ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

TÄTIGKEITSBERICHT
2020

ULD – SCHLESWIG-HOLSTEINS ZENTRUM FÜR DATENSCHUTZ UND INFORMATIONSZUGANG

Tätigkeitsbericht 2020
des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein

BERICHTSZEITRAUM: 2019

REDAKTIONSSCHLUSS: 31.12.2019

LANDTAGSDRUCKSACHE 19/1992

(38. TÄTIGKEITSBERICHT DER LANDESBEAUFTRAGTEN FÜR DATENSCHUTZ)

Marit Hansen

Landesbeauftragte für Datenschutz Schleswig-Holstein

Leiterin des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein

Impressum

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstraße 98

24103 Kiel

Mail: mail@datenschutzzentrum.de

Web: https://www.datenschutzzentrum.de

Satz und Lektorat: Gunna Westphal, Kiel

Umschlaggestaltung: Martin Papp, Eyekey Design, Kiel

Titelfoto: ULD, Kiel unter Verwendung eines Fotos von Robert Kneschke/stock.adobe.com

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

Inhaltsverzeichnis

01

KERNPUNKTE

Instrumentenkoffer der Aufsicht

Behördliche und betriebliche Datenschutzbeauftragte als Fundament

Datenpannen ernst nehmen

1 Datenschutz und Informationsfreiheit

1.1 Datenschutz aus Europa – der Instrumentenkoffer für die Aufsicht

Die europäische Datenschutzreform hat einiges Neues mit sich gebracht. Darunter waren gar nicht so viele überraschende oder vorher unbekannte Anforderungen an die Verarbeitung personenbezogener Daten, denn vorher bestanden die meisten Rechte und Pflichten schon in ähnlicher Form. Neu ist aber der europaweit stärker vereinheitlichte und umfassendere Katalog an Aufgaben und Befugnissen für die Datenschutzaufsichtsbehörden.

Die Aufgaben ergeben sich aus Artikel 57 der Datenschutz-Grundverordnung, der sie von A bis (fast) Z (genau genommen von Buchstabe a bis Buchstabe v, also 22 Aufgabenbereiche) aufzählt.

Aufgaben in Artikel 57 DSGVO

[…] muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet

a) die Anwendung dieser Verordnung überwachen und durchsetzen;

b) die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder; […]

f) sich mit Beschwerden […] befassen, […]

h) Untersuchungen über die Anwendung dieser Verordnung durchführen, […]

v) jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen.

Aus den Aufgaben ergibt sich, dass die Datenschutzaufsichtsbehörde sowohl anlassbezogene Prüfungen (aufgrund von Beschwerden) als auch anlasslose Untersuchungen vornehmen kann. Wenn Beschwerden einer betroffenen Person in eigener Sache erhoben werden, muss die Aufsichtsbehörde dem nachgehen. Handelt es sich dagegen um Hinweise oder Prüfanregungen an die Aufsichtsbehörde, weil jemand ein möglicherweise datenschutzrechtswidriges Verhalten beobachtet hat, ist die Untersuchung in ihr pflichtgemäßes Ermessen gestellt.

Im öffentlichen Bereich, besonders bei Polizei und Verfassungsschutz, werden in gesetzlichen Regelungen oder in der Rechtsprechung des Bundesverfassungsgerichts Prüfpflichten für die Aufsicht festgeschrieben (37. TB, Tz. 4.2.1). Prüfungen ohne konkreten Anlass sind generell dann sinnvoll oder sogar notwendig, wenn die betroffenen Personen Datenschutzmängel nicht so leicht erkennen können und daher keine Beschwerden bei der Aufsichtsbehörde eingehen. Dazu gehören auch Probleme bezüglich der Informationssicherheit, bei denen vielleicht über Jahre kein Missbrauch von Daten passiert (oder jedenfalls nicht bemerkt wird – das ist ein weiteres Problem!), doch erhebliche Risiken für die betroffenen Personen bestehen können.

Die Befugnisse der Datenschutzaufsicht werden in Artikel 58 DSGVO in Untersuchungs-, Abhilfe- und Genehmigungsbefugnisse unterteilt. Vertreterinnen und Vertreter der Medien fragen regelmäßig die Anzahl und Höhe der verhängten Bußgelder ab – doch die Geldbuße ist nur eine von zahlreichen Abhilfebefugnissen. Es gilt nämlich die für den Einzelfall geeigneten Maßnahmen zu treffen. Dazu können Geldbußen gehören, aber mindestens ebenso wichtig sind Anordnungen (in der DSGVO auch Anweisung genannt) der Aufsichtsbehörde, um die Datenverarbeitung in Einklang mit den rechtlichen Anforderungen zu bringen. Während die Geldbuße in die Vergangenheit wirkt und einen bereits stattgefundenen Verstoß ahndet, wirken Anordnungen in die Zukunft. Das kann so weit gehen, dass die Verarbeitung der personenbe-

zogenen Daten beschränkt oder sogar endgültig untersagt wird.

Abhilfebefugnisse nach Artikel 58 DSGVO

Warnung, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen,

Verwarnung, wenn ein Verstoß vorliegt,

Anweisung, Anträgen der betroffenen Personen auf Ausübung der Betroffenenrechte zu entsprechen,

Anweisung, Verarbeitungsvorgänge in Einklang mit den rechtlichen Anforderungen zu bringen,

Anweisung der Benachrichtigung von betroffenen Personen über Datenpannen,

Verhängung einer Beschränkung der Verarbeitung, einschließlich eines Verbots,

Anordnung zur Berichtigung oder Löschung von personenbezogenen Daten o. Ä.,

Verhängung einer Geldbuße,

Anordnung, eine Übermittlung von Daten an einen Empfänger in einem Drittland auszusetzen.

Der Rahmen für Geldbußen ist in Artikel 83 festgelegt: Für die meist formalen, weniger schweren Verstöße gilt ein Rahmen bis zu 10.000.000 Euro oder im Fall eines Unternehmens bis zu zwei Prozent seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs. Für die schwereren Verstöße gilt ein Bußgeldrahmen bis zu 20.000.000 Euro bzw. vier Prozent des Vorjahresumsatzes. Geldbußen müssen in jedem Einzelfall „wirksam, verhältnismäßig und abschreckend" sein, die Bemessung muss sich an zahlreichen Kriterien orientieren (Artikel 83 DSGVO). Im Interesse einer nachvollziehbaren, transparenten und einzelfallgerechten Form der Bußgeldzumessung sammeln die Aufsichtsbehörden seit Kurzem mit der Anwendung eines Konzepts der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder Erfahrungen.

https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf

Kurzlink: *https://uldsh.de/tb38-11*

Der Umfang der Prüfungen wird durch die zur Verfügung stehenden Ressourcen begrenzt. Ein weiteres Problem besteht aber darin, dass die Verantwortlichen ihrer Rechenschaftspflicht nicht nachkommen können, weil ihnen konkrete Kenntnisse über die Verarbeitung durch Dienstleister fehlen oder weil insgesamt ein undokumentierter und unkontrollierbarer Zustand der Datenverarbeitung zu einer mangelnden Prüfbarkeit führt.

Der Verantwortliche muss einen Bescheid der Datenschutzaufsichtsbehörde nicht hinnehmen, sondern kann dagegen Klage erheben. Gerichtliche Klärungen sind positiv für mehr Rechtssicherheit – gerade angesichts vieler abstrakter Formulierungen in der DSGVO, die einer Konkretisierung bedürfen. Jedoch nimmt der Weg durch die gerichtlichen Instanzen längere Zeit in Anspruch. Wenn am Ende des Gerichtsverfahrens ein rechtskräftiges Urteil steht, hat es manchmal nur noch historischen Wert, weil die beanstandete Verarbeitungstechnik mittlerweile geändert wurde – nicht unbedingt aber im Sinne des Datenschutzes. Dann beginnt die Arbeit der Aufsichtsbehörde quasi von vorne.

Was ist zu tun?

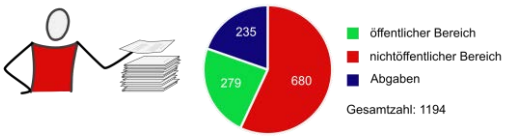
Die Datenschutzaufsichtsbehörden werden sich weiter abstimmen, um deutschland- und europaweit in vergleichbarer Weise das Datenschutzrecht anzuwenden, Prüfungen durchzuführen und Sanktionen zu verhängen.

1.2 Zahlen und Fakten zum Jahr 2019

Rückblende: Kurz bevor die Datenschutz-Grundverordnung am 25. Mai 2018 Geltung erlangte, wurde es hektisch in Deutschland: Alle Datenschutzaufsichtsbehörden wurden mit Tausenden von Fragen bombardiert, wie man denn nun die neuen gesetzlichen Regelungen umsetzen solle. Die Materialien, z. B. Kurzpapiere, die Praxis-Reihe „Datenschutzbestimmungen praktisch umsetzen", Muster und Anleitungen waren online und offline stark nachgefragt. Wer in Sachen Datenschutz schon gut aufgestellt war, wollte dies auch beim Übergang in die neue Ära der DSGVO so beibehalten und konnte konkrete und manchmal auch sehr spezielle Bedarfe formulieren. Für wen allerdings Datenschutz Neuland war, der wurde sich immer deutlicher bewusst, dass vermutlich in den Jahren davor Versäumnisse bestanden, wenn nämlich Rechtsgrundlagen gar nicht klar waren oder bei den technisch-organisatorischen Sicherheitsmaßnahmen quasi bei null angefangen werden musste.

Mittlerweile haben sich die Wogen geglättet. Das Grundbewusstsein ist nun viel stärker bei den Verantwortlichen ebenso wie bei den Dienstleistern und vor allem bei den betroffenen Personen ausgeprägt. Vielfach gibt es Standardlösungen, die die Verantwortlichen für ihre jeweiligen Spezifika anpassen können. Dienstleister und Hersteller sind nur selten völlig ahnungslos bezüglich des Datenschutzes und unterstützen zunehmend diejenigen, die die Dienste und Produkte nutzen, auch in Datenschutz- und Informationssicherheitsfragen.

2019 erreichten uns 1194 schriftliche Beschwerden, von denen 235 nicht in unserer Zuständigkeit (öffentliche und nichtöffentliche Stellen in Schleswig-Holstein mit Ausnahme bestimmter Bereiche in Bundeszuständigkeit, z. B. Telekommunikation) lagen und an zuständige Kollegen abgegeben werden mussten. Nur eine kleine Anzahl der abgegebenen Beschwerden betraf Fälle, die von Kollegen in anderen Mitgliedstaaten, z. B. Dänemark, übernommen wurden.

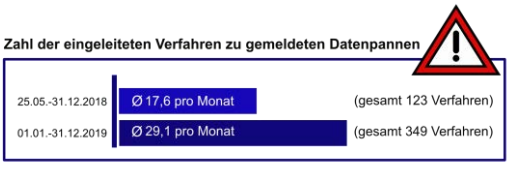


Zahl der eingeleiteten Verfahren aufgrund von Beschwerden im Jahr 2019

Insgesamt wurden in eigener Zuständigkeit 959 Verfahren eröffnet, davon richteten sich mehr als zwei Drittel der Beschwerden gegen Unternehmen (680), der Rest gegen Behörden (279).

Dazu kamen 758 Beratungen für den öffentlichen und den nichtöffentlichen Bereich.

Die Zahl von 349 eingeleiteten Verfahren zu Verletzungen des Schutzes personenbezogener Daten (Datenpannen) ist zwar schon recht hoch – an jedem Arbeitstag erreichen uns mehrere Meldungen oder nähere Erläuterungen zu schon getätigten Meldungen. Dennoch erfahren wir auch immer wieder von Datenpannen, bei denen die Verantwortlichen der Meldepflicht nicht nachgekommen sind.



Nach unserem Eindruck wird die Dienststelle der Landesbeauftragten für Datenschutz in Gesetzgebungsvorhaben auf Landesebene schon weitgehend eingebunden, wenn Aspekte des Datenschutzes oder des Informationszugangs betroffen sein könnten. Dies geschah im Berichtsjahr über die Arbeitsebene parallel zur Anhörung von Verbänden oder über die Ausschüsse im Landtag in 39 Fällen.

Von den Abhilfemaßnahmen wurde im Berichtsjahr wie folgt Gebrauch gemacht:

- 37 Warnungen
- 26 Verwarnungen
- 2 Anordnungen

Eine Geldbuße wurde im Jahr 2019 nicht verhängt.

Ohne vorherige Beschwerde wurden 10 Prüfungen im öffentlichen und 13 im nichtöffentlichen Bereich durchgeführt.

1.3 Die behördlichen und betrieblichen Datenschutzbeauftragten – tragende Säulen

Wer ist für den Datenschutz verantwortlich? Na klar, der „Verantwortliche" – so nennt die DSGVO die natürliche oder juristische Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Solche Entscheidungen trifft die Chefin oder der Chef – vielleicht nicht immer persönlich, aber auch dann verbleibt die Verantwortlichkeit in der Chefetage. Einige mögen sich nun verwundert die Augen reiben: „Dafür haben wir doch unsere Datenschutzbeauftragte" oder „Aber wozu haben wir denn gerade unseren Datenschutzbeauftragten auf Schulung geschickt?" Ein häufiges Missverständnis, das bei uns auch immer wieder zu Nachfragen führte (Tz. 4.1.1 und 4.1.2 für die behördlichen Datenschutzbeauftragten). Außerdem finden sich Aufgaben und Anforderungen in der Broschüre „Datenschutzbeauftragte" unserer Praxis-Reihe „Datenschutzbestimmungen praktisch umsetzen":

https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-2-Datenschutzbeauftragte.pdf

Kurzlink: *https://uldsh.de/tb38-13*

Deutschland hat eine jahrzehntelange Tradition der betrieblichen Datenschutzbeauftragten, die sich in verschiedenen Berufsverbänden, Vereinen oder Arbeitskreisen austauschen können. In den meisten Bundesländern gab es zudem die Pflicht für Behörden, Datenschutzbeauftragte zu benennen. Dies gilt jetzt flächendeckend in der EU.

Für einen Austausch über die Grenzen hinweg hat die Landesbeauftragte für Datenschutz die vielen Errungenschaften der Datenschutzbeauftragten bei den österreichischen Nachbarn vorstellen dürfen. Dort gibt es für den öffentlichen Bereich eine Besonderheit: Die dort benannten Datenschutzbeauftragten haben eine Pflicht zum regelmäßigen Erfahrungsaustausch.

§ 5 Abs. 5 Österreichisches Datenschutzgesetz

(5) Die Datenschutzbeauftragten im öffentlichen Bereich gemäß Abs. 4 pflegen einen regelmäßigen Erfahrungsaustausch, insbesondere im Hinblick auf die Gewährleistung eines einheitlichen Datenschutzstandards.

Dies geschieht auf freiwilliger Basis auch in Schleswig-Holstein: Schon vor Geltung der DSGVO waren die behördlichen Datenschutzbeauftragten (soweit vorhanden) in einem Arbeitskreis zusammengeschlossen. Mittlerweile haben sie sich in verschiedenen Arbeitskreisen organisiert: So gibt es Arbeitskreise der behördlichen Datenschutzbeauftragten für die Städte und Gemeinden, für die Kreise und kreisfreien Städte, für die Ämter und Zweckverbände und für die obersten Landesbehörden.

Dieser Austausch zielt auch auf die Gewährleistung einheitlicher Datenschutzstandards, wie es unsere österreichischen Nachbarn geregelt haben. Zusätzlich helfen Informationen zu den an einer Stelle gefundenen Lösungen im Sinne von Best Practices anderen Datenschutzbeauftragten bei ihren Beratungs- oder Prüfungsaufgaben. Oftmals profitiert man von den Perspektiven der anderen, um daraus zu lernen oder die bisherigen Abläufe bei der Wahrnehmung der Aufgaben zu verbessern.

Nicht Pflicht, aber hilfreich ist es, wenn die Datenschutzbeauftragten vor Ort eine besondere Aufmerksamkeit für das Thema schaffen und zu motivieren wissen. Daher haben wir im Austausch mit den österreichischen Kollegen Ideen behördlicher Datenschutzbeauftragter diskutiert, die mal mit Ernst, mal mit Spaß zur Sensibilisierung der Belegschaft beitragen:

- Aktionstage „Löschen/Schreddern“,
- „Gamification“-Ansätze von Datenschutz mit Preis (Obst/Schokoriegel),
- Datenschutzquiz,
- Datenpannensimulation,
- anonymisiert realisierte Phishing-Tests,
- Selbstdatenschutz mit Mehrwert für die Beschäftigten,
- im Team produzierte Kurzvideos für Schulungszwecke.

Wir kennen es auch in anderen Bereichen: Wer einmal eine Brandschutzschulung mit Praxisteil – also echtem Feuer – gemacht hat, wird dies nicht mehr vergessen und künftig insgesamt aufmerksamer für damit zusammenhängende Risiken sein.

Was ist zu tun?

Die Verantwortlichen sollen ihre Datenschutzbeauftragten beim Erfahrungsaustausch mit anderen unterstützen.

1.4 Datenpannen auch in Schleswig-Holstein – ein Grund zur Sorge

Jeden Tag erreichen uns Meldungen zu Verletzungen des Schutzes personenbezogener Daten – das zeigt, dass jemand in der Organisation von der Meldepflicht nach der DSGVO wusste (z. B. Tz. 4.1.13 und Tz. 5.4). Immer öfter erhalten wir auch professionelle Meldungen, die alle vorgeschriebenen Informationen beinhalten und bei denen man erkennt, dass interne Abläufe definiert sind, damit zeitgerecht reagiert wird. Das betrifft nicht nur das Ausfüllen eines Meldungsformulars, sondern der Vorfall wird bewertet und es werden geeignete Maßnahmen getroffen, um das Risiko für die betroffenen Personen einzudämmen und nach Möglichkeit zu verhindern, dass eine solche Datenpanne erneut geschieht.

Kritisch sehen wir solche Bereiche, in denen gar nicht oder sehr sparsam gemeldet wird, obwohl uns dann später doch irgendwie Vorfälle bekannt werden, die hätten gemeldet werden müssen. Es wäre auch ungewöhnlich, wenn bei Tausenden von Beschäftigten, die mit personenbezogenen Daten umgehen, nie Datenschutzfehler geschähen (beispielsweise siehe Tz. 4.2.5).

Anlass zur Sorge besteht, wenn Trojaner und andere Schadsoftware im großen Maßstab Rechner infizieren und personenbezogene Daten abfließen oder vernichtet werden können (Tz. 6.3.4). Nicht alle dieser Vorfälle betreffen personenbezogene Daten, sodass nur ein Teil

dieser Schadsoftware-Infektionen meldepflichtig ist. Aber bedenklich ist in einer zunehmend digitalisierten Welt, wenn die Datenverarbeitungen angegriffen und geschädigt werden können. Es gibt nach unserer Einschätzung in vielen Unternehmen und Behörden einen Nachholbedarf zum Umsetzen von Informationssicherheit. Das bedeutet wiederum, dass aktualisierte und geschützte Computersysteme bei den betroffenen Stellen nicht der Standardfall sind. Hier ist fraglich, ob die DSGVO-Regelungen zu technischem Datenschutz wie Artikel 25 und Artikel 32 DSGVO umgesetzt wurden.

Auf Bundesebene werden Reisewarnungen für das Mitführen von Geräten in Staaten, bei denen eine erhöhte Spionagegefahr vermutet wird, ausgegeben. Das ist alles gar nichts Neues. Was aber überrascht, ist die Empfehlung, man solle bei solchen gefahrenträchtigen Auslandsreisen Wegwerf-Handys verwenden, die im Anschluss an die Reise dann auch wirklich weggeworfen werden.

Das bedeutet nicht weniger als eine Bankrotterklärung zur Beherrschbarkeit der Informationstechnik. Sollte es wirklich so sein, dass es nicht mehr möglich ist, einen vertrauenswürdigen „Leerzustand" herzustellen, der ein neuer Startpunkt für eine korrekte Installation ist, fehlen jegliche Garantien in der digitalisierten Welt. Denn wer sagt, dass nicht schon der Auslieferungszustand manipuliert war? Wie soll denn eine Informationsgesellschaft ohne Integrität von Systemen und Daten funktionieren?

Was ist zu tun?

Verantwortungsvolle Digitalisierung braucht eine valide Basis, sonst ist der Nutzen fraglich und das Risiko immens – für die Menschen, die Gesellschaft, den Staat und die Wirtschaft.

Für Schleswig-Holstein bedeutet dies, dass sich alle Stellen – im öffentlichen und im nichtöffentlichen Bereich – im Datenschutz wie auch in der Informationssicherheit überprüfen sollten. Nicht zu kurz kommen darf die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter, damit Probleme und Pannen schnell erkannt und behoben werden können.

1.5 Nächste Schritte für mehr Transparenz – das Transparenzportal & mehr

Im letzten Bericht haben wir zu Informationsfreiheit „by Design" berichtet (37. TB, Tz. 2.2.4). Zusammen mit den anderen Kollegen der Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder haben wir dieses Thema aufgegriffen und einige Beispiele vorgestellt, wie sich Informationsfreiheit mit technischen und organisatorischen Werkzeugen verbessern lässt.

Für unsere interne Organisation bedeutet dies auch, dass – wie schon lange im Bereich Datenschutz – Aufgaben im Informationsfreiheitsbereich ebenso juristische wie auch technische Expertise benötigen, sodass einige Fragestellungen am besten von interdisziplinären Teams bearbeitet werden.

Informationsfreiheit „by Design"

Zu Informationsfreiheit „by Design" zählt die Gesamtheit technischer und organisatorischer Instrumente unter Berücksichtigung des Stands der Technik, die dazu dient, die informationspflichtigen Stellen in Bund und Ländern bei der Erfüllung ihrer Aufgaben im Bereich der Informationsfreiheit (einschließlich Transparenzgesetzen) zu unterstützen.

Das betrifft z. B. praktische Details zum Transparenzportal, das vom Land Schleswig-Holstein bereitgestellt wird (Tz. 6.3.2 und Tz. 12.5) und sich nun als Instrument für mehr Transparenz entfalten soll.

https://www.datenschutzzentrum.de/artikel/1317-Informationsfreiheit-by-Design.html

Kurzlink: *https://uldsh.de/tb38-15a*

https://www.datenschutzzentrum.de/uploads/sommerakademie/2019/SAK2019_IB06_Walczak-Informationsfreiheit-by-Design.pdf

Kurzlink: *https://uldsh.de/tb38-15b*

Gleichzeitig wird die Transparenz der Datenverarbeitungen selbst für eine Beherrschbarkeit der Systeme immer wichtiger. Zu Transparenz bei Algorithmen und in Systemen der künstlichen Intelligenz (KI) hatten wir letztes Jahr berichtet (37. TB, Tz. 2.2.3).

https://www.datenschutzzentrum.de/artikel/1255-Transparenz-Verwaltung-Algorithmen-KI.html

Kurzlink: *https://uldsh.de/tb38-15c*

Dieses Thema wird mittlerweile, eingebracht von Deutschland, bei der Internationalen Konferenz der Informationsfreiheitsbeauftragten diskutiert.

Außerdem war KI ein Schwerpunktthema der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Tz. 10.2).

Was ist zu tun?

Im Bereich Transparenz und Informationszugang ist mit dem Transparenzportal ein wichtiger Schritt getan, auf den nun weitere Schritte folgen müssen. Naheliegend gehört dazu das Befüllen des Transparenzportals; es lohnt sich aber weiterzudenken, um das Bereitstellen von Informationen unter Wahrung der Persönlichkeitsrechte von Personen oder Berufs- und Geschäftsgeheimnissen von Unternehmen zu erleichtern.

02

KERNPUNKTE

Zusammenarbeit der Aufsichtsbehörden

Datenethikkommission

Chance auf bessere Sicherheit nicht vertun

2 Datenschutz – global und national

2.1 Zusammenarbeit der Beauftragten des Bundes und der Länder

Eine Datenschutzharmonisierung in Europa bedeutet, dass alle Datenschutzaufsichtsbehörden zusammenarbeiten müssen. Dazu dient auf europäischer Ebene der Europäische Datenschutzausschuss (EDSA), in dem alle Mitgliedstaaten vertreten sind. Die nationale Zusammenarbeit in Deutschland geschieht über die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), in der wir ebenfalls vertreten sind. Die DSK hat zudem Arbeitskreise (AKs), die regelmäßig tagen und teilweise eigene Unterarbeitsgruppen (UAGs) eröffnet haben. Außerdem werden für kurzzeitigere Themenbehandlungen Taskforces zusammengestellt.

Wir bringen uns aktiv bei der Zusammenarbeit ein. Eine leitende Funktion haben wir bei dem AK Sicherheit und bei dem AK Zertifizierung (Tz. 9.1) sowie in der UAG ePrivacy des AK Medien und der UAG Standard-Datenschutzmodell (SDM) des AK Technik (Tz. 6.2.3). Die Taskforce Facebook-Fanpages, die von der DSK eingerichtet wurde, leiten wir ebenfalls – dies ergab sich aus dem gerichtlichen Verfahren, das wir 2018 vor dem EuGH geführt haben (Tz. 7.1).

Wegen der Fülle der Aufgaben schaffen wir es nicht, an jedem Treffen aller Arbeitskreise mitzuwirken – das können wohl auch nur die wenigsten Aufsichtsbehörden leisten.

Wir müssen bei den eingeschränkten Ressourcen selbstverständlich Prioritäten setzen. Dennoch hat es bislang funktioniert, dass wir unser Wissen und unsere Einschätzungen auch bei wichtigen Themen der Digitalisierung einbringen, beispielsweise bei der Taskforce zur künstlichen Intelligenz. Zudem engagieren wir uns auch in den europäischen Arbeitsgruppen (Subgroups) des EDSA (Tz. 11.1 und Tz. 11.2).

Im Bereich der Informationsfreiheit gibt es übrigens nur einen Arbeitskreis, der direkt der Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder (IFK) zuarbeitet. Dieses Gremium umfasst (noch) nicht alle Bundesländer, da nicht in jedem Land ein Informationsfreiheits- oder Transparenzportal geschaffen wurde.

Sowohl bei der DSK als auch bei der IFK rotiert der Vorsitz jährlich. Der letztjährige Vorsitz gibt die Leitung an das Bundesland (oder den Bund) an nächster Stelle im Alphabet ab, wobei manches Mal auch der Platz getauscht wird. 2019 war Rheinland-Pfalz Vorsitzland der DSK, 2020 ist dies Sachsen. Nach der jetzigen Planung wird Schleswig-Holstein den DSK-Vorsitz für das Jahr 2023 übernehmen. Dies schließt sich gut an den planmäßigen schleswig-holsteinischen IFK-Vorsitz im Jahr 2022 an.

Was ist zu tun?

Alle Beauftragten des Bundes und der Länder für Datenschutz und für Informationsfreiheit sollten sich weiterhin abstimmen und austauschen und dabei im Rahmen der jeweils zur Verfügung stehenden Ressourcen anteilig auch Gemeinschaftsaufgaben übernehmen.

2.2 Die Landesbeauftragte für Datenschutz in der Datenethikkommission

Im September 2018 gestartet, dann ein Jahr lang Zeit, um Empfehlungen zu Datenrechten und Datenpflichten auf Basis unserer Werte und Grundrechte zu erarbeiten: Das war die eigentlich unlösbare Aufgabe der Datenethikkommission, die von der Bundesregierung eingesetzt worden war, um sich mit einem umfangreichen Fragenkatalog zu beschäftigen. Zu den in die Datenethikkommission berufenen Mitgliedern zählte auch Marit Hansen, die Landesbeauftragte für Datenschutz. Die 16 Mitglieder kamen überwiegend aus dem wissenschaftlichen Bereich, außerdem waren der Verbraucherzentrale Bundesverband e. V. (vzbv), der Bundesverband der Industrie e. V. (BDI) und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit vertreten.

Datenethikkommission

„Der Einsatz von Algorithmen und künstlicher Intelligenz sowie der Umgang mit Daten birgt große Potenziale. Gleichzeitig stellen sich zahlreiche ethische und rechtliche Fragen.

Die Datenethikkommission der Bundesregierung sollte hierauf Antworten geben und auf der Basis wissenschaftlicher und technischer Expertise ethische Leitlinien für den Schutz des Einzelnen, die Wahrung des gesellschaftlichen Zusammenlebens und die Sicherung und Förderung des Wohlstands im Informationszeitalter entwickeln."

https://datenethikkommission.de/

Entstanden ist ein 240 Seiten starkes Gutachten, das viel Stoff für weitere Diskussionen enthält. Aus unserem Projektbereich (Kapitel 8) kennen wir die typischen Missverständnisse in interdisziplinären Teams – schon aufgrund der unterschiedlichen Bedeutungen von Fachbegriffen in den jeweiligen Disziplinen. Dies ist besonders ausgeprägt, wenn es um die Anwendung von in der eigenen Disziplin bekannten Konzepten auf neue – hier primär technische – Sachverhalte der künftigen Welt mit einer weiter fortgeschrittenen Digitalisierung geht. Hilfreich waren die Diskussionen anhand von „Use Cases" und Szenarien, die später zu den weiter abstrahierten Empfehlungen geführt haben.

Schwerpunkte des Gutachtens sind Regulierungsmöglichkeiten von algorithmischen Systemen anhand deren Kritikalität sowie eine faire Ausgestaltung von Datenrechten und Datenpflichten. Der Auftrag bestand nicht darin, einen umfassenden Gesetzentwurf zu erarbeiten – das wäre auch nicht gut gewesen, weil dringend der politische und gesellschaftliche Diskurs geführt werden sollte, bevor derart wesentliche Entscheidungen über Weichenstellungen für unsere künftige Gesellschaft getroffen werden. Außerdem griffe es zu kurz, lediglich das juristische Instrumentarium zu beleuchten. Stattdessen geht das Gutachten der Datenethikkommission auf vielfältige nötige und mögliche Steuerungsinstrumente im Sinne einer „Governance" ein.

Wer sich einen Kurzüberblick über die Ergebnisse verschaffen will, kann die Zusammenfassung hier lesen:

https://datenethikkommission.de/gutachten/gutachten-der-dek-kurzfassung/

Kurzlink: *https://uldsh.de/tb38-22*

Was ist zu tun?

Die Bundesregierung als Auftraggeberin des Gutachtens sollte die Empfehlungen der Datenethikkommission auswerten und die weiteren Schritte planen. Die Beschäftigung mit den Empfehlungen kann auch für andere Adressaten auf Landes-, Bundes- und europäischer Ebene bis hin zu internationalen Standardisierungsgremien sinnvoll sein.

2.3 Chance auf bessere Sicherheit nicht vertun

So ganz passt es nicht zusammen: Die Bundesregierung beauftragt einerseits die Datenethikkommission, Empfehlungen für eine faire Gestaltung unserer Welt im Informationszeitalter zu entwickeln (Tz. 2.2), und auf der anderen Seite kommen von Bund und Ländern immer wieder Forderungen auf den Tisch, die dazu geeignet sind, die für unsere Gesellschaft nötige zukunftsfähige Digitalisierung auf Basis der Grundwerte zu sabotieren.

Dazu gehören Formulierungen in Gesetzgebungsverfahren, die eine Kriminalisierung von Anbietern bestimmter datenschutzfreundlicher Techniken nahelegen (Entwurf zu § 126a StGB – Anbieten von Leistungen zur Ermöglichung von Straftaten, Tz. 8.2). Oder Ideen zur Herausgabepflicht von Kundenpasswörtern durch Anbieter (Entwurfspaket für Gesetzesänderungen gegen Hasskriminalität und Rechtsextremismus des Bundesministeriums für Justiz und Verbraucherschutz), was schon deswegen problematisch ist, weil sie doch aus Informationssicherheitssicht – im Einklang mit der DSGVO – gar nicht über Passwörter im Klartext verfügen sollten.

