aufweist, die geeignet sind, die Intensität des Eingriffs in die Grundrechte und Grundfreiheiten der betroffenen Personen auf ein vertretbares Maß zu reduzieren. Insbesondere sollte die Aufnahme nur anlassbezogen auslösen. Das bedeutet, dass eine entsprechende Sensorik vorhanden sein muss, die erst z. B. bei einer Kollision, starker Erschütterung oder starker Bremsung die Aufnahmefunktion der Kamera aktiviert. Sofern hierfür ein Pre-Recording erforderlich ist, sollte dieses in kurzen Zeitintervallen (wenige Sekunden) überschrieben werden und dem Zugriff des Verantwortlichen entzogen sein. Denkbar ist auch die effektive und nicht reversible Verpixelung von Personen sowie ein automatisiertes und dem Eingriff des Verwenders entzogenes Löschen.

Bundesgerichtshof, Urteil vom 15.05.2018 – VI ZR 233/17

Der Verantwortliche ist bei der Verarbeitung personenbezogener Daten zudem verpflichtet, die betroffenen Personen gemäß Artikel 12 ff. über die Datenverarbeitung zu informieren.

Weitere Fragestellungen wirft die Videoüberwachung aus parkenden Fahrzeugen heraus auf.

Aus den Beschwerden und Hinweisen, die uns zu diesem Thema erreichen, geht hervor, dass Fahrzeuge häufig auf öffentlichen Straßen, Parkflächen oder in Parkhäusern abgestellt werden und entweder permanent oder bei der Erkennung von Bewegung in einer bestimmen Entfernung zum Fahrzeug eine Videoaufnahme gestartet wird. Für das Auslösen der Aufnahmefunktion genügt es teilweise bereits, am Fahrzeug vorbeizugehen. Manche Hersteller ermöglichen es zudem, die Kameras in Echtzeit über das eigene Smartphone anzusteuern und die Umgebung des Fahrzeuges zu beobachten. Somit fehlt es oft schon an einem konkreten Anlass für die Verarbeitung personenbezogener Daten. Darüber hinaus wird die Umgebung ab Aktivierung der Kameras für einen zum Teil mehrere Minuten langen Zeitraum mitsamt unbeteiligter Passanten und gegebenenfalls weiterer personenbezogener Daten (wie z. B. Kfz-Kennzeichen) gefilmt und die Aufzeichnungen gespeichert.

Durch eine anlasslose, dauerhafte Aktivierung einer solchen Funktion werden die Grundrechte und Grundfreiheiten der betroffenen Personen in einem **unverhältnismäßigen Umfang** beeinträchtigt, sodass die Nutzung solcher Systeme in der beschriebenen Ausgestaltung nicht mit den Vorgaben der Datenschutz-Grundverordnung vereinbar ist.

06

KERNPUNKTE

Einsatz von KI im Landesbereich

Standard-Datenschutzmodell 3.0

Microsoft 365

E-Rezept – Datenübermittlungen an Patientinnen und Patienten?

6 Systemdatenschutz

6.1 Landesebene

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

Wie in den vergangenen Berichtszeiträumen war das ULD als Gast in der Konferenz der IT-Beauftragten (ITBK) und den Koordinierungsrunden der IT-anwendenden Behörden beteiligt und wurde dort über aktuelle und geplante IT-Projekte informiert. Anders als in den Vorjahren gab es im Berichtszeitraum weniger Einbindungen in konkrete Verfahren oder in Regelwerke, die im Rahmen der Mitbestimmung entstanden und eine landesweite Bedeutung haben.

Eine formelle Beteiligung im Rahmen von Stellungnahmen und Anhörungen zu Verordnungsentwürfen und zu Nutzungsvereinbarungen für IT-Verfahren erfolgte u. a. zur Erweiterung von Basisdiensten in der Basisdiensteverordnung.

Auch mit anderen IT-Stellen des Landes gibt es eine Zusammenarbeit, beispielsweise mit dem Amt für Informationstechnik (AIT) und im Bereich des Bildungsministeriums.

Schwerpunkte sind hier die gegenseitige Information und die Abklärung von Grundsatzfragen eines datenschutzgerechten IT-Einsatzes, insbesondere im Vorfeld der Einführung neuer Verfahren.

Basisdiensteverordnung und Zentrale-Stelle-Basisdiensteverordnung

Das Zentrale IT-Management der Landesregierung Schleswig-Holstein (ZIT SH) betreibt zentral und federführend **Basisdienste** für die Landesverwaltung und teilnehmende weitere Verwaltungen, beispielsweise zentrale Portale und Nutzerkonten im Rahmen der OSI-Plattform, Bezahlsysteme und Portale zur Entgegennahme elektronischer Rechnungen. Diese können durch die sogenannten beteiligten Stellen genutzt werden. Details dazu sind in der Basisdiensteverordnung (BasisdiensteVO) und insbesondere in deren Anlage geregelt. Diese Verordnung wird flankiert von der **Zentrale-Stelle-Basisdiensteverordnung** (ZStBaDiVO), die die datenschutzrechtlichen Verantwortlichkeiten zwischen dem ZIT SH und den beteiligten Stellen regelt, etwa zur Dokumentation, zu Umsetzung von Rechten betroffener Personen oder bei der Meldung von Datenschutzvorfällen gemäß Artikel 33 und 34 DSGVO.

Was ist zu tun?

Die frühzeitige Information und Einbindung des ULD sollte fortgesetzt bzw. wieder intensiviert werden.

6.1.2 Einsatz von KI im Landesbereich – Sachstandserhebung

Am 14. April 2022 wurde das „Gesetz über die Möglichkeit des Einsatzes von datengetriebenen Informationstechnologien bei öffentlich-rechtlicher Verwaltungstätigkeit“ (**IT-Einsatz-Gesetz – ITEG**) im Gesetz- und Verordnungsblatt für Schleswig-Holstein 2022 veröffentlicht.

Ein datengetriebener Ansatz im Zusammenhang mit automatisierten Verarbeitungstätigkeiten bedeutet zunächst allgemein, dass ein Fachverfahren Entscheidungen trifft, die auf der Analyse und Interpretation von Daten basieren. Im allgemeinen Sprachgebrauch werden diese Verfahren auch als KI-Systeme (KI: künstliche Intelligenz) bezeichnet.

Der wesentliche Grundsatz des Gesetzes betrifft die Zuverlässigkeit des Einsatzes von datengetriebenen Informationstechnologien: Jede öffentliche Stelle stellt *„… die **Transparenz**, **Beherrschbarkeit**, **Robustheit** und **Sicherheit** der von ihr eingesetzten, datengetriebenen Informationstechnologien durch geeignete technische und organisatorische Maßnahmen sicher“* (§ 2 Abs. 1 ITEG). Dabei soll die Zuordnung in die drei verschiedenen Automationsstufen

- Assistenzsysteme,
- Delegation,
- autonome Entscheidung

als Grundlage dienen, die Risiken zu beurteilen und geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit auszuwählen.

„Für den Einsatz von datengetriebenen Informationstechnologien und dessen Folgen sowie die Beachtung der Vorgaben dieses Gesetzes ist die öffentliche Stelle verantwortlich, die diese Technologien zur Erledigung der ihr übertragenen Aufgaben einsetzt“ (§ 4 Abs. 1 ITEG). Sie muss

- im Sinne der Transparenz den Algorithmus der datenbasierten Informationstechnologien und die diesem zugrunde liegende Datenbasis offenlegen (§ 6 Abs. 1),
- zur Gewährleistung der Beherrschbarkeit umso umfangreichere Maßnahmen ergreifen, je höher die Automationsstufe der datengetriebenen Informationstechnologie ist (z. B. Vorrangmöglichkeit menschlicher Entscheidungen vor automatisierten Entscheidungen und Korrektionsmöglichkeiten automatisierter Entscheidungen (§ 9 Abs. 1 ITEG)),
- die Robustheit von datengetriebenen Informationstechnologien in Bezug auf unerwünschte oder unerlaubte Veränderungen bzw. Manipulation gewährleisten (§ 10 ITEG) und
- die Sicherheit datengetriebener Informationstechnologien durch Maßnahmen sicherstellen, die dem Stand der Technik sowie dem Schutzbedarf entsprechen. Das betrifft sowohl die Datenbasis als auch die beteiligten Daten, Systeme und Prozesse (§ 6 Abs. 2 ITEG).

Verantwortliche führen ein Verzeichnis aller Verarbeitungstätigkeiten (Artikel 30 DSGVO) in ihrer Zuständigkeit. Kommen datengetriebene Informationstechnologien zum Einsatz, dann müssen die Angaben nach Artikel 30 DSGVO um **weitere Angaben** ergänzt werden, um eine ausreichende Transparenz gemäß ITEG zu erreichen. Dazu gehören z. B.

- Zuordnung der datengetriebenen Informationstechnologie zu einer Automationsstufe in einer gesonderten Erklärung,
- Offenlegung des Algorithmus von datenbasierten Informationstechnologien sowie der zugrunde liegenden Datenbasis sowie eine Beschreibung der grundsätzlichen Funktionsweise und die Entscheidungslogik des Algorithmus in einer allgemein verständlichen Sprache,
- Erstellung einer Handreichung für Betroffene, wenn Entscheidungen auf die „teilweise oder vollständige Bearbeitung und gegebenenfalls Entscheidungsfindung mittels datengetriebener Informationstechnologien“ basieren.

Ergänzend fordert § 6 Abs. 2 ITEG, dass datengetriebene Informationstechnologien, die **keine**

personenbezogenen Daten verarbeiten, ebenfalls **in einem Verzeichnis** analog zu Artikel 30 DSGVO geführt werden.

Die öffentlichen Stellen sollten weiterhin beachten, dass vor einem erstmaligen Training oder dem erstmaligen Einsatz von datengetriebenen Informationstechnologien eine **Datenschutz-Folgenabschätzung** nach Artikel 35 DSGVO (bei der Verarbeitung personenbezogener Daten) bzw. eine **Technik-Folgenabschätzung** (sofern keine personenbezogenen Daten verarbeitet werden) durchgeführt werden muss. Auch diese Folgenabschätzungen sind mit Dokumentationspflichten versehen.

Das ULD wird eine exemplarische Erhebung der Verarbeitungsverzeichnisse von datengetriebenen Informationstechnologien starten, um einen Überblick über den Einsatz von datengetriebenen Informationstechnologien in den Behörden in Schleswig-Holstein zu erhalten. Diese Erhebung soll sich (in zeitlichen Abschnitten) über alle Verwaltungsebenen erstrecken.

Das ULD wird anhand der Ergebnisse, die diese Erhebung liefert, die Verbreitung von datengetriebenen Informationstechnologien in öffentlichen Stellen in Schleswig-Holstein und deren technische und organisatorische Einbindung in die behördliche Datenverarbeitung bewerten. Dabei liegt das Hauptaugenmerk darauf, ob Betroffene ihre Rechte (Betroffenenrechte) wirksam ausüben können und inwieweit sie durch Transparenzmaßnahmen der öffentlichen Stelle über ihre Rechte informiert werden.

6.1.3 Sicherheitskonzepte mit SiKoSH

Bereits seit einigen Jahren beteiligt sich das ULD am Projekt SiKoSH des ITV.SH. Ziel dieses Projektes ist es, Kommunen und kleinere Organisationen dabei zu unterstützen, die an sie gestellten Anforderungen an Informationssicherheit umzusetzen (36. TB, Tz. 6.1).

Dazu lehnt sich das Projekt stark an die Vorgaben des IT-Grundschutzes des BSI an und fasst die für kommunale Datenverarbeitung typischen Aspekte zusammen. Ein wichtiger Aspekt im IT-Grundschutz ist die Flexibilität, Sicherheitsvorgaben für viele denkbare Situationen zu machen – je nach Größe der Organisation, ihrer Geschäftsprozesse, eingesetzter Soft- und Hardware, genutzter Dienstleister bis hin zum Steuerungs- und Organisationsmodell. Der „Preis" dieser Flexibilität ist die Verpflichtung, organisationsinterne Vorgaben mithilfe von Richtlinien, Anweisungen und Konzepten zu entwerfen und diese umzusetzen.

Dieser erste Schritt der Steuerung, nämlich der **Entwurf zentraler Dokumente**, fällt schwer, wenn man bislang noch gar nicht mit dem Thema befasst war. Andererseits gibt es im kommunalen Bereich häufig vergleichbare Situationen hinsichtlich der internen Organisation und Zuständigkeiten, der IT-Ausstattung und der eingesetzten Soft- und Hardware. Daher liegt es nahe, sich bei dem Entwurf solcher Dokumente an Vorlagen zu orientieren und bei guten Vorlagen „abzugucken".

An dieser Stelle setzt SiKoSH mit der **Bereitstellung von Musterdokumenten** an. Zwar müssen sie an die jeweilige Situation vor Ort angepasst werden, geben aber ein gutes Gerüst vor und haben viele Aspekte integriert – dies ist für diejenigen wichtig, die bisher nur wenig Kontakt zum IT-Grundschutz hatten.

Ein zweiter Aspekt ist eine **Priorisierung von Sicherheitsmaßnahmen**: In der Theorie kann man nicht genug davon haben, um auf alle denkbaren Fälle vorbereitet zu sein. In der Praxis konzentriert man sich auf die relevanten Maßnahmen, um das Risiko eines Sicherheitsvorfalls auf ein akzeptables Maß zu reduzieren. Ebenso ist es häufig notwendig, bei der Umsetzung zu priorisieren: Beispielsweise ist es aus Sicherheitssicht zwar wichtig, dass in einem Zutrittskontrollsystem auch das Betriebssystem der Chipkarten gegen Hackerangriffe geschützt sind – doch solange Türen und Fenster unverschlossen sind, liegt in diesem Punkt eine größere Gefahr, dass Unbefugte ein Gebäude oder IT-Räume betreten.

SiKoSH

SiKoSH (Sicherheit für Kommunen in Schleswig-Holstein) ist ein Projekt, um Kommunen und kleineren Organisation beim Aufbau eines Informationssicherheitsmanagements zu unterstützen.

ITV.SH

Der IT-Verbund Schleswig-Holstein (ITV.SH) wird von den Kommunen des Landes Schleswig-Holstein getragen. Seine Aufgaben sind u. a., verwaltungsübergreifende Projekte zu realisieren.

BSI

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

Für vergleichbare Situationen und IT-Strukturen gibt es im IT-Grundschutz die Möglichkeit, Maßnahmenbündel in sogenannten Profilen zusammenzufassen und hierbei Prioritäten vorzugeben. Ziel ist dabei, konzeptionelle Arbeiten „vor die Klammer zu ziehen" und die Ergebnisse auch anderen Organisationen zur Verfügung zu stellen. Zusätzliche Sicherheitsmaßnahmen sind immer möglich.

Das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung" ist hier abrufbar:

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

Kurzlink: *https://uldsh.de/tb41-6-1-3*

Das ULD beteiligt sich an dem Projekt SiKoSH, um die Sicherheitsanforderungen des Datenschutzes (u. a. Vorgaben aus dem Artikel 32 DSGVO) und spezifische Dokumentationsvorgaben (z. B. zu Test und Freigabe) mit einfließen zu lassen. Dies ist bei der Sicherheitsanforderung auf der Ebene der Infrastruktur und der zentralen Konzepte (z. B. dem Pachtmanagement) vergleichsweise einfach. Werden die Anforderungen jedoch spezifischer (etwa bei der Umsetzung in Fachverfahrenssoftware) oder umfassen sie Aspekte, die die Informationssicherheit (zunächst) nicht im Fokus hat (etwa Pseudonymisierung, Datensparsamkeit, Löschfristen oder Funktionalitäten zur Umsetzung vor den Rechten Betroffener gemäß Artikel 12-23 DSGVO), so müssen diese Anforderungen zusätzlich betrachtet werden.

Da das prinzipielle Vorgehen (Analyse, Risikobetrachtung, Maßnahmenauswahl, Implementierung und Kontrolle) im Bereich Datenschutz große Ähnlichkeiten zum Vorgehen im Informationssicherheitsmanagement hat, liegt der Gedanke nahe, beide Vorgehensweisen zu integrieren – bis dahin, eine Person mit beiden Aufgaben (Informationssicherheitsbeauftragte und Datenschutzbeauftragte) zu betrauen.

In größeren Organisationen ist Letzteres nicht zu empfehlen: Zum einen gibt es genügend Aufgaben für mehrere Personen. Zum anderen gibt es teilweise gegenläufige Interessen zwischen Datenschutz und Informationssicherheit, etwa im Bereich der Protokollierung oder des Beschäftigtendatenschutzes, die gegeneinander abzuwägen sind. Hierbei ist eine unabhängige Sicht wichtig – eine konstruktive Zusammenarbeit und die Nutzung von Synergien, etwa bei der Dokumentation, sind hingegen ausdrücklich gewünscht.

Das Ziel der Beauftragung mehrerer Personen lässt sich in kleineren Organisationseinheiten nicht immer umsetzen. Während die Beauftragungen einer oder eines Datenschutzbeauftragten in Behörden gesetzliche Pflicht ist, ist dies bei Informationssicherheitsbeauftragten meist nicht der Fall. Wenn die Alternative darin besteht, keine Person mit der Bearbeitung von Informationssicherheitsfragen zu betrauen, ist eine Doppelbeauftragung die sinnvollere Alternative.

Was ist zu tun?

Das Thema Informationssicherheit ist auch für den Datenschutz wichtig. Mit SiKoSH ist insbesondere für kleinere Organisationen ein Einstieg in dieses Thema möglich.

6.1.4 Arbeitskreis IT der Rechnungsprüfungsämter

Schon seit vielen Jahren beteiligt sich das ULD, wie auch der Landesrechnungshof, am „Arbeitskreis IT der Rechnungsprüfungsämter der Kreise und der Städte Schleswig-Holsteins".

Beschäftigte der Rechnungsprüfungsämter sind auch mit dem Thema IT-Prüfung befasst. Meist liegt der Fokus im Bereich der Beschaffung und Vergabe. Bei der IT-Prüfung geht es auch um den ordnungsgemäßen Einsatz von IT. Dies schließt neben weiteren Vorgaben auch Fragen des Datenschutzes sowie der Informationssicherheit (auch jenseits der Verarbeitung personenbezogener Daten) ein. Daher sind die IT-Prüferinnen und Prüfer an den Vorgaben und Prüfmaßstäben interessiert, die die Datenschutzaufsichtsbehörde und der Landesrechnungshof anwenden.

Innerhalb der Kreise und der Städte arbeiten Rechnungsprüfungsamt und Datenschutzbeauftragte meist eng zusammen und sind teilweise in Personalunion tätig – auch dies erklärt das Interesse des Arbeitskreises am Thema Datenschutz. So werden bei den halbjährlichen Treffen des Arbeitskreises häufig auch Detailfragen an uns herangetragen. Diese Treffen sind daher eine gute Gelegenheit, diese zu beantworten, miteinander ins Gespräch zu kommen, Informationen auszutauschen und auch aus übergeordneten Gremien zu berichten.

Für den Arbeitskreis bietet sich die Gelegenheit, zusammen tätig zu werden und lokale Prüfungen und Sachstandserhebungen gemeinsam zu entwerfen und auszuwerten. Dabei kann die Arbeitslast der Konzeption auf mehrere Schultern verteilt und Doppelarbeit vermieden werden. Für das ULD ist wichtig, dass die behördlichen Datenschutzbeauftragten an den Ergebnissen teilhaben, soweit es Datenschutzaspekte betrifft. Es spricht auch nichts gegen ihre Mitwirkung bei der Prüfungsgestaltung.

Was ist zu tun?

Die bisherige gute Zusammenarbeit sollte fortgesetzt und für Synergien genutzt werden.

6.2 Deutschlandweite und internationale Zusammenarbeit der Datenschutzbeauftragten

6.2.1 Neues aus dem AK Technik

Der AK Technik ist der Arbeitskreis der Datenschutzaufsichtsbehörden des Bundes und der Länder, der sich mit technischen Fragestellungen beschäftigt. Ihm gehören zusätzlich als Gäste u. a. auch Vertreter des Datenschutzes aus den Bereichen Kirchen und Rundfunk an; daneben

gibt es Kontakte in das deutschsprachige Ausland.

Ein wichtiges Thema des Arbeitskreises ist das Standard-Datenschutzmodell (SDM), das in einer Unterarbeitsgruppe entwickelt wird (Tz. 6.2.2). Der AK Technik ist hier die erste Freigabeinstanz. Die weitere Arbeit des Arbeitskreises war im Berichtszeitraum stärker als sonst von der Zuarbeit zu Dokumenten anderer Arbeitskreise geprägt.

Dies betrifft zunehmend auch Dokumente auf europäischer Ebene: In der europäischen **Technology Subgroup**, einer Arbeitsgruppe des **Europäischen Datenschutzausschusses (EDSA)** zu Technikaspekten, gibt es Vertretungen einzelner EU-Staaten, so auch aus einzelnen Aufsichtsbehörden in Deutschland. Deren Aufgabe ist es, die Sicht der deutschen Aufsichtsbehörden in Europa zu vertreten und umgekehrt die europäische Sicht nach Deutschland zu transportieren. Auf fachlicher Ebene erfolgt dies im AK Technik, der hier wie ein Spiegelgremium agiert.

Im Berichtszeitraum wurden insbesondere Dokumentenentwürfe zu Pseudonymisierung und Anonymisierung diskutiert; ein wichtiges Dokument des Vorjahres waren Leitlinien zu Datenpannenmeldungen gemäß Artikel 33 DSGVO. Die Arbeit ist besonders wichtig, wenn es sich bei den Dokumenten um sogenannte **Leitlinien** des EDSA handelt: Diese dienen der europaweiten einheitlichen Interpretation der DSGVO und anderer europäischer Datenschutzregelungen und wirken einerseits als Orientierungshilfen nach außen, entfalten aber im Hinblick auf die Datenschutzbehörden eine gewisse Bindungswirkung. Daher ist eine sorgfältige Formulierung und Betrachtung der zahlreichen nationalstaatlichen Besonderheiten wichtig, denn das Autorenteam auf europäischer Ebene deckt nicht alle Staaten ab.

6.2.2 Standard-Datenschutzmodell 3.0

Das Standard-Datenschutzmodell (SDM) wurde unter der Leitung des ULD überarbeitet. Die Überarbeitung war notwendig, um der zentralen Stellung von „Verarbeitung" und „Risiken" in der DSGVO besser als bislang gerecht zu werden. Die wesentlichen Modellkomponenten wurden in der Grafik **„SDM-Würfel"** zusammengezogen mit dem Ziel, auf einen Blick alle wesentlichen Risiken einer Verarbeitung zu erfassen und diese analysieren zu können.

Der neu erstellte Abschnitt D2.1 „Aufbereitung einer Verarbeitungstätigkeit in Vorgänge oder in Phasen eines Datenlebenszyklus" empfiehlt, bei Verarbeitungen mit hohem Risiko zumindest neun Vorgänge zu unterscheiden. Für weniger riskante Verarbeitungen kann dagegen die Unterscheidung in vier unterschiedliche Phasen des Lebenszyklus eines Datums – von der Kollektion der Daten über deren Bereithaltung, deren Nutzung und Beseitigung – ausreichen. Die Darstellung einer Verarbeitung in Vorgänge oder Phasen stellt vor Augen, dass bei der Erhebung von Daten z. B. andere Risiken bei der Sicherung der Vertraulichkeit als bei der Nutzung oder der Beseitigung von Daten bestehen und entsprechend abgestimmte Schutzmaßnahmen bestimmt und implementiert werden müssen. Die Auffächerung legt außerdem den Gedanken nahe zu prüfen, ob die bestehenden Rechtsgrundlagen alle Vorgänge bzw. die vier Phasen jeweils ausreichend abdecken.

Der Abschnitt D2.2 „Ebenen einer Verarbeitung oder Verarbeitungstätigkeit" verweist darauf, bei einer Verarbeitung außerdem noch drei Ebenen einer Verarbeitung zu unterscheiden. Dadurch geraten ebenenspezifische Risiken in den Blick. Die Ebene 1 entspricht dem, was abstrakt unter einem „Fachverfahren" und „Geschäftsprozess" mit einem bestimmten funktionalen Ablauf verstanden wird. Das ist die Ebene, in der die Logik einer Verarbeitung im Zentrum der Betrachtung steht, ohne dass auch schon die dafür verwendete Technik beachtet werden muss. Wesentlich für die datenschutzrechtlich angemessen funktionale Gestaltung dieser Ebene ist die Bestimmung des Zwecks einer Verarbeitungstätigkeit, dessen Bindung auf den beiden nachfolgenden Ebenen sichergestellt werden muss.

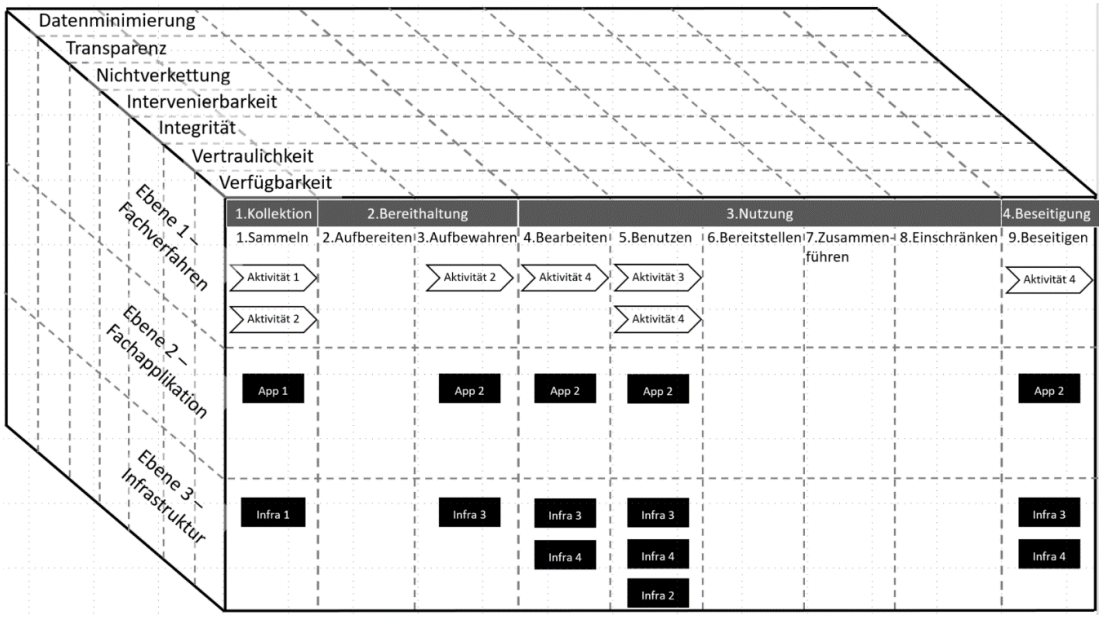


Abbildung: „SDM-Würfel“

Auf der Ebene 2 ist die zweckgemäße praktische Umsetzung der Verarbeitung angesiedelt. Diese umfasst zum einen die Sachbearbeitung sowie die Fachapplikation(en). Ebene 3 umfasst die IT-Infrastruktur, die Funktionen für die IT der Ebene 2, typisch in Form von Rechenzentrumsdiensten, zur Verfügung stellt.

Der ebenfalls neu erstellte Abschnitt D2.5 „Überblick über die Modellierungstechniken des SDM („SDM-Würfel“)“ stellt die neun Verarbeitungsvorgänge bzw. vier -phasen, die drei Ebenen und die sieben Gewährleistungsziele des SDM in einen grafischen Zusammenhang. Jeder kleine Würfel aus dem Gesamtwürfel steht für ein aus der DSGVO abgeleitetes Risiko für die Rechte und Freiheiten einer Person, das bei einer Verarbeitung zu betrachten und grundsätzlich zu verringern ist. Der „SDM-Würfel“ entwirft insofern ein sinnvolles Gesamtbild der zu bearbeitenden Datenschutzrisiken von Verarbeitungstätigkeiten (siehe „SDM-Würfel“).

Das bereits in der Version SDM-V2 enthaltene Kapitel D3 „Risiken und Schutzbedarf“ wurde um eine Risikotypologie erweitert, wonach vier Risikotypen zu unterscheiden sind. Diese Typologie ist wortgleich im Abschnitt „CON.2 – Datenschutz“ des IT-Grundschutz-Kompendiums 2023 des BSI (Bundesamt für Sicherheit in der Informationstechnik) enthalten. Es ist mit dem BSI abgesprochen, dass IT-Grundschutz und SDM bei gegenseitigen Verweisen explizit auf einen gemeinsamen Anker für das Verständnis von Datenschutzrisiken zurückgreifen können.

Vier Risikotypen im Datenschutz

Risikotyp A: Der Grundrechtseingriff bei natürlichen Personen durch die Verarbeitung ist nicht hinreichend milde gestaltet.

Risikotyp B: Die Maßnahmen zur Verringerung der Eingriffsintensität einer Verarbeitung sind in Bezug auf die Gewährleistungsziele nicht vollständig oder werden nicht hinreichend wirksam betrieben oder nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.

Risikotyp C: Die Maßnahmen, die nach der Informationssicherheit geboten sind (vgl. z. B. IT-Grundschutz nach BSI), sind nicht vollständig oder werden nicht hinreichend wirksam betrieben oder werden nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.

Risikotyp D: Die Maßnahmen der Informationssicherheit werden nicht ausreichend datenschutzgerecht im Sinne des Risikotyps A und Risikotyps B betrieben.

6.2.3 Microsoft 365 – aktuelle Entwicklungen der Arbeitsgruppe

Im Herbst 2020 wurde eine Arbeitsgruppe der Datenschutzkonferenz (DSK) mit dem Auftrag eingesetzt, im Austausch mit Vertreterinnen und Vertretern von Microsoft die Vertragsunterlagen für den Einsatz von Microsoft 365 zu prüfen und datenschutzgerechte Nachbesserungen zu erreichen. Diskutiert und am Ende bewertet wurde insbesondere der Datenschutznachtrag, zuletzt in der Aktualisierung vom 15. September 2022. Durch die notwendige Eingrenzung erfolgten keine technischen Untersuchungen über tatsächliche Datenflüsse, keine Untersuchungen über die tatsächlichen Verarbeitungen, keine Prüfung von Einzelkomponenten sowie keine vollständige datenschutzrechtliche Bewertung des Dienstes anhand des gesamten Vertragswerks von Microsoft.

Bereits mit diesem engen Fokus konnte die DSK jedoch unter Bezugnahme auf den Bericht der Arbeitsgruppe feststellen, „dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten ‚Datenschutznachtrags vom 15. September 2022' nicht geführt werden kann". Besonders herausgehoben wurde die mangelnde Transparenz über die Verarbeitung von personenbezogenen Daten und dass Microsoft Daten zu eigenen Zwecken verwendet, die nicht klar beschrieben und eingegrenzt sind.

Microsoft 365

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

Die Arbeitsgruppe hat in zwei Jahren gemeinsamer Arbeit und intensivem Austausch mit Ansprechpartnerinnen und Ansprechpartnern der Microsoft Deutschland GmbH sowie der Microsoft Corporation in 14 mehrstündigen Videokonferenzen diverse Fragestellungen diskutiert, die sich aus einer Bewertung des AK Verwaltung der DSK im Jahr 2020 und aus den gemeinsamen Gesprächen ergeben haben.

Festlegung der DSK und Berichte der Arbeitsgruppe

Die Arbeitsgruppe hat einen umfangreichen Bericht über die Untersuchungen erstellt und der DSK vorgelegt. Die beschlossene Festlegung der DSK wurde zusammen mit einer Zusammenfassung des Berichts veröffentlicht.

Festlegung der DSK:
https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf

Kurzlink: *https://uldsh.de/tb41-6-2-3a*

Zusammenfassung des Berichts:
https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf

Kurzlink: *https://uldsh.de/tb41-6-2-3b*

Kurzlink zum freigegebenen Gesamtbericht:

https://uldsh.de/tb41-6-2-3c

In mehreren Themenbereichen konnten keine signifikanten Verbesserungen erreicht werden, beispielsweise bei der Festlegung von Art und Zwecken der Verarbeitung sowie der Art der personenbezogenen Daten, sodass der Gegenstand der Auftragsverarbeitung noch nicht spezifisch und detailliert genug beschrieben ist. Ähnlich fehlen bei der Verarbeitung „für legitime Geschäftsinteressen" von Microsoft noch klare vertragliche Grenzen und mehr Informationen darüber, welche Daten Microsoft zu welchen Geschäftszwecken verarbeitet. Gleiches gilt für

Telemetrie- und Diagnosedaten, deren Nutzung für eigene Zwecke von Microsoft ebenfalls unklar bleibt.

Demgegenüber konnten durch die Gespräche Verbesserungen bei der Information von Verantwortlichen über Unterauftragsverarbeiter erreicht werden. Auch die Verlagerung der Datenverarbeitung in die EU wird grundsätzlich begrüßt. Weitere Schritte sind aber notwendig, damit Verantwortliche mit geringerem Aufwand Microsoft 365 auch wirklich datenschutzkonform einsetzen können.

Was ist zu tun?

Verantwortliche müssen den Einsatz von Microsoft 365 eigenständig prüfen und nachweisen können, dass ihre Verarbeitungsprozesse datenschutzkonform sind. Dieser Nachweis kann nicht allein mithilfe der Unterlagen von Microsoft erbracht werden. In den Berichten der DSK werden zum Teil Möglichkeiten aufgezeigt, die allerdings kundenspezifische vertragliche Konkretisierungen erfordern.

6.2.4 Taskforce Souveräne Cloud

Schon seit vielen Jahren nimmt die Nutzung von Cloud-Dienstleistungen zu. Nutzen Verantwortliche oder Auftragsverarbeiter solche Dienstleistungen, so geben sie einen großen Teil der Aufgaben ab, die zum Betrieb einer technischen Infrastruktur notwendig sind. Gleichzeitig fallen damit Steuerungsmöglichkeiten weg.

Dieser Effekt steigt mit der Spezialisierung der Cloud-Dienstleistung: Können Cloud-Anwendende bei der Nutzung einer technischen Infrastruktur („Infrastructure as a Service", beispielsweise Hardware und Netzanbindung) noch weitgehend selbst über Betriebssysteme, Datenbanken und Anwendungssoftware bestimmen, ist dies am anderen Ende des Spektrums bei der Nutzung bereitgestellter Software („Software as a Service") nur sehr eingeschränkt möglich: Hier geben die Cloud-Anbieter die Software bis hin zur eingesetzten Version vor; Änderungen und Anpassungen sind nur soweit möglich, wie die Konfiguration der angebotenen Software dies zulässt. Darüber entscheidet allein der Cloud-Anbieter.

Diese Erkenntnis ist nicht neu, und bei der privaten Nutzung von Cloud-Diensten haben die meisten Nutzenden solche Einschränkungen schon kennengelernt, besonders bei der Nutzung von Apps. Dies kann auch Datenschutzfragen betreffen, etwa beim Einsatz von Tracking-Tools oder bei der Einbindung von Drittanbietern. Je nach Ausmaß der Änderung und Alternativen reicht die Reaktion dann von Verärgerung bis zum Entschluss, die Apps zu löschen oder durch andere auszutauschen.