Für besonders kritisch halten wir Planungen der Innenministerkonferenz vom Juni 2019, Sicherheitsbehörden den Zugriff auf die verschlüsselte Kommunikation über Messenger-Anwendungen und auf die Daten im Smart Home zu erleichtern. Was hier mehr oder weniger unverblümt gefordert wird, sind eingebaute Hintertüren in Hard- und Software, die von den Sicherheitsbehörden für ihre Zugriffe genutzt werden sollen. Mit dem vom Bundesverfassungsgericht festgestellten Grundrecht auf Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme sind solche Ideen nicht vereinbar. Seit Jahrzehnten fordern Fachleute für IT-Sicherheit, dass Hersteller das Sicherheitsniveau der eingesetzten Technik für unsere Informationsgesellschaft dringend erhöhen müssen, statt es auf gesetzlichen Zwang hin auszuhöhlen. Denn nichts anderes passiert, wenn Hintertüren oder gezielte Schwachstellen implementiert werden: Unbefugte können dann ebenso zugreifen wie Befugte und z. B. die Kommunikation mitschneiden oder Daten kopieren, löschen, verändern oder gar gezielt unterschieben.

Anfang 2019 wurden persönliche Daten über Politiker und andere Prominente, die mithilfe von Internetangriffen gesammelt worden waren, veröffentlicht. Dieser Doxing-Skandal hatte kurzfristig die Diskussion um mehr Verschlüsselung und besseren Zugriffsschutz befeuert. Fast vergessen war zu diesem Zeitpunkt, dass schon vor einigen Jahren die Bundesregierung – wohl als Reaktion auf die Snowden-Enthüllungen – die Marschroute ausgegeben hatte: „Deutschland wird Verschlüsselungsstandort Nr. 1."

https://www.krypto-charta.de/

Auf dem Weg zu diesem hehren Ziel ist die Bundesregierung in den letzten Jahren kaum vorangekommen und scheint nun sogar falsch abzubiegen: Statt Datenschutz „by Design" umzusetzen, könnten die Telekommunikations- und Telemedienanbieter verpflichtet werden, die Möglichkeit zu schaffen, Inhalte wie Chats, Telefonate oder andere Kommunikationen unverschlüsselt zur Verfügung zu stellen. Das ginge nur, wenn die wichtige Ende-zu-Ende-

Verschlüsselung mit Sollbruchstellen torpediert würde. Von wirklicher Sicherheit kann dann keine Rede mehr sein.

Auch dort, wo sich gerade Sicherheitsstandards etablieren, gibt es Gegenwind von Ministerebene. Für kritisch halten wir den Beschluss der Justizministerkonferenz vom Juni 2019 zum neuen Mobilfunkstandard 5G, der endlich einen verbesserten Sicherheitsstandard aufweist, sodass ein Abhören nicht ohne Weiteres möglich ist – eigentlich. Denn die Mehrheit der Landesjustizministerinnen und -minister verlangt eine Aufweichung, um technische Angriffe, vor denen der neue Standard eigentlich schützen soll, weiterhin zu ermöglichen. Diese sogenannten Stingray-Angriffe (auch „IMSI-Catcher") lassen sich dabei weder gezielt auf verdächtige Personen eingrenzen, noch ist ihre Nutzung auf die Strafverfolgung beschränkbar. Vielmehr sind stets alle Endgeräte im Umkreis des Angriffs betroffen. Auch die Notruffunktionen werden unterbrochen. Vertraulichkeit und Integrität der zur persönlichen Kommunikation genutzten IT-Systeme (nichts anderes sind Mobiltelefone heutzutage) in 5-G-Netzen werden so nicht gewährleistet, sondern für alle Nutzenden massiv untergraben.

Verschlüsselung nach dem Stand der Technik stellt einen großen Mehrwert dar: Die digitalisierte Welt wird ein starkes Fundament für Informationssicherheit benötigen. Vertrauliche Kommunikation und verlässliche Datenverarbeitung müssen garantiert werden. Dies ist unabhängig davon, ob es um einen Datenaustausch beim vernetzten Autofahren, in der Telemedizin oder in der Industrie um 4.0-Anwendungen geht oder ob Smart Homes für den Privathaushalt oder Smart Cities im Sinne des Gemeinwohls gesteuert werden. Man muss kein Prophet sein, um vorherzusagen, dass sich die Nutzung von Hintertüren und Sollbruchstellen nicht auf die staatlichen Akteure für rechtmäßige Aktionen begrenzen lässt. Eine solche Idee schützt nicht vor Straftaten, sondern eröffnet im Gegenteil weitere Möglichkeiten für kriminelles Handeln.

Was ist zu tun?

Der Staat, Hersteller und Standardisierungsgremien sollten für eine Implementierung von mehr Datenschutz und Informationssicherheit sorgen und sich zu diesem Zweck die bisher erreichten Fortschritte in der sicheren Technik zunutze machen, statt den Einbau von Hintertüren voranzutreiben und damit die Sicherheit zu schwächen.

2.4 Anpassungsbedarf der Datenschutz-Grundverordnung?

Die Datenschutz-Grundverordnung sieht selbst vor, dass man sie evaluiert und auf dieser Basis überlegt, ob und wie sie verändert werden sollte: In Artikel 97 DSGVO wird geregelt, dass die Europäische Kommission bis zum 25. Mai 2020 und dann alle vier Jahre einen Bericht zur Bewertung und Überprüfung der DSGVO vorlegen muss.

Lange vor Geltung der DSGVO – eigentlich sogar schon, als die ersten Textversionen bekannt wurden – wurden Konzepte und Regelungen der DSGVO kontrovers diskutiert. Auch aus unserer Sicht sind nicht alle Wünsche an ein solches Gesetzeswerk erfüllt worden. Zugegeben: Das Üben von Kritik ist sehr einfach, jedoch ist es schwierig, perfekte Gesetze zu schreiben, die auch noch eine Zustimmung aus allen Mitgliedstaaten finden.

Einige Gremien, an denen wir uns beteiligen, haben Vorschläge zur Evaluation und Verbesserung der DSGVO vorgelegt. So enthält der Erfahrungsbericht der DSK zahlreiche Punkte:

https://www.datenschutzkonferenz-online.de/media/dskb/20191213_erfahrungsbericht_zur_anwendung_der_ds-gvo.pdf

Kurzlink: *https://uldsh.de/tb38-24a*

Auch das Forum Privatheit (Tz. 8.1) hat sich zu Verbesserungsmöglichkeiten der DSGVO geäußert:

https://www.forum-privatheit.de/wp-content/uploads/Policy-Paper-Evaluation-der-DSGVO.pdf

Kurzlink: *https://uldsh.de/tb38-24b*

Aber wo muss nun ganz dringend nachgebessert werden? Aus unserer Sicht besteht weniger ein Anpassungsbedarf der DSGVO selbst, sondern in ihrer Umsetzung. Das betrifft insbesondere die Angebote von Herstellern und Dienstleistern. Wenn diese nämlich bereits ihre Angebote datenschutzgerecht gestalten und die nötigen Materialien bereitstellen, wird alles leichter: Die Verantwortlichen können dann ihrer Rechenschaftspflicht nachkommen, das Risiko abschätzen und die geeigneten Maßnahmen treffen. Wenn auch noch passende Vorlagen bei den Informationspflichten und bei der Dokumentation unterstützen, muss nicht jeder das Rad noch mal neu erfinden. Das bedeutet: Die Realität der Datenverarbeitungsangebote ist teilweise noch massiv von den Anforderungen der DSGVO entkoppelt – da besteht aus unserer Sicht dringender Nachbesserungsbedarf.

Auch knirscht es manchmal im Getriebe der Zusammenarbeit auf europäischer Ebene. Dies ist schon deswegen nicht erstaunlich, weil die Aufsichtsbehörden der verschiedenen Mitgliedstaaten unterschiedliche Regelungen des Verwaltungsverfahrensrechts befolgen müssen. Aber solche Unterschiede dürfen nicht dazu führen, dass die Schlagkraft der Datenschutzaufsicht gerade gegenüber den globalen Marktakteuren, die großenteils ihren Sitz nicht in Deutschland haben, geschwächt wird.

Bug und Feature zugleich sind die oft abstrakten Formulierungen der DSGVO. Bug, weil ein Anwender, der nur den Gesetzestext liest, gar nicht verstehen kann, was genau gefordert ist, um Rechtssicherheit zu haben. Feature, weil eine gewisse Abstraktheit gewiss nötig war, um einen Konsens der Mitgliedstaaten aus unterschiedlichen Datenschutzkulturen zu erringen, und weil das Gesetzeswerk dann auch bei einem Wandel der verwendeten Informationstechnik vermutlich eine längere Haltbarkeit aufweist. Dazu enthält die DSGVO ebenfalls Lösungsansätze: Zu den Aufgaben des Europäischen Datenschutzausschusses gehört die Bereitstellung von „Leitlinien, Empfehlungen und bewährten Verfahren“ (Artikel 70 DSGVO), die gemeinsam von den Datenschutzaufsichtsbehörden der Mitgliedstaaten erarbeitet werden. Hier sind stetige Fortschritte zu verzeichnen.

In solchen Leitlinien und Empfehlungen könnte auch ein Fokus auf Konkretisierungen für neue Technikentwicklungen gelegt werden, beispielsweise im Bereich der künstlichen Intelligenz oder bei den zentral verteilten Crowd-Anwendungen, bei denen die Verantwortlichkeiten der Beteiligten unterschiedlich ausgeprägt sein können. Solche Technikregulierungen betreffen nicht nur Datenschutzaspekte, sondern es geht um die Beherrschbarkeit von Informationstechnik insgesamt. Hier sind unreife Schnellschüsse zu vermeiden. Ähnliches gilt für Bestrebungen, das individualisierte Daten(schutz)recht um kollektive Aspekte zu erweitern – beispielsweise wenn Gruppen von Personen schlechtergestellt werden, ohne dass eine Identifizierbarkeit der Individuen gegeben ist.

Einen konkreten Wunsch hätten wir allerdings, um zur Entbürokratisierung beizutragen: Wir könnten uns vorstellen, dass auf die Meldepflicht der Datenschutzbeauftragten bei den Aufsichtsbehörden (Art. 37 Abs. 7 DSGVO) verzichtet wird – das sind viele Zehntausende Mitteilungen, die bei den Aufsichtsbehörden eingehen und zumeist in Registern gespeichert werden.

Art. 37 Abs. 7 DSGVO

Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

Die Datenverarbeiter haben also die Pflicht, die Kontaktdaten ihrer oder ihres Datenschutzbeauftragten (sofern benannt) der Aufsichtsbehörde mitzuteilen. Andernfalls würden sie gegen die DSGVO verstoßen. Die meisten Aufsichtsbehörden haben dafür Formulare online gestellt, nehmen aber auch unstrukturiertere Meldungen (Schreiben per Papier, Fax, E-Mail ...) entgegen.

https://www.datenschutzzentrum.de/formular/meldung-dsb.php

Kurzlink: *https://uldsh.de/dsb-meld*

Der Nutzen dieser Mitteilungen ist jedoch beschränkt, weil keiner eine vollständige Aktualität der bei der Aufsichtsbehörde abgelegten Daten garantieren kann. Es ist auch nicht mit einer Mitteilung getan, sondern wir bekommen täglich Änderungsmeldungen und Nachfragen zu bisherigen Einträgen. Wir würden die dafür nötigen Ressourcen lieber für andere Aufgaben der DSGVO verwenden. Unserer Ansicht nach würde es ausreichen, wenn die Kontaktdaten der Datenschutzbeauftragten nur veröffentlicht (und nicht zusätzlich uns mitgeteilt) würden.

Was ist zu tun?

Die Datenschutz-Grundverordnung muss mit Bedacht evaluiert werden. Bei allen Änderungen sind Schnellschüsse zu vermeiden.

03

KERNPUNKTE

Als Gast im Datenschutzgremium

Datenschutz und Informationsfreiheit für Abgeordnete

3 Landtag

3.1 Die Landesbeauftragte als Gast im Datenschutzgremium

Wie bekannt fällt auch nach Geltung der DSGVO und des LDSG in der neuen Fassung die Wahrnehmung parlamentarischer Aufgaben nicht unter die Kontrolle der Landesbeauftragten für Datenschutz. In Schleswig-Holstein hat sich der Landtag schon vor vielen Jahren eine Datenschutzordnung für die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben gegeben und ein Datenschutzgremium gebildet.

Im Berichtsjahr hat dieses Datenschutzgremium getagt und die Landesbeauftragte für Datenschutz als Gast zur Sitzung eingeladen. Gerne steht sie dem Datenschutzgremium beratend zur Verfügung.

§ 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.

3.2 Service für Abgeordnete: Beratung zu Datenschutz und Informationsfreiheit

Auch ohne eine Zuständigkeit für Datenschutzfragen im parlamentarischen Bereich besteht die Möglichkeit, dass sich die Mitglieder des Landtages oder ihre Teams bei der Landesbeauftragten für Datenschutz vertrauensvoll beraten lassen. Dieser Service der Landesbeauftragten und ihrer Dienststelle wird auch von den Abgeordneten in Anspruch genommen.

Teilweise handelt es sich um den Wunsch nach rechtlichen Einschätzungen, teilweise um Technikfragen. Einiges betrifft ganz allgemeine oder globalpolitische Aspekte, anderes ist spezifisch für unser Bundesland. Manchmal wird nachgefragt, wie die eigene Datenverarbeitung der Parlamentarier am besten gestaltet werden sollte, manchmal sind die Fragen von Bürgerinnen und Bürgern aus dem ganzen Land an die Abgeordneten herangetragen worden. Oft möchte die anfragende Person sich nur bestätigen lassen, was sie sich schon selbst überlegt hat; es kommt aber auch vor, dass sie vorher noch gar keine Berührungspunkte mit dem spezifischen Sachverhalt hatte.

§ 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; [...]

Während wir manches Mal schnell kurze Antworten auf die Fragen geben können, han-

delt es sich in anderen Fällen um komplexe Fragen, bei denen erst der Sachverhalt im Gespräch genau analysiert und geprüft werden muss, um möglichst konkret antworten zu können.

Eines ist aber bei allen Fragen klar: Es besteht ein unmittelbarer praktischer Bedarf der Anfragenden an einer umsetzbaren Lösung, und diesem Bedarf versuchen wir – im Rahmen unserer Ressourcen – nachzukommen.

Was ist zu tun?

Die Abgeordneten des Schleswig-Holsteinischen Landtages können gern den Service der Landesbeauftragten für Datenschutz nach Beratung in Anspruch nehmen.

04

KERNPUNKTE

Behördliche Datenschutzbeauftragte

Nachbesserungen für Datenschutz in Gesetzgebungsverfahren

Datenpannenmeldepflichten – wo klappt's, wo nicht?

4 Datenschutz in der Verwaltung

4.1 Allgemeine Verwaltung

4.1.1 Anforderungen an die Benennung und Ausstattung von Datenschutzbeauftragten – Rundschreiben an Kreis-, Amts- und Gemeindeverwaltungen

Auch nach mehr als einem Jahr der Geltung der Datenschutz-Grundverordnung und des neuen Landesdatenschutzgesetzes erreichten uns regelmäßig Fragen zur Benennung von behördlichen Datenschutzbeauftragten sowie zu deren Ausstattung. Teilweise erhielten wir auch Beschwerden von behördlichen Datenschutzbeauftragten, die ihre Aufgaben mit den ihnen zugesprochenen Ressourcen nicht erfüllen konnten.

Die Landesbeauftragte für Datenschutz versandte daher am 02.04.2018 ein Rundschreiben an die Leitungen von Kreisen, Städten, Ämtern und Gemeinden sowie an die Arbeitskreise der behördlichen Datenschutzbeauftragten mit entsprechenden Hinweisen.

Darin wurde verdeutlicht, dass Behörden und sonstige öffentliche Stellen stets einen behördlichen Datenschutzbeauftragten benennen müssen. Unabhängig davon, ob eine interne oder externe Person benannt wird, ist auf hinreichende Qualifikationsnachweise zu achten. Sollen eigene Mitarbeiterinnen und Mitarbeiter benannt werden, sind diese für entsprechende Fortbildungen freizustellen.

Die Vergütung interner Datenschutzbeauftragter unterhalb von E11/A12 ist als unangemessen anzusehen. Zudem verbieten sich „Rechenspiele", die Vergütung einer nur zeitanteilig als behördliche Datenschutzbeauftragte benannte Person zu reduzieren. Da die inhaltliche Komplexität der Aufgaben auch bei einer 50-Prozent-Stelle dieselbe ist wie bei einer 100-Prozent-Stelle, kann eine niedrigere Vergütung nicht angemessen sein.

Als Orientierungsmarke zur Bestimmung, ob ein Datenschutzbeauftragter seine Aufgaben allein erfüllen kann oder ob weitere Personen z. B. als Datenschutzmanager zu beauftragen sind, wurde empfohlen, ab 1.000 Beschäftigten eine Vollzeitstelle einzuplanen. Dieser Personalschlüssel ist allerdings nicht als feste Rechenformel zu verstehen: Beispielsweise kann bei weiten Distanzen zwischen den Verantwortlichen und Außenstellen, bei sehr komplexer Datenverarbeitung oder sehr unterschiedlichen Systemen auch schon eine geringere Anzahl von Beschäftigten weiteres Personal zur Umsetzung datenschutzrechtlicher Vorgaben abzustellen sein.

Den Adressaten des Schreibens wurde verdeutlicht, dass die Datenschutzbeauftragten weisungsfrei und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden sind.

Zu den Ressourcen, die den Datenschutzbeauftragten bereitzustellen sind, zählt u. a.

- eine vertrauliche Arbeitsumgebung,
- aktuelle Fachliteratur,
- die Teilnahme an Fortbildungsveranstaltungen,
- die Teilnahme an Sitzungen mit anderen Datenschutzbeauftragten.

Ein Scan des Rundschreibens ist über die Webseite des ULD abrufbar:

https://uldsh.de/behDSB-Rundschreiben

Was ist zu tun?

Behörden und sonstige öffentliche Stellen in Schleswig-Holstein müssen eine oder einen behördlichen Datenschutzbeauftragten benennen und mit den erforderlichen Ressourcen ausstatten.

Sollten Verantwortliche dieser Verpflichtung noch nicht nachgekommen sein, ist dies unverzüglich nachzuholen.

Die Kontaktdaten der oder des Datenschutzbeauftragten sind im Übrigen zu veröffentlichen und der Landesbeauftragten für Datenschutz mitzuteilen (Online-Formular: *https://uldsh.de/dsb-meld*).

4.1.2 Aufgaben der Datenschutzbeauftragten

Im Berichtszeitraum erreichten das ULD einige Anfragen von Datenschutzbeauftragten, die von Unternehmen oder auch Behörden hinsichtlich ihrer Funktion pflichtgemäß benannt wurden. Dabei war von Interesse, welche Aufgaben die benennende Stelle und – davon zu trennen – welche Aufgaben die oder der Datenschutzbeauftragte wahrnehmen muss. Dabei konnten wir zunächst auf die Ausführungen in unserer Informationsbroschüre verweisen, die unter folgendem Link abrufbar ist:

https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-2-Datenschutzbeauftragte.pdf

Kurzlink: *https://uldsh.de/tb38-412*

Der oder dem Datenschutzbeauftragten obliegen nach Art. 39 Abs. 1 DSGVO zumindest folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten,
- Überwachung der Einhaltung der DSGVO, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen,
- Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35 DSGVO,
- Zusammenarbeit mit der Aufsichtsbehörde,
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36 DSGVO, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Aus der Aufzählung wird deutlich, dass in Abgrenzung zum Aufgabenkreis eines Datenschutzbeauftragten insbesondere die Verantwortung für die Einhaltung der Datenschutzvorschriften einschließlich der Umsetzung technisch-organisatorischer Sicherungsmaßnahmen beim datenschutzrechtlich Verantwortlichen bzw. bei der benennenden Stelle verbleibt. Dies wird u. a. in Art. 24 Abs. 1 DSGVO hervorgehoben.

Verantwortlichkeit nach Art. 24 Abs. 1 Satz 1 DSGVO

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

Aus dieser Abgrenzung der Aufgabenkreise von Verantwortlichen und deren Datenschutzbeauftragten ergeben sich u. a. folgende Konsequenzen:

- Die Erstellung von Verzeichnissen von Verarbeitungstätigkeiten (Artikel 30 DSGVO) und von Verträgen mit Auftragsverarbeitern (Art. 28 Abs. 3 DSGVO) ist nicht Aufgabe der oder des Datenschutzbeauftragten. Gleiches gilt für die Dokumentation von technisch-organisatorischen Maßnahmen, was etwa die Erarbeitung von Konzepten zur Protokollierung, die Festlegung von Löschregeln, die Erstellung von Berechtigungskonzepten sowie die Aufstellung von Anweisungen und internen Richtlinien zum Umgang mit personenbezogenen Daten gegenüber Mitarbeitern betrifft. Ferner zählt auch die Aktualisierung entsprechender Dokumente nicht zum Aufgabenkreis einer oder eines Datenschutzbeauftragten. Sämtliche Aufgaben müssen durch den Verantwortlichen wahrgenommen werden. Datenschutzbeauftragte sind in diesem Kontext nur beratend tätig und verpflichtet, die ordnungsgemäße Umsetzung der Maßnahmen einschließlich der konformen Erstellung von relevanten Verträgen und weiterer Dokumente zu überprüfen.
- Datenschutz-Folgenabschätzungen (Artikel 35 DSGVO) sind durch den Verantwortlichen durchzuführen. Die oder der Datenschutzbeauftragte nimmt dabei eine Beraterrolle wahr.
- Die Verpflichtung zur Schulung und Sensibilisierung von Beschäftigten im Hinblick auf die Verarbeitung personenbezogener Daten obliegt grundsätzlich dem Verantwortlichen. Die oder der Datenschutzbeauftragte überwacht hingegen die ordnungsgemäße Durchführung der Schulungen und Sensibilisierungen. Es bleibt aber möglich, dass die oder der Datenschutzbeauftragte eigene Schulungen für Beschäftigte anbietet und so die Aufgaben der Unterrichtung und Beratung gegenüber diesem Personenkreis erfüllt.
- Die Bearbeitung von Anträgen betroffener Personen zur Ausübung ihrer Rechte (z. B. Auskunft, Löschung, Berichtigung, Widerspruch, Widerruf) einschließlich der Zusammenstellung der benötigten Informationen ist eine Aufgabe des Verantwortlichen. Die oder der Datenschutzbeauftragte kann hierbei jedoch mitwirken. Die Mitwirkung kann z. B. bei der Zusammenstellung der gespeicherten Daten erfolgen. Zudem sollte die oder der Datenschutzbeauftragte die durch den Verantwortlichen erstellte Antwort einer Schlusskontrolle unterziehen. Bezüglich der Absendung der Antworten kann die oder der Datenschutzbeauftragte die Funktion eines Boten für den Verantwortlichen übernehmen.
- Die Erstellung einer Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Artikel 33 DSGVO), die Benachrichtigung betroffener Personen (Artikel 34 DSGVO) sowie die Umsetzung von Sicherheitsmaßnahmen zählen zu den Aufgaben des Verantwortlichen. Die oder der Datenschutzbeauftragte überwacht hingegen die ordnungsgemäße Erfüllung der Melde- und Benachrichtigungspflichten sowie die künftige Gewährleistung von Sicherheitsmaßnahmen. Hinsichtlich der Absendung der Meldung kann die oder der Datenschutzbeauftragte wiederum eine Botenfunktion übernehmen, zumal dieser im Rahmen der Zusammenarbeit mit der

Aufsichtsbehörde als Ansprechperson in Betracht kommt.

- Datenschutzbeauftragte nehmen Prüfungen der personenbezogenen Datenverarbeitung des Verantwortlichen oder des Auftragsverarbeiters wahr.

Was ist zu tun?

Verantwortliche dürfen ihre nach der DSGVO obliegenden Pflichten nicht auf den benannten Datenschutzbeauftragten übertragen. Die Verantwortlichen können aber erwarten, dass ihre Datenschutzbeauftragten vor allem ihre Beratungs-, Unterrichtungs- und Überwachungsaufgaben gewissenhaft wahrnehmen und ihre Ergebnisprüfung nachvollziehbar dokumentieren. Möglich bleibt für Datenschutzbeauftragte die Erstellung von Tätigkeitsberichten.

4.1.3 Künftig verpflichtende Nutzung der landesweiten Kitadatenbank

Die landesweite Datenbank wurde im Jahr 2016 als freiwilliges Angebot für alle Träger von Kindertageseinrichtungen (Kitas) in Betrieb genommen. Mit diesem IT-Verfahren ist es für die Kommunen und die Träger möglich, wesentlich genauere Bedarfsplanungen vorzunehmen. Das damit verbundene KitaPortal ermöglicht es den Eltern, freie Kitaplätze zu suchen und online eine unverbindliche Voranmeldung für die Kita ihrer Wahl abzugeben.

Wir haben den Aufbau des IT-Verfahrens und die neu zu schaffenden rechtlichen Vorschriften damals aus datenschutzrechtlicher Sicht begleitet.

Das freiwillige Angebot wurde mittlerweile von vielen Trägern angenommen. Mit dem KiTa-Reform-Gesetz 2020, das zum 1. August 2020 in Kraft treten soll, will die Landesregierung hinsichtlich der Nutzung noch einen Schritt weitergehen. Zukünftig soll die Nutzung der landesweiten Kitadatenbank für alle Träger von Kindertageseinrichtungen verpflichtend sein. Ferner ist eine Erweiterung der Funktionalität vorgesehen.

Die hierfür im KiTa-Reform-Gesetz vorgesehenen Vorschriften hat das Sozialministerium mit uns abgestimmt. Diese werden die Vorschriften im bisherigen Kindertagesstättengesetz ablösen.

Allerdings wird es damit noch nicht getan sein. Durch die zukünftige Pflicht der Nutzung ist es aus unserer Sicht erforderlich, den gesamten Verarbeitungsprozess im Kontext mit der landesweiten Kitadatenbank und dem KitaPortal auf den datenschutzrechtlichen Prüfstand zu stellen. Dabei sind die folgenden Fragestellungen zu prüfen und zu lösen:

- Sind die Regelungen der Kitadatenbankverordnung noch aktuell oder besteht Anpassungsbedarf?
- Werden die Informationspflichten über die Datenverarbeitung im KitaPortal vorbildlich im Sinne der DSGVO erfüllt?
- Soll es einheitliche Erhebungsformulare für alle Kindertageseinrichtungen in Schleswig-Holstein geben?

Es wurde mit dem Sozialministerium vereinbart, dass diese Fragen gemeinsam bearbeitet werden.

Was ist zu tun?

Das Sozialministerium sollte die genannten Fragen bis zum Inkrafttreten des KiTa-Reform-Gesetzes mit dem ULD klären.

4.1.4 Verordnung über eine zentrale Stelle beim Zentralen IT-Management in Schleswig-Holstein (ZIT SH)

Das ULD wurde vom Zentralen IT-Management des Landes (ZIT SH) bezüglich des Neuerlasses einer Verordnung um Beratung gebeten. Durch diese Verordnung soll die Tätigkeit einer sogenannten **zentralen Stelle** geregelt werden, die Koordinierungsfunktionen wahrnimmt und behördenübergreifende Verfahren des Landes (z. B. elektronische Aktenführung, Bürokommunikation, interne Zeiterfassung) in technischer Hinsicht betreibt. Sie wirkt damit auf die Datenverarbeitung anderer Behörden ein, sodass datenschutzrechtliche Verantwortlichkeiten zu klären sind.

Grundlage für eine solche Verordnung sind § 7 Abs. 3 und Abs. 4 Landesdatenschutzgesetz (LDSG), wonach auf Landesebene nach bestimmten Anforderungen sogenannte gemeinsame Verfahren eingerichtet werden dürfen (Absatz 3) und per Verordnung Zuständigkeiten auf zentrale Stellen übertragen werden können.

Gemeinsames Verfahren

Ein automatisiertes Verfahren, das mehreren Verantwortlichen gemeinsam die Verarbeitung personenbezogener Daten (gemeinsames Verfahren) oder die Übermittlung personenbezogener Daten durch Abruf (Abrufverfahren) ermöglicht, darf eingerichtet werden, soweit dies unter Berücksichtigung der schutzwürdigen Interessen der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist (§ 7 Abs. 3 LDSG).

In einer Verordnung gemäß § 7 Abs. 4 LDSG kann die zuständige oberste Landesbehörde Regelungen nach Art. 26 Abs. 1 DSGVO festlegen und unter mehreren Verantwortlichen eine zentrale Stelle bestimmen, der die Verantwortung für die Gewährleistung der Ordnungsmäßigkeit des automatisierten Verfahrens übertragen wird. Die zentrale Stelle und die beteiligten Stellen agieren dabei als gemeinsam Verantwortliche.

Gemeinsam Verantwortliche

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß der DSGVO erfüllt (Art. 26 Abs. 1 DSGVO).

Auch im Landesdatenschutzgesetz in der Fassung, die bis zum 24. Mai 2018 galt, gab es die Möglichkeit, Verantwortlichkeiten zu bündeln und per Verordnung einer zentralen Stelle zuzuweisen. Davon wurde auf Landesebene auch häufig Gebrauch gemacht. Ausgangspunkt der geplanten Veränderung war eine inhaltliche Anpassung an die Regelungen des Artikels 26 der DSGVO.

Zentrale Stelle im Entwurf der beabsichtigten Verordnung ist die für das Zentrale IT-Management zuständige oberste Landesbehörde (ZIT SH). Beteiligte Stellen sollen diejenigen Landesbehörden und ihre zugeordneten Ämter

und nachgeordneten Behörden sein, welche die im Anhang näher zu bestimmenden automatisierten Verfahren nutzen.

Die zentrale Stelle soll u. a. geeignete technisch-organisatorische Maßnahmen zur Einhaltung der Vorgaben nach der DSGVO gewährleisten; die beteiligten Stellen sollen für die Umsetzung von Informationspflichten und die Erfüllung der Rechte betroffener Personen, wie etwa Auskunft oder Löschung, zuständig sein.

Das ULD konnte in Bezug auf den Verordnungsentwurf insbesondere zur Frage beraten, wie im Falle der Feststellung von Verfahrensmängeln im laufenden Betrieb die Meldepflicht nach Artikel 33 DSGVO und die sich oftmals anschließende Benachrichtigungspflicht nach Artikel 34 DSGVO eingehalten werden können – diese Aspekte waren nach dem Inkrafttreten der DSGVO zu regeln: Im Falle der Verletzung des Schutzes personenbezogener Daten und einer Risikolage für Rechte und Freiheiten natürlicher Personen kann für Verantwortliche die Verpflichtung zur unverzüglichen Meldung des Vorfalls an die Datenschutzaufsichtsbehörde bestehen. Sollten hohe Risiken für die betroffenen Personen festgestellt werden, so besteht zusätzlich eine Pflicht zur Benachrichtigung dieses Personenkreises. Zu regeln war hier insbesondere, wie die Beteiligten zusammenarbeiten, welche gegenseitigen Informationspflichten bestehen und welcher Verantwortliche für die Durchführung der Meldung nach Artikel 33 sowie die Benachrichtigung nach Artikel 34 DSGVO zuständig ist.

4.1.5 Umsetzung des Onlinezugangsgesetzes (OZG)

Das Onlinezugangsgesetz verpflichtet Bund, Länder und Kommunen, bis Ende 2022 ihre Verwaltungsleistungen über Verwaltungsportale auch digital anzubieten und diese Portale zu einem Verbund zu verknüpfen. Die Kommunen sind von den Ländern in die Planung einzubeziehen.

Onlinezugangsgesetz (OZG)

Der Volltext des „Gesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen" ist abrufbar unter:

https://www.gesetze-im-internet.de/ozg/BJNR313800017.html
Kurzlink: *https://uldsh.de/tb38-415a*

Weitere Informationen über die Umsetzung des OZG finden sich u. a. auf den hierzu eingerichteten Webseiten folgender Institutionen:

IT-Planungsrat:

https://www.it-planungsrat.de/DE/ITPlanungsrat/OZG-Umsetzung/OZG_Umsetzung_node.html
Kurzlink: *https://uldsh.de/tb38-415b*

Bundesministerium des Inneren, für Bau und Heimat:

https://informationsplattform.ozg-umsetzung.de/iNG/app/intro
Kurzlink: *https://uldsh.de/tb38-415c*

Land Schleswig-Holstein:

https://digitalisierung.schleswig-holstein.de/

IT-Verbund Schleswig-Holstein – ITVSH:

https://www.itvsh.de/projekte/ozg/

Die Landesbeauftragte für Datenschutz wurde in dieser Sache bisher weder vom Land noch von den Kommunen eingebunden. Aufgrund vereinzelter Beratungsersuchen kommunaler Datenschutzbeauftragter, die innerhalb ihrer Behörden Datenschutzfragen zu Digitalisierungsbestrebungen identifiziert haben, haben wir Gespräche mit dem für die Kommunen zur OZG-Umsetzung gegründeten IT-Verbund Schleswig-Holstein – ITVSH (AöR) und dem Zentralen IT-Management der Landesregierung (ZIT SH) geführt und dabei eine frühzeitige

Beratung angeboten. Dieses Angebot besteht auch weiterhin.

Es besteht keine Verpflichtung von Land und Kommunen, die Landesbeauftragte für Datenschutz oder ihre Dienststelle proaktiv in die Planungen zur OZG-Umsetzung einzubeziehen. Sie müssen aber sicherstellen, dass die Umsetzung der OZG-Verfahren vor deren Inbetriebnahme im Einklang mit den datenschutzrechtlichen Vorgaben erfolgt.

Bei der Vielzahl der zu digitalisierenden Verfahren rechnen wir ab 2020 mit einem Anstieg von Beschwerden betroffener Personen. Wir appellieren daher auch an dieser Stelle ausdrücklich an die Verantwortlichen, die Anforderungen nach der DSGVO und dem LDSG nicht zu unterschätzen.

Was ist zu tun?

Land und Kommunen müssen für eine datenschutzkonforme Umsetzung des Onlinezugangsgesetzes sorgen. Auf Wunsch unterstützt das ULD dieses Vorhaben.

4.1.6 Keine Rechtsgrundlage für Personalaktenweitergabe an einen Verein vor dem Betriebsübergang

In einem Verfahren wurde ermittelt, dass eine Behörde mit einem Verein auf Basis eines Dienstleistungsvertrags die wirtschaftliche Führung einer Seniorenwohnanlage neu strukturieren wollte, die bisher als Eigenbetrieb geführt wurde. Beabsichtigt war auch ein Betriebsübergang der Beschäftigten des Eigenbetriebs. Mit dem Dienstleistungsvertrag sollte der Verein ermächtigt werden, die Geschäftsführung für die Seniorenwohnanlage zu übernehmen. Die Betriebsleitung für den Eigenbetrieb wurde schließlich von der Behörde dem Verein zugewiesen. Dabei übertrug die Behörde an den Verein mehr als 60 Personalakten von Beschäftigten des Eigenbetriebs. Der Betriebsübergang selbst erfolgte erst mehr als ein Jahr nach Zuweisung der Betriebsleitung.

Auf Nachfrage des ULD zur Rechtsgrundlage der Weitergabe der Personalakten verwies die Behörde auf den geschlossenen Dienstleistungsvertrag. Da dieser Vertrag nicht die Anforderungen an eine zulässige Weitergabe der Personalakten erfüllte, wurden nach Bekanntwerden des Verstoßes die Akten vom Verein an die Behörde zurückgegeben.

Verweis auf das Beamtenrecht

Gemäß § 15 Abs. 1 LDSG dürfen öffentliche Stellen personenbezogene Daten ihrer Beschäftigten vorbehaltlich besonderer gesetzlicher oder tarifvertraglicher Regelungen nur nach Maßgabe des LBG verarbeiten. Damit gelten die beamtenrechtlichen Regelungen zum Umgang mit Personalaktendaten auch für Tarifbeschäftigte.

Bis zum Betriebsübergang auf den Verein war die Behörde verpflichtet, für die Verarbeitung der Personalaktendaten der Beschäftigten des Eigenbetriebs insbesondere die datenschutzrechtlichen Vorgaben aus dem Landesbeamtenrecht einzuhalten.

Die Voraussetzungen für eine zulässige Weitergabe von Personalaktendaten waren mit der Zuweisung der Geschäftsführung und bis zum Betriebsübergang nicht erfüllt. Der dem ULD vorgelegte Dienstleistungsvertrag genügte vor allem nicht den Anforderungen an eine zulässi-

ge Auftragsverarbeitung auf Basis von § 89a Landesbeamtengesetz in Verbindung mit Art. 28 Abs. 3 DSGVO. Weder die verpflichtenden Vertragsinhalte nach Art. 28 Abs. 3 DSGVO waren ersichtlich, noch lag eine Zustimmung der obersten Dienstbehörde nach § 89a Abs. 2 Landesbeamtengesetz vor. Weiterhin fehlte die Aufnahme einer Kontrollklausel. Demnach ist in dem Auftrag schriftlich festzulegen, dass der Auftragsverarbeiter eine Kontrolle durch die oder den Landesbeauftragten für Datenschutz zu dulden hat.

Vor Abschluss des Vertrags mit dem Verein hätte die Behörde etwa prüfen müssen, ob der Verein überhaupt in der Lage ist, die erforderlichen technisch-organisatorischen Anforderungen umzusetzen, um die Personalakten sicher zu verwalten. Hierzu zählen etwa die Steuerung von Zugriffsrechten auf die Personalakten und die Aufbewahrung der Akten. Weiterhin hätte die Behörde ein Weisungsrecht zum Umgang mit den Akten vereinbaren müssen. Die Behörde war verpflichtet, die Umsetzung der notwendigen Maßnahmen beim Verein zu kontrollieren. Ferner durften im Verein nur solche Personen mit den Personalaktendaten Umgang haben, die zuvor auf die Einhaltung der datenschutzrechtlichen Vorgaben verpflichtet wurden. Die Behörde hatte nicht verstanden, dass sie vor dem Betriebsübergang noch die Verpflichtung hatte, die Verwaltung der Personalakten selbst zu steuern. Im geführten Prüfverfahren wurde deutlich, dass sich die Behörde hinsichtlich der datenschutzrechtlichen Verpflichtungen keine Gedanken gemacht hatte. Vielmehr entstand der Eindruck, dass die Behörde mit der bloßen Zuweisung der Geschäftsführung über die Seniorenanlage an den Verein davon ausging, dass damit alle Anforderungen umgesetzt wurden.

Die Behörde räumte nach Darlegung der Rechtslage durch das ULD den Verstoß ein. Es wurde vonseiten der Behörde zugesichert, dass künftig die gesetzlichen Anforderungen an die Verarbeitung von Personalaktendaten eingehalten werden. Gegenüber der Behörde hat das ULD eine Verwarnung ausgesprochen.

4.1.7 Schwangerschaftsberatungsstellen der Kreise – wer ist für was verantwortlich?

Das ULD wurde um eine Einschätzung gebeten, ob die Stiftung „Familie in Not“ mit den Schwangerschaftsberatungsstellen in Schleswig-Holstein Verträge zur Auftragsverarbeitung nach Art. 28 Abs. 3 der Datenschutz-Grundverordnung (DSGVO) schließen muss. Die Bundesstiftung „Mutter und Kind – Schutz des ungeborenen Lebens“ vertrat dabei die Auffassung, dass alle Landesstiftungen mit den Beratungsstellen entsprechende Verträge vereinbaren müssen. Nach unserer Bewertung besteht hierfür keine Veranlassung.

Auf Grundlage einer Umfrage bei den anderen deutschen Datenschutzaufsichtsbehörden hat sich ein sehr differenziertes Bild der Verarbeitung personenbezogener Daten ergeben.

In einem Bundesland erfolgt etwa eine eigenverantwortliche Prüfung über die Gewährung der Mittel durch die jeweilige Beratungsstelle. Nach dieser Prüfung leitet die Beratungsstelle sämtliche Antragsdaten an eine Landesstiftung weiter, die auf einer zweiten Stufe eine weitere und endgültige Entscheidung über die Mittel trifft. Hier werden die Landesstiftung wie auch die Beratungsstellen von der Datenschutzbehörde als gemeinsam Verantwortliche (Artikel 26 DSGVO) angesehen. Es bleibt kein Raum für eine Auftragsverarbeitung.

In einem anderen Bundesland erfolgte eine Aufteilung der Entscheidungskompetenzen zwischen der Landesstiftung und den Beratungsstellen hinsichtlich des Ob und des Wie einer Mittelbeantragung. Auch hier werden beide Beteiligte als datenschutzrechtlich Verantwortliche qualifiziert.

In einem weiteren Bundesland prüfen die Beratungsstellen die Antragsunterlagen der schwangeren Personen nur auf deren Vollständigkeit

und senden diese zur Entscheidung über die Mittelvergabe an die Landesstiftung. Doch auch in diesem Fall tendiert die dort zuständige Datenschutzaufsicht zu der Auffassung, dass keine Auftragsverarbeitung vorliegt, zumal die Beratungsstellen dabei in ihren Aufgabenbereichen gleichzeitig eigene Beratungspflichten eigenverantwortlich erfüllen.

In einem anderen Bundesland erfolgt teilweise eine Budgetierung der Beratungsstellen, wobei diese auch eigenverantwortlich über die Mittelvergabe entscheiden und als datenschutzrechtlich Verantwortliche qualifiziert werden. Nicht budgetierte Beratungsstellen entscheiden dort allerdings nicht in letzter Instanz über die Mittelvergabe, was abweichend dort durch Spitzenverbände erfolgt, die zwischen den Beratungsstellen und einer Landesstiftung stehen. Die zuständige Datenschutzaufsicht nimmt im letzteren Fall eine gemeinsame Verantwortlichkeit an.

In zwei Bundesländern wird die Entscheidung über die Vergabe von Mitteln an die antragstellenden Personen allein durch die Landesstiftung getroffen. Die Beratungsstellen haben kein eigenes Budget und treffen keine Entscheidungen über die Anträge. Es erfolgt dort lediglich eine Weiterleitung der Anträge an die Landestiftung in der Funktion eines Boten. In diesen Fällen qualifizieren die dort zuständigen Datenschutzaufsichtsbehörden die Beratungsstellen als Auftragsverarbeiter.

Bereits diese Unterschiede in den Systemen der Mittelvergabe in den einzelnen Bundesländern zeigen deutlich, dass ein generelles Verlangen, Auftragsverarbeitungsverträge zwischen den Landesstiftungen und den Beratungsstellen zu schließen, weder aus praktischer noch aus rechtlicher Sicht richtig sein kann.

Für Schleswig-Holstein ergibt sich das Folgende:

- Die Beratungsstellen erheben die personenbezogenen Daten der Schwangeren, prüfen unter Beachtung der Richtlinien zur Mittelvergabe deren gestellte Anträge und vergeben bzw. bewilligen die Mittel aus der ihnen bereitgestellten Summe.
- Die Landesstiftung erhält keine personenbezogenen Daten der Antragstellerinnen. Die Bundesstiftung erhält ebenfalls keine personenbezogenen Daten der Schwangeren. Die Bundesstiftung hat in ihrem Webauftritt darüber hinaus einen Hinweis veröffentlicht, wonach sie weder am Antrags- noch am Bewilligungsverfahren beteiligt ist und dass Voraussetzung für die Gewährung der Mittel ein Antrag bei einer Schwangerschaftsberatungsstelle ist.
- Allenfalls im Rahmen einer Rechnungsprüfung (Stichprobe) hätten die Landesstiftung oder die Bundesstiftung die Befugnis, einen (ausgefüllten) Antragsvordruck einzusehen.

Vor diesem Hintergrund geht das ULD davon aus, dass die Schwangerschaftsberatungsstellen im Rahmen der Verarbeitung der personenbezogenen Daten der Schwangeren als Verantwortliche im Sinne von Art. 4 Ziff. 7 DSGVO tätig sind. Der gesamte Beantragungs- und Bewilligungsprozess wird von den Beratungsstellen eigenverantwortlich durchgeführt. Ein streng weisungsgebundenes Verhältnis, personenbezogene Daten der Antragstellerinnen auf eine bestimmte Weise zu verarbeiten, wird aus unserer Sicht zwischen der Landesstiftung und den Beratungsstellen nicht begründet.

4.1.8 Abruf von Meldedaten für öffentlich-rechtliche Entsorgungsträger?

Die Abfallwirtschaft Südholstein GmbH (AWSH) – ein von den Kreisen Stormarn und Herzogtum-Lauenburg gegründetes kommunales Entsorgungsunternehmen – hat durch ihren externen Datenschutzbeauftragten eine Handreichung für die eigenen Beschäftigten dazu anfertigen lassen, welche personenbezogenen Daten diese zur Aufgabenerfüllung von anderen Behörden oder sonstigen öffentlichen Stellen anfordern dürfen. Aufgrund von Unstimmigkeiten insbe-

sondere darüber, ob die Vorschriften des BDSG oder des LDSG für die AWSH gelten, wurde die Landesbeauftragte für Datenschutz um eine Beratung gebeten.

Maßgeblich für die Feststellung des richtigen Rechtsrahmens ist, ob die AWSH als Beliehene gemäß § 24 Abs. 1 Landesverwaltungsgesetz (LVwG) tätig wird und somit Aufgaben der öffentlichen Verwaltung zur Erledigung in den Handlungsformen des öffentlichen Rechts übertragen wurden. Dann würde die AWSH als GmbH ausnahmsweise als öffentliche Stelle im Sinne von § 2 Abs. 4 Satz 2 BDSG gelten.

Erst in einem gemeinsamen Gesprächstermin wurde dargelegt, dass keine Beleihung erfolgte, sondern die AWSH als Verwaltungshelferin tätig würde. Die einzig in § 3 Abs. 5 der Abfallwirtschaftssatzungen der Kreise genannte Aufgabenübertragung zur Entsorgung von Abfällen „anderer Herkunftsbereiche" stelle einen Spezialfall dar und betreffe nicht die Abfallentsorgung bei Privathaushalten. Es bestünden sogar Auftragsdatenverarbeitungsverträge mit den Kreisen nach altem Recht.

Im Ergebnis musste demnach eine Anpassung der Auftragsverarbeitungsverträge an die Vorgaben des Art. 28 Abs. 3 DSGVO erfolgen. Es wurde außerdem auf § 21 der Landesverordnung zur Durchführung des Landesmeldegesetzes (Landesmeldeverordnung – LMVO) hingewiesen, wonach eine Zertifizierung beim ULD zu beantragen wäre. Zwar kann die Landesbeauftragte für Datenschutz zum jetzigen Zeitpunkt keine Zertifizierungen vornehmen (siehe hierzu Kapitel 9). Um der Verpflichtung zu genügen, könne jedoch ein entsprechender Antrag beim ULD gestellt werden.

Bezogen auf die nachgelagerte Frage, in welchem Umfang und auf welcher Rechtsgrundlage die Verarbeitung personenbezogener Daten durch die AWSH erfolgen dürfte, war die gegenständliche Handreichung (Stand Februar 2019) zu weitreichend und missverständlich formuliert.

§ 21 LMVO

Erfolgen Datenabrufe an Behörden oder sonstige öffentliche Stellen aus der Spiegeldatenbank bei der Vermittlungsstelle des Landes Schleswig-Holstein im Wege der Auftragsdatenverarbeitung durch eine andere als in § 34 Abs. 1 BMG genannte Stelle, ist der Abruf nur zulässig, wenn die abrufende Stelle durch das Unabhängige Landeszentrum für Datenschutz zertifiziert worden ist.

Neben den in § 13 der Abfallwirtschaftssatzungen der Kreise für eine Verarbeitung benannten Daten besteht unter den oben genannten Voraussetzungen die Möglichkeit einer melderechtlichen Auskunft nach § 34 Bundesmeldegesetz (BMG). Unter den strengen Voraussetzungen des § 31 Abs. 3 der Abgabenordnung (AO) – der u. a. eine Interessenabwägung vorsieht – dürfen Namen und Anschriftsdaten von Grundstückseigentümern übermittelt werden, die den für die Verwaltung der Grundsteuer zuständigen Behörden bekannt sind, sofern die empfangenden Stellen explizit zur Aufgabenerfüllung auf diese Daten angewiesen sind. Die regelmäßige Abfrage von Anschriften von Baubehörden auf Grundlage von Amtshilfeersuchen nach §§ 32, 33 LVwG halten wir dagegen für nicht vertretbar.

Der AWSH wurde nahegelegt, die Handreichung anzupassen, um eine rechtswidrige Datenverarbeitung zu verhindern.

Was ist zu tun?

Abfallwirtschaftsbetriebe, die nicht als Beliehene, sondern als Verwaltungshelfer tätig werden, müssen einen Auftragsverarbeitungsvertrag gemäß Art. 28 Abs. 3 DSGVO abschließen. Auch die weiteren Voraussetzungen des Artikels 28 DSGVO müssen erfüllt sein.

Daneben ist gemäß § 21 LMVO bis auf Weiteres eine Zertifizierung beim Unabhängigen Landeszentrum für Datenschutz zu beantragen.

4.1.9 Einbeziehung eines Betriebsarztes

Das ULD wurde gebeten zu prüfen, inwieweit eine Behörde Informationen einer beschäftigten Person aus einem Antrag zur behinderungsgerechten Gestaltung des Arbeitsplatzes an einen Betriebsarzt weitergeben durfte.

Antragstellung Schwerbehinderter

Nach § 164 Abs. 4 Nr. 4 SGB IX haben schwerbehinderte Menschen gegenüber ihren Arbeitgebern Anspruch auf behinderungsgerechte Einrichtung und Unterhaltung der Arbeitsstätten einschließlich der Betriebsanlagen, Maschinen und Geräte sowie der Gestaltung der Arbeitsplätze, des Arbeitsumfelds, der Arbeitsorganisation und der Arbeitszeit, unter besonderer Berücksichtigung der Unfallgefahr.

Die Weitergabe der Informationen im Zusammenhang mit dem gestellten Antrag musste an den Vorgaben des Landesdatenschutzgesetzes und den beamtenrechtlichen Regeln gemessen werden. Der Dienstherr darf personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten (z. B. Gesundheitsdaten einschließlich Angaben zur Schwerbehinderung) über seine Beschäftigten verarbeiten, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift oder eine Vereinbarung nach dem Mitbestimmungsgesetz Schleswig-Holstein dies erlaubt.

Die entsprechende Datenverarbeitung bzw. Informationsweitergabe an den Betriebsarzt war nach Einschätzung des ULD zulässig. Maßgebend war dabei auch, dass eine besondere gesetzliche Vorgabe nach dem Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit (ASiG) als Grundlage herangezogen werden konnte.

Einbeziehung von Betriebsärzten

Gemäß § 3 Abs. 1 Satz 1 und 2 Nr. 1 Buchst. f und g ASiG haben die Betriebsärzte die Aufgabe, den Arbeitgeber beim Arbeitsschutz und bei der Unfallverhütung in allen Fragen des Gesundheitsschutzes zu unterstützen. Sie haben insbesondere den Arbeitgeber und die sonst für den Arbeitsschutz und die Unfallverhütung verantwortlichen Personen zu beraten, insbesondere bei Fragen des Arbeitsplatzwechsels sowie der Eingliederung und Wiedereingliederung Behinderter in den Arbeitsprozess (f) und der Beurteilung der Arbeitsbedingungen (g).

Aus organisatorischen Gründen kann es dabei erforderlich sein, zur Ermittlung einer effektiven Hilfe für den Antragsteller einen Betriebsarzt

hinzuzuziehen. Die betriebsärztliche Stellungnahme soll den Dienstherrn in die Lage versetzen, auf die Belange der schwerbehinderten Person optimal einzugehen und eine sachgerechte Entscheidung über den gestellten Antrag zu treffen.

4.1.10 Einordnung von kommunalen Fraktionen als nichtöffentliche Stellen

Im Rahmen einer Anfrage war zu beurteilen, inwieweit kommunale Mandatsträger als öffentliche Stellen im Sinne der Vorschriften des Landesdatenschutzgesetzes anzusehen sind. Aus einer entsprechenden Einordnung ergeben sich dabei vielfältige Konsequenzen. Bei der Annahme einer öffentlichen Stelle würde nach den Regeln der DSGVO beispielsweise die Pflicht bestehen, eine oder einen Datenschutzbeauftragten zu benennen.

Benennung Datenschutzbeauftragter

Nach Art. 37 Abs. 1 Buchst. a DSGVO benennen der Verantwortliche und der Auftragsverarbeiter auf jeden Fall eine oder einen Datenschutzbeauftragten, wenn die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln.

Wird hingegen angenommen, kommunale Mandatsträger sind als nichtöffentliche Stellen Verantwortliche, so hat dies etwa haftungsrechtliche Auswirkungen. Bei Verstößen gegen datenschutzrechtliche Bestimmungen durch nichtöffentliche Stellen kann die Prüfung der Einleitung eines Ordnungswidrigkeitenverfahrens von Bedeutung sein. Gegenüber öffentlichen Stellen werden bei entsprechenden Verstößen dagegen keine Bußgelder verhängt.

Geldbußen bei öffentlichen Stellen

Gemäß § 19 Abs. 1 Landesdatenschutzgesetz werden gegen Behörden oder sonstige öffentliche Stellen im Sinne von § 2 Abs. 1 und 2 LDSG keine Geldbußen verhängt.

Für die Einordnung als öffentliche Stellen könnte zunächst sprechen, dass für kommunale Mandatsträger auch öffentlich-rechtliche Normen Anwendung finden, insbesondere Bestimmungen der Gemeindeordnung und der Kreisordnung.

Nach den Vorgaben des Landesdatenschutzgesetzes sind öffentliche Stellen Behörden und sonstige öffentliche Stellen der im Landesverwaltungsgesetz genannten Träger der öffentlichen Verwaltung. Kommunale Mandatsträger dürften jedoch nicht als „Behörde“ im Sinne von § 3 Abs. 2 LVwG gelten, da keine öffentlich-rechtliche Verwaltungstätigkeit entfaltet wird (etwa Erlass von Verwaltungsakten, Abschluss öffentlich-rechtlicher Verträge). Auch eine Einordnung der kommunalen Mandatsträger als „sonstige Behörden“ (§§ 12 f. LVwG) erscheint nicht sachgerecht. Insbesondere stehen kommunale Mandatsträger nicht in einem Beleihungsverhältnis (§§ 13, 24 LVwG).

In der Rechtsprechung wurde losgelöst von einer datenschutzrechtlichen Bewertung im Bereich des Strafrechts entschieden, dass kommunale Mandatsträger grundsätzlich keine Amtsträger im Sinne von § 11 Abs. 1 Nr. 2 StGB sind. Die Mandatsträger sind nicht in eine Behördenstruktur eingegliedert, wie dies etwa für Beschäftigte einer öffentlichen Stelle angenommen werden kann. Kommunale Mandatsträger nehmen bei der Tätigkeit in den Volksvertretungen der Gemeinden ihre öffentlichen Aufgaben nicht im Rahmen eines Dienst- oder Auftragsverhältnisses wahr, sondern in freier Ausübung ihres durch Wahl erworbenen Mandats. Diese Rechtsprechung ist für die vorliegende Fragestellung nicht übertragbar, zeigt jedoch, dass kommunale Mandatsträger nicht dazu bestellt sind, öffentliche Aufgaben bei einer Behörde oder sonstigen Stelle oder in deren Auftrag wahrzunehmen.

Nach der Gemeindeordnung können sich Gemeindevertreterinnen und Gemeindevertreter durch Erklärung gegenüber der oder dem Vorsitzenden der Gemeindevertretung zu einer Fraktion zusammenschließen. Fraktionen werden in der Rechtsprechung überwiegend als bürgerlich-rechtliche Zusammenschlüsse in Form des nicht rechtsfähigen Vereins angesehen. Für kommunale Fraktionen wird daher eine Qualifizierung als nichtöffentliche Stellen in Betracht kommen. Kommunale Mandatsträger, die für ihre Fraktionen tätig sind, werden dann nicht als Verantwortliche (Art. 4 Nr. 7 DSGVO) qualifiziert, sondern vielmehr die jeweilige Fraktion. Eine Stellung als Verantwortliche (nichtöffentliche Stelle als natürliche Person) kommt gegebenenfalls für fraktionslose Mandatsträger in Betracht.

4.1.11 Prüfung kommunaler Rechenzentren

Da viele Verwaltungen ihre IT inzwischen von Dienstleistern betreiben lassen, haben wir Anfang 2019 mit der Prüfung zweier kommunaler Rechenzentren begonnen. Dabei wurden teilweise alarmierende Mängel bei der technischen und organisatorischen Ausgestaltung der Systeme festgestellt.

Bei einem Dienstleister konnte u. a. eine unverhältnismäßig hohe Anzahl von Personen – darunter auch Subunternehmer – mit Administrationskonten nahezu unkontrolliert auf die Systeme sämtlicher angeschlossener Verwaltungen zugreifen. Darunter waren auch Gruppenkonten, die von einer unbestimmten Zahl von Personen genutzt werden konnten. Auch wurde eine Vielzahl von Benutzernamen und Kennwörtern zu Standardadministrationskonten und Fachverfahren in einer Datei gespeichert, zu der eine unbekannte Anzahl von Personen unkontrollierten Zugang hatte. Eine Dokumentation der eingesetzten Komponenten und Verfahren war größtenteils nicht vorhanden, sodass teilweise keine Prüffähigkeit gegeben war. Verträge zur Auftragsverarbeitung befanden sich über Jahre im Entwurfsmodus.

Bei dem anderen Dienstleister waren dagegen technische und organisatorische Maßnahmen weitgehend umgesetzt. Jedoch waren u. a. die Dokumentation der Verfahren und Prozesse sowie die formelle Ausgestaltung der Vertragsverhältnisse verbesserungswürdig.

Beide Dienstleister haben sich in den Prüfungsterminen kooperativ gezeigt und mit der Beseitigung der festgestellten Mängel begonnen. Die Verfahren sind noch nicht abgeschlossen.

Was ist zu tun?

Verantwortliche müssen bereits bei der Auswahl von Auftragsverarbeitern, aber auch im Rahmen der Aufgabenübertragung genau darauf achten, dass Klarheit über die Rollen der Parteien und den Umfang der wahrzunehmenden Aufgaben besteht. Sofern eine Auftragsverarbeitung gegeben ist, muss ein Vertrag nach Artikel 28 DSGVO geschlossen werden. Liegt eine gemeinsame Verantwortlichkeit vor, sind Vereinbarungen zu treffen, die den Anforderungen des Artikels 26 DSGVO gerecht werden.

Auch im Rahmen laufender Vertragsverhältnisse sind die Verantwortlichen gut beraten, regelmäßig ihre Dienstleister zu kontrollieren. Sofern sie selbst nicht über das für die Prüfung nötige Know-how verfügen, müssen sie sich Unterstützung von Experten hinzuholen.

4.1.12 Anfertigung von Tonaufzeichnungen eines Bürgerdialogs

Aufgrund einer Beschwerde wurde festgestellt, dass im Rahmen eines Bürgerdialogs verdeckt Tonaufnahmen angefertigt wurden. Die Gemeinde hatte für die Veranstaltungstechnik eine Firma beauftragt und diese angewiesen, eine Tonaufzeichnung der Redebeiträge herzustellen. Hierfür konnte jedoch keine Rechtsgrundlage im Sinne von Art. 6 Abs. 1 DSGVO benannt werden. Auch wurde kein Vertrag über eine Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO mit dem Dienstleister geschlossen. Die Landesbeauftragte für Datenschutz Schleswig-Holstein hat aus diesem Grund eine Verwarnung gemäß Art. 58 Abs. 2 Buchst. b DSGVO ausgesprochen. Die Gemeinde hat die Löschung der Aufnahmen sowohl im eigenen Hause als auch beim Dienstleister veranlasst.

Was ist zu tun?

Verantwortliche müssen vor der Anfertigung von Tonaufzeichnungen gewährleisten, dass eine Rechtsgrundlage dafür gegeben ist und Transparenz für die betroffenen Personen hergestellt wird. Werden Dienstleister im Rahmen einer Auftragsverarbeitung eingebunden, sind diese vertraglich nach Art. 28 Abs. 3 DSGVO zu verpflichten.

4.1.13 Infektion von Verwaltungsrechnern – und was man dagegen tun muss

Im Laufe des Jahres 2019 erreichten uns zahlreiche Datenpannenmeldungen nach Artikel 33 DSGVO, in denen Schulverwaltungen, Städte, Ämter und Gemeinden anzeigten, dass ein oder mehrere Computerarbeitsplätze durch Malware (Schadsoftware) infiziert worden seien.

Emotet

Emotet gehört zu den Malware-Programmen, die über unverlangt eingehende E-Mails verteilt werden und die Empfänger dazu bringen wollen, auf schädliche Links zu klicken oder Dateien im Anhang zu öffnen. Ist der Rechner infiziert, liest Emotet die Kontakte und E-Mail-Inhalte aus. Mit diesen Informationen generiert Emotet authentisch wirkende E-Mails an neue Opfer. Durch nachgeladene Schadfunktionen können Daten vom infizierten Rechner abfließen und ein Angreifer kann die Kontrolle über das IT-System übernehmen.

Sofern die Infektion zu einer Verschlüsselung der Systeme führte, konnten die so unzugänglichen Daten durch Back-ups wiederhergestellt werden. In der Regel wurden die in den Adressbüchern der infizierten Rechner enthaltenen Kontaktadressen angeschrieben und betroffene Personen über möglicherweise versandte Spam-E-Mails informiert.

Ein Abfluss von personenbezogenen Daten wurde in keinem der gemeldeten Fälle festgestellt.

Wenn Datenpannen an uns gemeldet werden, zeigt dies zumindest, dass in dem Fall ein Bewusstsein für die datenschutzrechtlichen Pflichten besteht und es einen organisatorischen Prozess zum Melden gibt.

Wichtig ist aber, dass solche Malware-Infektionen kein leichtes Spiel haben sollten:

- Die Verantwortlichen müssen präventiv sicherstellen, dass Sicherheitsupdates

für Betriebssysteme und Anwendungsprogramme (Webbrowser, E-Mail-Clients, Office-Anwendungen usw.) zeitnah installiert werden.

- Die Antivirensoftware muss ständig aktualisiert werden.
- Auch regelmäßige Datensicherungen sind Pflicht.
- Die Beschäftigten müssen hinreichend sensibilisiert sein, um gefälschte E-Mails auch bei vermeintlich bekannten Absendern zu erkennen.
- Dateianhänge (insbesondere Office-Dokumente) oder Links sollten geprüft werden, bevor sie geöffnet werden. Bei einer verdächtigen E-Mail sollte im Zweifel der Absender angerufen werden.