Digitale Souveränität

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

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

Für Verantwortliche und Auftragsverarbeiter ist ein solcher Wechsel meist nicht ganz so einfach umsetzbar. An dieser Stelle setzen Projekte an, die sich die **digitale Souveränität** auf die Fahne geschrieben haben und eine selbstständige,

selbstbestimmte und sichere Nutzung der digitalen Welt anstreben. Dies umfasst u. a., dass solche Angebotswechsel aus technischer und rechtlicher Sicht möglich sind. Es bedeutet aber auch, dass Anbieter von Cloud-Dienstleistungen ihrerseits souverän agieren können. Dies schließt auch Fragen der Gesetzgebung ein, denen sie unterliegen – ein ständiger Diskussionspunkt bei Angeboten außerhalb der EU.

Die Taskforce „Souveräne Cloud" der Datenschutzkonferenz arbeitet derzeit an einem Positionspapier, das diese Fragen aufgreift und als Anforderungen formuliert. Der Blick ist dabei bewusst etwas weiter gefasst als die Frage der aktuellen Einhaltung der Datenschutzregelungen (insbesondere der DSGVO) und beinhaltet auch Aspekte wie

- Nachvollziehbarkeit durch Transparenz,
- Datenhoheit und Kontrollierbarkeit,
- Offenheit,
- Vorhersehbarkeit und Verlässlichkeit,
- geeignete Garantien zum Nachweis der aufgestellten Forderungen.

Ziel ist es, sowohl Cloud-Anwendenden (z. B. Verantwortlichen) als auch Cloud-Anbietern Prüfpunkte für Souveränitätseigenschaften an die Hand zu geben, damit „souveräne Cloud" nicht nur ein Marketingbegriff ist.

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

6.3.1 E-Rezept – Datenübermittlungen an Patientinnen und Patienten?

Schleswig-Holstein ist neben Westfalen-Lippe eine der Regionen, in denen das elektronische Rezept (E-Rezept) für Versicherte gesetzlicher Krankenkassen praktisch erprobt wird.

Dabei soll der klassische Weg eines Papierrezeptes nachgebildet werden: die Ausstellung in Arztpraxen und die Einlösung durch die Patientinnen und Patienten in einer Apotheke ihrer Wahl. In der Papierwelt ist dies für Arztpraxen vergleichsweise einfach: Rezepte werden auf Papier ausgedruckt und übergeben. Sie enthalten Daten der Patientin oder des Patienten sowie der verordneten Arzneimittel und werden in Apotheken vorgelegt. Im Gegenzug werden die verordneten Arzneimittel ausgegeben; die Apotheken behalten das Rezept und rechnen dann mit der jeweiligen Krankenkasse ab.

E-Rezepte sind technisch gesehen Datensätze, mit dem genau dies ermöglicht werden soll. Anders als Papierrezepte können und sollen sie auch elektronisch übertragen werden. Auf diese Weise kann mancher Gang in die Arztpraxis oder die Apotheke entfallen, und auch die Weitergabe an Angehörige zur Abholung eines Medikamentes wäre einfacher.

Ein Datensatz könnte aber auch kopiert werden, um ihn mehrfach in Apotheken einzulösen. Was in der Papierwelt durch Aufdruck, Stempel, Entwertung und Einbehalten des Rezeptes in der Apotheke erfolgt, muss in der elektronischen Welt nachgebildet werden. Deswegen ist die technische Umsetzung aufwendiger: Arztpraxen erzeugen einen Verordnungsdatensatz (mit Patienten- und Arzneimitteldaten) und legen ihn in einer zentralen Datenbank ab. Patientinnen und Patienten bekommen anstelle des Rezeptes einen sogenannten **Token** (ein kleiner Datensatz vergleichbar einer Postfach- oder Schließfachnummer), mit dessen Hilfe die Verordnungsdaten aus der Datenbank abgerufen werden können. Der Token wird an die Apotheke übergeben, die den Verordnungsdatensatz aus der Datenbank abruft und bearbeitet – in diesem Augenblick wird der Datensatz gesperrt und eine Doppeleinlösung unterbunden. Ist ein Arzneimittel nicht vorrätig, muss der Datensatz wieder entsperrt werden, damit das Rezept bzw. der Token in einer anderen Apotheke eingelöst werden kann.

Der Zugriff auf die Datenbank ist abgesichert und liegt in der sogenannten **Telematikinfrastruktur**, an die Arztpraxen, Krankenhäuser und Apotheken über besonders gesicherte Netze angebunden sind. Über die Telematikinfrastruktur und die darin abgebildeten Fachanwendungen werden dann Zugriffsberechtigungen umgesetzt. Im Fall der Apotheken bedeutet dies, dass technisch ein Zugriff auf alle aktuellen elektronischen Verordnungen möglich ist, sofern der entsprechende Token vorliegt.

Telematikinfrastruktur (TI)

Die Telematikinfrastruktur (TI) ist die zentrale Plattform für digitale Anwendungen im deutschen Gesundheitswesen.

Patientinnen und Patienten können auch an die Telematikinfrastruktur angebunden werden, um darüber beispielsweise Zugang zur geplanten elektronischen Patientenakte und auch zu ihren E-Rezepten zu bekommen, um diese (genauer: die dazugehörigen Token) einer Apotheke vorlegen zu können. Da Versicherte erst einmal zuverlässig durch ihre Krankenkasse identifiziert und mit verlässlicher Software angebunden werden müssen (vergleichbar einer Zulassung im Online-Banking), ist diese Anbindung bei Patientinnen und Patienten derzeit nicht weit verbreitet.

Wie sollen Patientinnen und Patienten nun E-Rezepte bekommen und an Apotheken übertragen, wenn sie nicht über die sichere Anbindung verfügen? Eine Möglichkeit ist ein Papierausdruck ähnlich dem klassischen Rezept, der den Token in Form eines DataMatrix-Codes (ähnlich wie ein QR-Code) enthält. Dieser wird in Apotheken bei der Vorlage des Rezeptes eingescannt und erlaubt dann den Apotheken den oben beschriebenen Abruf der elektronischen Verordnung aus der Telematikinfrastruktur und seine Weiterverarbeitung.

Verständlicherweise ist ein Papierausdruck nicht die Vorstellung, die man von einem elektronischen Rezept und der Möglichkeit, es auch elektronisch zu übertragen, hat. Daher wurde die Idee geboren, den Token an Patientinnen und Patienten per E-Mail zu übertragen. Diese E-Mail kann dann, beispielsweise auf einem Smartphone, in Apotheken vorgelegt und der enthaltene **DataMatrix-Code** eingescannt werden.

An das ULD wurde nun im Sommer 2022 von der Kassenärztlichen Vereinigung (KVSH) die Frage herangetragen, ob der Versand der Token per E-Mail datenschutzrechtlich unproblematisch sei – er enthalte ja nicht die Daten der Verordnung (Patientendaten und Arzneimittel), sondern sei lediglich ein Zugriffsschlüssel, mit dem Teilnehmende an der Telematikinfrastruktur, also insbesondere Apotheken, die Verordnungsdaten abrufen könnten. Werde eine solche E-Mail abgefangen oder kopiert, könnten Unbefugte mit dem Token die Rezeptdaten nicht abrufen, da sie keinen Zugriff auf die Telematikinfrastruktur haben. Der Versand des Tokens per E-Mail sei folglich unproblematisch. Anders wäre es, den kompletten E-Rezept-Ausdruck (mit DataMatrix-Code, Versicherten- und Verordnungsdaten) zu versenden, etwa als PDF-Datei: Hier lägen die Daten im Klartext vor – ein Versand des Komplettausdrucks sei unverschlüsselt nicht möglich.

Dieses Argument scheint schlüssig, lässt aber bestimmte Funktionalitäten aufseiten der Apotheken außer Acht: Einige von ihnen bieten Patientinnen und Patienten, beispielsweise über **Apotheken-Apps**, die Möglichkeit, E-Rezepte einzulösen. Dazu muss der Token des E-Rezeptes an die Apotheke übermittelt werden (z. B. durch Einscannen des DataMatrix-Codes), die dann die Verordnung aus der Telematikinfrastruktur abruft, die Warenverfügbarkeit prüft und Verfügbarkeit und Arzneimittel in der App anzeigt. Vor dieser Anzeige findet aber keine verlässliche Identitätsprüfung statt – im Prinzip können auf diese Weise alle (auch abgefangene oder kopierte) Token mithilfe der App eingescannt und die Arzneimittel der zugeordneten Verordnung sichtbar gemacht werden.

Im Ergebnis ist ein Token ebenso sprechend wie ein Rezept oder ein E-Rezept-Ausdruck, und daher ebenso sensibel. Die Sicherheitsannahme, dass ausschließlich Apotheken die Verordnung zu einem Token auslesen können, ist durch die Bereitstellung der Apotheken-Apps nicht mehr tragfähig. Von einer unverschlüsselten Versendung per E-Mail hat das ULD daher abgeraten.

Unabhängig von der Tatsache, dass das E-Rezept zumindest mit Papierausdrucken und der Nutzung der (wenig verbreiteten) Patienten-App pilotiert werden könnte, hat die KVSH die Teilnahme am E-Rezept-Pilotversuch vorerst gestoppt.

Gematik

Die Gematik ist die Nationale Agentur für Digitale Medizin. Als Koordinierungsstelle für Interoperabilität setzt sie Standards und trägt die Gesamtverantwortung für die Telematikinfrastruktur (TI), betreibt sie aber technisch nicht selbst.

Die **Gematik** arbeitet derzeit an einer Spezifikation, mit der Apotheken nur anhand von Daten der Versichertenkarte, die bei einer Abholung vorgelegt werden müsste, die Verordnungsdaten abrufen – sozusagen die Versichertenkarte als Ausweis. Aber auch hier stellen sich Fragen, die in der Papierwelt einfach zu beantworten sind: Wie können Patientinnen und Patienten, die zeitgleich mehrere Verordnungen bekommen haben, entscheiden, welche Verordnung durch welche Apotheke abgerufen werden kann? Dies kann durchaus eine Rolle spielen, wenn Verordnungen bei verschiedenen Apotheken oder auch gar nicht eingelöst werden sollen. Und ist sichergestellt, dass Daten aus den Versichertenkarten nicht unbefugt gespeichert und für weitere Abrufe ohne Wissen und Wollen der Versicherten genutzt werden?

Zusammenfassend lässt sich feststellen, dass es zahlreiche Detailprobleme gibt, aber auch widerstreitende Interessen: Aus medizinischer Sicht wird eine Gesamtschau auf Gesundheitsdaten präferiert mit der Folge, dass Ärztinnen und Ärzte sowie Apotheken einen Überblick haben, welche Krankheiten mit welchen Medikamenten behandelt werden. Aus Sicht der Patientinnen und Patienten ist häufig eine Selbstbestimmung gewünscht mit der Folge, dass über die Weitergabe von Verordnungsdaten an Apotheken individuell entschieden werden kann. Dies erfordert eine Steuerungsmöglichkeit, deren sichere Umsetzung in der elektronischen Welt deutlich komplexer ist als die Ausgabe eines Stück Papiers. Ebenso erfordert die Möglichkeit, dass Rezepte ohne persönliche Anwesenheit ausgestellt werden sollen (Telemedizin), an Versicherte übertragen werden und von ihnen auch ohne Vorsprache eingelöst werden können (Versandapotheken), entsprechend sichere Kommunikationswege.

All dies betrifft aber nicht nur Schleswig-Holstein, sondern alle Bundesländer. Die Regelungen gelten bundesweit, denn die Spezifikation erfolgt durch die Gematik aufgrund einer Bundesgesetzgebung. Daher gibt es einen engen Austausch mit den anderen Datenschutzaufsichtsbehörden.

Das im Rahmen der Beratung der KVSH versandte Schreiben des ULD vom 19. August 2022, die daraufhin veröffentlichte Presseerklärung der KVSH vom 22. August 2022 sowie die Presseerklärung des ULD vom 23. August 2022 mit weiteren Hinweisen sind unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/artikel/1414-1.html

Kurzlink: *https://uldsh.de/tb41-3-6-1*

Was ist zu tun?

Bei der Digitalisierung von Prozessen im Gesundheitswesen müssen alle Beteiligten mit ihren Bedürfnissen berücksichtigt werden. Eine Sicherheitsbetrachtung muss übergreifend erfolgen und kann sich nicht auf Sicherheitsannahmen, die für einzelne Verarbeitungsschritte isoliert gelten, verlassen. Wegen der großen Anzahl der Beteiligten (Versicherte, Ärztinnen und Ärzte, Apotheken und andere Leistungserbringer) ist auch damit zu rechnen, dass einzelne Sicherheitsmaßnahmen nicht immer vollständig umgesetzt werden – dies zeigen die Datenpannenmeldungen, die uns vorliegen.

6.3.2 Datenpannen im nichtöffentlichen Bereich – alles beim Alten

Im Berichtsjahr 2022 sind aus technischer Sicht keine Schwerpunktverschiebungen der Ereignisse und Vorfälle im Rahmen der Meldungen von Verletzungen des Schutzes personenbezogener Daten (Artikel 33 DSGVO) zu erkennen. Abgesehen von der im Jahr 2021 hervorstechenden Angriffswelle auf die Microsoft-Exchange-Server durch die Hafnium-Hackergruppe verteilen sich die anderen Ursachen der Datenschutzvorfälle nach Artikel 33 DSGVO ähnlich zu diesem Jahr. Die größten Einfallstore zur Erlangung eines nicht autorisierten Zugriffs auf personenbezogene Daten stellen weiterhin **Phishing-Attacken und nicht zeitnah geschlossene Sicherheitslücken** dar. Die häufig in den Medien dargestellten Erpressungsversuche durch Verschlüsselung von Daten mittels sogenannter **Ransomware** (Tz. 5.13.2) stellen zumeist nur den letzten Schritt eines Angriffs dar, der mit dem Einstieg durch eines der beiden genannten Einfallstore seinen Ursprung hatte.

Da die Qualität der **Phishing-E-Mails** und auch der **Fake-Webseiten**, auf welche die Opfer gelenkt werden, immer besser wird, fallen auch weiterhin viele Menschen darauf rein. Die Bandbreite der von den Angreifern begehrten Zugangsdaten reicht dabei von Postfächern, Online-Banking, Bezahldiensten, Office-Cloud-Diensten und Streaming-Diensten bis zu Verkaufsshops bei Portalen wie eBay oder Amazon. Die Spannbreite der Missbrauchsszenarien ist dabei ebenfalls groß: Missbrauch eines Postfachs zum Versenden von Mails (Spam, Phishing, Schadsoftware), unautorisierte Geldtransfers, Identitätsdiebstahl, Datendiebstahl, unautorisiertes Nutzen von Diensten, Einstellen von Fake-Angeboten in Shops, Erpressung durch Verschlüsselung. Bei allen erfolgreichen Phishing-Angriffen ist zu beachten, dass – unabhängig vom Missbrauchsszenario – Angreifer Vollzugriff auf die Daten hatten und diese zumindest einsehen, vielleicht verändern bzw. löschen oder sogar herunterladen konnten. Daher sind im Fall eines erfolgten Phishing-Angriffs sämtliche Daten zunächst als kompromittiert zu betrachten.

Das zweite Einfallstor zur Erlangung eines nicht autorisierten Zugriffs entsteht durch verspätetes Einspielen von Sicherheitsupdates. Diese Patches werden von den Herstellern von Software bereitgestellt, um bekannte Sicherheitslücken zu schließen. Beim Einsatz von Software müssen die Verantwortlichen sich daher täglich über mögliche Sicherheitsaktualisierungen informieren, Sicherheitswarnungen sichten und mögliche Risiken bewerten. Sollte ein Patch zu einer eingesetzten Software veröffentlicht werden, ist dieser schleunigst einzuspielen. Leider wurde dies von einigen Verantwortlichen nicht beherzigt, sodass Angreifer ausreichend Zeit hatten, das vulnerable System zu finden und die nicht geschlossene Sicherheitslücke auszunutzen. Betroffen waren hier insbesondere E-Mail-Server, Webshops und Content-Management-Systeme. Je nach Größe der Sicherheitslücke kann das versäumte Einspielen eines Patches verheerende Folgen haben.

Phishing & Fake-Webseiten

Als „Phishing" bezeichnet man Versuche Unbefugter, mittels gefälschter Webseiten (Fake-Webseiten) oder E-Mails Zugangsdaten und Passwörter zu erlangen. Dabei werden Betroffene dazu veranlasst, Zugangsdaten auf Systemen einzugeben, die unter der Kontrolle von Angreifenden stehen.

Wie ist den beiden Einfallstoren beizukommen? Um das Risiko eines erfolgreichen Phishing-Angriffs zu verringern, sind zwei Maßnahmen hervorzuheben: **Sensibilisierung** und **Zwei-Faktor-Authentifizierung**. Die Sensibilisierung der Mitarbeiterschaft in Bezug auf schadhafte E-Mails sollte zum grundsätzlichen Schulungsangebot eines jeden Unternehmens gehören. In regelmäßigen Abständen ist das Personal über neue Phishing-Kampagnen zu informieren, am besten mit beispielhaften Bildern und Angaben, wie betrügerische Absichten zu erkennen sind. Viele Anbieter von Online-Diensten, insbesondere im Bezahl- und Bankingsektor, aber auch bei Office-Clouds und Shops bei Amazon und eBay, bieten inzwischen die Möglichkeit, eine Zwei-Faktor-Authentifizierung einzurichten. Diese Option sollte stets in Betracht gezogen werden. Zusätzlich sollte jedes Unternehmen abwägen,

ob die Deaktivierung von Makros in der Bürokommunikationssoftware sowie restriktivere Firewallregeln umsetzbar sind, ohne die betrieblichen Tätigkeiten zu beeinträchtigen. Solche Maßnahmen helfen, automatisierte Angriffe zu erschweren.

Das zeitnahe Schließen von Sicherheitslücken sollte eigentlich ein Standardprozess im IT-Sicherheitsmanagement sein. Wie die Datenpannenmeldungen aber zeigen, gibt es dabei in vielen Unternehmen Optimierungsbedarf. Dies gilt ebenso für das Monitoring der IT-Systeme und des Netzverkehrs sowie für die anschließenden Informations- und Meldewege. Häufig werden bei der Auswertung von Protokolldaten nach einer Datenpanne charakteristische Einträge zu ungewöhnlichen Prozessen und unbefugten Tätigkeiten gefunden, die auf einen Eindringling hinweisen. Da aber entweder kein regelmäßiges Kontrollieren der Protokolldaten stattfand oder entsprechende Warnmeldungen nicht oder verkehrt zugestellt wurden, konnten frühzeitige Gegenmaßnahmen nicht getroffen werden. Auch für diese Sorglosigkeiten gilt: Alles beim Alten!

Was ist zu tun?

Sensibilisierung, sichere Konfiguration und das schnelle Einspielen von Sicherheitspatches helfen, das Risiko von Datenschutzverletzungen durch Phishing einzudämmen und etwaige schädigende Auswirkungen zu begrenzen.

07

KERNPUNKTE

Facebook-Fanpages

Verbraucherschutzvorschriften über digitale Produkte

7 Neue Medien

7.1 Gutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages

Im vergangenen Berichtszeitraum informierte das ULD über die Beendigung des Rechtsstreits zum Betrieb von Facebook-Fanpages (40. TB, Tz. 7.3). Das OVG Schleswig hatte mit Urteil vom 25.11.2021 entschieden, dass die Deaktivierungsanordnung aus dem Jahr 2011 rechtmäßig war. Die Adressatin der Anordnung reagierte konsequent und schaltete die von ihr betriebene Facebook-Fanpage ab.

Ein von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eingesetztes Arbeitsgremium (**Taskforce Facebook-Fanpages**) befasste sich in der Folge mit den im Rechtsstreit ergangenen Entscheidungen der durchlaufenen gerichtlichen Instanzen und prüfte die aktuellen Datenverarbeitungen und Prozesse im Zusammenhang mit den Facebook-Fanpages unter Berücksichtigung der Facebook-Datenrichtlinien und der bestehenden Gesetzeslage. Das ULD unterstützt die Arbeit der Taskforce Facebook-Fanpages und war an der Erstellung des Kurzgutachtens maßgeblich beteiligt. Ein besonderes Augenmerk legte das Autorenteam auf die Anwendung des **Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG)** in Bezug auf den **Einsatz von Cookies**. Das Kurzgutachten liegt inzwischen in einer aktualisierten Fassung vor.

Prozesse und Verarbeitungen von personenbezogenen Daten, die im Rahmen des Kurzgutachtens vordergründig berücksichtigt werden, sind folgende:

- Speichern und Auslesen eines Cookies und nachfolgendes Verarbeiten personenbezogener Daten in Form der Verknüpfung der Nutzungsdaten mit den zuvor von den registrierten Nutzerinnen und Nutzern im Rahmen des Registrierungsprozesses hinterlegten Informationen zu Statistiken (sogenannten Insights) mittels des c_user-Cookies,
- Setzen und Auslesen eines Cookies und nachfolgende Verarbeitungen personenbezogener Daten u. a. in Form der Verknüpfung der Nutzungsdaten zu Statistiken (sogenannten Insights) mittels des datr-Cookies,
- Setzen und Auslesen eines Cookies und nachfolgende Verarbeitungen personenbezogener Daten in Form der Verknüpfung der Nutzungsdaten zu Zwecken der Profilerstellung und – aufbauend darauf – zielgerichteten Ansprache und Werbung (Targeting) mittels des fr-Cookies u. a.

Die Taskforce Facebook-Fanpages gelangt bei ihren Prüfungen zu folgenden Ergebnissen:

- Durch die Bereitstellung einer Fanpage übernimmt die die Fanpage betreibende Stelle die Rolle eines Anbieters von Telemedien im Sinne des § 2 Abs. 2 Nr. 1 TTDSG. Dadurch ergibt sich nach § 25 Abs. 1 TTDSG die Pflicht, eine wirksame Einwilligung für das Speichern von Informationen in den Endeinrichtungen der Nutzerinnen und Nutzer sowie den Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, für nicht im Sinne des § 25 Abs. 2 Nr. 2 TTDSG unbedingt erforderliche Cookies einzuholen. Eine solche Einwilligung wird beim Betreiben einer Facebook-Fanpage nicht eingeholt.
- Darüber hinaus besteht aufgrund sich ergänzender Interessen der Betreiberinnen und Betreiber von Fanpages und Meta eine gemeinsame Verantwortlichkeit mindestens für die Verarbeitung der auf Basis der gesetzten Cookies erhobenen personenbezogenen Daten. Diesbezüglich sind keine wirksamen Rechtsgrundlagen gegeben.

- Die sich aus Artikel 13 DSGVO ergebenden Informationspflichten werden nicht hinreichend erfüllt.

Das Kurzgutachten ist unter folgendem Link abrufbar:

https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Kurzgutachten_Facebook-Fanpages_V1_1_clean.pdf

Kurzlink: *https://uldsh.de/tb41-7-1*

Das ULD stellte folglich einen datenschutzrechtlichen Verstoß fest und erteilte dem Unternehmen Maßgaben, in welchem Rahmen personenbezogene Daten der Kundinnen und Kunden verarbeitet werden dürfen und dass der Grundsatz der Zweckbindung der Datenverarbeitung einzuhalten ist.

Was ist zu tun?

Die Erläuterungen und Ergebnisse der Analyse in dem Kurzgutachten zeigen, dass der Betrieb von Facebook-Fanpages auch unter Berücksichtigung der aktuellen tatsächlichen Begebenheiten und rechtlichen Anforderungen derzeit nicht rechtskonform möglich ist: Es fehlen vor allem wirksame Einwilligungserklärungen der Nutzerinnen und Nutzer hinsichtlich deren Daten, die beim Besuch von Facebook-Fanpages erhoben und weiterverarbeitet werden. Ferner fehlt bis zum heutigen Tag eine transparente und ausreichende Vereinbarung zur gemeinsamen Verantwortung von Fanpage betreibenden Stellen und Meta. Zudem mangelt es an Pflichtinformationen zur Datenverarbeitung im Zusammenhang mit den Fanpages. Betreiberinnen und Betreiber von Facebook-Fanpages sind aufgerufen, sich ernsthaft die Frage eines Weiterbetriebs zu stellen. Die bestehenden Rechtsverstöße sind evident.

7.2 Auswirkungen der neuen Verbraucherschutzvorschriften über digitale Produkte

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat zu den neuen Vorschriften zu Verbraucherverträgen über digitale Produkte einen Beschluss gefasst. Die zugrunde liegenden rechtlichen Bestimmungen des Bürgerlichen Gesetzbuchs (BGB) sind am 1. Februar 2022 in Kraft getreten. Der Begriff der „digitalen Produkte“ ist weit gefächert. Erfasst werden u. a. Softwarelösungen, Cloud-Services oder digitale Unterlagen.

Die neuen Vorschriften werfen die Frage auf, ob mit deren Anwendung Vorgaben des europäischen Datenschutzrechts eingeschränkt werden. Diese Thematik gewinnt vor allem dann an Bedeutung, wenn ein Verbraucher einem Unternehmer personenbezogene Daten zur Verfügung stellt und zu prüfen ist, ob dies im Rahmen einer Leistungspflicht erfolgt. Im Ergebnis bleiben sowohl die Datenschutzvorschriften der DSGVO als auch jene des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) unberührt.

Der Gesetzgeber hat zur Bereitstellung personenbezogener Daten in § 312 Abs. 1a BGB eine Aussage getroffen.

Die DSK hat hierzu ausgeführt, dass die Verarbeitung personenbezogener Daten im Rahmen von Geschäftsmodellen (z. B. „Bezahlen mit Daten“) nach den gesetzlichen Erlaubnistatbeständen gemäß Art. 6 Abs. 1 Buchst. a, b oder f DSGVO zulässig sein muss und auch die sonstigen Anforderungen der DSGVO erfüllt sein müssen. Die neuen Verbraucherschutzvorschriften des BGB stellen keine eigene Rechtsgrundlage für die

Verarbeitung von personenbezogenen Daten dar.

§ 312 Abs. 1a BGB

Die Vorschriften [...] sind auch auf Verbraucherverträge anzuwenden, bei denen der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder sich hierzu verpflichtet. Dies gilt nicht, wenn der Unternehmer die vom Verbraucher bereitgestellten personenbezogenen Daten ausschließlich verarbeitet, um seine Leistungspflicht oder an ihn gestellte rechtliche Anforderungen zu erfüllen, und sie zu keinem anderen Zweck verarbeitet.

Weiterhin wird verdeutlicht, dass die Ausübung von Rechten betroffener Personen, wie etwa die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruchsrecht, keinen Einfluss auf die Wirksamkeit eines Vertrags über digitale Produkte haben. Dies ergibt sich aus § 327q Abs. 1 BGB.

§ 327q Abs. 1 BGB

Die Ausübung von datenschutzrechtlichen Betroffenenrechten und die Abgabe datenschutzrechtlicher Erklärungen des Verbrauchers nach Vertragsschluss lassen die Wirksamkeit des Vertrags unberührt.

Die DSK hat die maßgeblichen Punkte wie folgt zusammengefasst:

- Die §§ 327 ff. BGB sind nur anwendbar, wenn ein Vertrag über digitale Produkte geschlossen wurde.
- Wurde zwischen dem Unternehmen und dem Verbraucher ein Vertrag über digitale Produkte geschlossen, ist jede Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem geschlossenen Vertrag nur rechtmäßig, wenn sie auf eine Rechtsgrundlage der Datenschutz-Grundverordnung gestützt werden kann.
- § 327q BGB trifft keine Aussage zu den Auswirkungen der zivilrechtlichen Verbraucherschutzvorschriften auf das Datenschutzrecht. Es werden nur umgekehrt die zivilrechtlichen Auswirkungen auf den Verbrauchervertrag festgelegt, wenn Verbraucher von ihren datenschutzrechtlichen Rechten Gebrauch gemacht haben, eine Einwilligung zu widerrufen oder einer Datenverarbeitung, die auf Art. 6 Abs. 1 Buchst. f DSGVO gestützt wird, gemäß Artikel 21 DSGVO zu widersprechen.
- Die neuen Verbraucherschutzvorschriften im BGB haben keine Auswirkungen auf die Anwendung von § 25 TTDSG.

https://www.datenschutzkonferenz-online.de/media/dskb/20221129_dskb_08_Beschluss_Verbrauchervorschriften.pdf

Kurzlink: *https://uldsh.de/tb41-7-2*

08

KERNPUNKTE

Plattform Privatheit

Digitale Arbeitswelten

IuK-Forschung

Transparenz und Einwilligungsmanagement

8 Modellprojekte und Studien

Das Unabhängige Landeszentrum für Datenschutz hat als Behörde der Landesbeauftragten für Datenschutz seine Aktivitäten in Initiativen im Bereich drittmittelfinanzierter Projekte und Studien fortgesetzt. Damit ist das ULD weiterhin im Bereich der Kooperation mit der Wissenschaft aktiv und erhält sich damit die Möglichkeit, 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. Beteiligungen an Projekten erfolgten weiterhin dort, wo entweder besondere datenschutzfördernde Lösungen (englisch: „Privacy-Enhancing Technologies", kurz PETs) erforscht und entwickelt werden sollen oder wo besondere Risiken für die Rechte und Freiheiten natürlicher Personen bestehen.

Im Jahr 2022 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 Plattform Privatheit: PRIDS – Privatheit, Demokratie und Selbstbestimmung

Im letztjährigen Tätigkeitsbericht hatten wir darüber berichtet, dass das „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt" nach sieben Jahren zu Ende gegangen ist, aber wir unsere thematische Arbeit im Nachfolgeprojekt **„PRIDS – PRIvatheit, Demokratie und Selbstbestimmung im Zeitalter von künstlicher Intelligenz und Globalisierung"** fortsetzen konnten (40. TB, Tz. 8.1).

Aus dem Forum Privatheit wurde nun die Plattform Privatheit, aber wer sich den Begriff „Forum Privatheit" gemerkt hat, braucht sich nicht umzugewöhnen: Das Logo des „Forum Privatheit" kennzeichnet weiter die Tätigkeiten im interdisziplinären Verbund von spannenden Projektpartnern, deren Arbeit an dem Thema Privatheit vom Bundesministerium für Forschung und Bildung (BMBF) gefördert wird. Man darf also von Forum Privatheit oder von Plattform Privatheit sprechen.

Im Jahr 2022 war unsere Arbeit nicht nur von wissenschaftlichen und gesellschaftlichen Themen geprägt, sondern wir haben uns auch damit beschäftigt, wie die Erkenntnisse aus diesen und weiteren Initiativen in der Praxis verortet und umgesetzt werden können. Ein wichtiges Dokument, das wir dazu ausgewertet haben, war der Koalitionsvertrag 2021-2025 der Bundesregierung, in dem wir verschiedene Ansätze zur Stärkung von Daten- und Grundrechtsschutz identifizierten. Die Ergebnisse haben wir in dem Policy Paper „Mehr Fortschritt wagen – durch Stärkung des Datenschutzes. Vorschläge zur Ausgestaltung des Koalitionsvertrags" zusammengefasst, das unter dem folgenden Link verfügbar ist:

https://www.forum-privatheit.de/download/mehr-fortschritt-wagen-durch-staerkung-des-datenschutzes-vorschlaege-zur-ausgestaltung-des-koalitionsvertrags/

Kurzlink: *https://uldsh.de/tb41-8-1a*

Ein Punkt im Koalitionsvertrag des Bundes ist die **Überwachungsgesamtrechnung** (40. TB, Tz. 2.3). Auch damit haben wir uns im Projekt PRIDS beschäftigt und Vorschläge zu einer pragmatischen Umsetzung einer Überwachungsgesamtrechnung ausgearbeitet.

Wir sehen in einer solchen Überwachungsgesamtrechnung einen großen Vorteil für die **Transparenz**: Die Überwachungsgesamtrechnung soll dem Gesetzgeber und allen Interessierten als Übersicht über die bestehenden Überwachungsgesetze und die damit verbundenen

Grundrechtsbeschränkungen dienen. Darauf aufbauend ermöglicht der dokumentierte Status quo eine gesellschaftliche Debatte über das akzeptable Maß der Überwachung und über notwendige Korrekturen in Umfang und Ausgestaltung. Auch die Gesetzgebung an sich, gerade in sensiblen Bereichen wie Strafverfolgung und Justiz, kann von einer derartigen Überwachungsgesamtrechnung profitieren, wenn beispielsweise Gesetzesfolgenabschätzungen vorgenommen werden, in denen auch die Evaluation und die Reversibilität der Maßnahmen eine Rolle spielen können.

Überwachungsgesamtrechnung

Die Überwachungsgesamtrechnung basiert auf einer strukturierten Sammlung und Zusammenfassung bestehender staatlicher Überwachungsmaßnahmen. Der Gesetzgeber muss bei Einführung neuer Überwachungsmaßnahmen die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen im Blick behalten. Statt reflexhaft immer neue Überwachungsinstrumente zu schaffen, ist rechtsstaatlich geboten, die bisherigen Maßnahmen zu überprüfen und gegebenenfalls wieder zurückzunehmen.

Das Policy Paper „Zur Einführung einer Überwachungsgesamtrechnung" steht unter dem folgenden Link zum Abruf bereit:

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

Kurzlink: *https://uldsh.de/tb41-8-1b*

PRIDS und die Plattform Privatheit bieten jedes Jahr verschiedene Veranstaltungen zum Vorstellen der Ergebnisse, zum Diskutieren und zum Erarbeiten von Lösungsvorschlägen an. Das Highlight ist die Jahreskonferenz, die im Jahr 2022 zum Thema „Daten-Fairness in einer globalisierten Welt – Grundrechtsschutz und Wettbewerb für eine internationale Data Governance" ausgerichtet wurde. Diese Veranstaltungen profitieren vom Weitblick und der interdisziplinären Rund-um-Perspektive zu Datenschutz und Privatheit, die von den Teilnehmenden engagiert eingebracht werden.

Aktuelle Informationen sind hier verfügbar:

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

Kurzlink: *https://uldsh.de/tb41-8-1c*

8.2 Projekt EMPRI-DEVOPS – Datenschutz in digitalen Arbeitswelten

Das Projekt **„Employee Privacy in Software Development and Operations" (EMPRI-DEVOPS)** (40. 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 übertragen. Das ULD beantwortete dabei Fragen des Datenschutzrechts, insbesondere des Beschäftigtendatenschutzrechts.