Liegt eine Infektion vor, ist in der Regel eine Meldung von Verletzungen des Schutzes personenbezogener Daten nach Artikel 33 DSGVO bzw. § 41 LDSG erforderlich. Zudem sollten die Mailkontakte über die Infektion informiert werden, denn diese sind besonders gefährdet. Daneben sollten alle auf dem betroffenen System gespeicherten und eingegebenen Zugangsdaten geändert werden. Im Fall von Emotet und Konsorten kommt es teilweise zu tief greifenden sicherheitsrelevanten Änderungen des infizierten IT-Systems – dann müssen die betroffenen Rechner neu aufgesetzt werden, wie es auch vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen wird.

Was ist zu tun?

Die Verantwortlichen müssen eine ausreichende Sicherheit der Verarbeitung personenbezogener Daten und das notwendige Niveau dauerhaft gewährleisten. Ist doch mal etwas passiert, muss dies der Datenschutzaufsichtsbehörde gemeldet werden.

4.1.14 Einräumung falscher Zugriffsrechte

Weitere Meldungen nach Artikel 33 DSGVO betrafen die Einräumung falscher Zugriffsrechte in der Netzumgebung der IT-Systeme verschiedener von einem kommunalen Rechenzentrum betreuten Verwaltungen. Beschäftigte konnten im Windows-Explorer ihrer Clients im Ordner „Netzwerk“ Ordnerbezeichnungen sehen: Teilweise war kein weiterer Zugriff möglich, aber die Bezeichnungen ließen auf die Verarbeitungen schließen. Teilweise konnten jedoch zahlreiche Beschäftigte auf Unterordner mit personenbezogenen Daten zugreifen, ohne dass sie zuständig waren und diese Zugriffsrechte hätten haben dürfen.

Was ist zu tun?

Verantwortliche müssen penibel darauf achten, dass ihre Beschäftigten nur Zugang zu den personenbezogenen Daten erlangen können, die für die Erfüllung ihrer Aufgaben erforderlich sind. Dies kann durch ein ordentliches Rechte- und Rollenkonzept gewährleistet werden, sofern es auch akkurat umgesetzt und regelmäßig – auch im Hinblick auf ausscheidende Beschäftigte – gepflegt wird.

4.1.15 Datenpanne beim Buß-Bericht zur Rockeraffäre

Im Rahmen der Aufklärung der Rockeraffäre (37. TB, Tz. 4.2.7), die im Einzelnen im Parlamentarischen Untersuchungsausschuss bearbeitet wird, wurde der ehemalige Innenminister Klaus Buß als Sonderbeauftragter beauftragt, einen Bericht zu erstellen. Dieser Bericht, der im März 2018 fertiggestellt war, enthält zahlreiche sensible Informationen, auch über Personen. Im August 2019 wurde dem Innenministerium bekannt, dass Journalisten einer Zeitung diesen Bericht eingesehen hätten. Das Innenministerium vermutete einen Zusammenhang mit einem Versand einer E-Mail, die irrtümlich Teile des Berichts in einer vertraulichen Fassung enthielt. Es handelte sich demnach um eine Datenpanne, die das Innenministerium an die Datenschutzaufsichtsbehörde nach Artikel 33 DSGVO meldete.

Wie es in solchen Fällen üblich ist, haben wir ein Verfahren eingeleitet und um die Beantwortung zahlreicher Fragen zur Sache gebeten. Unserer Einschätzung, dass aus der fehlerhaften Weitergabe von Teilen des sensiblen Dokuments ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen resultiert, ist das Innenministerium nicht entgegengetreten. Es wurde zugesagt, dass die betroffenen Personen nach Artikel 34 DSGVO von der Datenpanne unterrichtet werden. Daraufhin konnte das aufsichtsbehördliche Verfahren eingestellt werden.

4.2 Polizei und Verfassungsschutz

4.2.1 Änderung des Landesverwaltungsgesetzes

Das Innenministerium hat uns im Berichtszeitraum einen Entwurf zur Änderung des Landesverwaltungsgesetzes vorgelegt, mit dem das Polizeirecht novelliert werden soll. Mit der Novelle werden drei Ziele verfolgt: Die EU-Richtlinie über den Datenschutz bei der Strafverfolgung soll umgesetzt werden, die Eingriffsbefugnisse der Polizei sollen an die Vorgaben des Bundesverfassungsgerichts aus dem Urteil zum BKA-Gesetz und die Befugnisse der Polizei sollen an eine geänderte Gefahrenlage angepasst werden.

Obwohl zwei der Ziele des Entwurfs darin bestehen, gestiegene datenschutzrechtliche Anforderungen umzusetzen, dominiert in dem vom Innenministerium vorgelegten Entwurf ganz klar der Sicherheitsgedanke. Zwar enthält der Entwurf einige Verbesserungen für den Datenschutz. Diese können aber nicht darüber hinwegtäuschen, dass mehr Befugnisse für die Erhebung und Verarbeitung personenbezogener Daten eingeführt werden und die Datenverarbeitung in diesem sensiblen Bereich dadurch insgesamt erweitert wird. Im Entwurf finden sich eingriffsintensive Maßnahmen wie z. B. die Einführung von Befugnissen für GPS-Tracking, der Einsatz verdeckter Ermittler oder die Durchführung von verdachtsunabhängigen Kontrollen in Verkehrsmitteln und auf Verkehrswegen. Diese schwerwiegenden Eingriffe können durch die vorgesehenen, aus dem EU-Recht stammenden Maßnahmen zur Verbesserung des Datenschutzes, die eher technisch-organisatorischer Natur sind und Vorkehrungen zur Einhaltung der Zweckbindung der Daten und zur Verbesserung der nachträglichen Kontrolle treffen, nicht kompensiert werden. In der Gesamtbetrachtung führt der Gesetzentwurf daher in einem größeren Maße zu Einbußen für die Grundrechte der Bürgerinnen und Bürger, als dass er Verbesserungen für ihre Rechte brächte.

Auch zu einzelnen Regelungen haben wir Bedenken, die wir gegenüber dem Innenministerium in einer Stellungnahme vorgetragen haben. Dies betrifft insbesondere folgende Regelungen:

- die Einführung einer Befugnis zur anlasslosen Identitätsfeststellung in Verkehrsmitteln und auf Durchgangsstraßen für den grenzüberschreitenden Verkehr,
- den Einsatz von Bodycams auch auf Wohngrundstücken und die Befugnis für einen anlasslosen Einsatz von Bodycams im Pre-Recording-Modus,
- die neu eingeführte Definition der dringenden Gefahr,
- die Absenkung des Schutzes des Kernbereichs privater Lebensgestaltung.

Im Entwurf ist zudem eine Pflicht für die Landesbeauftragte für Datenschutz vorgesehen, verdeckte Maßnahmen und Übermittlungen in Drittstaaten mindestens alle zwei Jahre zu überprüfen. Dies entspricht einer Vorgabe des Bundesverfassungsgerichts. Es muss jedoch sichergestellt sein, dass die Wahrnehmung bestehender Aufgaben hierdurch nicht beeinträchtigt wird. Anderenfalls befürchten wir, dass tatsächliche Problemfelder unbearbeitet bleiben müssen, die manchmal weitaus mehr Anlass für Beschwerden geben können als die Verarbeitungen, zu deren Überprüfung wir gesetzlich verpflichtet sind.

Um diese Flexibilität zu erhalten, halten wir zwei Voraussetzungen für wesentlich: Zum einen dürfen die Prüfpflichten nicht derart starr ausgestaltet sein, dass sie selbst keinen Spielraum mehr lassen. Diese Voraussetzungen sind durch die Regelung des Entwurfs erfüllt, die wir so verstehen, dass alle zwei Jahre die Datenverarbeitung zu einer Auswahl an Maßnahmen und Übermittlungen geprüft werden muss, nicht aber, dass die Datenverarbeitung zu allen Maßnahmen im zweijährigen Abstand zu prüfen ist. Zum anderen ist für die Erfüllung der Prüfpflichten Voraussetzung, dass hierfür ausreichende Ressourcen bereitstehen. Auch ohne die neue Regelung bestehen bereits im nationalen und im EU-Recht zahlreiche Prüfpflichten für die Datenverarbeitung in polizeilichen Dateien (37. TB, Tz. 4.2.1). Die Erfüllung weiterer Prüfpflichten wird ohne Bereitstellung zusätzlicher Ressourcen nicht möglich sein. Wir begrüßen daher, dass ein erhöhter Verwaltungsaufwand und damit auch ein erhöhter Kostenaufwand für das ULD im Gesetzentwurf berücksichtigt sind.

Was ist zu tun?

Der Gesetzentwurf muss in einigen Punkten überarbeitet werden, um die Persönlichkeitsrechte betroffener Personen angemessen zu wahren. Die Einführung neuer Prüfpflichten für das ULD erfordert zusätzliche personelle Ressourcen.

4.2.2 Flugdrohnen bei der Landespolizei

Seit einigen Jahren erfreuen sich Flugdrohnen einer immer größeren Beliebtheit. Ob als Hobby oder im professionellen Einsatz, immer häufiger sieht man derartige Fluggeräte. Häufig ist nicht erkennbar, wer die Drohne steuert. Auch sind diese Fluggeräte in der Regel mit Kameras ausgestattet.

Mit Wirkung vom 7. April 2017 wurde die Luftverkehrsverordnung daher um Regelungen zum Betrieb von unbemannten Fluggeräten erweitert. Demnach ist der Flug z. B. über Menschenansammlungen oder Wohngrundstücken in der Regel verboten. Sieht man eine Drohne in diesem Kontext, könnte es sich jedoch um eine Drohne der Landespolizei handeln, für die die Verbote der Verordnung nicht gelten.

Die Landespolizei hat bisher zwei Flugdrohnen angeschafft. Zu den möglichen Einsatzzwecken gehören z. B. die Suche nach vermissten Personen oder Straftätern in unübersichtlichem Gebiet und die Erstellung von Übersichtsaufnahmen für einsatztaktische Zwecke an Unfall-

oder Tatorten sowie bei Schadenslagen. Die Drohnen sind mit Kameras ausgestattet und können Aufnahmen anfertigen.

Auch wenn die Verbote der Drohnenverordnung für die Polizei nicht gelten, so sind beim Einsatz der Drohnen die grundlegenden Regelungen des Landesverwaltungsgesetzes sowie die allgemeinen Datenschutzgrundsätze zu beachten. Das Einsatzkonzept sieht deshalb u. a. vor, dass der Einsatz bei Versammlungen nach dem Versammlungsgesetz ausgeschlossen ist. Wohngrundstücke sollen nur überflogen werden, wenn dies unbedingt erforderlich ist, und dies in einer Höhe und mit einem Zoom, dass Personen zwar erkennbar, aber nicht identifizierbar sind.

Werden die Videodaten aufgezeichnet, beträgt die Löschfrist – abhängig vom Anlass der Aufzeichnung und deren Rechtsgrundlage – wenige Tage bis hin zu mehreren Jahren (z. B. bei Aufnahmen für die Aus- und Fortbildung). Personen, die vermuten, durch den Einsatz einer Polizeidrohne betroffen zu sein, können sich an die behördlichen Datenschutzbeauftragten der Landespolizei wenden und um Auskunft darüber bitten, ob und wenn ja welche personenbezogenen Daten erhoben wurden und wie diese verarbeitet werden (Tz. 4.2.3).

4.2.3 Erweitertes Auskunftsrecht für Bürger

Immer wieder wenden sich Bürgerinnen und Bürger an die Landesbeauftragte für Datenschutz, weil sie wissen möchten, welche Daten über sie bei der Landespolizei gespeichert sind. Viele wissen nicht, dass sie einen datenschutzrechtlichen Auskunftsanspruch gegenüber der Polizei haben. Durch die Umsetzung europäischer Rechtsakte ist der Umfang dieses Auskunftsanspruchs sogar noch erweitert worden.

Das Auskunftsrecht umfasst grundsätzlich alle personenbezogenen Daten, die verarbeitet werden. Es dient dazu, sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Neben den personenbezogenen Daten selbst besteht auch ein Anspruch auf weitere Informationen, wie z. B. zu welchen Kategorien die verarbeiteten Daten gehören, die verfügbaren Informationen über die Herkunft der Daten, die Zwecke der Verarbeitung und deren Rechtsgrundlage, die Empfänger oder die Kategorien von Empfängern der Daten, die geltende Speicherdauer oder die Regeln, nach denen sie festgelegt wird, der Hinweis auf das Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung durch den Verantwortlichen sowie der Hinweis auf das Beschwerderecht bei der Landesbeauftragten für Datenschutz.

Bei allgemeinen Auskunftsersuchen werden zurzeit nicht alle diese Informationen standardmäßig durch die Polizei zur Verfügung gestellt. Dies ist u. a. dem Umstand geschuldet, dass die IT-Verfahren nicht in der Lage sind, diese Informationen automatisiert zusammenzustellen. Außerdem sind personenbezogene Daten teilweise über verschiedene Dateien und Verfahren verteilt. Viele Informationen müssen daher händisch abgefragt und zusammengetragen werden. Bei konkreten Fragestellungen bietet es sich daher an, diese explizit in das Auskunftsersuchen aufzunehmen oder gegebenenfalls bei der Polizei nachzufragen, wenn wesentliche Fragen unbeantwortet geblieben sind.

Wo erhalte ich Auskunft?

Ihr unterschriebenes Auskunftsersuchen richten Sie formlos an das:

Landeskriminalamt, Mühlenweg 166,
24116 Kiel.

Um missbräuchliche Anfragen zu verhindern, besteht die Polizei auf eine Kopie des Personalausweises als Anlage.

Um zukünftig eine zeitnahe und umfassende Bearbeitung von Auskunftsersuchen zu ermöglichen, ist es erforderlich, die polizeilichen IT-Verfahren vor dem Hintergrund der rechtlichen Vorgaben weiterzuentwickeln. Zur Aus-

kunft berechtigte Stellen müssen in die Lage versetzt werden, zeitnah alle relevanten Informationen zusammenzutragen und bürgerfreundlich aufzuarbeiten.

Wird die Auskunft versagt oder eingeschränkt, besteht u. a. die Möglichkeit, sich an die Landesbeauftragte für Datenschutz zu wenden, um die Rechtmäßigkeit der Datenverarbeitung unabhängig prüfen zu lassen.

Was ist zu tun?

Betroffene sollten ihr Auskunftsersuchen so konkret wie möglich stellen.

Die IT-Verfahren der Landespolizei müssen so weiterentwickelt werden, dass Auskünfte durch die dafür berechtigten Stellen umfassend und zeitnah erteilt werden können.

4.2.4 Welche personenbezogenen Daten muss ich der Polizei geben?

Im Berichtszeitraum meldete sich ein Bürger bei der Landesbeauftragten für Datenschutz, der bei der Polizei eine Ruhestörung angezeigt hatte. Im Zuge des folgenden Polizeieinsatzes wurde seine Identität festgestellt. Außerdem wurde er nach seiner Handynummer und seinem Familienstand gefragt. Der Betroffene war verunsichert, welche Informationen er in dieser Situation der Polizei mitteilen muss.

Bei der Beseitigung einer Ruhestörung handelt es sich in der Regel um eine gefahrenabwehrrechtliche Maßnahme, an die sich häufig (aber nicht zwingend) ein Ordnungswidrigkeitenverfahren anschließt. Zur Dokumentation des polizeilichen Handelns sowie zur Vorbereitung eines möglichen Ordnungswidrigkeitenverfahrens darf die Polizei die Identität des Anzeigenden feststellen. Doch wie steht es mit der Handynummer und dem Familienstand?

Sowohl nach Gefahrenabwehrrecht als auch im Rahmen eines Ordnungswidrigkeitenverfahrens gibt es allgemeine Befugnisnormen zur Erhebung personenbezogener Daten. Nach § 22 LDSG gelten jedoch die Grundsätze der Erforderlichkeit und der Verhältnismäßigkeit. Sind bestimmte Daten z. B. zur Durchführung eines Ordnungswidrigkeitenverfahrens erforderlich, müssen Personen die entsprechenden Angaben machen.

Bei der Handynummer handelt es sich jedoch um eine Angabe, die – im vorliegenden Sachverhalt – lediglich der Verfahrensvereinfachung dient. Anstatt den Anzeigenden postalisch anzuschreiben oder aufzusuchen, kann man z. B. im Falle von Rückfragen anrufen. Ein Polizeibeamter kann in diesem Fall nicht auf die Herausgabe der Handynummer bestehen. Inwiefern der Familienstand für die Bearbeitung des Sachverhalts erforderlich war, konnte die Polizei nicht darlegen. Die Frage nach dem Familienstand war daher unzulässig.

Für betroffene Bürgerinnen und Bürger ist es schwer zu erkennen, welche von einem Polizisten abgefragten Informationen sie preisgeben müssen und bei welchen es sich um freiwillige Angaben handelt. Was kann man tun, wenn man sich nicht sicher ist oder sich bei der Frage unwohl fühlt?

Im Zweifelsfall sollte man die Beamtin oder den Beamten freundlich fragen, ob man zur Auskunft verpflichtet ist, und sich gegebenenfalls nach der Rechtsgrundlage erkundigen. Außerdem kann man sich auch nachträglich an die behördlichen Datenschutzbeauftragten der Polizei oder die Landesbeauftragte für Datenschutz wenden.

Was ist zu tun?

Die Polizei sollte ihre Bediensteten dafür sensibilisieren und entsprechend schulen, dass nicht zu viele Daten abgefragt werden und für die befragten Personen deutlich wird, wann es sich um freiwillige Informationen handelt.

4.2.5 Null Datenpannenmeldungen im Polizeibereich?!

Seit der jüngsten Anpassung des Landesdatenschutzgesetzes besteht nach § 41 LDSG eine gesetzliche Pflicht, Verletzungen des Schutzes personenbezogener Daten der Landesbeauftragten für Datenschutz zu melden. Diese Meldung muss unverzüglich und möglichst innerhalb von 72 Stunden nach Bekanntwerden erfolgen. Worum geht es bei der Meldepflicht solcher Datenpannen, und wie kommt die Landespolizei dieser Pflicht nach?

Mit dieser Regelung werden europarechtliche Vorgaben umgesetzt. Gemeldet werden müssen Verletzungen der Sicherheit, die unbeabsichtigt oder unrechtmäßig u. a. zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung personenbezogener Daten führen. Dabei kann es sich z. B. um falsch zugestellte E-Mails, Briefpost oder Faxe handeln, den Verlust von Unterlagen oder Datenträgern, die Möglichkeit der Einsichtnahme durch Unbefugte (z. B. Reinigungskräfte) in herumliegende oder nicht durch Verschluss gesicherte personenbezogene Daten oder Dateien oder ein Versagen von technisch-organisatorischen Schutzmaßnahmen bei Malware (Tz. 4.1.13), wenn personenbezogene Daten betroffen sind.

Eine Verletzung des Schutzes personenbezogener Daten kann – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für betroffene Personen nach sich ziehen. Dazu zählen etwa der Verlust der Kontrolle über ihre personenbezogenen Daten oder die Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von personenbezogenen Daten, die dem Berufsgeheimnis unterliegen, oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene Person.

Deshalb ist die Polizei verpflichtet, sobald ihr eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde unverzüglich zu unterrichten. Von der Meldung kann abgesehen werden, wenn die Polizei im Einklang mit dem Grundsatz der Rechenschaftspflicht nachweisen kann, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten betroffener Personen geführt hat. Ein Beispiel wäre der Verlust eines – nach dem Stand der Technik verschlüsselten – USB-Sticks mit personenbezogenen Daten, sofern nicht das Passwort für die Entschlüsselung ebenfalls betroffen sein könnte, z. B. weil jemand es auf dem USB-Stick notiert hat. In diesem Fall (ohne lesbares Passwort) bestünde voraussichtlich kein Risiko für die Rechte der betroffenen Personen, und eine Meldung an die Aufsichtsbehörde wäre nicht erforderlich.

Kann ein Risiko nicht ausgeschlossen werden, besteht jedoch die gesetzliche Pflicht zur Meldung. Die Aufsichtsbehörde wird dadurch in die Lage versetzt zu prüfen, ob die ergriffenen Maßnahmen ausreichen, um das Risiko einzudämmen und zukünftige Vorfälle dieser Art zu vermeiden.

Bei einem hohen Risiko für die Rechte betroffener Personen muss die Polizei diese sogar benachrichtigen (§ 42 LDSG). Die Benachrichtigung muss eine Beschreibung der Art der Ver-

letzung des Schutzes personenbezogener Daten sowie an die betroffene Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten. Die betroffenen Personen sollten so schnell wie möglich benachrichtigt werden.

Obwohl die gesetzliche Meldepflicht bereits seit Mai 2018 besteht, wird dieses Instrument zur Stärkung der Rechte schleswig-holsteinischer Bürgerinnen und Bürger im Polizeibereich anscheinend bis heute nicht angewendet. Während bei Aufsichtsbehörden anderer Bundesländer beinahe wöchentlich Meldungen der Polizei eingehen, gibt es in Schleswig-Holstein bisher keine einzige Meldung aus diesem Bereich. Seit Januar 2019 hat die Landesbeauftragte für Datenschutz dieses Thema wiederholt auf unterschiedlichen Ebenen der Landespolizei zur Sprache gebracht. Die gesetzliche Meldepflicht zu Datenpannen kann nur funktionieren, wenn die Mitarbeiterinnen und Mitarbeiter der Landespolizei sowie ihre Führungskräfte Verletzungen des Schutzes personenbezogener Daten erkennen und einen definierten Meldeweg einhalten. Bis heute gibt es weder ein Konzept zur Schulung der ca. 6.500 Bediensteten im Polizeibereich, noch ist uns ein Konzept zur Meldung und Bewertung entsprechender Verletzungen bekannt. Es wäre fatal, wenn der Eindruck entstehen würde, dass die Polizei zwar ihre gesetzlichen Befugnisse zum Eingriff in Bürgerrechte nutzt, auf der anderen Seite aber nicht dafür Sorge trägt, selbst ihre gesetzlichen Pflichten zu erfüllen, die die Bürgerrechte stärken sollen.

Die Meldepflicht zu Datenpannen dient in erster Linie dem Schutz der Rechte betroffener Bürgerinnen und Bürger. Wird sie richtig umgesetzt, bietet sie jedoch auch einen großen Mehrwehrt für die Organisation. Sind die Mitarbeitenden entsprechend sensibilisiert, führt dies insgesamt zu einem besseren Umgang mit personenbezogenen Daten. Dadurch wird auch die im Organisationsinteresse liegende Datensicherheit erhöht und möglichen „Datenskandalen“ präventiv entgegengewirkt.

Was ist zu tun?

Gesetzliche Pflichten müssen ernst genommen werden. Die Polizei muss ein Konzept für ein Verfahren zur Meldung von Datenpannen erstellen und landesweit umsetzen.

4.3 Justiz

4.3.1 Mitteilung an den Arbeitgeber über ein Strafverfahren

Staatsanwaltschaften und Gerichte sind verpflichtet, den Arbeitgeber eines Beschuldigten über das Strafverfahren zu informieren, wenn diese Information für arbeitsrechtliche Maßnahmen des Arbeitgebers, wie z. B. eine Kündigung, erforderlich ist. Dies setzt im Wesentlichen zwei Dinge voraus: Erstens muss der Tatvorwurf für die berufliche Tätigkeit relevant sein. Es muss sich um eine Verletzung von Berufsausübungspflichten handeln, oder es müssen sich aufgrund des Tatvorwurfs Zweifel an der Eignung, Zuverlässigkeit oder Befähigung des Betroffenen für seine berufliche Tätigkeit ergeben. Zweitens darf eine Übermittlung erst erfolgen, wenn die Ermittlungen so weit vorangeschritten sind, dass von einem gefestigten Tatverdacht ausgegangen werden kann. Dies ist z. B. der Fall, wenn die Staatsanwaltschaft Anklage erhoben hat.

In einem Fall hat sich ein Arbeitnehmer an uns gewandt, weil er der Meinung war, der Staatsanwalt hätte seinen Arbeitgeber nicht über das gegen ihn geführte Strafverfahren informieren

dürfen. Nach Prüfung dieser Übermittlung haben wir die Auffassung des Arbeitnehmers bestätigt und gegenüber der Staatsanwaltschaft eine Beanstandung nach dem Landesdatenschutzgesetz (in der Fassung, die bis zum 24. Mai 2018 galt) ausgesprochen.

Die Besonderheit in diesem Fall lag darin, dass gegen den Arbeitnehmer zwei Strafverfahren geführt wurden. In dem ersten Verfahren ging es um den eigentlichen Vorwurf. Das zweite Verfahren wurde wegen des Verdachts der falschen Verdächtigung eingeleitet, weil der Arbeitnehmer in dem Ausgangsverfahren Beschwerde eingelegt und darin aus Sicht der Staatsanwaltschaft wahrheitswidrige Behauptungen aufgestellt hatte.

Der eigentliche Vorwurf, der mit dem ersten Strafverfahren verfolgt wurde, war zwar möglicherweise relevant für die Berufsausübung des Beschwerdeführers. In diesem Verfahren war jedoch keine Information an den Arbeitgeber erfolgt, vielleicht weil die Ermittlungen noch nicht weit genug vorangeschritten waren. Dagegen war im zweiten Strafverfahren eine Übermittlung vorgenommen worden. Dies war vom Stand des Ermittlungsverfahrens aus betrachtet zwar zulässig. Es fehlte hier jedoch die Relevanz des Strafverfahrens für die Berufsausübung des Arbeitnehmers. Die Staatsanwaltschaft konnte nicht begründen, warum der Verdacht einer falschen Verdächtigung für die Ausübung des Berufs erheblich war. Vielmehr begründete sie die Übermittlung mit dem Tatvorwurf aus dem ersten Verfahren. Hier lag jedoch offenbar noch keine Anklage oder eine ähnliche Zwischenentscheidung der Staatsanwaltschaft vor, sodass eine Information des Arbeitgebers darüber jedenfalls zu diesem Zeitpunkt nicht zulässig war.

Die gesetzlichen Vorgaben dürfen nicht durch den Abschluss eines zweiten – damit zwar zusammenhängenden, für sich genommen aber für den Arbeitgeber nicht relevanten – Verfahrens umgangen werden.

4.3.2 Änderungen für Notare durch die Datenschutz-Grundverordnung

Für Notare hat die Datenschutz-Grundverordnung zwei wichtige Neuerungen gebracht. Mitteilungen von Notaren an das ULD zeigen, dass diese den Notaren oft nicht bewusst sind.

Pflicht zur Benennung eines Datenschutzbeauftragten

Notare sind als Träger eines öffentlichen Amts öffentliche Stellen im Sinne des Art. 37 Abs. 1 Buchst. a DSGVO und § 2 Abs. 1 Satz 2 LDSG. Öffentliche Stellen sind nach Art. 37 Abs. 1 Buchst. a DSGVO verpflichtet, einen Datenschutzbeauftragten zu benennen. Diese Pflicht knüpft allein an die Eigenschaft der öffentlichen Stelle an und gilt damit unabhängig von der Zahl der Beschäftigten oder anderer Größen. Eine Erleichterung mag es für kleine öffentliche Stellen wie Notare darstellen, dass mehrere Stellen gemeinsam einen Datenschutzbeauftragten benennen können. Damit reicht es aus, wenn Rechtsanwälte und Notare einen gemeinsamen Datenschutzbeauftragten benennen. Nach der DSGVO muss es sich bei dem Datenschutzbeauftragten auch nicht mehr um einen Beschäftigten der öffentlichen Stelle oder einen Beschäftigten im öffentlichen Dienst handeln. Es können auch externe Datenschutzbeauftragte benannt werden.

Wegfall der Pflicht zur Vorlage des Verfahrensverzeichnisses beim ULD

Nach § 7 Abs. 3 des Landesdatenschutzgesetzes in der bis zum 24. Mai 2018 geltenden Fassung waren öffentliche Stellen verpflichtet, dem ULD den Einsatz von automatisierten Datenverarbeitungsverfahren zu melden, wenn sie keinen Datenschutzbeauftragten bestellt hatten.

Diese Meldepflicht ist mit Wirksamwerden der DSGVO weggefallen. Die Datenschutz-Grundverordnung enthält keine solchen Meldepflichten mehr. Bestehen geblieben ist allerdings die Pflicht für Notare, ein Verzeichnis der Verarbeitungstätigkeiten zu führen (Artikel 30 DSGVO). Wir haben die Notarkammer über die neue Rechtslage informiert und darum gebeten, die Notare entsprechend zu unterrichten.

4.3.3 Meldepflicht zu Datenpannen im Justizbereich wohl noch nicht umfassend umgesetzt

Unter der Textziffer 4.2.5 hatten wir die Meldepflicht zu Verletzungen des Schutzes personenbezogener Daten im Polizeibereich beschrieben: Sobald eine Datenpanne bekannt geworden ist, muss dies unverzüglich, möglichst innerhalb von 72 Stunden, der Landesbeauftragten für Datenschutz gemeldet werden. Diese Meldepflicht besteht auch für den Justizbereich.

Aus der schleswig-holsteinischen Justiz hat uns im Berichtszeitraum nur eine Meldung erreicht. Die Meldungen aus anderen Bereichen zeigen, dass Verletzungen des Schutzes personenbezogener Daten im Tagesgeschäft deutlich häufiger vorkommen. Dies lässt vermuten, dass die gesetzliche Meldepflicht in der Justiz noch nicht überall umgesetzt ist. Die gesetzliche Meldepflicht kann nur funktionieren, wenn die Mitarbeiterinnen und Mitarbeiter der Justiz sowie ihre Führungskräfte Verletzungen des Schutzes personenbezogener Daten erkennen und einen definierten Meldeweg einhalten. Es muss daher in den Behörden ein Prozess etabliert werden, an dem von den einzelnen Mitarbeiterinnen und Mitarbeitern bis zur Behördenleitung alle mitwirken, um Verletzungen zu erkennen und die erforderlichen Maßnahmen zu ergreifen. Empfehlenswert ist es, in diesen Prozess beratend auch die oder den Datenschutzbeauftragten der Behörde einzubinden. Denn mit der Meldung an die Datenschutzaufsichtsbehörde ist vielfach noch nicht alles getan. Wichtig ist es für den Verantwortlichen, die Ursachen und die möglichen Folgen einer Verletzung zu erkennen und gegebenenfalls Schutzmaßnahmen zu ergreifen, beispielsweise um die Folgen eines Angriffs mit Schadsoftware zu beseitigen und dafür zu sorgen, dass sich die Datenpannenfälle künftig nicht wiederholen. Besteht aufgrund der Verletzung für die betroffenen Personen ein hohes Risiko für ihre Rechte und Freiheiten, sind auch die betroffenen Personen zu benachrichtigen.

Was ist zu tun?

Auch im Justizbereich muss die Meldepflicht zu Datenpannen landesweit in der Praxis bekannt gemacht und umgesetzt werden.

4.4 Soziales

4.4.1 Verpflichtung von Beschäftigten auf das Sozialgeheimnis

Eine Stadtverwaltung möchte wissen, ob Beschäftigte im Sozialamt gesondert auf das Sozialgeheimnis verpflichtet werden müssen. Tatsächlich sieht Art. 32 Abs. 4 DSGVO vor, dass der Verantwortliche Schritte unternehmen muss, um sicherzustellen, dass ihm unterstellte natürliche Personen (Beschäftigte), die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten.

Die Datenschutzbehörden des Bundes und der Länder empfehlen, dies in Form einer schriftlichen oder elektronischen Verpflichtungserklärung umzusetzen. In dem Kurzpapier Nr. 19 der Datenschutzkonferenz findet sich zudem ein Musterbeispiel für eine schriftliche Verpflichtung.

Auch wenn die Vorschriften des Sozialgesetzbuches keine gesonderte Verpflichtung auf das

Sozialgeheimnis für Beschäftigte bei Sozialleistungsträgern vorsehen, ist es doch zu begrüßen, wenn diese Beschäftigten auf diesem Weg auf die besondere Bedeutung des Sozialgeheimnisses hingewiesen werden.

Bei einer einmaligen datenschutzrechtlichen Verpflichtung darf es aber nicht bleiben. Es empfiehlt sich, die Beschäftigten regelmäßig über die speziellen Regelungen des Sozialdatenschutzrechts zu informieren. Bei Schulungen zu diesen Themen können auch die behördlichen Datenschutzbeauftragten unterstützen.

Das Kurzpapier Nr. 19 der Datenschutzkonferenz ist unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/dsgvo/

Was ist zu tun?

Sozialleistungsträger müssen ihre Beschäftigten nachweisbar zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen nach der DSGVO verpflichten. Es empfiehlt sich, in dieser Verpflichtung ausdrücklich auf die besonderen Anforderungen des Sozialdatenschutzrechts hinzuweisen.

4.4.2 Kann Nachbarschaftshilfe am Sozialgeheimnis scheitern?

Eine ältere Dame ist erkrankt. Wie kann die Pflegekasse helfen? Ein junger Flüchtling beherrscht die deutsche Sprache nicht. Welche Leistungen kann er beim Jobcenter beantragen? Beide benötigen Unterstützung bei den anstehenden Behördengängen. Eine Nachbarin möchte helfen. Aber als sie bei den Behörden vorspricht, erhält sie mit Verweis auf das Sozialgeheimnis keine Auskünfte.

Tatsächlich müssen Sozialleistungsbehörden neben den allgemeinen Vorschriften der DSGVO zudem die besonderen Vorschriften des Sozialdatenschutzrechts beachten. Die Anforderungen an den Schutz von Sozialdaten sind hoch. Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt verarbeitet werden (§ 35 Abs. 1 Satz 1 SGB I).

Einer Nachbarin darf daher – egal mit welchen guten Absichten sie fragt – nur mit Kenntnis und Willen der betroffenen Person Auskunft gegeben werden. Der Sozialleistungsträger muss sich vergewissern, dass die betroffene Person mit der Auskunftserteilung einverstanden ist.

Diese Einwilligung muss nicht zwingend schriftlich erfolgen (Art. 7 Abs. 2 DSGVO). Allerdings muss der Sozialleistungsträger nachweisen können, dass die betroffene Person in die Auskunftserteilung eingewilligt hat (Art. 7 Abs. 1 DSGVO). Denkbar wäre also, dass die hilfsbereite Nachbarin das Gespräch mit der Pflegekasse bzw. dem Jobcenter im Beisein der betroffenen Personen führt. So wäre es den Beschäftigten dieser Behörden möglich, sich zu vergewissern, dass die Betroffenen hiermit einverstanden sind. Alternativ besteht die Möglichkeit, dass sich die betroffenen Personen schriftlich damit einverstanden erklären, dass die Nachbarin Auskunft erhalten, vielleicht sogar Anträge stellen darf.

Was ist zu tun?

Datenschutz verhindert nicht die Nachbarschaftshilfe. Sind Sozialdaten betroffen, dürfen Sozialleistungsträger nur personenbezogene Daten an Nachbarn herausgeben, wenn die betroffenen Personen in die Auskunftserteilung eingewilligt haben.

4.5 Schutz des Patientengeheimnisses

4.5.1 Anhörung zum Entwurf für ein neues Landeskrankenhausgesetz

Das federführende Ministerium für Soziales, Gesundheit, Jugend, Familie und Senioren Schleswig-Holstein hat den Landtag über den Entwurf für ein neues Landeskrankenhausgesetz (LKHG) informiert, zugleich eine Anhörung zu beteiligender Verbände eingeleitet und dabei auch vom ULD eine Stellungnahme erbeten. Der Gesetzentwurf ist abrufbar unter:

www.landtag.ltsh.de/infothek/wahl19/unterrichtungen/00100/unterrichtung-19-00184.pdf

Kurzlink: *https://uldsh.de/tb38-451*

Landeskrankenhausgesetz

Ziel des Gesetzes ist es, eine qualitativ hochwertige, patienten- und bedarfsgerechte Versorgung der Bevölkerung des Landes Schleswig-Holstein mit leistungsfähigen, wirtschaftlich gesicherten, sparsam und eigenverantwortlich wirtschaftenden Krankenhäusern sicherzustellen und zu sozial tragbaren Entgelten beizutragen, eine vernetzte kooperative und sektorübergreifende Gesundheitsversorgung zu ermöglichen und die Patientenrechte zu stärken.

In den §§ 35-40 des Gesetzentwurfs wurden nähere Regelungen zum Bereich des Patientendatenschutzes eingefügt. Im Rahmen der Erarbeitung des Entwurfs wurde das ULD beratend beteiligt. Dabei konnten Hinweise Berücksichtigung finden, die sich etwa auf folgende Punkte bezogen:

- Von Bedeutung war, dass vom Landeskrankenhausgesetz sowohl Einrichtungen in öffentlicher als auch in privater Trägerschaft erfasst werden und damit neben der DSGVO auch Regelungen des Bundesdatenschutzgesetzes (BDSG) und des Landesdatenschutzgesetzes (LDSG) zu beachten sind.
- Bezüglich der Datenverarbeitung durch Auftragsverarbeiter bestehen vorrangige Bestimmungen in der DSGVO.
- Werden Patientendaten zu Forschungszwecken verarbeitet, so bestehen je nach Einordnung der Trägerschaft der Einrichtung flankierende Bestimmungen in § 13 LDSG und § 27 BDSG.
- Bezüglich der Auskunftsrechte der Patienten in Bezug auf ihre personenbezogenen Daten gilt ergänzend Artikel 15 DSGVO, wobei auch die Bereitstellung kostenfreier Kopien der Daten in Betracht kommt.

Zu erörtern bleibt noch, dass Einwilligungen zur Verarbeitung personenbezogener Daten nach Artikel 7 DSGVO keiner Schriftform bedürfen, um wirksam zu sein. Infolge der Rechenschaftspflicht der Verantwortlichen, die auch die Obliegenheit betrifft, nachweisen zu können, dass die Verarbeitung auf Basis einer Rechtsgrundlage (z. B. einer Einwilligung) erfolgte, sollte die Einwilligung aber schriftlich dokumentiert werden.

Ferner sieht der Gesetzentwurf vor, dass eine Verarbeitung von Patientendaten auch dann zulässig sein soll, soweit dies zur Überprüfung der Tätigkeit der Mitarbeiterinnen und Mitarbeiter des Krankenhauses erforderlich ist. Hierbei sind insbesondere im Bereich der privaten Träger vorrangige Bestimmungen in § 26 BDSG zu beachten, was nach Auffassung des ULD noch nicht hinreichend zum Ausdruck kommt.

Schließlich sollten die Regelungen im Gesetzentwurf, die Bezug zu einer Anonymisierung oder einer Pseudonymisierung nehmen, kritisch durchgeschaut werden, da im Text begriffliche Unklarheiten durchscheinen: Beispielsweise spielt es eine Rolle, dass es sich bei pseudonymisierten Daten – anders als bei anonymen oder anonymisierten Daten – um personenbezogene Daten handelt, für deren Verarbeitung eine Rechtsgrundlage erforderlich ist (zu Pseudonymisierung siehe Tz. 10.1).

Was ist zu tun?

Der Gesetzgeber sollte die gegebenen Hinweise prüfen und gegebenenfalls durch Änderungen im Text des Landeskrankenhausgesetzes umsetzen.

4.5.2 Anhörung zum PsychHG-Entwurf

Das federführende Ministerium für Soziales, Gesundheit, Jugend, Familie und Senioren Schleswig-Holstein hat den Landtag über den Entwurf eines Gesetzes zur Hilfe und Unterbringung von Menschen mit Hilfebedarf in Folge psychischer Störungen (PsychHG) informiert und eine Anhörung durchgeführt. Der Gesetzentwurf ist abrufbar unter:

https://www.landtag.ltsh.de/infothek/wahl19/unterrichtungen/00100/unterrichtung-19-00166.pdf

Kurzlink: *https://uldsh.de/tb38-452*

PsychHG

Das Gesetz soll die Gewährung von Hilfen für Menschen regeln, die aufgrund einer psychischen Störung hilfsbedürftig sind, sowie die Durchführung von Schutzmaßnahmen und Unterbringung zur Abwendung von Eigen- oder Fremdgefährdungen aufgrund einer psychischen Störung.

In den §§ 31-38 des Gesetzentwurfs wurden nähere Regelungen zum Bereich Verschwiegenheitspflichten, Datenschutz und Dokumentation getroffen. Beabsichtigt war damit auch eine Anpassung an die Vorgaben der DSGVO. Das ULD hat zu dem Gesetzentwurf Stellung genommen und insbesondere folgende Punkte benannt:

- Für öffentliche Stellen wird im Entwurf etwa die Geltung des Bundesdatenschutzgesetzes (BDSG) normiert. Ausgehend von § 2 Abs. 4 Landesdatenschutzgesetz (LDSG) findet das BDSG für öffentliche Stellen Anwendung, soweit diese am Wettbewerb teilnehmen und personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten. Die Kreise und kreisfreien Städte haben nach dem Entwurf die Befugnis, natürliche und juristische Personen des Privatrechts mit Aufgaben der öffentlichen Verwaltung beim Vollzug der Unterbringungsanordnung und der Unterbringung zu beleihen. Die Beliehenen sind öffentliche Stellen im

Sinne von § 2 Abs. 1 LDSG. Es wird im Entwurf zum PsychHG nicht ausgeführt, mit welcher Begründung sich die Beliehenen bei der Wahrnehmung von Aufgaben zum Vollzug von Unterbringungsanordnungen und der Unterbringung im Wettbewerb mit anderen Stellen befinden sollen. Diese Aufgaben im Rahmen einer Beleihung sind nicht vergleichbar mit dem Zugang zu Leistungen einer Patientenversorgung, die von öffentlichen wie auch von privaten Trägern angeboten wird und bei welcher eine Wettbewerbssituation angenommen werden kann. Die Anwendung des BDSG ist daher nicht klar nachvollziehbar.

- Weiterhin berücksichtigt der Entwurf nach Auffassung des ULD bisher nicht hinreichend, dass in der DSGVO vorrangige Bestimmungen zur Zulässigkeit der Verarbeitung sensibler Datenkategorien wie Gesundheitsdaten existieren, wodurch für landesrechtliche Regelungen nur ein eingeschränkter Raum für zusätzliche landesrechtliche Bestimmungen verbleibt.
- Die Löschfristen für die verarbeiteten Gesundheitsdaten werden im PsychHG nicht erläutert. In der Gesetzesbegründung wird bisher ausschließlich der Gesetzestext wiederholt. Es bleibt etwa offen, aus welchem Grund anstelle der für Behandlungen üblichen zehnjährigen Aufbewahrung von Patientenunterlagen für Krankenhäuser nun eine 15-jährige Frist gewählt wurde. Es sollte zumindest in der Gesetzesbegründung deutlich werden, welche Erwägungen hierfür Anlass gaben.
- Die Einräumung eines Wahlrechts für den Arzt, der betroffenen Person die Auskunft zu den zur Person gespeicherten Daten auch mündlich erteilen zu können, widerspricht der DSGVO. Art. 15 Abs. 3 DSGVO räumt der betroffenen Person das Recht ein, eine Kopie der Unterlagen zu verlangen.

Was ist zu tun?

Die Aufnahme datenschutzrechtlicher Konkretisierungen in einem neuen PsychHG wird vom ULD unterstützt. Bei der Neufassung des Gesetzes sollten die mitgeteilten Anregungen Berücksichtigung finden. Europarechtliche Vorgaben nach der DSGVO müssen eingehalten werden.

4.5.3 Kein Beschlagnahmeverbot, wenn Arzt nicht Zeuge, sondern Beschuldigter ist

Die Kriminalpolizei will vor Ort auf Patientenunterlagen einer Klinik zugreifen. Es geht um ein Strafverfahren gegen eine Person, die sich als Ärztin ausgegeben und offenbar in der Klinik gearbeitet hat.

Wir haben auf Folgendes hingewiesen: Ärzte sind zur Verweigerung des Zeugnisses im Strafverfahren nach § 53 Abs. 1 Nr. 3 Strafprozessordnung (StPO) berechtigt. Hinsichtlich der Beschlagnahme gilt § 97 Abs. 1 StPO.

Aber: Das Beschlagnahmeverbot gilt nach herrschender Meinung nur im Strafverfahren gegen den Patienten, nicht jedoch bei einem Strafverfahren gegen den Arzt selbst.

Dies bedeutet, dass nach unserer Einschätzung die ärztliche Schweigepflicht dann einer Beschlagnahme der Patientenunterlagen nicht entgegensteht, wenn sich das Ermittlungsverfahren gegen den Arzt als Beschuldigten richtet – eine Einschätzung, die auch vom Bundesverfassungsgericht vertreten wird.

§ 97 Abs. 1 StPO

Der Beschlagnahme unterliegen nicht:

1. schriftliche Mitteilungen zwischen dem Beschuldigten und den Personen, die nach § 52 oder § 53 Abs. 1 Satz 1 Nr. 1 bis 3b das Zeugnis verweigern dürfen;

2. Aufzeichnungen, welche die in § 53 Abs. 1 Satz 1 Nr. 1 bis 3b Genannten über die ihnen vom Beschuldigten anvertrauten Mitteilungen oder über andere Umstände gemacht haben, auf die sich das Zeugnisverweigerungsrecht erstreckt;

3. andere Gegenstände einschließlich der ärztlichen Untersuchungsbefunde, auf die sich das Zeugnisverweigerungsrecht der in § 52 oder § 53 Abs. 1 Satz 1 Nr. 1 bis 3b Genannten erstreckt.

In der Rechtsliteratur finden sich Ausführungen dahin gehend, dass „die strafprozessualen Aufklärungsmöglichkeiten einer Staatsanwaltschaft im Interesse des Schutzes des Patienten gegen eine unbegrenzte Weitergabe seiner persönlichen Daten insofern eingeschränkt sind, als Verletzungen des Geheimnisschutzes nur soweit zwingend erforderlich vorgenommen werden dürfen und jeder übermäßige Eingriff in diesen sensiblen Bereich unzulässig ist". „Das Wissen um die grundsätzlich der ärztlichen Schweigepflicht unterfallenden Tatsachen" muss „auf den Kreis der unmittelbar am Verfahren Beteiligten" begrenzt bleiben.

Dies bedeutet praktisch:

- Einsichtsmöglichkeit in die Unterlagen nur für die unmittelbar mit den Ermittlungen befassten Beamten,
- Sicherung vor Missbrauch,
- Ausschluss der Öffentlichkeit in der mündlichen Verhandlung vor Gericht gemäß § 172 Nr. 2 Gerichtsverfassungsgesetz (GVG) bei Erörterung ärztlicher Aufzeichnungen.
- Unter Abwägung der berechtigten Belange des Betroffenen und des öffentlichen Interesses an einer wirksamen Strafverfolgung darf die Staatsanwaltschaft Sachverständige, auch aus dem Bereich der geschädigten Krankenkasse, zu Durchsuchungen hinzuziehen.

Soweit es also um ein Strafverfahren gegen den Arzt selbst geht, ist die Beschlagnahme nicht ausgeschlossen.

4.5.4 Keine Behandlung, wenn eine Patientin die Datenschutzerklärung nicht unterschreibt?

Seit dem 25. Mai 2018 unterliegen Verantwortliche einer Informationspflicht bei der Erhebung von personenbezogenen Daten bei der betroffenen Person. Somit sind auch Arzt- und Zahnarztpraxen in der Pflicht, neuen Patientinnen und Patienten anlässlich des ersten Kontakts Informationen über die beabsichtigte Verarbeitung der Patientendaten zu geben.

Zu den in Artikel 13 DSGVO benannten Informationen gehören neben dem Namen und den Kontaktdaten der Praxis und gegebenenfalls Kontaktdaten der oder des betrieblichen Datenschutzbeauftragten insbesondere Angaben über die Zwecke und Rechtsgrundlage der beabsichtigten Datenverarbeitung, über mögliche Empfänger der Patientendaten, die Dauer der Datenspeicherung, bestehende Patientenrechte wie z. B. Auskunftsansprüche und darüber, welche Beschwerderechte die Patientin oder der Patient bei welcher Aufsichtsbehörde hat.

Viele Praxen verwenden eine schriftliche Datenschutzerklärung. Patientinnen und Patienten werden bei ihrer ersten Vorsprache auf diese Datenschutzerklärung hingewiesen bzw. ihnen

wird ein Exemplar ausgehändigt. Allerdings müssen sie nicht zwingend diese Datenschutzerklärung unterschreiben.

Der Verantwortliche bzw. die Praxis muss im Rahmen der allgemeinen Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) nachweisen können, dass diese Informationspflicht beachtet wurde, also neuen Patientinnen und Patienten die zuvor genannten Informationen gegeben wurden. Es bestehen daher keine Einwände, wenn sich Praxen von ihren Patientinnen und Patienten den Erhalt der Datenschutzerklärung schriftlich bestätigen lassen. Alternativ kann auch ein Hinweis auf die Datenschutzerklärung im Anamnesebogen ein ausreichender Nachweis sein, wenn sichergestellt ist, dass jede neue Patientin und jeder neue Patient diesen Anamnesebogen selbst ausfüllt. Auch eine entsprechende Verfahrensvorgabe in der verwendeten Arztpraxissoftware (als auszufüllendes Feld) wird von Aufsichtsbehörden als Nachweis akzeptiert.

Die DSGVO fordert nicht, dass sich Patientinnen und Patienten mit den in der Datenschutzerklärung aufgeführten Informationen einverstanden erklären. Dies würde auch wenig Sinn ergeben. Wie bzw. wieso sollte sich eine Patientin oder ein Patient z. B. mit dem Namen der behandelnden Person einverstanden erklären? Auch sieht die DSGVO nicht vor, dass eine medizinische Behandlung einer kranken Person unterbleiben muss, nur weil sie die Datenschutzerklärung nicht unterschreibt. Es ist die freie Entscheidung der Patientin und des Patienten, das Informationsangebot der Praxis anzunehmen oder zu verweigern. Die Praxis muss lediglich nachweisen können, dass sie ihren Patientinnen und Patienten die Informationen angeboten hat.

Hilfreiche Ausführungen dazu gibt es in der Broschüre „Informationspflichten" unserer Praxis-Reihe „Datenschutzbestimmungen praktisch umsetzen":

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

Kurzlink: *https://uldsh.de/tb38-454*

Noch mehr Hilfestellung und ein Muster einer Kurzinformation („Datenschutz-Steckbrief", 37. TB, Tz. 6.1.4) gibt es unter dem folgenden Link:

https://www.datenschutzzentrum.de/dokumentation/

4.5.5 Mehrere Kubikmeter Patientenunterlagen in der Innenstadt frei zugänglich

Im Januar 2019 schilderte ein aufmerksamer Bürger, dass mitten in Kiel in einer belebten Straße ein großer Container mit Patientenunterlagen stehe. Der Container sei offen, frei zugänglich und niemand sei da, um aufzupassen. Wir konnten kaum glauben, was uns berichtet wurde. Selbstverständlich wurde sofort vor Ort eine Prüfung durchgeführt.

Unsere Prüfung bestätigte die Angaben. Der unverschlossene Container (6 m^3!) war randvoll mit unzähligen Aktenordnern mit sensibelsten Patientendaten wie histologischen bzw. pathologischen Untersuchungsergebnissen eines Labors gefüllt. Niemand bewachte den Container. Jeder hätte sich an den Patientenunterlagen bedienen können.

Noch vor Ort wurde die Geschäftsführung des Labors aufgesucht und mit den Prüffeststellungen konfrontiert. Die Antwort: Man habe einen externen Dienstleister damit beauftragt, Patientenunterlagen, die nicht mehr benötigt werden, auszusortieren und zu vernichten. Die Beschäftigten des Dienstleisters hierbei zu beaufsichtigen habe man nicht für notwendig gehalten. Da die Beschäftigten des Dienstleisters bereits Feierabend hatten, wurde ihr Chef telefonisch zum Tatort gebeten. Dieser erklärte den offenen Container damit, dass seine Beschäftigten kein Schloss gehabt hätten, um diesen zu verschließen. Am nächsten Morgen sollte der Container zum eigentlichen Aktenvernichter gebracht werden.

Die Prüffeststellungen sind ein gutes Beispiel dafür, was passiert, wenn sich jeder auf den anderen verlässt und keiner die Verantwortung übernehmen will. Der Geschäftsführer des Labors gab an, sich schon gewundert zu haben, dass der Container mit den Patientenunterlagen offen auf der Straße stand. Seine Mitarbeiterin erklärte, nichts von schriftlichen Vereinbarungen mit dem beauftragten Dienstleister zu wissen, und eine andere Mitarbeiterin sagte, nicht die Zeit gehabt zu haben, um nach dem Rechten zu schauen. Die Beschäftigten des Dienstleisters waren ohnehin schon zu Hause, und ihr Chef war ahnungslos.

Datenschutzrechtlich verantwortlich war in diesem Fall das Labor, das es versäumt hatte, eine ordnungsgemäße Entsorgung der personenbezogenen Daten zu gewährleisten. Gegen den Verantwortlichen wurde ein Ordnungswidrigkeitenverfahren eingeleitet. Es droht eine empfindliche Geldbuße.

Weitere Hinweise zu den Anforderungen an eine Auftragsverarbeitung finden sich in der Broschüre „Mustervereinbarung für einen Vertrag zur Auftragsverarbeitung" unserer Praxis-Reihe „Datenschutzbestimmungen praktisch umsetzen":

https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-3-ADV.pdf

Kurzlink: *https://uldsh.de/tb38-455*

Was ist zu tun?

Wird ein externer Dienstleister mit der Vernichtung von Patientenunterlagen beauftragt, so muss der Verantwortliche als Auftraggeber in einem schriftlichen Vertrag detaillierte Vorgaben zur beabsichtigten Datenverarbeitung festlegen. Artikel 28 DSGVO regelt die Rechte und Pflichten von Auftraggebern und Auftragnehmern sowie die Vertragsinhalte. Auftragnehmer von Arztpraxen sind auf das Datengeheimnis zu verpflichten und unterliegen damit regelhaft – wie die Ärztin oder der Arzt selbst – der ärztlichen Schweigepflicht (§ 203 Strafgesetzbuch (StGB)).

4.5.6 Gesundheitsdaten aus der Tüte – wenn die Nachbarn die gelieferten Medikamente sehen

Ein Beispiel aus der Rubrik: „Gut gemeint, aber schlecht gemacht."

Eine Apotheke bietet ihren Kundinnen und Kunden an, Medikamente direkt nach Hause zu liefern. Hierfür hat die Apotheke extra einen Boten angestellt, der das Medikament an der eigenen Haustür übergibt. Vorausgesetzt die Kundin oder der Kunde ist da, sonst wird das Medikament eventuell bei den Nachbarn abgegeben. Die Medikamente werden in hübschen, aber leider nicht blickdichten Tüten transportiert – alles im Blick der Nachbarschaft.

Apotheken bzw. die dort tätigen Personen müssen nicht nur die Vorschriften der DSGVO und des BDSG, sondern zudem besondere berufsrechtliche Vorschriften, die sich insbesondere aus den Berufsordnungen der jeweiligen Apothekerkammern ergeben, beachten. Apothekerinnen und Apotheker sowie deren berufsmäßig tätige Gehilfen unterliegen der ärztlichen Schweigepflicht (§ 203 StGB). Auch bei dem Transport und der Lieferung von Medikamenten muss sichergestellt werden, dass Unbefugte keine Kenntnis von personenbezogenen Daten erhalten. Schließlich handelt es sich um Gesundheitsdaten, also um besondere Kategorien personenbezogener Daten mit einem hohen Schutzbedarf.

Die Apotheke hat zugesichert, durch schriftliche Vorgaben für die Boten zu gewährleisten, dass Medikamentenlieferungen zukünftig nur noch

an Befugte übergeben werden (organisatorische Maßnahme). Zudem sollen für den Transport der Medikamentenlieferungen blickdichte Verpackungen verwendet werden (technische Maßnahme).

4.5.7 Änderung des Maßregelvollzugsgesetzes: Auskunftsrecht soll beschnitten werden?

Das Ministerium für Soziales, Gesundheit, Jugend, Familie und Senioren hat im Berichtszeitraum einen Entwurf zur Änderung des Maßregelvollzugsgesetzes erarbeitet. Damit soll u. a. die EU-Richtlinie 2016/680 für den Datenschutz im Bereich der Strafverfolgung umgesetzt werden. Das ULD hat zu dem Entwurf Stellung genommen.

Wir haben zu einer Reihe von Regelungen Nachfragen gestellt oder Änderungen vorgeschlagen. Der aus unserer Sicht große Änderungsbedarf mag sich daraus erklären, dass das Maßregelvollzugsgesetz aus dem Jahr 2000 stammt und seit 2008 nicht mehr nennenswert geändert wurde. Neuere Entwicklungen im Landesrecht, insbesondere durch das Justizvollzugsdatenschutzgesetz aus dem Jahr 2016, sind somit bislang im Maßregelvollzugsgesetz nicht berücksichtigt. Dies betrifft z. B. die Regelungen zur Videoüberwachung. Hier ist mit dem Justizvollzugsdatenschutzgesetz ein guter Standard etabliert worden, der, soweit passend, auch auf den Maßregelvollzug übertragen werden sollte.

Bei der Regelung des Auskunftsanspruchs der betroffenen Personen haben wir erhebliche Bedenken geäußert, ob damit die Vorgaben der EU-Richtlinie ausreichend umgesetzt werden. Der Umfang der Informationen, die der betroffenen Person mitzuteilen sind, ist im Entwurf deutlich knapper vorgesehen, als die Richtlinie es verlangt. Außerdem geht der Entwurf beim Auskunftsanspruch über die in der EU-Richtlinie vorgesehenen Ausnahmen hinaus. Das bedeutet: Der Entwurf zur Änderung des Maßregelvollzugsgesetzes beschneidet den Auskunftsanspruch doppelt – das wäre unserer Ansicht nach europarechtswidrig.

Was ist zu tun?

Der Entwurf muss in einigen Punkten geändert werden, um dem EU-Recht sowie den Anforderungen des Datenschutzes zu entsprechen. Das Ministerium muss hier nachbessern.

4.5.8 Diebstahl von (Patienten-)Unterlagen aus dem Auto – was tun?

Im letzten Jahr wurde uns wiederholt gemeldet, dass dienstliche, aber auch private Fahrzeuge aufgebrochen und dort aufbewahrte (Patienten-)Unterlagen gestohlen wurden. Die Diebe entwendeten handschriftliche Notizen der Beschäftigten, Abrechnungsunterlagen, vollständige Akten und in einem Fall sogar ein Notebook mit sensiblen Daten.

Die Verantwortlichen müssen in diesen Fällen ihrer Meldepflicht bei der Verletzung des Schutzes personenbezogener Daten nach Artikel 33 DSGVO nachkommen und prüfen, ob die betroffenen Personen zu benachrichtigen sind.

Im Zentrum steht die Frage: Wie kam es zu dem Diebstahl, und wie hätte dieser verhindert

werden können? Zu klären sind die folgenden Punkte:

- Wann und wo wurde das Auto geöffnet? Wurde es aufgebrochen?
- Welche konventionellen oder elektronischen Datenträger mit personenbezogenen Daten wurden entwendet?
- Welche Daten und wie viele Personen sind von dieser Datenschutzverletzung betroffen?
- Wurden von dem Verantwortlichen für die Beschäftigten (schriftliche) Vorgaben für den Transport derartiger Datenträger erlassen? Wurden diese beachtet?
- Ist z. B. festgelegt, dass grundsätzlich nur Datenträger verwendet werden dürfen, die vom Verantwortlichen zur Verfügung gestellt werden? Die Nutzung privater Datenträger sollte unterbleiben und darf auf keinen Fall ohne Wissen und Zustimmung des Verantwortlichen erfolgen.
- Ist geregelt, ob der Beschäftigte sein privates Auto nutzen darf?
- Wird für den Transport der Papierunterlagen ein blickdichtes Behältnis (z. B. eine Aktentasche) verwendet?
- Erfolgt eine ausreichende Verschlüsselung der Daten, wenn mobile elektronische Geräte verwendet werden (Notebook, Smartphone, USB-Stick …)?
- Wo sind die Datenträger im Auto zu verwahren (Kofferraum oder Rücksitzbank)?
- Wie ist mit den Datenträgern zu verfahren, wenn der Beschäftigte das Auto z. B. für eine Pause oder für das eigentliche Dienstgeschäft verlässt?
- Wie ist mit den Datenträgern nach Dienstschluss zu verfahren? Dürfen die Datenträger z. B. über Nacht oder am Wochenende im Auto verbleiben?
- Wurde eine Strafanzeige gestellt?

Für die Meldung einer Verletzung des Schutzes personenbezogener Daten ist unter dem folgenden Link ein Meldeformular abrufbar:

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

Was ist zu tun?

Werden konventionelle oder elektronische Datenträger mit personenbezogenen Daten in einem Auto transportiert, sind vom Verantwortlichen geeignete technische und organisatorische Maßnahmen zum Schutz dieser Daten zu treffen.

4.5.9 Übermittlung von Patientendaten an die private Krankenversicherung ohne Einwilligung?

Für gesetzlich krankenversicherte Patientinnen und Patienten sehen die Vorschriften des Sozialgesetzbuches V (SGB V) detaillierte Regelungen vor, wie und auch mit wem die Ärztin oder der Arzt die Leistungen abrechnen muss. Regelhaft wird bei ambulanten Heilbehandlungen die Kassenärztliche bzw. die Kassenzahnärztliche Vereinigung und bei stationären Heilbehandlungen die jeweilige gesetzliche Krankenkasse erster Ansprechpartner sein. Anders hingegen, wenn die Patientin oder der Patient bei einer privaten Krankenversicherung (PKV) versichert ist. In diesem Fall ist die versicherte Person die eigentliche Empfängerin der Rechnung. Sie kann sich frei entscheiden, ob sie die Rechnung bei ihrer PKV einreicht.

Bei einer Krankenhausbehandlung entstehen schnell hohe Kosten, die viele Patientinnen und Patienten nicht aus eigener Tasche zahlen

möchten oder können. Die Kosten übernimmt im vereinbarten Rahmen die PKV. Damit die versicherte Person den Rechnungsbetrag nicht vorstrecken muss, kann es ratsam sein, dass sie sich mit einer direkten Abrechnung des Krankenhauses mit ihrer PKV einverstanden erklärt.

Krankenhäuser dürfen aber erst dann ihre Rechnungen an die PKV der Patientin oder des Patienten schicken, wenn eine (schriftliche) Einwilligung vorliegt.

Hinweise und Muster für die datenschutzgerechte Gestaltung derartiger Einwilligungserklärungen (Schweigepflichtentbindungserklärung) sind unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/medizin-soziales/

4.5.10 Sensible Daten unverschlüsselt auf USB-Sticks – immer noch!

So klein ein USB-Stick auch ist, so groß können doch die darauf gespeicherten Datenmengen sein. 2017 wurde in einer schleswig-holsteinischen Gemeinschaftspraxis für Neurologie, Psychiatrie, Psychosomatik und Psychotherapie eingebrochen. Gestohlen wurden u. a. die Datenträger mit der Datensicherung. Auf den unverschlüsselten USB-Sticks waren die Daten von weit über 40.000 Patienten der letzten 20 Jahre gespeichert. Wir forderten alle Arztpraxen auf, ihre digitalen Sicherungskopien von Patientendaten zu verschlüsseln (36. TB, Tz. 4.6.3).

Diese Forderung wird anscheinend nicht von jeder Arztpraxis beachtet. Auch im letzten Jahr erhielten wir vergleichbare Meldungen derartiger Verletzungen des Schutzes personenbezogener Daten.