Bereits zuvor wurde an dieser Stelle (39. TB, Tz. 8.2) der Bedarf legislativer Klarheit im Beschäftigtendatenschutz benannt und damit ein Wunsch bekräftigt, der nicht zuletzt von Arbeitnehmervertretern, Gewerkschaften und einigen Parteien geteilt wurde. So hieß es 2017 in der Gesetzesbegründung zum BDSG: *„Der Gesetzgeber behält sich vor, Fragen des Datenschutzes im Beschäftigungsverhältnis innerhalb dieser Vorschrift oder im Rahmen eines gesonderten Gesetzes konkretisierend bestimmte Grundsätze, die im Rahmen der Rechtsprechung zum geltenden Recht bereits angelegt sind, zu regeln."* (BT-Drucksache 18/11325). Im Jahr 2022 nahm

Bundesarbeitsminister Heil den Faden mit der Ankündigung auf: *„Die neue Koalition will in dieser Legislatur Regelungen zum Beschäftigtendatenschutz schaffen, um Rechtsklarheit für Arbeitgeber und Beschäftigte zu erreichen und die Persönlichkeitsrechte der Beschäftigten effektiv zu schützen."* Das lässt auf die Gestaltung eines eigenständigen Beschäftigtendatenschutzgesetzes hoffen.

Der Gesetzgeber kann durch eine Novellierung der Regelungen für Rechtsklarheit und dadurch gesteigerte Rechtssicherheit sorgen, insbesondere um die zukünftige Entwicklung datenschutzfreundlicher Technikinnovationen im Soft- und Hardwarebereich zu gewährleisten. Auch die Datenschutzkonferenz (DSK) hat sich im Berichtszeitraum mit einer Entschließung inklusive konkreter Vorschläge positioniert (Tz. 2.2).

So ist es wünschenswert, die Begriffsbestimmung von Beschäftigtendaten mit dem klarstellenden Zusatz zu erweitern, dass dazu auch personenbezogene oder personenbeziehbare Beschäftigtenmetadaten zählen, die bei der Nutzung von betrieblichen Softwareanwendungen für die Erbringung der vertraglich geschuldeten Tätigkeiten oder Aufgaben automatisiert erzeugt werden oder anfallen.

Weiter kann etwa beim Verbot heimlicher oder verdeckter Verhaltens- und Leistungskontrollen klargestellt werden, dass hierbei auch die Verarbeitung von personenbezogenen oder personenbeziehbaren Metadaten unzulässig ist, die bei der Nutzung von betrieblichen Softwareanwendungen für die Erbringung geschuldeter Tätigkeiten oder Aufgaben automatisiert erzeugt werden oder anfallen.

Der Gesetzgeber könnte zudem die Chance nutzen, ein Verwertungsverbot missbräuchlich verarbeiteter Daten und Metadaten zu normieren oder jedenfalls in Kollektiv- oder Betriebsvereinbarungen verankerten Beweisverwertungsverboten im gerichtlichen Verfahren effektive Wirksamkeit einzuräumen.

https://www.datenschutzzentrum.de/projekte/empri-devops/

Kurzlink: *https://uldsh.de/tb41-8-2*

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

Im Berichtsjahr 2022 endete das durch die EU-Kommission geförderte Projekt **„Participatory Approaches to a New Ethical and Legal Framework for ICT" (PANELFIT)** (40. TB, Tz. 8.3). Ziel des Projektes war es, Akteuren im Bereich der Forschung zur Informations- und Kommunikationstechnik (IuK) den Weg für eine Adaption der DSGVO in ihren Bereichen zu ebnen.

Die Tätigkeit im Jahr 2022 stand im Lichte der Konsolidierung und Veröffentlichung der vorhandenen Projektergebnisse durch das Konsortium. Ausgewählte Resultate des Gesamtprojekts wurden dabei in einem Dokument zentral als Leitlinien zusammengeführt. Diese nun in fünf Sprachen verfügbaren „PANELFIT Guidelines" richten sich an Forschende, die bei ihrer Tätigkeit personenbezogene Daten verarbeiten. Während sich PANELFIT zentral mit der Datenverarbeitung für Forschung im Bereich der Informations- und Kommunikationstechnik befasste, sind die Darstellungen der rechtlichen und ethischen Aspekte auch allgemeingültig für eine Vielzahl anderer Forschungsbereiche.

Die vom ULD erstellten Erläuterungen sind mit Blick auf die Zielgruppen bewusst allgemein verständlich gehalten: Zum einen eine erste Einführung in die DSGVO. Abweichend von der Mehrzahl bestehender DSGVO-Einführungen ist das Augenmerk nicht darauf beschränkt darzustellen, welche Rechte Betroffene haben oder welche Anforderungen Verantwortliche erfüllen müssen und gegebenenfalls welche Sanktionen bei Verstößen drohen. Der Leserschaft soll vielmehr vermittelt werden, warum die geforderten Schutzmaßnahmen sich im Recht etabliert haben. Die Mechanismen und Prinzipien der DSGVO werden dabei konkret auf das Machtgefälle zwischen dem Verantwortlichen und den

Betroffenen zurückgeführt. Die zweite allgemein gehaltene Darstellung beschreibt die Grundprinzipien der DSGVO. Diese Darstellung folgt gleichsam dem Grundgedanken, dass das Warum der DSGVO-Prinzipien dem Ausgleich von Interessen und dem Machtgefälle dient. Die Prinzipien und deren Bezug zum Text der DSGVO werden dargestellt sowie Hinweise zu technischen und organisatorischen Maßnahmen zwecks Umsetzung der jeweiligen Prinzipien gegeben.

Weitere vom ULD zuvor erstellte und vom Projektkonsortium veröffentlichte Beiträge zum Leitfaden betreffen Datenschutz-Folgenabschätzungen (39. TB, Tz. 8.3) und Ausführungen zur Anonymisierung und Pseudonymisierung (40. TB, Tz. 8.3).

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

Kurzlink: *https://uldsh.de/tb41-8-3*

8.4 Projekt TRAPEZE – Transparenz und Einwilligungsmanagement

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" (40. 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 der europäischen Gesetzgebung.

Das Projekt entwickelt eine innovative Technologie (die „TRAPEZE Platform"), die in drei Anwendungsszenarien (use cases) demonstriert wird.

Eines der Interessen, die das ULD durch seine Projektarbeit verfolgt, ist, Ansätze und Komponenten zu identifizieren, die Relevanz über das Projekt hinaus haben. Solche Komponenten können dann durch geeigneten Technologietransfer einem weiteren Publikum für Datenschutz durch Technologiegestaltung (data protection by design) präsentiert werden.

In diesem Sinne bestand eine der Tätigkeiten des ULD in einer Analyse des **Dashboard-Konzepts**, wie es zur Erfüllung der Anforderungen der DSGVO eingesetzt werden kann. Die betrifft vor allem Transparenz und Einwilligung. Dazu hat das ULD eine detaillierte Studie der notwendigen

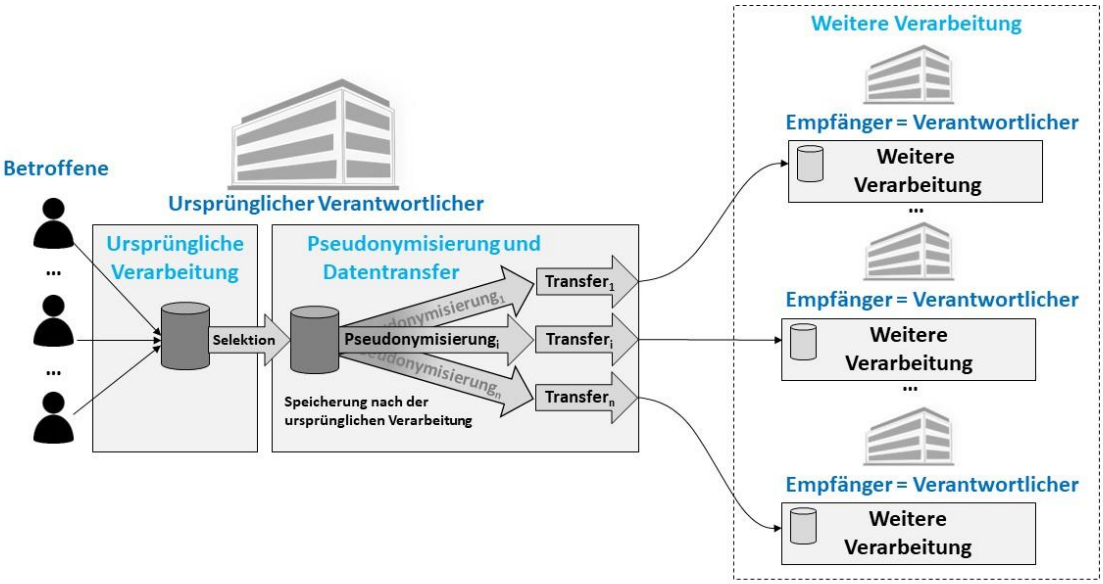


Abbildung: Datennutzung und -weitergabe zu anderen Zwecken

Funktionalität und Eigenschaften eines Dashboards mit Datenschutzfunktionalität erstellt, sodass die rechtlichen Anforderungen an Transparenz und Einwilligung tatsächlich erfüllt werden können.

Privacy Dashboard

Dashboard steht wörtlich übersetzt für Armaturenbrett. Im IT-Bereich versteht man darunter eine grafische Benutzeroberfläche, die zur Visualisierung und Verwaltung von Daten oder Systemen dient. Vertraut sein dürfte etwa die Verwaltung von Berechtigungen für Apps auf Mobilgeräten. Damit eignet sich eine solche Schnittstelle, um Betroffenenrechte umzusetzen, indem Nutzerinnen und Nutzer ihre Daten einsehen, Begehren auf Auskunft, Berichtungen oder Löschungen übermitteln oder Rechte für weiter gehende Nutzungszwecke oder Übermittlungen an Dritte vergeben und entziehen zu können.

Das ULD hat dann den weitverbreiteten Anwendungsbereich der weiteren Verarbeitung für weiterführende Studien, für Technologietransfer oder andere Zwecke (Sekundärnutzung) gewählt (siehe Abbildung). In diesem Anwendungsszenario ist es besonders schwierig, Transparenz verständlich herzustellen, aber zugleich besonders wichtig. Die Analyse hat bestehende Datenschutzrisiken aufgezeigt und dargestellt, wie ein Dashboard eingesetzt werden kann, um diesen Risiken entgegenzuwirken und durch einen zentralen Zugangspunkt (Single Point of Access) auch bei einer Vielzahl von Verarbeitungstätigkeiten durch mehrere Verantwortliche die vom Gesetz geforderte Transparenz und Informationsbereitstellung realistisch umzusetzen.

Zukünftige Arbeiten sollen dazu beitragen, das Konzept eines Dashboards in die weitere Praxis zu bringen und damit durch geeignete Technikgestaltung die Transparenz und damit das Datenschutzniveau anzuheben.

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

Kurzlink: *https://uldsh.de/tb41-8-4*

8.5 Projekt AnoMed – Kompetenzcluster Anonymisierung für medizinische Anwendungen

Im November 2022 startete das Kompetenzcluster **„Anonymisierung für medizinische Anwendungen" (AnoMed)**. Ziel des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts ist es, die Forschung an Technologien, Verfahren und Methoden zur Pseudonymisierung und Anonymisierung zu bündeln. Im Verbund soll unter Leitung der Universität zu Lübeck die Grundlage für eine Test- und Evaluationsplattform für Anonymisierungslösungen im Bereich medizinischer Anwendungen gestaltet werden. Die Plattform soll eine Reihe medizinischer Referenzaufgaben einschließlich passender Referenzdatensätze für die Tests enthalten. Parallel werden in AnoMed Angriffsverfahren zur Re-Identifikation entwickelt und neue, sogenannte Differentially-Private-Anonymisierungsverfahren als erste Pilotlösungen für die zu testenden Anonymisierungslösungen auf der Plattform erforscht.

Die Aufgaben des ULD im AnoMed-Kompetenzcluster bestehen darin, einerseits den datenschutzrechtlichen Hintergrund darzustellen und andererseits Lösungsansätze zur Pseudonymisierung und Anonymisierung zu evaluieren und zusammen mit den Forschungspartnern der Universität zu Lübeck den bekannten und klassischen Anonymisierungslösungen gegenüberzustellen. Eine hinreichende Anonymisierung im Verständnis der DSGVO geht fast zwingend mit einem erheblichen Informationsverlust einher, der erforderlich ist, um den Personenbezug hinreichend zu beseitigen und eine Re-Identifika-

tion auszuschließen. Das verringert indes zugleich den für die Forschung oft nötigen Informationsgehalt der Daten.

Die vom Projektkonsortium unter datenschutzrechtlicher Begleitung des ULD zu betrachtenden alternativen Lösungsvorschläge zielen darauf ab, die Daten derart zu verändern, dass einerseits eine Re-Identifikation zuverlässig verhindert wird und andererseits die jeweils nötigen Informationen erhalten bleiben.

Kann der von der DSGVO für eine Anonymisierung vorausgesetzte Schutz vor einer Identifikation nicht erreicht werden, gelten die Daten weiterhin als personenbezogen. Dann sind flankierende technische und organisatorische Maßnahmen und eine enge Zweckbindung für die Forschungsdaten sowie mittelfristig legislative Lösungen erforderlich. Solche Gesetze können einerseits den notwendigen Schutz definieren und andererseits klarstellend bestimmte Verarbeitungen in ausgewählten und klar beschriebenen Szenarien gestatten. Solche rechtlichen Aspekte werden gegenwärtig etwa im Rahmen der Entwürfe für einen **Europäischen Raum für Gesundheitsdaten (European Health Data Space, EHDS)** erörtert.

Weitere Informationen zu AnoMed:

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

Kurzlink: *https://uldsh.de/tb41-8-5*

Was ist zu tun?

Gesundheitsdaten zu Forschungszwecken zu verarbeiten ist wichtig, doch es ist nötig, die Risiken für die betroffenen Personen mittels technischer, organisatorischer und rechtsgestaltender Maßnahmen einzudämmen.

09

KERNPUNKTE

Leitung Arbeitskreis Zertifizierung

Prüfkriterienkatalog

Erste Genehmigungen

Eigenes Zertifizierungsverfahren

9 Zertifizierung und Akkreditierung

Nach Inkrafttreten der Regelungen zur Akkreditierung und Zertifizierung in der DSGVO 2018 konnten in diesem Jahr nun die ersten Genehmigungsverfahren für Kriterienkataloge in Europa bzw. auch in Deutschland vorangetrieben und teilweise sogar abgeschlossen werden (Tz. 9.3). Damit ist zu erwarten, dass 2023 auch in Deutschland erste Zertifizierungsstellen akkreditiert werden und damit endlich auch Datenschutzzertifizierungen erfolgen können. In Schleswig-Holstein bestehen noch keine derartigen Verfahren, wobei weiterhin auch Überlegungen bestehen, dass das ULD ein Zertifizierungsverfahren anbietet (Tz. 9.4). Allerdings haben wir die Entwicklung bis hierin als Leiter des Arbeitskreises Zertifizierung der deutschen Aufsichtsbehörden begleitet (Tz. 9.1) und werden dies auch weiterhin tun. Im Berichtszeitraum konnte u. a. eine neue Version eines Prüfkriterienkatalogs verabschiedet werden, der eine einheitliche Bewertung von Kriterienkatalogen in Deutschland sicherstellen soll (Tz. 9.2). Wir waren auch an der für den Zertifizierungs- und Akkreditierungsbereich zuständigen europäischen Expert Subgroup beteiligt, die die ersten Stellungnahmeverfahren und Genehmigungsverfahren zu den Kriterien vorliegen hatte (Tz. 11.4).

9.1 Leitung des AK Zertifizierung

Das ULD hat auch 2022 den Arbeitskreis Zertifizierung geleitet. Die Treffen fanden virtuell statt. Dabei wurde auf einen monatlichen Turnus gewechselt (unterbrochen nur in den Sommerferien), der es ermöglichte, zeitnah **aktuelle Entwicklungen bei der Genehmigung von Zertifizierungskriterien und beginnende Akkreditierungsverfahren in Deutschland und der EU zu besprechen**. Flankiert wurde dieses durch den Unterarbeitskreis (UAK) Prüfkriterien, der sich zunächst auf die Finalisierung der neuen Version des Prüfkriterienkatalogs (Tz. 9.2) konzentrierte und dabei und gerade auch im Folgenden ein Gremium zum Austausch zu aktuellen Verfahren darstellte. Geleitet wird der UAK von der LfD Nordrhein-Westfalen und findet alle 14 Tage statt.

Ein Thema, das den AK Zertifizierung fast durch das ganze Jahr begleitet hat, waren erste Verfahren zur Anerkennung von Zertifizierungskriterien in Europa. Konkret waren es nationale und auch europaweite Kriterien (Tz. 11.4). Wichtig war dabei, dass über den AK Zertifizierung eine geschlossene deutsche Haltung erreicht werden konnte. Das galt auch bei der Mitwirkung an einem europäischen Papier zu den Verfahren bei der Betrachtung nationaler und europäischer Kriterien. In diesem Jahr hat sich durchaus gezeigt, dass es in Europa unterschiedliche Positionen bei den Ansprüchen an eingereichte Zertifizierungskriterien gibt. Wichtig bleibt es, dass über den AK Zertifizierung alle Aufsichtsbehörden informiert bleiben und hier im Rahmen unserer Kooperationsvereinbarung (39. TB, Tz. 9.2) miteinander abgestimmt agieren.