In einem Fall ist einem Arzt ein unverschlüsselter USB-Stick mit Patientendaten „versehentlich abhandengekommen". Er wird den USB-Stick irgendwann irgendwo verloren haben. In anderen Fällen wurde uns geschildert, dass unverschlüsselte USB-Sticks mit Patientendaten auf dem Postweg verloren gegangen sind. Die eigentlichen Empfänger erhielten geöffnete Briefumschläge ohne Inhalt.

Gelangen solche USB-Sticks in falsche Hände, besteht ein hohes Risiko, dass die sensiblen Patientendaten der betroffenen Personen gesichtet oder verwendet werden. Dabei ist Verschlüsselung digitaler Daten kein Hexenwerk – viele Softwaretools garantieren einen guten Schutz gegen unberechtigte Zugriffe.

Was ist zu tun?

Krankenhäuser und Kliniken, Arzt- und Zahnarztpraxen, Pflegeeinrichtungen und Pflegedienste, Apotheken und alle weiteren vergleichbaren Einrichtungen, die besondere Kategorien personenbezogener Daten (Patientendaten) verarbeiten, müssen diese Daten bei einer digitalen Speicherung grundsätzlich verschlüsseln. Dies gilt insbesondere bei der Verwendung mobiler Datenträger wie USB-Sticks, Notebook-Festplatten oder Speichermedien bei Tablets.

4.5.11 Achtung: Abholung und Entsorgung von Röntgenbildern durch eine Fake-Firma!

Wohin mit den alten Röntgenbildern, wenn die Aufbewahrungsfristen abgelaufen sind? Na klar, die Patientenunterlagen müssen vernichtet werden. Gut, dass es Firmen gibt, die eine sichere Vernichtung anbieten.

Entsprechend war eine Arztpraxis aus Schleswig-Holstein hocherfreut, als man von einer Firma Drehkopf Recycling GmbH, angeblich aus München (nicht zu verwechseln mit der Firma Drekopf Recyclingzentrum Velbert GmbH!), per „Geschäftsrundschreiben" (Fax) das Angebot erhielt, die Röntgenbilder abzuholen und hierfür sogar bis zu 2 € für jedes Kilogramm zu zahlen. Schließlich enthalten Röntgenbilder Silber. Eine kurze Auftragsbestätigung und wenig später kam auch schon jemand und holte die Röntgenbilder ab. Es gab sogar eine schriftliche „Datenträgervernichtungsbestätigung".

Wenig später beschlich die Arztpraxis ein ungutes Gefühl. War man auf einen Hochstapler, einen Betrüger reingefallen? Auf der Webseite dieser Firma wurde damit geworben, dass man rund 80.000 Kundinnen und Kunden in Deutschland und Polen habe. In Polen? Anders als beim Angebot auf der Webseite wurde hier ein Ort in Polen als Unternehmenssitz angegeben. Die Arztpraxis stellte eine Strafanzeige und meldete uns eine Verletzung des Schutzes personenbezogener Daten nach Artikel 33 DSGVO.

Unabhängig davon, zu welchen Ergebnissen die Polizei bei ihren Ermittlungen kommen wird, mussten wir der Arztpraxis einen erheblichen datenschutzrechtlichen Verstoß vorwerfen, für den sie ganz allein die Verantwortung trägt.

Arztpraxen dürfen einen externen Dienstleister mit der Abholung und Vernichtung von Patientenunterlagen beauftragen. Dieser muss nicht zwingend seinen Unternehmenssitz in Deutschland haben. Jedoch hat der Betreiber der Arztpraxis als Verantwortlicher eine Sorgfaltspflicht bei der Auswahl eines zuverlässigen Dienstleisters. Ohne weitere Prüfung auf ein Angebot einer unbekannten Firma einzugehen ist zu naiv. Besonders negativ ist aber, dass entgegen der Vorgabe des Artikels 28 DSGVO kein schriftlicher Vertrag über diese Auftragsverarbeitung abgeschlossen wurde. Es wurden keine Vereinbarungen über den Prozess der Abholung, den Transport und die Vernichtung der Röntgenbilder getroffen. Weder wurden Pflichten des Auftragnehmers noch Prüfrechte des Auftraggebers festgelegt. Die Arztpraxis war gar nicht in der Lage, ihre Kontroll- und Aufsichtspflichten wahrzunehmen.

Wir mussten gegenüber der Arztpraxis von unseren Abhilfebefugnissen Gebrauch machen. Es wurde eine formelle Warnung ausgesprochen und zudem die Stelle aufgefordert zu überprüfen, ob bei der Beauftragung anderer Auftragsverarbeiter die rechtlichen Anforderungen ausreichend beachtet wurden.

Näheres zu den Anforderungen an eine Auftragsverarbeitung gibt es in der Broschüre „Mustervereinbarung für einen Vertrag zur Auftragsverarbeitung" unserer Praxis-Reihe „Datenschutzbestimmungen praktisch umsetzen":

https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-3-ADV.pdf

Kurzlink: *https://uldsh.de/tb38-4511*

Was ist zu tun?

Verantwortliche, die Dienstleister einbinden, müssen die datenschutzrechtlichen Anforderungen berücksichtigen. Für eine Auftragsverarbeitung ist dabei Artikel 28 DSGVO umzusetzen. Bei Arztpraxen sind außerdem die Besonderheiten der ärztlichen Schweigepflicht (§ 203 StGB) zu beachten.

4.5.12 Patientenbriefe aus dem Briefkasten gestohlen

Ein Krankenhaus meldete uns, dass vermutlich Kinder Patientenbriefe aus einem Briefkasten der Klinik entwendet und in einen nahe liegenden Bach geworfen hätten. Man war nicht sicher, ob alle Briefe gefunden wurden. Auch bei einem Unternehmen für Behinderten- und Krankentransport wurden Abrechnungsunterlagen aus dem Briefkasten gestohlen. Diese Briefe wurden nicht wiedergefunden.

Verantwortliche, die besondere Kategorien von Daten verarbeiten, zu denen Patientendaten gehören, müssen alle geeigneten technischen und organisatorischen Maßnahmen treffen, die eine angemessene Sicherheit der Daten gewährleisten, einschließlich des Schutzes vor unbefugter Verarbeitung, unbeabsichtigtem Verlust und unbeabsichtigter Zerstörung. Nur so lässt sich verhindern, dass Unbefugte Kenntnis von den Patientendaten erhalten können und zudem sichergestellt wird, dass der Grundsatz der Integrität und Vertraulichkeit der Verarbeitung personenbezogener Daten ausreichend beachtet wird (Artikel 5 DSGVO).

Nicht jeder Briefkasten eignet sich, um Unterlagen mit sensiblen Patientendaten entgegenzunehmen. Es sollte ein Briefkasten mit einem ausreichenden Diebstahlschutz verwendet werden. Briefkästen mit einer sogenannten Schleusentechnik können verhindern, dass Langfinger eine Chance haben. Aber auch organisatorische Maßnahmen müssen getroffen werden. Ein Briefkasten sollte regelmäßig – wenn erforderlich sogar mehrmals täglich – geleert werden. Er darf nicht überquellen. Für den Fall, dass der für die Post zuständige Beschäftigte mal im Urlaub weilt oder erkrankt, sind Vertretungsregelungen zu treffen.

Die jeweilige Stelle muss dafür Sorge tragen, dass das Verfahren für die Postzustellung und die Vorgaben an den Briefkasten datenschutzkonform umgesetzt sind – dann lassen sich hoffentlich Datenpannen in diesem Bereich vermeiden.

4.5.13 Unbefugter Zugriff von Mitarbeitern auf Patientendaten (von Kollegen)

Gelegenheit macht Diebe. Und manchmal ist der Kollege der (Daten-)Dieb.

Im letzten Jahr wurden uns einige Fälle gemeldet, in denen Beschäftigte von Kliniken auf Patientendaten von Kolleginnen oder Kollegen zugegriffen haben, obwohl diese gar nicht in die Behandlung eingebunden waren. Oft ist es nur Neugier, manchmal steckt aber auch böse Absicht dahinter.

So wurde uns u. a. berichtet, dass eine Mitarbeiterin, die ihr Freiwilliges Soziales Jahr in einer Klinik ableistete, einen nicht gesicherten Computer nutzte, um Patientenunterlagen einer Kollegin zu fotografieren und in eine WhatsApp-Gruppe einzustellen. Sie drohte der Kollegin damit, diese bloßzustellen. Die Klinikleitung stellte die Mitarbeiterin mit sofortiger Wirkung von der Arbeit frei.

Allein im letzten Jahr mussten wir in drei großen Kliniken in Schleswig-Holstein feststellen, dass den dort tätigen Beschäftigten ein unbegrenzter Zugriff auf digitale Patientendaten eingeräumt wurde. Beschäftigte der Verwaltung, der Pflege und auch jede Ärztin und jeder Arzt konnten – ohne dass sie in die Behandlung eingebunden waren – die Patientenakten ihrer Vorgesetzten und der Kolleginnen und Kollegen lesen. Oft war es nur ehrliche Anteilnahme, die dazu verleitete, sich per Computer die Patientenakten von Kolleginnen oder Kollegen anzuschauen. Manchmal wurden die Informationen aber auch genutzt, um zu tratschen oder Mitarbeiterinnen und Mitarbeiter zu diffamieren. Betroffene beschwerten sich offiziell bei der Klinikleitung und auch bei uns.

Eine Kontrolle, ob Beschäftigte unbefugt auf die Patientenakte einer Kollegin oder eines Kolle-

gen zugegriffen haben, ist nur möglich, wenn eine Protokollierung nicht nur der schreibenden, sondern auch der lesenden Zugriffe erfolgt. Aber eine solche Protokollierung war nicht in allen Kliniken umgesetzt.

Im Rahmen unserer Abhilfebefugnisse wurden die Kliniken daher aufgefordert:

- zu prüfen, welche Beschäftigten zu welchem Zweck wann und in welchem Umfang Zugang zu den Daten welcher Patientinnen und Patienten haben müssen, und auf dieser Grundlage ein entsprechendes Berechtigungskonzept zu erstellen,
- befugte wie unbefugte lesende Zugriffe auf digitale Patientendaten zu protokollieren und
- in einem Protokollierungskonzept festzulegen, wie lange diese Protokolldaten aufzubewahren sind und wann und zu welchem Zweck sie von welchen Personen ausgewertet werden.

Das Fehlen eines ausreichenden Berechtigungskonzepts, die Vergabe von unbegrenzten Zugriffsmöglichkeiten auf digitale Patientendaten sowie das Fehlen einer Protokollierung und eines zugehörigen Konzepts wird regelhaft als datenschutzrechtlicher Verstoß gewertet und kann mit einer Geldbuße geahndet werden.

Detaillierte Hinweise zur Gestaltung eines Berechtigungs- bzw. Protokollierungskonzepts in einem Krankenhaus sind in der „OH KIS – Orientierungshilfe Krankenhausinformationssysteme“ der Datenschutzaufsichtsbehörden des Bundes und der Länder unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/artikel/1107-OH-KIS-Orientierungshilfe-Krankenhausinformationssysteme.html

Kurzlink: *https://uldsh.de/ohkis*

4.6 Kommunale Steuerverwaltung

Uns erreichen regelmäßig Beschwerden im Zusammenhang mit teils ausufernden behördlichen Ermittlungen zur Erhebung von Zweitwohnungssteuern. Die Befugnisse der Behörden haben sich jedoch auch unter Geltung der DSGVO nicht grundlegend geändert.

Aufgrund zahlreicher Nachfragen haben wir den bereits nach alter Rechtslage auf der Webseite des ULD veröffentlichten Artikel „Datenerhebung zur Festsetzung der Zweitwohnungssteuer“ an die neuen Fundstellen in der DSGVO angepasst. Der Artikel ist abrufbar unter:

https://www.datenschutzzentrum.de/artikel/1120-Datenerhebung-zur-Festsetzung-der-Zweitwohnungssteuer.html

Kurzlink: *https://uldsh.de/tb38-46*

05

KERNPUNKTE

Datenschutz für Mieterinnen und Mieter

Datenschutz beim Sport

Beschäftigtendatenschutz

Meldepflichtige Datenpannen

Neues zur Videoüberwachung

5 Datenschutz in der Wirtschaft

5.1 Keine Weitergabe von Mieterdaten an Wohnungslosenhilfe ohne Einwilligung

Vom Zentralverband der Deutschen Haus-, Wohnungs- und Grundeigentümer e. V. (Haus und Grund Deutschland) wurde das ULD gebeten, eine Einschätzung dazu abzugeben, ob Vermieter von Wohnraum personenbezogene Mieterdaten für Beratungszwecke und zur Stabilisierung der Mietverhältnisse an die Träger der Wohnungslosenhilfe übermitteln dürfen. Weiterhin wollte die anfragende Stelle wissen, welche konkreten Daten von einem solchen Datentransfer zulässigerweise erfasst würden und inwieweit diese Datenverarbeitung als Gegenstand einer notwendigen Leistung zur Erfüllung des Mietvertrags angesehen werden kann.

Eine Übermittlung personenbezogener Daten von Mietern an die Wohnungslosenhilfe bedarf einer Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO. Dabei wäre eine Verarbeitung der Mieterdaten etwa dann rechtmäßig, wenn diese für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen.

Zu prüfen ist in diesem Zusammenhang der bestehende Mietvertrag über die Nutzung von Wohnraum. Die Pflichten der Vermieter für Wohnraum ergeben sich bekanntlich aus den §§ 535 BGB. Insbesondere hat der Vermieter den Gebrauch der Mietsache während der Mietzeit zu gewähren. Hinzu kommen z. B. Reparatur- und Verkehrssicherungspflichten und verschiedene Verpflichtungen aufgrund anderer gesetzlicher Vorgaben, wie etwa die Mitwirkung bei einer Wohnungsgeberbestätigung nach den melderechtlichen Bestimmungen. Entsprechende Verpflichtungen aus dem Mietvertrag kann der Vermieter erfüllen. Eine Übermittlung von personenbezogenen Mieterdaten an die Wohnungslosenhilfe wäre hierfür nicht erforderlich. Dabei scheidet der Mietvertrag als Grundlage einer Datenweitergabe an die Wohnungslosenhilfe aus.

Zu prüfen war noch, inwieweit eine Übermittlung von personenbezogenen Mieterdaten an die Wohnungslosenhilfe zur Wahrung berechtigter Interessen des Vermieters oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten des betroffenen Mieters, die den Schutz personenbezogener Daten erfordern, überwiegen. Das berechtigte Interesse des Vermieters liegt insbesondere darin, dass der Mieter vereinbarungsgemäß seine Miete entrichtet und die Mietsache vertragsgemäß genutzt wird. Treten Unregelmäßigkeiten bei der Zahlung auf, so hat der Vermieter u. a. die Möglichkeit, mit dem Mieter Kontakt aufzunehmen und etwa darauf hinzuwirken, dass bei entsprechenden Anhaltspunkten aus Gesprächen mit dem Mieter auf Angebote einer Schuldnerberatung hingewiesen wird oder dass gemeinsam mit dem Mieter Anträge auf Direktzahlung der Miete an den Vermieter vorbereitet werden (§ 22 Abs. 7 Satz 1 SGB II).

Dem Vermieter kann der Umstand des Leistungsbezugs von der Wohnungslosenhilfe gegebenenfalls über die Vorlage eines Wohnberechtigungsscheins durch den Mietinteressenten bei Anmietung der Wohnung bekannt sein. Allerdings wird diese Kenntnis nicht in jedem Fall bestehen, und die Wohnungslosenhilfe wäre nach der Rechtsprechung des Bundessozialgerichts auch nicht ohne Einwilligung des Mieters befugt, den Umstand des Leistungsbezugs dem Vermieter mitzuteilen. Letzterer Umstand zeigt aber auch, dass die Interessen des Mieters Beachtung finden müssen, dass im Grundsatz gerade kein Datenaustausch zwischen Vermieter und der Wohnungslosenhilfe stattfindet. Der Mieter wäre nicht verpflichtet, eine entsprechende allgemeine Beratung wahrzunehmen, soweit hierfür keine gesetzliche Verpflichtung besteht.

Der Gesetzgeber hat die Entscheidung der Wohnungslosenhilfe über eine Direktzahlung an andere Empfangsberechtigte sehr restriktiv in

§ 22 Abs. 7 SGB II normiert. Demnach soll eine Direktzahlung vorgenommen werden, wenn vor allem Mietrückstände bestehen, die zu einer außerordentlichen Kündigung des Mietverhältnisses berechtigen. Bei diesem Beispiel erscheint es denkbar, dass bei Erfüllung der Voraussetzungen einer außerordentlichen Kündigung ein Hinweis des Vermieters an die Wohnungslosenhilfe zum Namen des Mieters, der Höhe der Mietrückstände und eine bevorstehende Kündigung ergeht – vorausgesetzt, der Vermieter hat zuvor überhaupt zulässigerweise davon Kenntnis, dass der Mieter Leistungen von der Wohnungslosenhilfe für die Unterkunft erhält. Der Mieter müsste aber vom Vermieter noch vor einer Datenweitergabe an die Wohnungslosenhilfe darüber belehrt werden, dass er dieser widersprechen kann (Art. 21 Abs. 1 DSGVO). Die Verpflichtung zur Unterrichtung über ein Widerspruchsrecht ergibt sich für den Vermieter aus Art. 21 Abs. 4 DSGVO. Der Mieter muss die Möglichkeit haben, sein Widerspruchsrecht noch vor einer Datenweitergabe ausüben zu können.

Die Angabe weiterer Daten wäre auf Basis von Art. 6 Abs. 1 Buchst. f DSGVO nicht zulässig. Die restriktive Handhabung einer Datenübermittlung wird auch dadurch untermauert, dass der Gesetzgeber nach § 22 Abs. 9 SGB II speziell für den Fall der Erhebung einer Räumungsklage auf Basis einer Kündigung des Mietverhältnisses wegen Mietrückständen eine Mitteilung des Gerichts zu bestimmten Angaben an die örtlichen Träger der Wohnungslosenhilfe legitimiert.

Im Übrigen wäre nur auf Grundlage einer Einwilligung eine Übermittlung bestimmter Mieterdaten an die Wohnungslosenhilfe zulässig, wobei diese Erklärung für den Mieter insbesondere freiwillig und frei widerrufbar sein muss. Gegen eine Freiwilligkeit würde bereits sprechen, wenn die Erklärung mit dem Abschluss des Mietvertrags verbunden wird, indem also nur bei Abgabe der Erklärung der Mietvertrag zustande kommt.

5.2 Einzelfälle

5.2.1 Missverständliche Werbeschreiben einer Tageszeitung

Den Zeitpunkt des Inkrafttretens der Datenschutz-Grundverordnung im Mai 2018 nahm ein schleswig-holsteinischer Zeitungsverlag zum Anlass, um seine Bestandskundinnen und -kunden postalisch zu kontaktieren. Dazu wurde den Bestandskundinnen und -kunden ein Anschreiben beigefügt, in dem der Werbecharakter nicht hinreichend zum Ausdruck kam. Neben dem Anschreiben war ein weiteres Schreiben als Anlage beigefügt, in dem diverse Werbeeinwilligungen für die telefonische Kontaktaufnahme und die Kontaktaufnahme per E-Mail zu Werbezwecken enthalten waren. Darüber hinaus wurden die Bestandskundinnen und -kunden dazu aufgefordert, ihre Kontaktdaten zu überprüfen oder zu ergänzen. Insbesondere sollte das Geburtsdatum angegeben werden. Die Datenerhebung wurde auch damit begründet, man wollte den Kundinnen und -kunden weiterhin gute Betreuung zukommen lassen.

In der beigefügten Anlage wurden neben der postalischen Anschrift weitere Daten abgefragt (E-Mail-Adresse, Telefonnummer und Geburtsdatum), wobei die Aufforderung, diese zu ergänzen, durch eine fett gedruckte Schrift hervorgehoben wurde. Dass per Ankreuzen eine Einwilligung zur Nutzung von Daten zu Werbezwecken gegeben werden sollte, wurde durch die Darstellung „**HÄKCHEN SETZEN**, dass wir Sie weiterhin informieren dürfen“ nahegelegt. Auf die Möglichkeit, die Einwilligung zu widerrufen, wurde hingewiesen.

Die Erhebung der Adressdaten begründete der Zeitungsverlag gegenüber dem ULD u. a. damit, man wolle die Richtigkeit der Daten prüfen. Die DSGVO sieht allerdings nicht vor, von Bestandskundinnen und -kunden Erklärungen hinsichtlich der Richtigkeit ihrer Adressdaten einzuholen. Eine Prüfung durch die Verantwortlichen

mit dem Ziel, den betroffenen Personen auf diese Weise die Wahrnehmung ihres Rechts auf Berichtigung zu ermöglichen, ist ebenfalls nicht vorgesehen.

Die Erhebung von Adress- und Geburtsdaten der Bestandskundinnen und -kunden erschloss sich dem ULD auch deshalb nicht, weil diese Angaben dem Zeitungsverlag bereits vorliegen mussten. Eine nachträgliche Erhebung von Geburtsdaten zu dem etwaigen Zweck, die Volljährigkeit der Bestandskundinnen und -kunden sicherzustellen, hätte hingegen das Versäumnis offenbart, bei Vertragsschluss zu prüfen, ob ein zivilrechtlich wirksamer Bezug einer Tageszeitung zustande kommt.

Die Erhebung von personenbezogenen Daten ist nur rechtmäßig, wenn hierzu eine Rechtsgrundlage gegeben ist. Eine solche Rechtsgrundlage kann eine Einwilligung darstellen. Zu deren Wirksamkeit bedarf es der Freiwilligkeit der Erklärung. Neben der zu Werbezwecken im Wege der Einwilligung anzugebenden Daten zu E-Mail-Adresse und Telefonnummer wurde auch die Abfrage des Geburtsdatums durch den Verantwortlichen als freiwillig bezeichnet – soweit bereits vorhanden unter dem Gesichtspunkt einer möglichen Berichtigung der Daten. Der Zweck der freiwilligen Erhebung bei Abschluss des Vertrags liege darin, Bestellungen von minderjährigen Kundinnen und -kunden nicht anzunehmen.

Hinweis zur Einwilligung

Eine Einwilligung ist jede freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung. Der Grundsatz einer Verarbeitung nach Treu und Glauben bedingt hier eine faire und transparente Darstellung der Zwecksetzung des Anschreibens und der Erhebung der Daten.

Dass die im vorliegenden Fall nachträgliche Erhebung freiwillig erfolgt, war jedoch weder durch das Anschreiben an die Kundinnen und -kunden noch durch die beigefügte Anlage deutlich geworden. Es war zudem nicht erkennbar, dass eine solche Datenerhebung erforderlich wäre, um bei sämtlichen Bestandskundinnen und -kunden nachträglich die Volljährigkeit als Nachweis für die Abgabe einer wirksamen Willenserklärung zum Abschluss eines Vertrags zu prüfen. Die vom Verlag vorgetragene Begründung legte daher nicht ausreichend dar, auf welcher Rechtsgrundlage eine Erhebung des Geburtsdatums erfolgt.

Zur besseren Gewährleistung der Transparenzanforderungen muss bei Werbeschreiben darauf geachtet werden, dass

- bereits im Anschreiben explizit auf die Datenerhebung für Werbezwecke hingewiesen wird,
- die Kundinnen und Kunden darüber aufgeklärt werden, dass eine Verweigerung der Datenpreisgabe keinen Einfluss auf die bestehende Kundenbeziehung hat, und
- eine vordergründige Zwecksetzung, nämlich die Nutzung der E-Mail-Adresse und der Telefonnummer für Werbezwecke, nicht erst am Ende der Anlage zum Anschreiben beiläufig aufgeführt wird.

Nach alledem wurde gegenüber dem Verantwortlichen eine Verwarnung aufgrund des Verstoßes gegen den Grundsatz der transparenten Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 Buchst. a DSGVO sowie aufgrund des Verstoßes gegen die Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO ausgesprochen und die Löschung der im Wege des Anschreibens erhobenen Geburtsdaten angeordnet.

Bereits im Verlauf des Verfahrens hatte der Verantwortliche sich dahin gehend geäußert, die Grundsätze der Rechtmäßigkeit der Verarbeitung insbesondere durch die Gestaltung und Formulierung eines möglichen zukünftigen ähnlichen Anschreibens sicherstellen zu wollen. Nach Angabe des Verantwortlichen wurden die Geburtsdaten mittlerweile gelöscht.

Was ist zu tun?

Werden personenbezogene Daten für Zwecke der werblichen Ansprache erhoben, muss die Verarbeitung auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise erfolgen. Dies ist nur dann der Fall, wenn es klar ist, dass es um Daten für Werbezwecke geht.

5.2.2 Informationen über eine frühere Behandlung bei Ausbildung in derselben Klinik

Nachdem eine Auszubildende für den Beruf einer Gesundheits- und Krankenpflegerin auf ihrer neu angetretenen Ausbildungsstation damit konfrontiert worden war, dass sie sieben Jahre zuvor einmal Patientin auf der Station gewesen sei und aufgrund dieser Tatsache nunmehr dort nicht mehr weiter beschäftigt werden könne, reichte der daraufhin von ihr bevollmächtigte Anwalt eine Beschwerde über ihren Arbeitgeber beim ULD ein.

Im Rahmen des Beschäftigungsverhältnisses dürfen lediglich die für die betrieblichen Zwecke erforderlichen Daten über Beschäftigte verarbeitet werden. Dabei ist vom Arbeitgeber zu begründen, warum welche Daten wofür erforderlich sind. Diese Daten sind dabei grundsätzlich unmittelbar bei dem Beschäftigten zu erheben.

Beschäftigte

Eine Definition, welche Personen als Beschäftigte im Sinne des Bundesdatenschutzgesetzes gelten, finden sich in § 26 Abs. 8 BDSG.

Bei der Verarbeitung von Patientendaten sind neben den allgemeinen datenschutzrechtlichen Vorschriften u. a. auch besondere berufsrechtliche Vorschriften zur ärztlichen Schweigepflicht zu beachten. Des Weiteren hat der Verantwortliche im Rahmen seiner zu treffenden technisch-organisatorischen Maßnahmen eine Trennung der von ihm verarbeiteten Patienten- und Mitarbeiterdaten sicherzustellen.

Die Verarbeitung der Patientendaten der Betroffenen erfolgte damals lediglich für den Zweck, die Behandlung durchzuführen, abzurechnen und zu dokumentieren. Die Verwendung von Patientendaten der Betroffenen für Zwecke des Beschäftigungsverhältnisses stellt eine Zweckänderung dar, für die eine entsprechende Rechtsgrundlage erforderlich ist.

Im Rahmen des eingeleiteten Verfahrens wurde vom Klinikgeschäftsführer mitgeteilt, dass die Beschwerdeführerin von verschiedenen Mitarbeitenden auf der Station als frühere Patientin lediglich erkannt wurde und kein Zugriff auf die Patientenakte erfolgt sei.

Aufgrund von verschiedenen Erfahrungen in ähnlich gelagerten Fällen sähen sich die dortigen Mitarbeitenden nicht mehr in der Lage, mit ihr zusammenzuarbeiten, und es sei zur Sicherstellung des ordnungsgemäßen Betriebsablaufes ein Stationswechsel erforderlich gewesen.

Gerade im Hinblick darauf, dass die Betroffene nach eigener Aussage ihre damalige Behandlung abgeschlossen habe, vollständig geheilt sei und darüber hinaus auch die Eignungsuntersuchung zur Aufnahme des Ausbildungsverhältnisses ohne Beanstandungen bestanden habe, ergaben sich aus Sicht des ULD zumindest weiterhin Zweifel an der Erforderlichkeit der Verwendung der Information über die damalige Behandlung für eine Entscheidung über den weiteren Verlauf der Ausbildung.

Selbst im Falle einer solchen Erforderlichkeit ist eine Verwendung nur zulässig, wenn kein Grund zu der Annahme besteht, dass das schutzwürdi-

ge Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Gerade bei der Verwendung von Daten, die den besonderen berufsrechtlichen Vorschriften zur ärztlichen Schweigepflicht unterliegen, ist dieses schutzwürdige Interesse der betroffenen Person im besonderen Maße zu berücksichtigen.

Da weder die Erforderlichkeit noch die ausreichende Beachtung der schutzwürdigen Interessen der Betroffenen nachgewiesen werden konnte, wurde der Klinik gegenüber eine Warnung erteilt.

5.2.3 Einführung von digitalen Spielerpässen – Begrenzung der Datensammlung

Im Rahmen der voranschreitenden Digitalisierung wurde von einem Sportverband entschieden, mit Beginn der Saison 2019/2020 digitale Spielerpässe zu nutzen. In diesem Zusammenhang erhielt das ULD verschiedene Beschwerden darüber, dass im Rahmen der Beantragung der Spielberechtigung die Erteilung einer Einverständniserklärung zur Verarbeitung verschiedener personenbezogener Daten und eines digital bereitzustellenden Fotos über das Internet Pflicht sei und ansonsten keine Spielerlaubnis erteilt werden würde. Darüber hinaus müsse auch ein Einverständnis für die Nutzung des Fotos auf Webseiten des Vereins, des Verbands und auf einer bundesweiten Online-Plattform sowie zu Marketingzwecken erteilt werden.

Eine in diesem Zusammenhang durchgeführte Überprüfung ergab, dass der Sportverband die einschlägige Satzung für die Saison 2019/2020 neu gefasst hatte und in dieser tatsächlich die Vorlage einer Erlaubnis zur Veröffentlichung eines zur Verfügung zu stellenden Passfotos verlangt wurde. Sollte diese entsprechende Erlaubnis nicht vorliegen, würde der Antragsteller keine Spielberechtigung erhalten.

Satzungen

Vereins- und Verbandssatzungen dürfen nicht im Widerspruch zu geltenden datenschutzrechtlichen Vorschriften stehen.

Grundsätzlich dienen digitale Spielerpässe der elektronischen Spielrechtsprüfung durch den Schiedsrichter. Hierfür ist bei diesem Sportverband lediglich eine Verarbeitung von verschiedenen Antragsdaten im Passbearbeitungssystem sowie in der vom Bundesverband zur Verfügung gestellten nicht öffentlich zugänglichen onlinebasierten Software erforderlich. Eine Veröffentlichung der Daten auf Webseiten des Verbands, etwaiger Mitgliedsvereine und auf einer Online-Plattform oder die Nutzung der Daten für Marketingzwecke sind hingegen weder zur Durchführung der Aufgaben des Sportverbands noch zur Sicherstellung des Ligabetriebes erforderlich, sodass hierfür jeweils eine zuvor erhobene Einwilligung erforderlich ist.

Eine solche Einwilligung ist jedoch nur wirksam, wenn sie freiwillig, d. h. ohne jeden Druck oder Zwang, abgegeben werden kann. Hierbei wird eine echte Wahlfreiheit der betroffenen Person verlangt, die in der Lage sein soll, die Einwilligung zu verweigern, ohne dadurch Nachteile zu erleiden. Da im Falle einer Verweigerung der Erlaubnis jedoch keine Spielberechtigung erteilt wurde, mangelte es an der erforderlichen Wahlfreiheit.

Nachdem der Sportverband im Rahmen des eingeleiteten Verfahrens auf die geltende Rechtslage hingewiesen worden war, beschloss dieser eine entsprechende Änderung der Satzung und die Überarbeitung der entsprechenden Formulare. In diesem Zusammenhang wurde u. a. auch die Zugriffsberechtigung auf die digitalen Spielerpässe reduziert.