Auch die **Deutsche Akkreditierungsstelle GmbH (DAkkS)** nahm regelmäßig an den Treffen des AK Zertifizierung teil und unterstützte damit die deutschen Aufsichtsbehörden mit ihren Erfahrungen und dem Fachwissen in dem Bereich Kriteriengenehmigung. Die Anträge hierzu gingen in der Regel über die DAkkS ein, die diese an die zuständige Aufsichtsbehörde weiterreichte. Soweit es nicht um die Kriterien nach der DSGVO geht, nimmt die DAkkS auch eigene Prüfungen vor. Wenn es 2023 insbesondere nach ersten Genehmigungen von Kriterienkatalogen nun auch darum geht, Zertifizierungsstellen zu akkreditieren, ist die DAkkS sogar federführend und nutzt die Mitarbeiterinnen und Mitarbeiter der jeweiligen Aufsichtsbehörden als Gutachterinnen und Gutachter. Dies zu begleiten und Erfahrungen zu verarbeiten wird im kommenden Jahr voraussichtlich einen großen Teil der Arbeit des AK Zertifizierung darstellen.

Was ist zu tun?

Der AK Zertifizierung wird sich weiterhin monatlich virtuell treffen und aktuelle Entwicklungen in Deutschland und Europa begleiten.

9.2 Prüfkriterienkatalog

Das im Frühjahr 2021 durch die DSK angenommene Papier **„Anforderungen an datenschutzrechtliche Zertifizierungsprogramme – Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6)“** wurde im Unterarbeitskreis (UAK) Prüfkriterien des AK Zertifizierung weiterentwickelt und liegt nun in der Version 2.0 vor. Die bisherige Struktur des Dokuments und insbesondere des Kapitels 2 aus

- gesetzlichen Tatbestandsmerkmalen,
- zu behandelnden Prüfthemen und deren Umsetzung durch die Kundinnen und Kunden der Zertifizierungsstelle sowie
- der Art und Weise der Prüfung durch die Zertifizierungsstelle

wurde hierbei beibehalten und um Inhalte zu verschiedenen Themenkomplexen ergänzt. So enthält das Papier nun u. a. umfangreiche Ausführungen zur gemeinsamen Verantwortlichkeit nach Artikel 26 und zur Datenübermittlung in Drittstaaten gemäß Artikel 46 DSGVO sowie Darstellungen zum Verfahrensablauf bei der Prüfung sowohl von nationalen als auch europäischen Zertifizierungskriterien. In die Überarbeitung bereits bestehender Inhalte sind dabei konkrete Erfahrungen mit der Anwendung des Papiers selbst sowie weiter ausdefinierter Vorgaben auf europäischer Ebene eingeflossen.

Es bildet somit in der aktuell vorliegenden Version eine breitere Basis für die einheitliche Bewertung von Zertifizierungsprogrammen durch die zuständigen unabhängigen Datenschutzaufsichtsbehörden in Deutschland und kann gleichermaßen als Orientierung für potenzielle Zertifizierungsstellen und bei der Erstellung von Zertifizierungsprogrammen dienen.

Darüber hinaus liegt das Papier der Version 2.0 mittlerweile auch in einer englischsprachigen Version vor, um die hierin entwickelten Vorgaben und Ansätze noch stärker auf europäischer Ebene sichtbar zu machen.

Das Papier ist unter dem folgenden Link abrufbar:

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

Kurzlink: *https://uldsh.de/tb41-9-2*

Was ist zu tun?

Der Unterarbeitskreis Prüfkriterien wird die Handhabbarkeit des Papiers bei der Prüfung eingereichter Zertifizierungsprogramme weiter beobachten und das Papier entsprechend fortlaufend anpassen und überarbeiten.

9.3 Erste Genehmigungsverfahren in Deutschland und der EU

Nach den sowohl auf europäischer als auch auf deutscher Ebene geleisteten Vorarbeiten (vgl. u. a. für Deutschland 40. TB, Tz. 9.2, und 39. TB, Tz. 9.2) war im abgelaufenen Berichtszeitraum eine deutliche Zunahme von Anträgen auf Genehmigung von Zertifizierungskriterien und Akkreditierung von Zertifizierungsprogrammen zu verzeichnen. Dies galt sowohl für Europa als auch für Deutschland, wobei eine Häufung solcher Anträge in einzelnen Mitgliedstaaten (u. a. Deutschland und Luxemburg) bzw. Bundesländern (Nordrhein-Westfalen, Hamburg, Bremen, Berlin) zu beobachten war.

Im Vorfeld einer Akkreditierung müssen die zukünftigen Zertifizierungsstellen oder hiervon losgelöste Programmeigner ein Zertifizierungsprogramm erstellen. Dieses Programm sowie auch die zukünftige Zertifizierungsstelle werden dann durch die Deutsche Akkreditierungsstelle GmbH (DAkkS) und in enger Zusammenarbeit mit der zuständigen Aufsichtsbehörde auf ihre Eignung geprüft. Wesentlicher Bestandteil eines solchen Zertifizierungsprogramms sind die Zertifizierungskriterien, die die Umsetzung der datenschutzrechtlichen Anforderungen beschreiben. Diese Zertifizierungskriterien werden neben den von der DAkkS durchgeführten Prüfungen anderer Teile des Programms durch die jeweils zuständige Aufsichtsbehörde fachlich geprüft und, vorbehaltlich der Stellungnahme durch den Europäischen Datenschutzausschuss (EDSA), genehmigt.

Einige dieser Anträge auf Genehmigung von Zertifizierungskriterien konnten im abgelaufenen Berichtszeitraum erfolgreich abgeschlossen werden, sodass es mittlerweile erste durch die zuständigen Datenschutzaufsichtsbehörden und den EDSA genehmigte Kataloge mit Zertifizierungskriterien gibt. Im Zuge dieser Verfahren waren im europäischen Kontext, aber auch bei den deutschen Aufsichtsbehörden, eine Vielzahl von Detailfragen zu klären, die einer engen Abstimmung aller Beteiligten bedurften. **In Schleswig-Holstein** sind bisher keine Anträge auf Akkreditierung als Zertifizierungsstelle eingegangen. Sofern sich in Schleswig-Holstein ansässige Verantwortliche dafür interessieren, ihre Verarbeitungsvorgänge zertifizieren zu lassen, könnten sie nunmehr auf genehmigte Zertifizierungsverfahren in Deutschland oder in anderen europäischen Mitgliedstaaten zurückgreifen.

Was ist zu tun?

Der Austausch und die Zusammenarbeit der Aufsichtsbehörden untereinander ist fortzuführen und zu intensivieren, auch um die Qualität der eingereichten Programme auf Dauer zu steigern und um damit das Instrument der Zertifizierung langfristig auf einem fachlich hohen Niveau zu verankern.

9.4 Planung eines eigenen Zertifizierungsangebots

Im Mai 2018 waren die Regelungen im LDSG zum Datenschutz-Gütesiegel Schleswig-Holstein entfallen. Weitere Zertifizierungen – insbesondere von IT-Produkten – waren für uns danach in dieser Form nicht mehr möglich. Allerdings könnte das ULD Zertifizierungen auch nach der DSGVO vornehmen. Dabei wäre jedoch zu beachten, dass keine Produkte wie etwa reine Softwarelösungen mehr zertifiziert werden könnten, sondern sich die Zertifizierung auf konkrete Datenverarbeitungsvorgänge (Verfahren, Prozesse, Dienstleistungen) bei Verantwortlichen oder Auftragsverarbeitern beziehen muss.

Wir wollten zunächst abwarten, wie die Entwicklung bei Zertifizierungskriterien, Akkreditierungen und schließlich Zertifizierungen auf dem Markt erfolgt (vgl. u. a. 40. TB, Tz. 9.4). 2023 ist mit ersten Akkreditierungen in Deutschland zu rechnen (Tz. 9.3), sodass damit bald erste Erfahrungen und Erkenntnisse vorliegen, ob und in welcher Form ein Zertifizierungsverfahren durch das ULD insbesondere für öffentliche Stellen eine sinnvolle Bereicherung für den Zertifizierungsbereich darstellen könnte. Dies werden wir beobachten.

Was ist zu tun?

Auf Basis der weiteren Entwicklung des Zertifizierungsbereichs in Deutschland und Europa ist zu eruieren, ob ein eigenes Zertifizierungsverfahren vom ULD sinnvoll ist.

10

KERNPUNKTE

Schnittstellen für Webbrowser-Plug-ins

„Soft Deletion“ in Datenbanken

Data Mesh

10 Aus dem IT-Labor

10.1 Schnittstellen für Webbrowser-Plug-ins – Bedrohungen der Softwarevielfalt

Moderne Browser bieten die Möglichkeit, ihre Funktionalität mithilfe von Erweiterungen (sogenannter Plug-ins) zu ergänzen. Dabei handelt es sich um Programmergänzungen, die über definierte Schnittstellen mit dem Browser kommunizieren und so die Darstellung von Webseiten beeinflussen oder im Browser selbst Funktionen nachrüsten können. Die wohl bekannteste Form der Browsererweiterungen stellen **Werbeblocker** dar. Wegen der standardmäßigen Verknüpfung von Werbedarstellung und gleichzeitiger Übertragung von Nutzungsdaten sind Werbeblocker inzwischen ein wichtiges Werkzeug zum Selbstdatenschutz.

Google hatte bereits 2018 angekündigt, die für Werbeblocker essenzielle Schnittstellendefinition Manifest v2 grundlegend zu ändern. Ziel war dabei – nach Aussagen von Google – der bessere Schutz der Privatsphäre: Plug-ins erhalten bislang Vollzugriff auf die empfangene Webseite. Werbeblocker können dann die Inhalte filtern, aber bösartige Plug-ins können womöglich in der Seite enthaltene personenbezogene Daten auch stehlen oder korrumpieren. Mit den neuen Schnittstellen soll die Verarbeitung der Seite stets durch den Browser geschehen. Plug-ins müssen dann Filterwünsche an den Browser übermitteln. Und genau in dieser Übermittlung liegt das Problem: Google sieht bislang ein Maximum von 30.000 URLs vor, die geblockt werden können. Aktuelle Werbeblocker greifen jedoch auf Regelsätze mit über 300.000 Adressen zurück. Vereinfacht gesagt werden Werbeblocker unter den durch Manifest v3 festgeschriebenen Schnittstellen damit weniger effektiv.

Die amerikanische NGO Electronic Frontier Foundation (EFF) beschreibt daher das Manifest v3 als Beispiel für den *„inhärenten Interessenkonflikt, der dadurch entsteht, dass Google sowohl den dominierenden Webbrowser als auch eines der größten Internetwerbenetzwerke kontrolliert"*. Aus Sicht der Verbraucherschützer leistet Manifest v3 nichts für den Datenschutz, sondern schwächt ihn stattdessen.

Ein weiteres Problem erwächst aus dem Umstand, dass das dem Chrome-Browser zugrunde liegende Chromium-Projekt inzwischen die Basis diverser Browser darstellt, nicht nur desjenigen aus dem Hause Google. So setzt neben Brave und Vivaldi auch Microsoft Edge auf **Chromium**. Googles rigide Änderungen der Plug-in-Schnittstelle haben somit Auswirkungen nicht nur auf den eigenen Browser, sondern eine Vielzahl von Derivaten und damit einen gewaltigen Teil des gesamten Browsermarktes. Hier zeigt sich einmal mehr der Nachteil von Monokulturen im Softwarebereich: Der einzige Browser, der nicht auf Chromium basiert, ist **Mozilla Firefox**. Dort hat man bereits angekündigt, zwar Manifest v3 unterstützen zu wollen, gleichzeitig jedoch Version 2 weiter aktiviert zu lassen. Auf diese Weise können Filter-Plug-ins wie uBlock Origin zunächst weiterhin ihre Arbeit ohne Einschränkung verrichten.

Die langfristigen Folgen dieser Entwicklung sind schwer abschätzbar. Brave hat hier eine bessere Ausgangsposition als viele Konkurrenten, weil der hauseigene Werbe- und Tracking-Blocker im Network-Stack eingebettet und vom eigentlichen Browser unabhängig ist. Allgemeine Erweiterungen sind hingegen auf die entsprechend verfügbaren Schnittstellen angewiesen. So dürfte es für einen Chromium-Abkömmling wie Brave schwer werden, die v2-Kompatibilität aufrechtzuerhalten, wenn Google den Code vollständig entfernt hat: Langfristig sind Erweiterungen, die die alte v2-Schnittstelle benötigen, somit nicht mehr lauffähig. Eine Abspaltung des Programmcodes vom ursprünglichen Chromium-Projekt (ein sogenannter Fork) würde langfristig viel Pflegeaufwand bedeuten, weil alle künftigen sicherheitsrelevanten Änderungen im Fork manuell nachgearbeitet werden müssten. Die Kompatibilität von Plug-ins unter den verschiedenen Browsern wird zusätzlich leiden, und Entwickelnde müssen nicht nur die Linien Chromium und Firefox bedenken, sondern künftig womöglich auch Forks.

Ursprünglich hatte Mozilla die eigene Plug-in-Struktur mit der WebExtensions API näher an Chrome herangerückt, um die Entwicklung von Cross-Platform-Erweiterungen zu unterstützen. Nun könnten sich die Wege wieder trennen: Erweiterungen für Firefox könnten künftig weniger leicht portierbar sein, wenn die Browserwelten in Sachen Plug-in-Schnittstellen getrennte Wege gehen. Mozilla hat bereits angekündigt, bei der Umsetzung des Manifest v3 für Firefox Schnittstellen wie das WebRequest API, auf das Werbe- und Tracking-Filter angewiesen sind, weiterhin bereitzustellen.

Was ist zu tun?

Wer einen Chromium-Abkömmling als Browser verwendet, sollte die Berichterstattung über die Leistung der verfügbaren Tracking-Blocker im Blick behalten und bei Bedarf die Browserplattform wechseln. Für Nutzende von Firefox bzw. darauf basierenden Browsern ändert sich nichts: Die Möglichkeiten, Tracking-Inhalte zu filtern, bleiben unverändert gut.

10.2 „Soft Deletion“ in Datenbanken – warum dies kein Löschen ist

Für komplexe Datenbankanwendungen etabliert sich das Entwurfsmuster (Pattern) **„Soft Deletion“**. Hintergrund ist häufig, dass Löschungen in einer Datenbank so durchgeführt werden sollen, dass einzelne Datensätze einfach wiederhergestellt werden können. In einigen Szenarien sind Löschprozesse auch so zeitaufwendig, dass sie andere Datenbankprozesse erheblich beeinträchtigen.

Kernidee von „Soft Deletion“ ist es, das Löschen eines Datenbankeintrags durch eine „Löschen“-Markierung zu ersetzen: Beispielsweise wird eine neue Tabellenspalte „isDeleted“ angelegt und der Löschbefehl wird dadurch ersetzt, dass der jeweilige Wert „isDeleted“ auf „1“ gesetzt wird.

In Datenbanken mit vielen Bezügen der Datensätze untereinander müssen diese – anders als beim normalen Löschen – nicht überall aufgelöst werden, was sonst sehr aufwendig sein kann.

Mit „Soft Deletion“ sind aber einige Risiken und Hürden zu bedenken – nicht nur bei personenbezogenen Daten:

So müssen dauerhaft und konsequent alle Such- und Leseanfragen an die Datenbankanwendung überarbeitet werden, sodass Datensätze mit einem positiven „isDeleted“-Feld aussortiert werden.

Ist die Löschung eines Eintrags aus datenschutzrechtlichen Gründen geboten – z. B. aufgrund der zeitlichen Speicherbegrenzung (Art. 5 Abs. 1 e) DSGVO) oder des Rechts auf Löschen (Artikel 17 DSGVO) – so wird die Umsetzung mithilfe des Ansatzes „Soft Deletion“ in der Regel nicht der gesetzlichen Anforderung genügen können.

Nicht zuletzt ist zu bedenken, dass beim Einsatz von „Soft Deletion“ in einer Datenbankanwendung immer noch die Bezüge zu einem (nun gelöschten) Eintrag erhalten bleiben. Aus der Information, dass es bei einer betroffenen Person überhaupt einen solchen Bezug gegeben hat, könnte bereits ein Risiko für die Rechte und Freiheiten der betroffenen Person entstehen.

Was ist zu tun?

Der Einsatz von „Soft Deletion" in Datenbankanwendungen mit personenbezogenen Daten ist mit einigen schwer absehbaren Risiken verbunden. Im Einzelfall muss geprüft werden, wie diese Risiken minimiert werden können.

10.3 Data Mesh

Data Mesh ist ein relativ neuer Ansatz für eine **dezentrale Datenarchitektur**. Damit sollen beispielsweise Teams in der Softwareentwicklung die Möglichkeit haben, selbstständig Datenanalysen über das Verhalten von Nutzerinnen und Nutzern durchzuführen und diese mit anderen Teams auszutauschen. Das Prinzip ist übertragbar auf Organisationen mit fachlich stark spezialisierten Teams, die gemeinsam Erkenntnisse aus Datensammlungen gewinnen wollen.

Der Unterschied zu zentralen Datenarchitekturen wie **Data Warehouses** (ein physischer Datenbestand mit vereinheitlichten Daten aus mehreren Quellen) oder **Data Lakes** (ein System von Daten, die im Rohformat vorliegen) ist, dass anstelle einer zentralen Organisationseinheit jedes Team verantwortlich für die Datensammlung und -kuration ist – jeweils in dem eigenen Fach- bzw. Wissensgebiet (Domäne).

Mit der Idee eines Data Mesh (deutsch in etwa: Datengewebe), die auf der Theorie des „Domain-driven Design" fußt, können die jeweils erfassten und aufbereiteten Daten als „Datenprodukte" verstanden werden, die auch über mehrere fachliche Domänen hinweg genutzt werden können. Die dezentrale Datenverantwortung legt dabei auch eine dezentrale Speicherung nahe.