Seit der erfolgten Anpassung werden lediglich die für den Spielbetrieb erforderlichen Daten erhoben und zunächst ausschließlich nicht öffentlich verarbeitet. Für alle darüber hinausgehenden möglichen Verarbeitungen werden nunmehr jeweils einzelne Einwilligungen getrennt vom eigentlichen Antrag erhoben. Da der

Spielerpass auch ausgestellt wird, wenn diese möglichen Einwilligungen für zusätzliche Zwecke nicht erteilt werden, kann nunmehr selbst entschieden werden, ob beispielsweise Spielerdaten für die Spielberichtserstattung genutzt werden dürfen oder ein Foto veröffentlicht werden darf.

5.2.4 Anmeldungen zu Sportveranstaltungen gekoppelt an die Veröffentlichung von Sportlerdaten

Immer wieder erreichen das ULD Eingaben darüber, dass im Zusammenhang mit der Anmeldung zu Sportveranstaltungen weitreichende Einwilligungen erhoben werden und ohne entsprechende Erteilung keine Teilnahme möglich sei.

Wie bereits unter Tz. 5.2.3 erläutert, ist eine solche Einwilligung jedoch nur wirksam, wenn sie freiwillig, d. h. ohne jeden Druck oder Zwang, abgegeben werden kann. Hierbei wird eine echte Wahlfreiheit der betroffenen Person verlangt, die in der Lage sein soll, die Einwilligung zu verweigern, ohne dadurch Nachteile zu erleiden. Da im Falle einer Verweigerung jedoch keine Teilnahme an der jeweiligen Sportveranstaltung möglich war, fehlt es auch hier wiederum an der erforderlichen Wahlfreiheit.

Im Rahmen der entsprechenden Prüfungen fiel allerdings auf, dass in vielen Fällen auch Einwilligungen für die Verarbeitung von Daten erhoben wurden, ohne die eine Teilnahme an der Veranstaltung überhaupt gar nicht möglich gewesen wäre (beispielsweise Name, Anschrift, oder Geschlecht). Eine solche Verarbeitung kann jedoch auch auf Grundlage der Erforderlichkeit zur Erfüllung eines Vertrags oder der Erforderlichkeit zur Wahrung eines berechtigten Interesses des Verantwortlichen erfolgen, sodass hierfür gar keine Einwilligung erhoben werden musste. Sollte der Veranstalter allerdings beabsichtigen, zusätzliche Daten zu erheben oder für eine weiter gehende Verarbeitung zu nutzen, wäre hierfür eine entsprechende Einwilligung des Betroffenen notwendig.

Das berechtigte Interesse eines Veranstalters beinhaltet häufig auch eine Berichterstattung über das sportliche Geschehen, sodass einzelne Informationen wie Ergebnislisten vorübergehend auch auf dieser Grundlage ohne vorherige Einwilligung veröffentlicht werden können. Ob im Einzelfall jedoch dieses berechtigte Interesse des Veranstalters gegenüber den schutzwürdigen Interessen der Betroffenen tatsächlich überwiegt, hängt im Wesentlichen von der Bedeutung des Ereignisses und dem daraus abzuleitenden Informationsinteresse der Öffentlichkeit ab.

Eine solche Veröffentlichung ohne vorherige Einwilligung ist allerdings auf die Nachnamen, Vornamen, Vereinszugehörigkeit und in begründeten Ausnahmefällen den Geburtsjahrgang zu beschränken. Darüber hinaus sind die Betroffenen im Vorwege entsprechend zu informieren, und es ist zu prüfen, ob im Einzelfall die Beachtung der schutzwürdigen Interessen oder Grundrechte und Grundfreiheiten einer Veröffentlichung entgegenstehen. Ein gegebenenfalls eingereichter Widerspruch ist selbstverständlich ebenfalls zu beachten und darf nicht zu einem rückwirkenden Entzug einer Teilnahmeberechtigung führen.

Im Rahmen einer solchen Berichterstattung kann gegebenenfalls auch eine Veröffentlichung von einzelnen Fotos erfolgen. Hierbei muss allerdings ein Bezug zum Spielgeschehen bzw. dem Charakter der Sportveranstaltung klar zu erkennen sein. Sollte dabei gegebenenfalls eine Person im Mittelpunkt stehen oder gezielt nur ein einzelner Teilnehmer fotografiert werden, wäre hierfür jedoch die Einwilligung des Betroffenen erforderlich, da in einem solchen Fall seine Interessen oder Grundrechte und Grundfreiheiten gegenüber den berechtigten Interessen des Veranstalters überwiegen. Eine Veröffentlichung von Fotos minderjähriger Teilnehmer ist ebenfalls immer nur mit einer ausdrücklichen Einwilligung zulässig, da bei diesen die schutzwürdigen Interessen generell überwiegen.

In den durchgeführten Verfahren haben sich die Veranstalter meist kooperativ gezeigt und die Anmeldeverfahren entsprechend angepasst. So werden bei diesen nunmehr zunächst lediglich die zur Durchführung der Veranstaltung erforderlichen Daten erhoben und die betroffenen Personen umfassend über die Verarbeitung, eine gegebenenfalls geplante Berichterstattung und das bestehende Widerspruchsrecht informiert.

Im Falle von weiter gehenden Verarbeitungen einschließlich etwaiger zusätzlicher Veröffentlichungen wurden die hierfür erforderlichen Einwilligungen vom eigentlichen Anmeldeverfahren getrennt und um entsprechende Hinweise zur Freiwilligkeit und zum bestehenden Widerrufsrecht ergänzt.

Was ist zu tun?

Bei der Auswahl der Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten ist im Wesentlichen zu unterscheiden zwischen den Verarbeitungen, die zur Erfüllung eines Vertrags oder zur Wahrung eines berechtigten Interesses erforderlich sind, und allen darüber hinausgehenden Verarbeitungen, für die eine Einwilligung notwendig ist.

5.2.5 Keine konkludente Einwilligung zur Veröffentlichung von Fotos bei Facebook beim Besuch einer Veranstaltung

Durch eine Beschwerde erhielt das ULD Kenntnis davon, dass anlässlich von kulturellen Veranstaltungen einer Verantwortlichen Fotografien von Besuchern angefertigt und von der Verantwortlichen in hoher Auflösung veröffentlicht worden sind. Dazu fand sich lediglich auf der Webseite des Veranstalters (sinngemäß) folgende Textpassage:

Mit dem Besuch einer unserer Veranstaltungen erklärst Du Dich bereit, dass Fotos und Filme Deiner Person im Rahmen der Veranstaltung angefertigt werden und auf unserer Website und unseren Social-Media-Kanälen bereitgestellt werden. Gerne löschen wir die Fotos nachträglich, wenn Du uns kontaktierst.

Sofern die Anfertigung und spätere Veröffentlichung von Bildaufnahmen auf eine Einwilligung nach Art. 6 Abs. 1 Buchst. a DSGVO zu stützen ist, ist ein solches Vorgehen nicht mit den Vorgaben an eine wirksame Einwilligung im Sinne des Artikels 7 DSGVO vereinbar. Den Besuchern wurde auch nicht hinreichend deutlich, dass eine Veröffentlichung in den entsprechenden Medien erfolgen soll.

Die Verantwortliche hat die Erhebungs- und Veröffentlichungspraxis auf Hinweis des ULD hin angepasst.

5.2.6 Tätigkeit als Verantwortlicher im Inkassobereich

Für Unternehmen, die im Inkassobereich tätig sind, stellt sich häufig die Frage nach dem Umfang einer datenschutzrechtlichen Verantwortung. Davon abzugrenzen sind in der Praxis streng weisungsgebundene Datenverarbeitungen, die einer Auftragsverarbeitung zuzuordnen wären. Die Beurteilung ist mitunter schwierig, hat aber erhebliche Bedeutung, insbesondere

für die Frage nach der Einhaltung vertraglicher sowie technisch-organisatorischer Anforderungen, die ein Auftraggeber beachten muss.

Begriff des Verantwortlichen

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

Maßgebend ist die Entscheidung über die Zwecke und Mittel der personenbezogenen Datenverarbeitung nach Art. 4 Nr. 7 DSGVO. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) haben in ihrem Kurzpapier Nr. 13 zur Auftragsverarbeitung Stellung genommen und lediglich eine Inkassotätigkeit „mit Forderungsübertragung" als verantwortliche Datenverarbeitung beurteilt. Für die Prüfung eines Inkassovertrags zwischen einem Auftraggeber und einem Inkassounternehmen sind hieraus oft nur bedingt Schlussfolgerungen möglich. Von Bedeutung ist die Prüfung im Einzelfall:

https://www.datenschutzzentrum.de/artikel/1205-Kurzpapier-Nr.-13-Auftragsverarbeitung.html

Kurzlink: *https://uldsh.de/tb38-526*

Eine Auftragsverarbeitung zeichnet sich insbesondere durch ein weisungsgebundenes Verarbeiten personenbezogener Daten durch einen Auftragnehmer aus, bei dem die Zwecksetzung vom Auftraggeber ausgeht und für den Auftragnehmer nahezu kein eigener Entscheidungsspielraum zur Herstellung eines Verarbeitungsergebnisses verbleibt. Dies kann etwa bei der Entsorgung personenbezogener Daten, der Bereitstellung von Speicherplatz oder im Falle der Verarbeitung personenbezogener Daten nach fest vorgegebenen Rechenwegen gegeben sein.

Im Rahmen einer Beratung war das ULD mit einem Sachverhalt befasst, in welchem das Inkassounternehmen eine Schlüssigkeitsprüfung übernahm, um den rechtlichen Bestand einer Forderung zu verifizieren. Weiterhin wurde die Wirtschaftlichkeit der Durchführung eines Inkassos untersucht, wobei auch Bonitätsprüfungen unter Nutzung eigener Datenbestände erfolgten. Schließlich führte das Inkassounternehmen Adressprüfungen durch und holte Melderegisterauskünfte im eigenen Namen ein. Auch den Forderungseinzug führte das Inkassounternehmen durch, wobei das Recht bestand, dem Schuldner Teilzahlungen zu gestatten. Nur für Vergleiche im Mahnverfahren bedurfte es der Genehmigung durch den Auftraggeber. Das Inkassounternehmen entschied ferner eigenverantwortlich über Stundungsabreden mit dem Schuldner, sofern Nachweise zur derzeitigen Zahlungsunfähigkeit vorlagen. Notwendige Maßnahmen im Zusammenhang mit dem Forderungseinzug standen im Ermessen des Inkassounternehmens.

Die vertraglichen Vorgaben zur Durchführung des Inkassos billigten dem Inkassounternehmen damit einen eigenen Entscheidungsspielraum beim Umgang mit den personenbezogenen Daten der Schuldner zu, der auch Raum für eigene Zwecksetzungen ließ. So fehlten insbesondere nähere Vorgaben dazu, nach welchen Kriterien Schlüssig- und Wirtschaftlichkeitsprüfungen erfolgen sollen, wie die Kommunikation mit dem Schuldner erfolgen soll und welche Maßnahmen zum Forderungseinzug im Einzelfall getroffen werden sollen. Weiterhin wurden auch eigene Datenbestände – bei der Bonitätsprüfung – für die Erledigung des Inkassovertrags herangezogen.

Im Ergebnis konnte festgestellt werden, dass das Inkassounternehmen nicht als weisungsgebundener Auftragsverarbeiter, sondern vielmehr selbst als datenschutzrechtlich Verantwortlicher tätig wird.

Was ist zu tun?

Um herauszufinden, ob eine Auftragsverarbeitung oder eine datenschutzrechtliche Verantwortlichkeit vorliegt, sind u. a. die vertraglichen Vereinbarungen zwischen den Beteiligten zu prüfen. Außerdem ist maßgebend, welche Verarbeitungen vom Dienstleister, losgelöst vom Vertrag, tatsächlich wahrgenommen werden.

5.2.7 Displayanzeigen bei Lottoannahmestellen

Im Frühjahr 2019 ging beim ULD eine Beschwerde ein, in der beklagt wurde, dass beim Spiel mit der LOTTO-Card in einer Lottoannahmestelle anwesende Dritte über die Displayanzeige sehen könnten, wie der jeweilige Kunde heiße, was er mit welchem Einsatz spiele und wie viel er gewonnen habe.

Die LOTTO-Card wird einerseits als Servicekarte für eine direkte Gewinnausschüttung auf das Konto des Inhabers und andererseits auch zur Identifizierung des Karteninhabers genutzt. Unabhängig von der Karte können Kundinnen und Kunden anonym über einen Tippschein an allen Spielen teilnehmen, für die keine Identifizierung erforderlich ist. Darüber hinaus haben Spielende auch die Möglichkeit, an den Spielen via Internet vom eigenen Computer von zu Hause aus teilzunehmen.

Bei Spielen wie Sportwetten und der täglichen Lottoziehung KENO müssen dem Spielenden als Schutzmechanismus vor Spielsucht der Stand des Spielkontos und die Spielhistorie dargestellt werden. Aufgrund der Pflicht zur Darstellung ist zunächst eine vorherige Identifizierung des Spielenden erforderlich, der seine Kenntnisnahme anschließend aktiv bestätigen muss, sodass auch keine Abschaltung des Displays erfolgen kann.

Entgegen der Beschreibung des Beschwerdeführers wird seit einiger Zeit jedoch nicht mehr der Name des Karteninhabers, sondern ausschließlich seine Kundennummer auf dem Display angezeigt. Darüber hinaus enthält die aktuelle LOTTO-Card im Gegensatz zu einer früheren auch keinen Aufdruck des Lichtbilds mehr.

Im Rahmen einer Überprüfung von Displayanzeigen konnte festgestellt werden, dass eine Einsichtnahme auf das Display durch andere Kundinnen und Kunden kaum möglich war, da das Display direkt oberhalb der Kundenservicefläche des Tresens installiert war, die Eingabe der PIN durch einen immer wieder neu gemischten Zahlenkreis erfolgte, auf dem Display nur ein schwacher Kontrast eingestellt war und die Kundennummer und der Spielverlauf auf weniger als einem Drittel der Bildschirmfläche dargestellt wurde.

Die entsprechende Installation der Displays wurde in einer für die Lottoannahmestellen verbindlichen Geschäftsanweisung geregelt, deren Einhaltung regelmäßig durch Mitarbeiter der Geschäftsstelle geprüft wird. Des Weiteren werden die Mitarbeiter der Annahmestellen in der Geschäftsstelle entsprechend geschult.

Was ist zu tun?

Verantwortliche haben dafür Sorge zu tragen, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes vor Offenlegung durch Übermittlung oder unbefugte Verbreitung. Dazu sind geeignete technische und organisatorische Maßnahmen einzusetzen, um sicherzustellen, dass eine Verarbeitung personenbezogener Daten gemäß der DSGVO erfolgt.

5.2.8 Aushang von Aufstellungen zu Betriebsratsstunden

Über die erforderliche Anzahl und die Dauer von Betriebsratssitzungen kann es naturgemäß unterschiedliche Auffassungen zwischen der Geschäftsführung eines Unternehmens und seinen Betriebsratsmitgliedern geben. Dieses führte in einem Unternehmen dazu, dass nach einer Zunahme der Anzahl der Betriebsratssitzungen der Senior-Geschäftsführer die Platzierung von Aushängen an verschiedenen Stellen des Betriebes veranlasste, aus denen das jeweilige Mitglied und die Anzahl seiner täglichen Betriebsratsstunden hervorging. Er begründete dies damit, dass die Belegschaft über die Zunahme der Anzahl der Betriebsratsstunden informiert werden müsse, da die Betriebsratsmitglieder in dieser Zeit ja nicht in ihren Teams mitarbeiten würden und nur so die Belegschaft gegenüber ihrem Betriebsrat entsprechend reagieren könne.

Nachdem sich ein Gewerkschaftsvertreter bei der Geschäftsführung über den Aushang beschwert hatte, die sofortige Entfernung gefordert und mitgeteilt hatte, den Vorgang beim ULD anzuzeigen, wurden diese umgehend entfernt.

Im weiteren Verlauf entschuldigte sich die Geschäftsführung zunächst schriftlich und im Rahmen eines regelmäßigen Monatsgespräches auch persönlich bei den Betriebsratsmitgliedern für die Veröffentlichung. Hierbei wurde eingeräumt, dass der Aushang der Betriebsratsstunden keine geeignete Maßnahme sei, um die unterschiedlichen Auffassungen zur erforderlichen Anzahl und Dauer von Betriebsratssitzungen zu lösen.

Gegenüber dem ULD teilte die Geschäftsführung mit, dass sich alle Mitglieder darüber einig sind und ihnen bewusst sei, dass ein solcher Vorfall nicht wieder vorkommen dürfe, sodass von weiteren Maßnahmen abgesehen werden konnte.

5.2.9 Kenntnis von Gehaltsdaten durch unbefugte Mitarbeiter

In einem anderen Fall reichte ein Betriebsrat selbst eine Beschwerde beim ULD über das Verhalten einer Führungskraft ein. Diese hatte im Rahmen einer Gesprächsrunde mit Schichtleitern, Teamleitern und Disponenten eine Excel-Liste über alle Beschäftigten einschließlich der Dauer ihrer Betriebszugehörigkeit und ihrer jeweiligen Gehaltsdaten präsentiert, um gemeinsam zu prüfen, ob einzelnen Beschäftigten ein Angebot zur Aufhebung des Arbeitsverhältnisses unterbreitet werden könne.

Wie bereits im 37. Tätigkeitsbericht unter Tz. 5.4.14 erläutert, hat der verantwortliche Arbeitgeber bei der Verarbeitung von Gehaltsdaten sicherzustellen, dass die Sicherheit der Verarbeitung und insbesondere die Vertraulichkeit der Informationen gewährleistet sind. Hier-

zu zählt u. a. auch ein entsprechendes Berechtigungskonzept, das den Zugriff auf vertrauliche Personaldaten einschränkt. Des Weiteren sind Maßnahmen zu treffen, die einen unbefugten Zugriff oder eine Offenlegung von personenbezogenen Daten der Beschäftigten gegenüber Unberechtigten verhindern.

Im Rahmen der erfolgten Prüfung wurde vom Geschäftsführer zwar eingeräumt, dass die erfolgte Offenlegung der Gehaltsdaten für das Gespräch mit Schichtleitern, Teamleitern und Disponenten nicht erforderlich war und somit einen datenschutzrechtlichen Verstoß darstellt, diese Offenlegung allerdings so auch nicht geplant gewesen sei und es sich um ein Versehen handele.

Aufgrund der im Unternehmen geltenden Datenschutzrichtlinie und des dort enthaltenen Need-to-know-Prinzips wurde in der Vorbereitung der Gesprächsrunde von der verantwortlichen Führungskraft eine zweite Datei erstellt, in der das Gehalt explizit entfernt war. In der Sitzung wurde dann jedoch die falsche Datei geöffnet, was die Vortragende erst nach einigen Minuten merkte, da sie während der Präsentation mit dem Rücken zur Projektion stand.

Need-to-know-Prinzip

Jede(r) Beschäftigte darf nur auf solche Daten zugreifen können, die er zur Erfüllung seiner Aufgaben tatsächlich benötigt (Kenntnis nur bei Bedarf).

Nach Mitteilung des Geschäftsführers waren alle Gesprächsteilnehmer auf Vertraulichkeit verpflichtet, und es sei ansonsten im Unternehmen über entsprechende Nutzer-Accounts sichergestellt, dass jede(r) Beschäftigte personenbezogene Daten nur im Rahmen des eigenen Aufgabengebiets verarbeiten könne.

Der Vorfall wurde im Unternehmen als Anlass genommen, den Verursacher noch einmal zu sensibilisieren und im Falle von sensiblen Daten zukünftig für Präsentationen u. Ä. separate Ordner anzulegen, in denen sich entsprechend überarbeitete Dateien befinden. Darüber hinaus entschuldigte sich der Verursacher beim Betriebsrat und zahlreichen betroffenen Beschäftigten für die Offenlegung.

5.2.10 Kopplung der Einwilligung zum E-Mail-Newsletter mit erweiterter Garantie

Sofern eine Verarbeitung personenbezogener Daten zur Erfüllung eines Vertrags mit der betroffenen Person erforderlich ist, kann eine Verarbeitung auf die Rechtsgrundlage Art. 6 Abs. 1 Buchst. b DSGVO gestützt werden. Bietet der Hersteller eines Produkts, unabhängig davon, über welchen Vertriebsweg seine Produkte erworben wurden, eine Garantie für seine Produkte an und müssen sich Käufer hierzu über ein Online-Formular registrieren, ist genau zu prüfen, welche personenbezogenen Daten hierfür erforderlich sind. So kann es erforderlich sein, den Vor- und Nachnamen sowie die Bestellnummer und das Kaufdatum zu erheben und für die Laufzeit der Garantie zu speichern, u. a. um im Garantiefall die von den Garantieberechtigten angeführten Daten abzugleichen. Ob die Erhebung einer E-Mail-Adresse zur Erfüllung des Garantievertrags erforderlich ist, bedürfte weiterer Prüfung. Sofern die E-Mail-Adresse nicht bereits im Rahmen der Kaufvertragsabwicklung erhoben wird, ist dieses Datum zum Abgleich untauglich. Dennoch kann eine Kontaktmöglichkeit zu den Kundinnen und Kunden zum Zweck der Garantievertragsdurchführung dienlich und die diesbezügliche Erhebung und Verarbeitung zu diesem Zweck von Art. 6 Abs. 1 Buchst. b DSGVO umfasst sein.

Wenn Verantwortliche die erhobene E-Mail-Adresse verwenden möchten, um Direktwerbung zu versenden, bedarf es für diesen Zweck jedoch einer gesonderten Rechtsgrundlage. In Betracht käme, die Verarbeitung der E-Mail-Adressen der Kundinnen und Kunden, die sich für eine erweiterte Garantie registrieren, zu Zwecken der Direktwerbung auf Art. 6 Abs. 1 Buchst. f DSGVO in Verbindung mit § 7 Abs. 3

UWG oder aber auf eine Einwilligung gemäß Art. 6 Abs. 1 Buchst. a DSGVO in Verbindung mit § 7 Abs. 2 UWG zu stützen. Voraussetzung der zuletzt genannten Variante ist, dass die jeweils betroffenen Personen eine wirksame Einwilligung abgegeben haben. Wirksamkeitsvoraussetzung einer Einwilligung ist u. a., dass eine Einwilligung freiwillig erteilt wird.

Der Europäische Datenschutzausschuss schreibt hierzu in den „Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679":

„Wenn die Einwilligung ein nicht verhandelbarer Teil von Geschäftsbedingungen ist, wird angenommen, dass die Einwilligung nicht freiwillig erteilt wurde. Entsprechend wird eine Einwilligung nicht als freiwillig angesehen, wenn die betroffene Person die Einwilligung nicht verweigern oder zurückziehen kann, ohne Nachteile zu erleiden." (Seite 6)

„Art. 7 Abs. 4 der DSGVO weist u. a. darauf hin, dass eine Situation, in der die Einwilligung mit der Annahme von Vertragsbedingungen „gebündelt" wird oder die Erfüllung eines Vertrags oder die Erbringung einer Dienstleistung mit dem Ersuchen um Einwilligung in eine Verarbeitung von personenbezogenen Daten „verknüpft" wird, die für die Erfüllung des Vertrags nicht erforderlich sind, als in höchstem Maße unerwünscht angesehen wird. Wird die Einwilligung in einer solchen Situation erteilt, gilt sie als nicht freiwillig erteilt (Erwägungsgrund 43). Mit Art. 7 Abs. 4 soll sichergestellt werden, dass der Zweck der Verarbeitung personenbezogener Daten nicht getarnt oder mit der Erfüllung eines Vertrags oder der Erbringung einer Dienstleistung gebündelt wird, für die diese personenbezogenen Daten nicht erforderlich sind. Dadurch stellt die DSGVO sicher, dass die Verarbeitung personenbezogener Daten, um deren Einwilligung ersucht wird, nicht direkt oder indirekt zur Gegenleistung für einen Vertrag werden kann. Die beiden Rechtsgrundlagen für die rechtmäßige Verarbeitung personenbezogener Daten, d. h. Einwilligung und Vertrag, können nicht zusammengeführt werden und ihre Grenzen dürfen nicht verschwimmen." (Seite 9)

„Der Verantwortliche muss nachweisen, dass es möglich ist, die Einwilligung zu verweigern oder zu widerrufen, ohne Nachteile zu erleiden (Erwägungsgrund 42). […]

Wenn ein Verantwortlicher nachweisen kann, dass eine Dienstleistung die Möglichkeit umfasst, die Einwilligung ohne negative Folgen zu widerrufen, z. B. ohne dass die Erbringung der Dienstleistung zum Nachteil des Nutzers herabgestuft wird, kann das helfen zu zeigen, dass die Einwilligung freiwillig erteilt wurde. Die DSGVO schließt nicht alle Anreize aus, aber die Beweislast für den Nachweis, dass die Einwilligung unter allen Umständen freiwillig erteilt wurde, würde beim Verantwortlichen liegen." (Seite 12)

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Kurzlink: *https://uldsh.de/tb38-5210*

Sofern dieser Nachweis gelingt, kann eine solche Einwilligung auch mit der Erbringung einer Dienstleistung verbunden werden.

5.2.11 Veröffentlichung einer Liste mit Namen von Privatpersonen mit Zuordnung zu einer politischen Haltung

Im Rahmen einer Kontrollanregung wurde mitgeteilt, dass auf einer Webseite eine Excel-Datei mit ca. 24.000 Adressdatensätzen zum Abruf bereitgestellt wurde. Die Bezeichnung der Excel-Datei ließ den Schluss zu, dass es sich bei den Datensätzen um Personen handeln solle, die einem anderen politischen Lager zugehörig sind.

Die Betreiberin der Webseite machte hingegen deutlich, in Abgrenzung zu den veröffentlichten Namen nebst den Adressangaben eine gänzlich abweichende politische Meinung zu vertreten.

Nach Ermittlung der Domain-Inhaberin wurde unter Androhung eines Zwangsgeldes die sofortige Löschung der Datei angeordnet.

Was ist zu tun?

Bei Angaben zur politischen Haltung von Personen handelt es sich nach den Vorgaben des europäischen Datenschutzrechts um besonders sensible Daten. Deren Verarbeitung bedarf immer einer spezifischen Rechtsgrundlage. Für die zusätzliche Veröffentlichung von privaten Adressdaten bestand ebenfalls keine Rechtsgrundlage. Entsprechende Daten dürfen grundsätzlich nicht veröffentlicht werden.

5.2.12 Faxversand durch Berufsgeheimnisträger – der Absender muss auf die Sicherheit achten!

Im Berichtszeitraum hat das ULD zahlreiche Beschwerden über Faxsendungen erhalten, die von Rechtsanwälten an den Arbeitgeber geschickt und an eine allgemeine Faxnummer adressiert werden. Beim Arbeitgeber kommen diese Faxe dann auf einem Faxgerät an, das gegen den Zugang durch Unbefugte nicht ausreichend gesichert und auch nicht für die Zusendung anwaltlicher Schreiben gedacht ist. Diese Faxe enthalten meist heikle Informationen über den betroffenen Beschäftigten; oft handelt es sich um Pfändungs- und Überweisungsbeschlüsse, die an den Arbeitgeber geschickt werden. Auf diese Weise haben z. B. Beschäftigte Kenntnis über Gehaltspfändungen ihrer Kollegen erhalten, obwohl diese Information nicht für sie bestimmt war. Die betroffenen Personen bringt dies in eine äußerst unangenehme Situation an ihrem Arbeitsplatz.

In der Regel erkennen die Verantwortlichen, die diese Faxe versenden, im Rahmen der Anhörung ihre Sorgfaltspflichtverletzung beim Versand des Faxes an und versichern, dass sie Maßnahmen ergreifen, um solche Fehler künftig zu verhindern.

Um die Vertraulichkeit eingehender Faxe zu gewährleisten, müssen sowohl Absender als auch Empfänger Vorkehrungen ergreifen. Der Empfänger muss Faxgeräte so aufstellen, dass Unbefugte keinen ungehinderten Zugriff auf eingehende Faxe haben, die nicht für sie bestimmt und für ihre Tätigkeit nicht erforderlich sind. Gerade bei größeren Stellen ist es empfehlenswert, für die Personalabteilung eigene Faxgeräte vorzusehen.

Der Absender muss sich vor dem Versand vergewissern, dass das Fax tatsächlich den bestimmungsgemäßen Empfänger erreicht und vertrauliche Inhalte nicht in die Hände von Unbefugten geraten. Wenn ihm die Zuordnung der Faxnummer z. B. zur Personalabteilung nicht bekannt ist, empfiehlt sich eine vorherige telefonische Kontaktaufnahme zur Abklärung der richtigen Faxnummer oder zur Absprache, wie der bestimmungsgemäße Empfänger das Fax doch direkt über die allgemeine Faxnummer erhalten kann, z. B. indem er sich beim Empfang neben das Faxgerät stellt.

In einem Fall hat der verantwortliche Absender eines Faxes in einer Personalsache die Auffassung vertreten, dass solche Maßnahmen von ihm als Absender nicht verlangt werden könnten. Er müsse sich vielmehr darauf verlassen können, dass der Empfänger für die Sicherheit und Vertraulichkeit eingehender Faxe Sorge trage. Dies wird jedoch der Verantwortlichkeit des Absenders nicht gerecht, insbesondere dann nicht, wenn es sich beim Absender, wie in diesem Fall, um einen Berufsgeheimnisträger handelt. Wir haben daher in diesem Fall eine Verwarnung ausgesprochen. Der Verantwortliche hat hiergegen Klage erhoben. Das Gerichtsverfahren läuft noch.

Was ist zu tun?

Für vertrauliche Mitteilungen sollte ein Fax nur im Ausnahmefall gewählt werden. Sowohl bei der Übertragung als auch beim Eingang beim Empfänger bestehen erhebliche Risiken für die Vertraulichkeit der Inhalte. Sofern auf den Versand per Fax im Einzelfall nicht verzichtet werden kann, muss der Absender einer vertraulichen Mitteilung sich vergewissern, dass das Fax ausschließlich den bestimmungsgemäßen Empfänger erreicht.

5.2.13 Weitergabe von Kontaktdaten und Einhaltung von Informationspflichten

Das ULD erreichten mehrere Eingaben, in denen Personen berichteten, dass ihre Kontaktdaten wie etwa private Telefonnummern oder E-Mail-Adressen ohne ihr Wissen von Unternehmen weitergegeben wurden. Teilweise war dies ohne rechtliche Grundlage erfolgt und somit rechtswidrig, teilweise war zwar die Weitergabe zulässig, die betroffene Person wurde jedoch hierüber nicht informiert.

So bat die Kundin eines Architekturbüros um die Vorlage eines Kostenvoranschlages für ein Bauvorhaben. Letztendlich wurde man sich nicht handelseinig, und die Kundin erteilte dem Architekturbüro eine Absage. Mehrere Wochen später wurde sie von einem Anruf auf ihrem privaten Telefon überrascht: Der ihr unbekannte Anrufer bezog sich auf das Architekturbüro, stellte Fragen zu das Bauvorhaben betreffenden Details und gab an, dass er Firmen mit der Ausführung beauftragen wolle.

Auf den Anruf angesprochen, erklärte das Architekturbüro, man habe mit dem Anrufer lediglich unverbindlich über die Baumaßnahmen gesprochen und könne ihm nicht verbieten, telefonisch Kontakt zu der Kundin aufzunehmen; das müsse diese ihm schon selbst klarmachen. Nach dem Hinweis der Kundin, dass die betreffende Telefonnummer nicht öffentlich verfügbar und anscheinend von dort herausgegeben worden sei, forderte das Architekturbüro den Anrufer auf, die Kontaktversuche einzustellen, und teilte dies der Kundin mit.