Der Begriff „Data Mesh" wurde erst 2019 in einem Aufsatz von Zhamak Dehghani geprägt. Die von ihr beschriebenen Probleme von zentralen Datenarchitekturen und die von ihr eingeführten Prinzipien für die Umsetzung eines Data Mesh haben vielfach zu einem Paradigmenwechsel in Datenstrategien von Organisationen geführt.

Domain-driven Design

Mit Domain-driven Design wird eine Herangehensweise an die Modellierung komplexer Software beschrieben, die einen Schwerpunkt auf Fachlichkeit und Fachlogik und die Zusammenarbeit und Einbeziehung von Fachleuten legt.

Sofern in einem Data Mesh auch personenbezogene Daten verarbeitet werden – wozu auch schon Daten zum Nutzungsverhalten zählen können –, müssen selbstverständlich die Vorgaben der Datenschutz-Grundverordnung eingehalten werden. So muss die datenschutzrechtliche Verantwortlichkeit geklärt werden und welche technischen und organisatorischen Maßnahmen für alle Beteiligten verbindlich vorgeschrieben werden – unabhängig von der beabsichtigten Selbstständigkeit der Teams.

Werden die Daten dezentral gespeichert und verarbeitet, müssen zudem Prozesse entwickelt werden, um die Wahrnehmung von Rechten der betroffenen Personen zu gewährleisten. Verfahren, die Betroffenen die Ausübung ihrer Rechte ermöglichen, beispielsweise des Auskunftsrechts oder des Rechts auf Löschung, sind dabei nicht immer trivial umzusetzen.

Daher bietet sich eine frühzeitige Anonymisierung und Aggregation von Daten an, um in weiteren Verarbeitungs- und Nutzungsschritten mehr Flexibilität zu erlangen. Dies kann schon bei der Datensammlung in den fachlich zuständigen Teams erfolgen.

Was ist zu tun?

Verantwortliche, die eine Umsetzung der Datenarchitektur „Data Mesh“ anstreben, müssen bei der Verarbeitung von personenbezogenen Daten die datenschutzrechtlichen Anforderungen prüfen und gegebenenfalls Maßnahmen ergreifen, um die Rechte und Freiheiten betroffener Personen zu schützen.

11

KERNPUNKTE

Themen der Key Provisions Expert Subgroup

Leitlinien zum Auskunftsrecht

Leitlinien zu Verantwortlichen und Auftragsverarbeitern

11 Europa und Internationales

11.1 Themen der Key Provisions Expert Subgroup

Das ULD ist als Vertreter der Aufsichtsbehörden der Länder Mitglied in der **Key Provisions Expert Subgroup (KEYP)** des Europäischen Datenschutzausschusses (EDSA). Die Arbeitsgruppe befasst sich mit allen Grundsatzfragen und wesentlichen Begrifflichkeiten der DSGVO. Die KEYP hat auch im Berichtszeitraum coronabedingt aus der Ferne – remote – zusammengearbeitet. Das ULD hat dabei die Funktion, die Themen und Diskussionspunkte unter den Ländern und mit dem BfDI abzustimmen und in der Expertenarbeitsgruppe zu vertreten. Eine intensive Betreuung von Leitlinien in der Rolle eines Berichterstatters (sogenannter Rapporteur) war aufgrund der knappen Personalressourcen nicht möglich.

Im Berichtszeitraum hat sich die Arbeitsgruppe mit einer Vielzahl von Themen beschäftigt. Abgeschlossen wurden die Arbeiten an den Leitlinien zum Auskunftsrecht (Tz. 11.2), die damit einen weiteren Baustein der Leitlinien zu den Betroffenenrechten zur Verfügung stellt. Hervorzuheben ist des Weiteren die Bearbeitung von Fragen zu den Leitlinien zur federführenden Behörde, die erstmals im Mai 2018 als WP 244 rev.01 und dann im Oktober 2022 als Leitlinien 8/2022 vom EDSA verabschiedet wurde. Die erarbeiteten Änderungen sind derzeit noch Gegenstand einer öffentlichen Konsultation und betreffen u. a. die Frage, wie die federführende Behörde in Fällen einer gemeinsamen Verantwortlichkeit zu bestimmen ist. Es wurde nochmals klargestellt, dass die Verantwortlichen bestimmen, wer welche Aufgaben im Rahmen einer gemeinsamen Verarbeitung übernimmt. Allerdings sind die Aufsichtsbehörden bei ihrer Aufsichtstätigkeit nicht an Vereinbarungen zwischen den Verantwortlichen bei der Bestimmung ihrer Zuständigkeit gebunden. Insbesondere hat auch die Festlegung einer Hauptniederlassung der gemeinsam Verantwortlichen für die gemeinsam zu verantwortenden Verarbeitungen nicht notwendig Auswirkungen auf die Zuständigkeit der Aufsicht.

Ein weiterer wesentlicher Schwerpunkt der Arbeit bestand in der Ausarbeitung der Leitlinien zum berechtigten Interesse nach Art. 6 Abs. 1 Buchst. f DSGVO. Die Rechtsgrundlage ermöglicht Verantwortlichen die Verarbeitung in einer Vielzahl von Fällen zur Wahrung ihrer berechtigten Interessen. Maßgeblich ist, dass dabei nicht die entgegenstehenden Interessen der betroffenen Person überwiegen. Die Rechtsgrundlage ermöglicht somit Verarbeitungen von Organisationen, die nicht in unmittelbarem Zusammenhang mit einer Vertragsabwicklung stehen oder mit einer gesetzlichen Aufgabenerfüllung einhergehen. Die Abwägung der Interessen der Organisation und der betroffenen Personen stellt hier einen wesentlichen Schwerpunkt dar. Die Finalisierung der Leitlinien wird für 2023 erwartet.

Art. 6 Abs. 1 Buchst. f DSGVO

[...] die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte oder Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

11.2 Leitlinien zum Auskunftsrecht

Die Leitlinien 01/2022 des EDSA zum Auskunftsrecht (englisch: Right of Access) behandeln ein wichtiges Recht der Menschen zur Gewährleistung des Grundrechts auf Datenschutz aus Artikel 8 Charta der Grundrechte der Europäischen Union (GRCh). Erst das Wissen über eine Verarbeitung ermöglicht es, die Richtigkeit personenbezogener Daten und die Berechtigung zur Verarbeitung selbst zu prüfen oder überprüfen zu lassen. Das Auskunftsrecht nach Artikel 15 DSGVO ermöglicht damit Transparenz über die Arten und Kategorien personenbezogener Daten bei einer Organisation. Zwar kann durch das Auskunftsrecht die Rechtmäßigkeit der Verarbeitung in Gänze nicht umfassend geprüft werden, doch ermöglicht es der von einer Verarbeitung betroffenen Person einen Überblick über den Umfang und die Zwecke der Verarbeitung.

Artikel 8 GRCh:
Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

Die Leitlinien zum Auskunftsrecht beleuchten die Grundlagen des Rechts auf Auskunft nach Maßgabe des Artikels 15 DSGVO und stellen – auch anhand von Beispielen – dar, welche Rechte betroffene Personen und welche Pflichten verantwortliche Organisationen bei der Beauskunftung haben. Dabei werden die Form und die Modalitäten der Auskunft dargestellt.

Grundsätzlich muss eine Auskunft erfragende Person keine Gründe angeben, warum sie die Auskunft verlangt. Unternehmen, öffentliche Stellen und andere Organisationen sind verpflichtet zu bestätigen, ob bei ihr personenbezogene Daten der anfragenden Person verarbeitet – d. h. beispielsweise aufbewahrt, weitergegeben oder genutzt – werden. Die betroffene Person muss Zugang zu diesen Daten erhalten. Dies geschieht in der Regel durch die Übersendung einer elektronischen oder analogen Kopie oder auch durch die Gewährung eines Online-Zugangs. Weitere Informationen, die bereitzustellen sind, umfassen die Zwecke der Verarbeitung, die Kategorien von Daten und Empfängern, die Dauer der Verarbeitung, die Betroffenenrechte sowie die Sicherheiten bei Übermittlungen der Daten in Drittländer außerhalb der EU, bei denen kein angemessenes Datenschutzniveau bestätigt wurde.

Die allgemeinen Prinzipien des Rechts auf Auskunft umfassen:

- Vollständigkeit der Information,
- Richtigkeit der Information,
- Eingang des Antrags als Referenzzeitpunkt für die Auskunft,
- Sicherheit der Übermittlung der Information.

Das Recht auf Auskunft ist vom Recht auf Zugang zu öffentlichen Informationen zu unterscheiden. Letzteres zielt darauf ab, die Transparenz von Entscheidungen und der Praxis der öffentlichen Verwaltung zu ermöglichen.

Die Leitlinien in englischer Sprache sind unter dem folgenden Link abrufbar:

https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf

Kurzlink: *https://uldsh.de/tb41-11-2a*

Zu den Leitlinien zum Auskunftsrecht wurde eine öffentliche Konsultation durchgeführt. Eine abschließende Fassung ist noch in Bearbeitung. Die Anmerkungen aus der öffentlichen Konsultation können unter dem folgenden Link eingesehen werden:

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en

Kurzlink: *https://uldsh.de/tb41-11-2b*

Was ist zu tun?

Die EDSA-Leitlinien zum Auskunftsrecht sollen Verantwortlichen, Bürgerinnen und Bürgern sowie der Datenschutzaufsicht eine Hilfestellung bei der einheitlichen Auslegung und Anwendung des Artikels 15 DSGVO zur Gewährleistung des Grundrechts auf Datenschutz geben.

11.3 Leitlinien zu Verantwortlichen und Auftragsverarbeitern – nun in Deutsch

Die deutsche Übersetzung der im Juli 2021 vom EDSA angenommenen Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO wurde im Berichtszeitraum abgeschlossen und steht nunmehr in deutscher Sprache zur Verfügung.

Die Leitlinien beschreiben die Komponenten der gesetzlichen Begriffsdefinitionen sowie die rechtlichen und praktischen Folgen der Zuweisung: die Beziehung zwischen Verantwortlichem und Auftragsverarbeiter und dessen Auswahl sowie bei einer gemeinsamen Verantwortlichkeit.

Ein klares Verständnis der Begriffe „Verantwortlicher", „gemeinsam Verantwortliche" und „Auftragsverarbeiter" ermöglicht eine passgenaue Zuordnung der bei der Verarbeitung personenbezogener Daten beteiligten Stellen. Sie bestimmt, wer für die Einhaltung der Datenschutzvorschriften verantwortlich ist und gegenüber welcher Organisation die betroffene Person ihre Rechte durchsetzen kann. Es handelt sich dabei um funktionelle Konzepte, d. h., es kommt nicht darauf an, wie sich die Organisation selbst bezeichnet, sondern darauf, welche Aufgaben und Rollen tatsächlich ausgeführt werden.

Die Leitlinien führen aus, wie Verantwortlichkeit nach der gesetzlichen Definition bestimmt werden kann. Danach legt ein Verantwortlicher die Zwecke und Mittel der Verarbeitung fest, d. h. das Warum und das Wie der Verarbeitung, und entscheidet über die dafür verwendeten wesentlichen Mittel. Eine gemeinsame Verantwortlichkeit liegt vor, wenn zwei oder mehr Stellen an der Festlegung der Zwecke und Mittel eines Verarbeitungsvorgangs beteiligt sind. Die Beteiligung muss relevante Auswirkungen auf die Bestimmung der Zwecke und Mittel der Verarbeitung haben, sodass die Verarbeitung ohne die Beteiligung beider Parteien nicht möglich wäre und ihre Beiträge notwendig miteinander verbunden sind. Ein Auftragsverarbeiter agiert demgegenüber als eine eigenständige Einheit, die personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen verarbeitet.

Die Leitlinien haben eine hohe praktische Bedeutung, insbesondere bei komplexen Verarbeitungssituationen, an denen unterschiedliche „Dienstleister" beteiligt sind. Nur bei einer exakten Bestimmung der Rollen können die Rechte und Pflichten der DSGVO wahrgenommen und es kann dem Grundsatz der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO Genüge getan werden.

Die Stellungnahme ist unter dem folgenden Link abrufbar:

https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_de.pdf

Kurzlink: *https://uldsh.de/tb41-11-3*

11.4 Akkreditierung und Zertifizierung in der europäischen Expert Subgroup

Die u. a. für Fragen der Akkreditierung und Zertifizierung auf europäischer Ebene zuständige **Compliance, eGovernment und Health Expert Subgroup (CEH Expert Subgroup)** hat sich im Berichtszeitraum wieder mit einer Vielzahl von Fragen rund um diese Themen beschäftigt, wobei wir unsere Erfahrungen auch dieses Mal an vielen unterschiedlichen Stellen einbringen konnten.

So wurden, ebenso wie das Papier zu den Anforderungen an datenschutzrechtliche Zertifizierungsprogramme in Deutschland (Tz. 9.2), die „Guidance – Addendum (Annex to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation) Certification criteria assessment" überarbeitet, um sie an neue Entwicklungen anzupassen.

Diese Überarbeitung war und ist eng verknüpft mit der Beratung und Klärung von Grundsatzfragen im Themenbereich der Zertifizierung, aber auch der Akkreditierung. Diese sich verändernden Anforderungen und zu klärenden Fragestellungen sind das Ergebnis der **zunehmenden Einreichung vielfältiger nationaler datenschutzrechtlicher Zertifizierungsprogramme**, die jeweils durch die zuständigen Datenschutzaufsichtsbehörden genehmigt werden müssen und für die der Europäische Datenschutzausschuss (EDSA) eine Stellungnahme abgeben muss – was bei den ersten Verfahren auch geschah. Hinzu kam ein erstes europäisches Verfahren, das durch den EDSA genehmigt werden musste und zu zahlreichen Diskussionen innerhalb der Subgroup führte.

Auch war es beispielsweise im Rahmen von Fragen zur Datenübermittlung in Drittstaaten gemäß Artikel 46 DSGVO notwendig, die Auffassungen der **International Transfer Subgroup (ITS)** zu beachten und diese bei der Klärung spezieller Aspekte in diesem Themenfeld einzubinden.

Darüber hinaus konnten wir uns auch im zurückliegenden Berichtszeitraum in die Bewertung von Zertifizierungskriterien aus Deutschland sowie aus anderen Mitgliedstaaten und in die Erstellung von Stellungnahmen zu diesen einbringen und so wichtige Erkenntnisse für die Verfahren deutscher Antragsteller gewinnen. Zudem haben wir uns wieder an der Erstellung von Stellungnahmen ergänzender Akkreditierungskriterien zur ISO 17065 anderer EU-Mitgliedstaaten beteiligt.

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/tb41-11-4*

Was ist zu tun?

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

12

KERNPUNKTE

Konferenz der Informationsfreiheitsbeauftragten Deutschlands

Leitung Arbeitskreis Informationsfreiheit

Grundlegendes aus Gesetzgebung und Rechtsanwendung

12 Informationsfreiheit

2022 war ein besonderes Jahr für uns. Das ULD hatte den Vorsitz über die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) inne (Tz. 12.1). Dies beinhaltete auch die Leitung des zugehörigen Arbeitskreises Informationsfreiheit mit entsprechenden Sitzungen in Kiel (Tz. 12.2). Daneben fand aber auch das normale Dienstgeschehen in der Behörde der Landesbeauftragten für Informationszugang statt. Nachdem in den letzten beiden Jahren Corona auch Thema vieler Verfahren war, waren es 2022 wieder viele Einzelthemen, die uns im Bereich der Informationsfreiheit beschäftigten (Tz. 12.3). Einige Gesetzesänderungen und besondere Fälle stachen heraus (Tz. 12.4).

12.1 Vorsitz der Konferenz der Informationsfreiheitsbeauftragten

Turnusgemäß übernahm das ULD Anfang des Jahres den Vorsitz der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) von dem Landesbeauftragten für Informationsfreiheit Sachsen-Anhalt. **Zwei jeweils zweitägige Konferenzen** fanden im Juni und November 2022 in Kiel statt. Teilnehmer waren die Landesbeauftragten der Länder und des Bundes, die schon über ein Transparenzgesetz bzw. Informationsfreiheitsgesetz verfügen. In Deutschland sind nur noch Bayern und Niedersachsen ohne eine entsprechende rechtliche Regelung ausgestattet. In Sachsen wurde im Berichtszeitraum ein entsprechendes Gesetz verabschiedet, sodass sie ebenfalls eingebunden wurden.

Insgesamt drei Entschließungen konnten unter unserer Leitung von der IFK verabschiedet werden:

- Keine Umgehung der Informationsfreiheit durch Errichtung von Stiftungen bürgerlichen Rechts!
- SMS in die Akte: Behördliche Kommunikation unterliegt umfassend den Regeln der Informationsfreiheit!
- Niedersachsen: Die Zeit für ein Transparenzgesetz ist gekommen!

Daneben wurden zwei Arbeitsgruppen ins Leben gerufen. Eine wird sich unter der Leitung von Baden-Württemberg und Schleswig-Holstein über den Berichtszeitraum hinaus mit Vorgaben für Transparenzportale beschäftigen. Die andere nimmt sich unter der Leitung Schleswig-Holsteins des Themas „Informationsfreiheit by Design“ an, entwickelt entsprechende Prinzipien und wird u. a. für die **E-Akte** Empfehlungen geben, wie Informationsfreiheit schon bei der Implementierung entsprechender Systeme mitgedacht und eingebunden werden kann.

Für spannende Diskussionen sorgten auch einige Gäste bei den Konferenzen. Dabei nutzten wir auch unsere Nähe zu Skandinavien und insbesondere Schweden, wo es schon seit dem 18. Jahrhundert ein Informationsfreiheitsrecht gibt. Prof. Dr. Meiko Jensen von der Karlstads Universitet in Schweden berichtete über „Datenreduktion vor Herausgabe von Informationen – der Werkzeugkasten der Kryptographen“. Nils Gunnar Indahl, Datenschutzbeauftragter der Norwegischen Kirche, stellte vor, welchen Zugang Bürgerinnen und Bürger in Schweden, Norwegen und Dänemark zu Informationen der öffentlichen Verwaltung haben und ob diese Praxis konform mit der DSGVO erfolgt. Auch Prof. Dr. Matthias Rossi von der Universität Augsburg kam nach Kiel, um Harmonisierungsbedarf und Harmonisierungspotenzial des Informationsfreiheitsrechts zu besprechen.

Die Protokolle und Materialien der Konferenzen sind öffentlich und können hier eingesehen werden:

https://www.datenschutzzentrum.de/artikel/1347-.html

Kurzlink: *https://uldsh.de/tb41-12-1*

2023 übernimmt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit den Vorsitz der IFK.

Was ist zu tun?

Auch nach unserem Vorsitz der IFK engagieren wir uns hierbei weiter. Insbesondere in den beiden von uns mitbetreuten Arbeitsgruppen gibt es noch viel zu tun.

12.2 Leitung Arbeitskreis Informationsfreiheit

Das ULD hat dieses Jahr den Arbeitskreis Informationsfreiheit (AKIF) geleitet, der insbesondere die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (Tz. 12.1) vorbereiten soll. Zwei Treffen fanden jeweils im Mai und September in Kiel statt. Letzteres war so terminiert, dass das Treffen direkt im Anschluss an die Sommerakademie des ULD stattfand. Dies ermöglichte es dem AKIF, sich und seine Arbeit auf der Sommerakademie im Rahmen einer sogenannten Infobörse den Besuchern zu präsentieren und für Fragen zur Verfügung zu stehen.

Auf Sitzungen wurden die Entwürfe für die Entschließungen der IFK (Tz. 12.1) erarbeitet und auch die Arbeiten der eingerichteten Arbeitsgruppen besprochen. Hinzu kamen Diskussionen zu Themen wie anonyme Antragstellungen, Regelungen zur Datennutzung, Data Act der EU, Datenqualität, Hinweispflichten von informationspflichtigen Stellen auch über die Auskunftserteilung hinaus und tagesaktuelle Fragen.

Wir haben zwei Vorträge für die Teilnehmerinnen und Teilnehmer organisiert. Dr. Moritz Karg vom Ministerium u. a. für Digitalisierung in Schleswig-Holstein berichtete zu Erfahrungen beim Aufbau des Transparenzportals des Landes Schleswig-Holstein. Weiterhin haben Philipp Waack und Christin Schäfer von acs plus zu „Blinder Fleck: Sensitive Geschäftsinformationen in technischen Daten" referiert, wobei sie die Fragen der Erkennbarkeit eines Personenbezugs in einem Datenbestand auf sensible Geschäftsinformationen übertragen haben.

Auch haben wir einen monatlichen virtuellen Austausch der Gruppe eingeführt, der sich schnell bewährt hat und ermöglicht, auch auf aktuelle Themen kurzfristig zu reagieren.

Protokolle und andere Dokumente zu den Sitzungen sind öffentlich und können hier eingesehen werden:

https://www.datenschutzzentrum.de/artikel/1398-Arbeitskreis-Informationsfreiheit-AKIF.html

Kurzlink: *https://uldsh.de/tb41-12-2*

2023 wird der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit turnusgemäß den AKIF leiten.

Was ist zu tun?

Das ULD wird sein Engagement im AKIF fortsetzen.

12.3 Top 5 der Themen in Schleswig-Holstein

Unsere Hauptaufgabe im Bereich der Informationsfreiheit war auch 2022 die **Vermittlung bei Beschwerden** von Antragstellenden über vermeintlich unzureichende Beantwortung ihrer Anträge durch informationspflichtige Stellen. Auch wurden wir von einigen informationspflichtigen Stellen zu speziellen Fragen eingebunden. Nachdem in den letzten beiden Jahren ein Schwerpunkt auf Informationsanfragen rund um Corona und den Umgang der Behörden mit diesem Thema lag, waren 2022 wieder viele unterschiedliche Problembereiche an der Tagesordnung. Dabei traten sehr ähnliche Missstände auf, wie wir sie regelmäßig hier aufgelistet haben (vgl. u. a. 40. TB, Tz. 12.3):

1. An erster Stelle steht weiterhin die **Nichtbeantwortung** von Anfragen. Das Informationszugangsgesetz Schleswig-Holstein (IZG-SH) verpflichtet informationspflichtige Stellen innerhalb eines Monats zu antworten. Dies kann zwar bei umfangreichen Angelegenheiten um einen weiteren Monat verlängert werden, aber auch hierüber muss innerhalb des ersten Monats begründet informiert werden. In vielen Fällen konnte nach Bitte um Stellungnahme und Hinweis durch uns dann doch die Beantwortung der Anfragen erreicht werden.

2. Sehr nah an dem vorherigen Punkt ist der Umstand, dass einige informationspflichtige Stellen Anfragen offensichtlich nicht als IZG-Anfrage verstanden haben und deshalb nicht fristgerecht reagierten. Eine Nennung des IZG-SH ist in der Anfrage nicht erforderlich, wie auch nicht Stichworte wie „Informationsfreiheit" oder „Informationszugang". Die Behörde ist verpflichtet, Anfragen nach Informationen entsprechend **auszulegen** und nach dem IZG-SH zu behandeln.

3. Wenn die informationspflichtigen Stellen Ablehnungsgründe nach §§ 9 oder 10 IZG-SH für ihren Fall identifiziert hatten, so wurde mehrfach übersehen, dass meist noch eine **Abwägung** zwischen dem Geheimhaltungsinteresse (etwa der Betroffenen bei personenbezogenen Daten oder Betriebs- und Geschäftsgeheimnissen) und dem Veröffentlichungsinteresse erfolgen musste und auch Anhörungen durchzuführen sind. Bezüglich der Abwägung reicht unseres Erachtens ein Halbsatz, dass eine Abwägung erfolgt sei, nicht als Begründung aus.

4. Auch besteht weiterhin bei einigen Stellen der Hang dazu, bei Vorliegen von Ausschlussgründen **pauschal** den Informationszugangsantrag abzulehnen. Dabei müsste genauer untersucht werden, welche Informationen tatsächlich etwa personenbezogen sind und welche nicht. Erstere könnten dann z. B. geschwärzt und letztere herausgegeben werden. Hierbei ist auch zu beachten, dass Schwärzungen stets im Rahmen des Bescheids begründet werden müssen.

In der Praxis trat diese Frage besonders oft im Rahmen von Bauakten auf. Hierbei war jedoch auch zu beachten, dass insbesondere bei dieser Art der Informationen der Personenbezug sehr weit gehen kann, da auch etwa die Ausgestaltung des Baus Bezug zur Person haben kann.

5. Immer wieder wurden die **Versagungen von Informationen** durch die Behörden eher informell an die Anfragende bzw. den Anfragenden übermittelt. Dabei handelt es sich jedoch um einen Bescheid, für den § 6 IZG-SH auch formelle Anforderungen aufstellt. So fehlten oft eine aussagekräftige Begründung und auch der Hinweis auf Rechtsschutzmöglichkeiten. Für die Petentin bzw. den Petenten hat Letzteres zwar den Vorteil, dass verlängerte Fristen etwa für den Widerspruch gelten, doch zeigt es auch, dass noch nicht bei allen informationspflichtigen Stellen der **verpflichtende Charakter** der Informationsfreiheit angekommen zu sein scheint.

Wir haben eine **Broschüre** mit den wichtigsten Hinweisen zum Informationsfreiheitsrecht in Schleswig-Holstein herausgegeben, die regelmäßig online aktualisiert wird:

https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-7-Informationszugang.pdf

Kurzlink: *https://uldsh.de/tb41-12-3*

Was ist zu tun?

Wir werden weiterhin bei Beschwerden von Antragstellenden vermitteln und gegebenenfalls bei informationspflichtigen Stellen auf die Einhaltung der gesetzlichen Vorgaben hinwirken. Mit Schulungen und Informationsmaterial soll die Sensibilisierung für diesen Bereich gesteigert werden.

12.4 Grundlegendes aus Gesetzgebung und Rechtsanwendung zum Informationszugang

Die Leiterin des ULD ist nach § 14 Informationszugangsgesetz Schleswig-Holstein (IZG-SH) auch die Landesbeauftragte für Informationszugang. Durch eine **Gesetzesänderung** in diesem Jahr wurden auch deren Befugnisse ausgeweitet. Das alte Recht berief sich insbesondere auf einen Verweis auf das LDSG, was jedoch spätestens seit dem Inkrafttreten der DSGVO Unklarheiten erzeugte (vgl. u. a. 39. TB, Tz. 12.1 und 40. TB, Tz. 12.1). Im Mittelpunkt steht weiterhin die Vermittlung in Streitfällen zwischen Antragsteller(inne)n und informationspflichtigen Stellen. Genauer geregelt ist jetzt, dass diese Stellen uns Auskünfte erteilen, Einsicht in Vorgänge und Aufzeichnungen und auch Zutritt zu ihren Diensträumen gewähren müssen. Auch können nunmehr Beanstandungen ausgesprochen werden.

Seit dem 1. Januar 2022 sind die Landesbehörden zu deutlich mehr aktiver **Transparenz** verpflichtet. Der § 11 IZG-SH zur Veröffentlichung von Informationen besteht zwar schon länger, doch erst mit dem oben genannten Stichtag sind einige weitere Teile der Regelung in Kraft getreten. Landesbehörden (mit einigen Ausnahmen wie Schulen oder Landrätinnen und Landräte) sollen zwar schon länger Erlasse, Haushaltspläne usw. aktiv veröffentlichen und in das Transparenzportal des Landes einstellen. Neu hinzugekommen sind nun aber u. a. Gutachten, Übersichten über Zuwendungen, Gerichtsentscheidungen, wesentliche Unternehmensdaten von Beteiligungen des Landes und Verträge. Auch schon länger erfasst sind elektronisch erteilte Auskünfte aufgrund der Anträge nach dem IZG-SH, was noch nicht überall vollumfänglich zu erfolgen scheint.

Im Berichtszeitraum ist auch das **Offene-Daten-Gesetz (ODaG)** des Landes in Kraft getreten. Dieses Gesetz regelt die Bereitstellung unbearbeiteter Daten der Träger der öffentlichen Verwaltung des Landes Schleswig-Holstein als offene Daten, um damit den freien und ungehinderten Zugang der Allgemeinheit zu allen nicht schützenswerten, digitalen Daten zu stärken (§ 1 Abs. 1 ODaG). Die Landesbehörden sollen hiervon im Rahmen ihrer verfügbaren Ressourcen Gebrauch machen. Allerdings wird ein Anspruch auf Bereitstellung unbearbeiteter Daten durch das Gesetz nicht begründet. Im Berichtszeitraum hatten wir hiermit noch keine konkreten Berührungspunkte außer einem grundsätzlichen Interesse der Kollegen der IFK an der Ausgestaltung in Schleswig-Holstein. Die weitere Entwicklung werden wir jedoch sehr interessiert beobachten.

Weiterhin beschäftigt uns immer wieder die Frage, wann auch **private Stellen** als informationspflichtige Stellen angesehen werden können (vgl. auch 39. TB, Tz. 12.3). Das Gesetz nimmt auch diese in die Pflicht, soweit ihnen Aufgaben der öffentlichen Verwaltung zur Erledigung in den Handlungsformen des öffentlichen Rechts, insbesondere Aufgaben in den Bereichen Wasserversorgung und Abwasserentsorgung, Abfallentsorgung, öffentlicher Nahverkehr, Energieerzeugung und -versorgung oder Krankenhauswesen, übertragen wurden. Konkret hatte in diesem Jahr ein städtisches Unternehmen im Bereich Fernwärme einen entsprechenden Antrag mit der Begründung abgelehnt, nicht vom IZG-SH erfasst zu sein. In einem anderen Fall betraf es den Betreiber einer Sportstätte. Während für Letzteres zumindest eine Teilauskunft

erreicht werden konnte, ist der Fall zur Fernwärme noch offen und spitzt sich auf die Frage zu, wann eine Erledigung in den Handlungsformen des öffentlichen Rechts konkret vorliegt. Wir werden im nächsten Tätigkeitsbericht dazu berichten.

Mit dem IZG-SH ging auch die Zusammenführung des Informationsfreiheitsrechts mit dem Umweltinformationsrecht einher. Für Umweltinformationen gibt es einige Erleichterungen. So gelten beim Zugang zu Informationen über **Emissionen** nicht die Versagungsgründe u. a. bezüglich personenbezogener Daten und Betriebs- und Geschäftsgeheimnisse. Im Berichtszeitraum betraf das beispielsweise die Frage, inwieweit potenzielle Grundwasserverunreinigungen im Zusammenhang mit einem Schießplatz unter diese Norm fallen. Dies haben wir grundsätzlich bejaht und daher zur näheren Beurteilung die Einsicht in die umstrittenen Informationen verlangt.

Immer noch steht der **Bericht des Landtages** zu den Auswirkungen des IZG-SH nach § 16 IZG-SH aus. Dieser hätte 2020 vorgelegt werden müssen.

Was ist zu tun?

Einige Gesetzesänderungen haben zu spürbaren Verbesserungen der Idee der Transparenz in Schleswig-Holstein geführt. Wo noch Unklarheiten bestehen, sollten diese in der nächsten Zeit ausgeräumt werden.

13

KERNPUNKTE

DATENSCHUTZAKADEMIE Schleswig-Holstein

Sommerakademie

13 DATENSCHUTZAKADEMIE Schleswig-Holstein

Die DATENSCHUTZAKADEMIE Schleswig-Holstein ist für die Konzeption und Organisation der **Fortbildungsveranstaltungen zu den Themenbereichen Datenschutz und Informationsfreiheit** zuständig. Im Einklang mit der Datenschutz-Grundverordnung (DSGVO) wird so beispielsweise den behördlichen und betrieblichen Datenschutzbeauftragten entsprechendes Fachwissen vermittelt.

13.1 Sommerakademie – jährliche Datenschutzkonferenz in Kiel

Nach der coronabedingten Pause war im Jahr 2022 die Teilnahme an der alljährlich an einem Montag im Spätsommer stattfindenden Sommerakademie der DATENSCHUTZAKADEMIE möglich. Diese erfreute sich wieder großer Beliebtheit und zog Datenschutzexpertinnen und -experten sowie andere Interessierte aus dem gesamten Bundesgebiet an die Kieler Förde.

Die **Sommerakademie 2022** stand ganz unter dem Zeichen der Informationsfreiheit. Das Thema lautete **„Informationsfreiheit by Design – und der Datenschutz?!“**. Aus unterschiedlichen Blickwinkeln wurden die teils kontroversen Meinungen ausgetauscht und durchaus konstruktiv um ein gemeinsames Verständnis der verschiedenen Fallgestaltungen gerungen.

Die Konferenz war geleitet von dem Grundgedanken der Informationsfreiheit und den damit einhergehenden weiteren Fragestellungen: Alle haben das Recht, Auskunft über Informationen bei öffentlichen Stellen zu verlangen. So soll mehr Transparenz über das Behördenhandeln und damit eine Nachvollziehbarkeit von Entscheidungen erreicht werden. Für viele Behörden war es in der Einführungszeit der Informationsfreiheitsgesetze ungewohnt, sich derart auf die Finger schauen zu lassen. Inzwischen werden die Gesetze zu modernen Transparenzgesetzen umgestaltet, die die öffentlichen Stellen verpflichten, proaktiv Informationen in Transparenzportalen zu veröffentlichen. Die Nachfrage nach nutzbaren Daten steigt – für das Gemeinwohl, für die Wirtschaft, für eine Berichterstattung in den Medien und auch zu ganz individuellen Zwecken von Privatpersonen.

Behörden stehen vor praktischen Problemen: Aus kleinen Anträgen kann ein großer Aufwand resultieren. Informationen müssen herausgesucht, Anhörungen durchgeführt und Abwägungen vorgenommen werden. Oft bleibt das Gefühl der Ungewissheit, ob zu wenig oder gar zu viel weitergegeben wurde. Auch kann es zu Problemen kommen, wenn direkt oder indirekt personenbezogene Daten (etwa Bauanträge) abgefragt werden. Transparenzgesetze dürfen nicht zum gläsernen Menschen 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 und vermeintlich anonymisierte Profile können in der Gesamtschau doch wieder einzelne Personen identifizierbar machen – und dann? Sind künstliche Intelligenz und algorithmische Systeme Teil der Lösung – oder werfen sie neue Probleme auf?

Die Diskussion auf der Sommerakademie kann als ein nützlicher Schritt in Richtung einer gemeinsamen Vision für eine rechtssichere, faire und gleichermaßen praktikable Behandlung von Informationszugangsanträgen sowie der proaktiven Bereitstellung von Verwaltungsinformationen verstanden werden. Vor allem mit Blick auf die Europäische Datenstrategie (Tz. 2.3) wird der Datenherausgabe, dem Datenteilen und der

Datennutzung durch Verwaltung und Wirtschaft eine höhere Bedeutung zukommen – umso wichtiger, dass praxisgerechte Möglichkeiten entwickelt werden, damit dies nicht mit den Anforderungen des Datenschutzes kollidiert und etwaige Risiken für die betroffenen Rechtsgüter der betroffenen natürlichen Personen, der Unternehmen und der staatlichen Stellen von Anfang an eingedämmt werden.

Die Beiträge der Vortragenden sind unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/sommerakademie/2022/

Kurzlink: *https://uldsh.de/tb41-13-1*

Index

E

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/