Im Rahmen der Prüfung der zu diesem Vorgang eingereichten Beschwerde verwies das Architekturbüro darauf, dass die Kundin darüber informiert worden sei, dass mit verschiedenen Firmen zusammengearbeitet werde und diese in die Planung und Erstellung des Angebots mit eingebunden werden müssten. Hierzu würden selbstverständlich Kontaktdaten der Ansprechpartner weitergeleitet, um ein vernünftiges, wirtschaftlich tragfähiges Angebot abgeben zu können.

Wenn auch der Hinweis darauf, dass mit verschiedenen Firmen zusammengearbeitet werde, aus Sicht des Architekturbüros dies eine klare Information darüber beinhaltet, dass in diesem Zuge auch personenbezogene Daten zur Kontaktaufnahme weitergegeben werden, so war dies für die Kundin nicht erkennbar.

Bei Nachfragen wäre es möglich gewesen – und entspricht in vielen Branchen auch der üblichen Praxis –, jegliche Kommunikation über dasjenige Unternehmen zu führen, welches das Angebot erstellt. Es steht jedoch dem Grundsatz einer transparenten Verarbeitung bereits eindeutig entgegen, der betroffenen Person aufzuerlegen, aus den ihr zur Verfügung gestellten unternehmerischen Informationen herauszulesen, dass eine weitere Verarbeitung (hier: Weitergabe) ihrer personenbezogenen Daten stattfinden könnte.

Dem Architekturbüro wurde daher der Hinweis erteilt, dass bei der Erhebung personenbezogener Daten die Informationspflichten der Datenschutz-Grundverordnung eingehalten werden müssen. Hierzu zählt auch die Mitteilung der Empfänger personenbezogener Daten.

Was ist zu tun?

Ist eine Weitergabe der personenbezogenen Kontaktdaten durch das Unternehmen an feststehende Subunternehmen oder andere Geschäftspartner zur Ausführung des Auftrags beabsichtigt, muss der Verantwortliche der betroffenen Person im Zeitpunkt der Erhebung dieser Daten die konkreten Empfänger mitteilen.

5.3 Datenpannen in der Wirtschaft

5.3.1 Allgemeines zu Datenschutzpannen

Die Meldung einer Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde ist durch den Verantwortlichen vorzunehmen. Dennoch erreichten das ULD mehrere Meldungen, in denen nicht der Verantwortliche, sondern ein Auftragsverarbeiter mit einer entsprechenden Meldung an die Aufsichtsbehörde herantrat.

Art. 33 Abs. 1 Satz 1 DSGVO

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Die eigentlichen Verantwortlichen wurden hierbei teilweise als „betroffene Personen“ oder „Kunden“ bezeichnet, sodass sich erst im Verlauf der Prüfung des vorgetragenen Sachverhalts Hinweise darauf ergaben, dass es sich bei den meldenden Unternehmen um Auftragsverarbeiter handelte. Die Verantwortlichen waren jeweils über die Vorfälle informiert worden, jedoch ihrer Verpflichtung, die Verletzung des Schutzes personenbezogener Daten selbst zu melden, nicht in jedem Fall nachgekommen.

Zur Überwachung und Durchsetzung der DSGVO haben wir jeweils die Verantwortlichen ermittelt und in eigener Zuständigkeit hierzu angehört oder die örtlich und sachlich zuständigen Aufsichtsbehörden über das Vorliegen einer Meldung durch den Auftragsverarbeiter informiert.

Die Verantwortlichkeit für die Einhaltung der Vorgaben der DSGVO verbleibt bei dem Verantwortlichen, auch wenn die Verletzung des Schutzes personenbezogener Daten in der Sphäre des Auftragsverarbeiters geschieht. Der Auftragsverarbeiter hat die Verpflichtung, den Verantwortlichen bei der Einhaltung seiner Pflichten zu unterstützen. Jedoch obliegt dem Verantwortlichen die Bewertung der ihm zur Verfügung gestellten Informationen.

So enthielt ein an sämtliche Verantwortliche versandter Abschlussbericht eines Auftragsverarbeiters, dessen IT-System durch Schadsoftware verschlüsselt wurde, neben der Darstellung des Vorfalls sowie der ergriffenen Maßnahmen den Hinweis, es habe „keine Datenschutzpanne vorgelegen“, da man sämtliche Daten habe wiederherstellen können. Bereits die mit der Verschlüsselung eines IT-Systems verbundene zeitweise Nichtverfügbarkeit der Daten kann jedoch für verschiedene Verantwortliche sehr unterschiedliche Auswirkungen haben, je nachdem welche Daten verarbeitet und welche Dienstleistungen durch den Auftragsverarbeiter wahrgenommen werden. Der Verantwortliche kann sich somit nicht auf die

Einschätzung des Auftragsverarbeiters berufen, sondern muss den Vorfall individuell prüfen und bewerten.

Die dargestellten Unklarheiten in Bezug auf die Verantwortlichkeit führten zudem zu Erschwernissen und Verzögerungen in der Prüfung, ob eine Benachrichtigung der betroffenen Personen über die Verletzung des Schutzes ihrer personenbezogenen Daten erforderlich war.

Werden die gesetzlichen Vorgaben hinsichtlich der Meldepflicht durch den Verantwortlichen nicht eingehalten, stellt dies einen Verstoß gegen die DSGVO dar.

Was ist zu tun?

Nicht der Auftragsverarbeiter, sondern der Verantwortliche wird nach der DSGVO zur Einhaltung der Meldepflicht verpflichtet. Der Auftragsverarbeiter könnte zwar vom Verantwortlichen zur Vornahme der unverzüglichen Meldung autorisiert werden. Eine solche Autorisierung muss für die Aufsichtsbehörde aus den übersandten Meldeunterlagen aber klar und beweisbar hervorgehen.

5.3.2 Fehlzusendung von Kontoanträgen und Mitteilungen zu Zinsen und Umsätzen

Bei der Versendung von Informationen an Kundinnen und Kunden durch Kreditinstitute ist zu berücksichtigen, dass es sich häufig um Informationen handelt, die – auch wenn es sich nicht zwangsläufig um personenbezogene Daten besonderer Kategorien handelt – eine erhöhte Sensibilität aufweisen.

Die Übermittlung speziell von Eröffnungsanträgen, Zinsmitteilungen und Girokontoumsätzen darf daher nur stattfinden, wenn hinreichende technische und organisatorische Maßnahmen von dem jeweiligen Kreditinstitut getroffen werden, wie z. B. eine Verschlüsselung der E-Mails bzw. der Inhalte der E-Mails.

Im Falle einer Fehlzustellung kann gegebenenfalls davon ausgegangen werden, dass kein hohes Risiko besteht und damit keine Benachrichtigungspflicht nach Artikel 34 DSGVO ausgelöst wird, da dem falschen Empfänger dann eine Entschlüsselung des Inhalts nicht möglich ist.

Benachrichtigung betroffener Personen

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung (Art. 34 Abs. 1 DSGVO).

Was ist zu tun?

Kreditinstitute sind dazu aufgerufen, im Falle einer Versendung von personenbezogenen Bankunterlagen an Kundinnen und Kunden mittels E-Mail für eine angemessene Transport- und Inhaltsverschlüsselung zu sorgen.

5.3.3 Unverschlüsselte mobile Datenträger mit Kundendaten

Werden personenbezogene Informationen mittels mobiler Datenträger versendet, sind diese ausreichend vor unbefugtem Zugriff zu sichern.

Sicherheit der Verarbeitung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen sind geeignete technische und organisatorische Maßnahmen zu treffen, was auch eine Verschlüsselung der Daten einschließen kann (Art. 32 Abs. 1 Buchst. a DSGVO).

Bei der Versendung von USB-Sticks oder CDs kommt es immer wieder zu Verlusten der Datenträger auf dem Postweg, weshalb hier stets eine Verschlüsselung der digitalen Daten zu prüfen ist (siehe auch Tz. 4.5.10 für Fälle, in denen Patientendaten betroffen waren).

Nicht selten enthalten entsprechende digitale Unterlagen Kontoverbindungsdaten, personenbezogene Fotos oder auch sensible Datenkategorien wie etwa Gesundheitsdaten und biometrische Daten. Zum Schutz der Kundschaft und Geschäftspartner muss das jeweilige Unternehmen dem Schutzbedarf angemessene Sicherungsmaßnahmen treffen, um eine Kenntnisnahme der Daten durch unbefugte Personen auszuschließen.

5.3.4 Kundendaten in offenen Umschlägen versendet

Schreiben eines Inkassodienstleisters enthalten neben allgemeinen Adressinformationen weitere Angaben, die in einem Mahnschreiben typisch bzw. erforderlich sind: z. B. Informationen über den Gläubiger, die dortige Kundennummer der Schuldner, die Rechnungsnummer, Rechnungsdatum, Rechnungsbetrag, Verzugszinsen, bereits geleistete Zahlungen und darüber hinaus das Aktenzeichen des Vorgangs zusammen mit einer Persönlichen Identifikationsnummer (PIN), mittels derer sich die Schuldner bei einem Portal anmelden/einloggen und weitere Informationen abrufen und eingeben können. Daher ist bei einer Fehlzustellung in der Regel von einem hohen Risiko im Sinne des Artikels 34 DSGVO auszugehen. Dies hat zur Folge, dass die betroffenen Personen im Falle der Fehlzustellung zu benachrichtigen sind.

Aus solchen Schreiben können sich zudem weitere Einschätzungen ergeben, z. B. über die mutmaßliche finanzielle Situation, die über die bloße Information, dass die betreffende Person ein säumiger Schuldner ist, hinausgehen. Das ist beispielsweise dann der Fall, wenn aus den Schreiben ersichtlich ist, dass eine Forderung schon lange besteht oder ein Forderungsverzicht angeboten wurde.

Auch können durch die jeweiligen Waren bzw. Dienstleistungen möglicherweise Rückschlüsse auf Verhaltensweisen, Lebensumstände (Familien mit Kleinkind) und das Konsumverhalten (Alkoholbestellungen) gezogen werden, sodass in solchen Fällen regelmäßig ein hohes Risiko für den Verlust der Kontrolle über ihre personenbezogenen Daten (Zugangscode und PIN), Diskriminierung, Identitätsdiebstahl oder -betrug, Rufschädigung oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffenen natürlichen Personen gegeben ist.

In einem Verfahren verwendete ein Unternehmen eine defekte Kuvertiermaschine. Hierdurch war nicht gewährleistet, dass die Post in ver-

schlossenem Zustand bei den Empfängern ankam. Eine Einsichtnahme durch unbefugte Personen blieb damit möglich. Das Unternehmen hat nach Entdeckung des Fehlers umgehend organisatorische Maßnahmen getroffen, um eine Versendung offener Post in Zukunft zu vermeiden.

5.3.5 Diebstahl einer Kamera mit Speicherkarte

Viele Unternehmen, Vereine und auch öffentliche Stellen verfügen über eigene Fotokameras, um für unterschiedliche Zwecke Aufnahmen anfertigen zu können. Dabei kann es sich etwa um Fotografien zur Pflege der internen Firmenkultur, zu Werbezwecken oder für die Ausgestaltung einer Vereinszeitschrift handeln.

Werden auf den Fotografien Personen abgebildet, so sind die rechtlichen Vorgaben der Datenschutz-Grundverordnung und des Kunsturhebergesetzes zu beachten (37. TB, Tz. 5.5.2). Neben der Anfertigung der Fotografien gilt dies – wie für sämtliche personenbezogenen Daten – auch für deren Speicherung; hier sind durch den Verantwortlichen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau vor unbefugter oder unrechtmäßiger Verarbeitung zu gewährleisten.

In einem dem ULD als Verletzung des Schutzes personenbezogener Daten gemeldeten Fall konnten auch eine verschlossene Bürotür und die Verwahrung der betriebseigenen Digitalkamera in einem Möbeltresor diese Sicherheit nicht bieten: Einbrecher verschafften sich gewaltsam Zutritt durch das Fenster des Büros, öffneten den durch Schlüssel bzw. Zahlencode geschützten Tresor und stahlen die Kamera mitsamt der enthaltenen Speicherkarte.

Auch die bereits durchgeführte Sicherheitsmaßnahme, die Fotografien nach der Aufnahme auf einen Server zu übertragen und auf der Speicherkarte der Kamera zu löschen, musste im Nachhinein im Hinblick auf den Schutz der personenbezogenen Daten als wirkungslos betrachtet werden, da sich die Fotografien auf dem Speichermedium wiederherstellen lassen. Der Verantwortliche meldete den Diebstahl daher als Verletzung des Schutzes personenbezogener Daten.

Um eine Wiederherstellung der Fotografien auszuschließen, wäre es notwendig gewesen, die auf der Speicherkarte hinterlegten Daten mithilfe einer besonderen Software unwiederbringlich zu löschen.

Neben dieser technischen Möglichkeit kann auch eine organisatorische Maßnahme Schutz bieten: Wird nach der Nutzung einer Digitalkamera die Speicherkarte entnommen und an einem anderen gesicherten Ort aufbewahrt, bleiben die Fotografien vor unbefugtem Zugriff geschützt, auch wenn die Kamera entwendet wird.

Im dargestellten Fall beurteilte der Verantwortliche das durch die Verletzung des Schutzes personenbezogener Daten entstandene voraussichtliche Risiko für die persönlichen Rechte und Freiheiten der abgebildeten Personen als hoch und benachrichtigte sie unverzüglich über den Diebstahl der Kamera sowie der Speicherkarte mit ihren Fotografien. Die beim Umgang mit dem Vorfall ergriffenen Maßnahmen wurden vom ULD als ausreichend betrachtet.

Dem Verantwortlichen wurde unter Darstellung der vorgenannten Verfahren zum künftigen Schutz der Daten der Hinweis erteilt, dass hinsichtlich der personenbezogenen Daten die Grundsätze der Sicherheit der Verarbeitung nach Maßgabe der Datenschutz-Grundverordnung eingehalten werden müssen.

5.3.6 Veröffentlichung von Teilnehmerdaten zu einem Kindersportprojekt

Initiieren Unternehmen abseits ihres Kerngeschäfts regionale soziale Projekte und unterstützen diese als Sponsoren, steht die erfolgreiche Durchführung des Projekts zum Wohle derjenigen, die davon profitieren sollen, im Vordergrund. Werden im Rahmen dieses Engagements personenbezogene Daten verarbeitet, ist zu betrachten, wer über die Zwecke und Mittel der Verarbeitung dieser Daten entscheidet und somit als Verantwortlicher im Sinne der Datenschutz-Grundverordnung anzusehen ist. Dies kann eine Stelle allein oder es können mehrere zusammen als gemeinsam Verantwortliche sein.

Eine dem ULD gemeldete Verletzung des Schutzes personenbezogener Daten betraf eine Sicherheitslücke im Internetauftritt der Projektpartner, die Kindern die Teilnahme an einem sportlichen Event ermöglichen wollten. Das Unternehmen, das die Internetseite erstellt hatte, sah sich selbst in der Verantwortung und teilte mit, dass durch die Sicherheitslücke ein Zugriff auf personenbezogene Daten von Kindern möglich war, die sich für eine Teilnahme an dem Projekt angemeldet hatten. Neben Adressdaten waren auch sensible Daten wie gesundheitliche Einschränkungen betroffen. Ein Zugriff war möglich, da ein Tool durch einen Beschäftigten versehentlich nicht vom Webserver gelöscht wurde. Das entsprechende Unterverzeichnis war allerdings auf der Webseite nicht verlinkt und auch nicht im Quelltext der Internetseite zu finden.

Die Internetseite war im Auftrag dreier Hauptsponsoren des Projekts erstellt worden, die untereinander einen Kooperationsvertrag geschlossen hatten. Aus der weiteren Prüfung ergab sich, dass der meldende technische Dienstleister nicht als Verantwortlicher, sondern als Auftragsverarbeiter tätig geworden war (Tz. 5.3.1). Die Hauptsponsoren waren in einer kurz nach Bekanntwerden der Sicherheitslücke stattfindenden Besprechung von dem meldepflichtigen Vorfall informiert worden, erkannten jedoch keine datenschutzrechtliche Relevanz für sich als Projektpartner. Die Projektpartner wiesen auch ihren Dienstleister nicht an, die ihnen selbst obliegende Meldung der Sicherheitslücke an das ULD vorzunehmen.

Da die Meldepflicht einer Verletzung des Schutzes personenbezogener Daten jedoch nicht den Auftragsverarbeiter, sondern den Verantwortlichen trifft, wurden die Hauptsponsoren zur Aufklärung des Sachverhalts angehört. Die Anhörung ergab, dass die Sponsoren die Zwecke und Mittel zur Verarbeitung der personenbezogenen Daten festlegten und somit bezüglich des Projekts als Verantwortliche in Betracht kamen.

Die drei Hauptsponsoren reichten infolgedessen jeweils eigenständige Meldungen der Verletzung des Schutzes personenbezogener Daten nach. Die bisherige Meldung des technischen Dienstleisters bzw. des Auftragsverarbeiters war weder gesetzlich gefordert noch ausreichend, um eine fristgemäße Meldung der auftraggebenden Hauptsponsoren zu ersetzen.

Da die Sicherheitslücke innerhalb weniger Minuten nach Bekanntwerden geschlossen und die Internetseite zudem wenige Tage später nach Rücksprache mit den Hauptsponsoren vollständig gelöscht wurde, waren keine weiteren Maßnahmen erforderlich.

Die Verantwortlichen wurden durch die Landesbeauftragte für Datenschutz verwarnt, da sie ihrer Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde nicht unverzüglich nachgekommen waren.

5.4 Videoüberwachung

Das Thema Videoüberwachung ist ein Dauerbrenner im ULD. Auch im Jahr 2019 erreichte uns eine Vielzahl an Beschwerden über die Videoüberwachung durch private oder öffentliche Stellen. Größtenteils handelt es sich um Fälle, die sich aufgrund ihrer Unterschiedlichkeit nicht zusammenfassen lassen. Oft beschwerten sich Personen über die Videoüberwachung ihres Nachbarn, die augenscheinlich auch auf ihr eigenes Grundstück gerichtet war. In den Sommermonaten häuften sich die Beschwerden über Webcams. Ebenso war ein fehlendes oder unvollständiges Hinweisschild mehrfach Anlass für eine Beschwerde beim ULD.

Beratungen zum Thema Videoüberwachung sind der Ausnahmefall: Das liegt daran, dass die Beratung nicht (mehr) zu den Kernaufgaben der Landesbeauftragten für Datenschutz gehört, sondern nur in bestimmten Fällen gesetzlich vorgesehen ist. So wird zum Thema Videoüberwachung zwar allgemein, beispielsweise telefonisch oder durch Veröffentlichung von Orientierungshilfen, beraten; eine einzelfallbezogene und abschließende Beratung oder gar die Genehmigung von geplanten Überwachungsmaßnahmen ist hingegen nicht vorgesehen.

5.4.1 Videoüberwachung im Fitnessstudio – Update

Nachdem im letzten Tätigkeitsbericht zum Verfahrensstand bei einer Videoüberwachung in einer Fitnessstudiokette nicht viel Neues berichtet werden konnte, lohnt sich in diesem Jahr ein Update. Zur Erinnerung:

- Gefilmt wurden in mehreren Fitnessstudios dieser Kette in Umkleidebereichen, Trainingsflächen und Aufenthaltsbereichen.
- Darin sieht das ULD eine schwerwiegende Beeinträchtigung der Grundrechte und Grundfreiheiten der betroffenen Personen.
- Im Jahr 2017 wurde der Fitnessstudiokette die Videoüberwachung bestimmter Bereiche in vier Fitnessstudios untersagt.
- Nach erfolglosem Widerspruchsverfahren wurden gegen die Anordnungen des ULD Klagen vor dem Verwaltungsgericht in Schleswig erhoben.

Im Berichtszeitraum hat das Verwaltungsgericht nun nach mündlicher Verhandlung über die Klagen entschieden. Es hat alle vier Klagen gegen die aufsichtsbehördlichen Anordnungen abgewiesen. Die Entscheidungen sind noch nicht rechtskräftig.

Was ist zu tun?

In Umkleidebereichen muss eine Videoüberwachung stets unterbleiben. Auch dort, wo Personen über längere Zeit beobachtet werden und ihr Verhalten aufgezeichnet wird, wie etwa im Trainingsbereich, ist eine Überwachung grundsätzlich unzulässig.

5.4.2 Videoüberwachung in Toilettenräumen

Bereits in der Vergangenheit wurden ab und zu Beschwerden über Videokameras, die angeblich in Toilettenräumen filmen, an das ULD herangetragen. In der Regel stellt sich heraus, dass es sich z. B. nur um einen Bewegungsmelder handelt oder ein sonstiges Missverständnis vorliegt. Nicht so dieses Mal: Auf einem Campingplatz in Schleswig-Holstein wurde tatsächlich eine Videoüberwachung innerhalb von Toilettenräumen vorgenommen. Die Kameras waren so angebracht, dass mit ihnen die Pissoirs, der Bereich vor den Waschbecken, der Bereich vor den einzelnen Toilettenkabinen und teilweise von oben ein Teil des Inneren der Toilettenkabinen eingesehen werden konnte. Als Begründung für die Installation der Anlage gab der Betreiber an, in den Räumlichkeiten seien vermehrt Fälle von Vandalismus aufgetreten. Außerdem fänden häufig Verunreinigungen oder eine unsachgemäße Benutzung der Toilettenräume statt, auf die die Verursacher dann angesprochen werden sollten.

Im Juli 2019 war unser Prüfteam vor Ort und führte eine Kontrolle durch. Aufgrund der dort festgestellten Erkenntnisse wurde dem Betreiber der Videoüberwachung gegenüber angeordnet, in den Toilettenräumen nicht länger eine Videoüberwachung durchzuführen, die Kameras aus den Räumlichkeiten zu entfernen und sämtliche bis dahin gespeicherten Videoaufnahmen irreversibel zu löschen. Der Betreiber der Videoüberwachung zeigte sich kooperativ und kam der Anordnung des ULD in sämtlichen Punkten nach. Er merkte aber auch an, dass der von ihm beauftragte Elektronikdienstleister versichert hatte, dass Videoüberwachung in diesem Bereich datenschutzrechtlich zulässig sei, da die Toilettenkabinen nicht überwacht würden.

Dieses Verfahren hat gezeigt, dass Verantwortliche sich in jedem Fall intensiv mit dem Thema Datenschutz beschäftigen müssen, wenn sie sich dazu entscheiden, eine Videoüberwachungsanlage zu installieren oder installieren zu lassen. Sie dürfen nicht darauf vertrauen, dass das mit der Installation und Einrichtung beauftragte (Kleinst-)Unternehmen die datenschutzrechtliche Zulässigkeit der Videoüberwachung beurteilen kann und im Zweifel von einer Installation absehen würde. Offenbar besteht nach wie vor bei einigen Verantwortlichen und auch bei Elektronikdienstleistern eine datenschutzrechtliche Wissenslücke. Gerade weil beim Betrieb einer Videoüberwachungsanlage die Situation je nach Standort der Kamera, Zweck, Ausrichtung und dem Ergreifen technischer Maßnahmen anders zu bewerten ist, darf man sich nicht leichtfertig für den Einbau von Überwachungskameras entscheiden. Man muss sich vielmehr vorher damit vertraut machen, was erlaubt und was unzulässig ist. Keinesfalls darf in Toilettenräumen oder ähnlich intimen Bereichen eine Videoüberwachung stattfinden.

Verantwortlichkeit

Trotz mangelnder rechtlicher Kenntnis bleibt der Betreiber der Videoüberwachungsanlage datenschutzrechtlich verantwortlich. Bereits bei einer kurzen Recherche im Internet zum Thema Videoüberwachung hätte der Betreiber darauf stoßen müssen, dass eine Überwachung in Toilettenräumen unzulässig ist. Die Verantwortlichkeit, die beabsichtigte Datenverarbeitung auf ihre Zulässigkeit hin zu überprüfen, kann auch nicht vollständig einem Dienstleister übertragen werden. Der Betreiber muss dafür Sorge tragen, dass alle datenschutzrechtlichen Vorschriften eingehalten werden, wenn er sich für die Installation einer Videoüberwachungsanlage entscheidet.

Wer Rat benötigt, findet Antworten in der Broschüre „Videoüberwachung" unserer Praxis-Reihe „Datenschutzbestimmungen praktisch umsetzen":

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

Kurzlink: *https://uldsh.de/tb38-542*

Was ist zu tun?

Jeder, der den Einbau einer Videoüberwachungsanlage plant, muss sich über die rechtliche Zulässigkeit informieren. Wenn Unsicherheiten bestehen oder Fragen offenbleiben, sollte einzelfallbezogen rechtlicher Rat eingeholt werden.

5.4.3 Die Gruß-Webcam – ein Sonderfall unter den Webcams

Webcams bilden nahezu jeden Sommer den Schwerpunkt der Beschwerden im Bereich der Videoüberwachung, die das ULD erreichen. Dieses Jahr sah sich das ULD mit einer Webcam der besonderen Art konfrontiert – einer sogenannten Gruß-Webcam. Die Webcam befand sich innerhalb einer Art Einkaufszentrum eines Urlaubsorts. In diesem Gebäude war die Kamera so angebracht, dass sie auf einen Durchgangsbereich ausgerichtet war. Auf dem Boden war ein Hinweis aufgedruckt: „Bitte lächeln" hieß es dort, und auf einem Aufsteller in der Nähe der Webcam wurde die Funktionsweise der Kamera erläutert. Man solle sich auf die auf dem Boden markierte Fläche stellen und in die Kamera schauen. Dann werde ein Bild erstellt und man könne auf diesem Wege seine Familie zu Hause grüßen. Das Bild war dann für einige Zeit im Internet abrufbar, wie auch bei einer herkömmlichen Webcam.

Problematisch hierbei war, dass die Kamera nicht nur auslöste, wenn Personen die Anweisungen auf dem Aufsteller befolgten. Zum einen war der Erfassungsbereich der Kamera viel weitgehender und nicht nur auf die markierte Fläche auf dem Boden beschränkt. Zum anderen erstellte die Kamera auch Aufnahmen, wenn eine Person lediglich den Erfassungsbereich durchquerte. Daher wurden viele Personen unfreiwillig von der Gruß-Webcam erfasst, und ein Bild von ihnen wurde für einige Zeit im Internet veröffentlicht. Zu einem großen Teil dürfte dies ohne das Wissen der betroffenen Personen geschehen sein. Da es sich um einen Durchgangsbereich handelte, ist davon auszugehen, dass nicht jede und jeder auf die Kamera oder die Bodenmarkierung aufmerksam geworden ist, besonders wenn man sich dem Erfassungsbereich der Kamera aus der „falschen" Richtung näherte. Auch dürften Personen, die lediglich die Bodenmarkierung und die Kamera sahen, nicht immer verstanden haben, dass es sich um eine Webcam handelt, die ab diesem Moment Aufnahmen von ihnen im Internet veröffentlicht.

Das ULD hielt den Betrieb dieser Gruß-Webcam für datenschutzrechtlich unzulässig, da seit Inbetriebnahme der Webcam Bildaufnahmen von einer nicht mehr nachvollziehbar großen Anzahl von Personen, vermutlich überwiegend ohne deren Kenntnis, erstellt und veröffentlicht wurden, ohne dass es dafür eine Rechtsgrundlage gab. Das ULD sprach daher gegenüber dem Verantwortlichen eine Verwarnung aus. Außerdem wurde der Betreiber davor gewarnt, die Kamera in Zukunft erneut und unverändert in Betrieb zu nehmen.

Die Idee einer Gruß-Webcam an sich muss aber gar nicht zwingend datenschutzrechtlich unzulässig sein. Wenn der Betreiber etwa die Kamera in einem Bereich zur Verfügung stellt, der kein Durchgangsbereich ist, der Erfassungsbereich der Kamera deutlich und vollständig am Boden markiert ist und derjenige, der diese Art von Urlaubsgrüßen versenden möchte, z. B. einen Knopf betätigen muss, um die Kamera zum Auslösen zu bringen, kann die Umsetzung im Ergebnis datenschutzkonform sein. In jedem Fall müssten aber die betroffenen Personen, bevor sie sich für das „Grüßen per Webcam" entscheiden, über die Datenverarbeitung informiert werden, wie dies Artikel 13 DSGVO vorsieht.

Datenschutzfragen bei Webcams werden in der Broschüre „Fotos und Webcams“ unserer Praxis-Reihe „Datenschutzbestimmungen praktisch umsetzen“ behandelt:

https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-6-Fotos-und-Webcams.pdf

Kurzlink: *https://uldsh.de/tb38-543*

5.4.4 Aktualisierte Orientierungshilfen der Datenschutzkonferenz: Bodycams, Dashcams, Drohnen, Kameras in Schwimmbädern

Die bereits vorhandenen Orientierungshilfen der Datenschutzaufsichtsbehörden des Bundes und der Länder zum Thema Videoüberwachung mussten an die neue Rechtslage angepasst werden. Bereits veröffentlicht wurden

- die Orientierungshilfe der Datenschutzaufsichtsbehörden zum Einsatz von Bodycams durch private Sicherheitsunternehmen,
- das Positionspapier zur Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sogenannte Dashcams),
- das Positionspapier zur Nutzung von Kameradrohnen durch nichtöffentliche Stellen und
- die Orientierungshilfe zur Videoüberwachung in Schwimmbädern.

Eine Veröffentlichung der neu gefassten allgemeinen Orientierungshilfe „Videoüberwachung durch nichtöffentliche Stellen“ steht noch aus, da diese sehr umfangreich ist und sich daher noch in der Überarbeitung befindet.

Hinweise zu Bodycams

Die Orientierungshilfe zum Thema Bodycams wurde erstellt, weil private Sicherheitsunternehmen vermehrt Bodycams einsetzen, z. B. um ihre Beschäftigten vor Übergriffen zu schützen. Dies kann unter bestimmten Voraussetzungen auch zulässig sein, darf aber nicht dazu führen, dass Veranstaltungen permanent und anlassunabhängig durch die Bodycams des beauftragten Sicherheitsunternehmens gefilmt werden. Die Orientierungshilfe beinhaltet Hinweise zum datenschutzgerechten Einsatz von Bodycams und gibt Schutzmaßnahmen vor, die beim Einsatz beachtet werden müssen. Beispielsweise darf die Bodycam nur aktiviert werden, wenn ein entsprechender Vorfall zu erwarten ist. Die Tatsache, dass gefilmt wird, ist den betroffenen Personen durch optische (z. B. rote Lampe) und akustische (z. B. Piepton, mündlicher Hinweis) Signale mitzuteilen. Die Funktionsweise der Bodycams muss vor der Implementierung in einem Konzept festgehalten werden. Tonaufnahmen sind grundsätzlich unzulässig.

Die Orientierungshilfe zum Thema Bodycams ist abrufbar unter:

https://www.datenschutzkonferenz-online.de/media/oh/20190222_oh_bodycams.pdf

Kurzlink: *https://uldsh.de/tb38-544a*

Hinweise zu Dashcams

Das Positionspapier zum Thema Dashcams bezieht sich auf die aktuelle Rechtsprechung des Bundesgerichtshofs (BGH). In seinem Urteil vom 15. Mai 2018 (VI ZR 233/17) ließ das Gericht Videoaufnahmen einer Dashcam als Beweis zu. Daraus schlussfolgerten viele Personen fälschlicherweise, dass Dashcams nunmehr datenschutzkonform seien und der Einsatz von Dashcams im Straßenverkehr zulässig wäre. Der BGH stellte aber im selben Urteil auch fest, dass der anlasslose Einsatz von dauerhaft aufzeichnenden Dashcams datenschutzrechtlich unzulässig ist. Eine Ausnahme kann nur in Betracht kommen, wenn (technische) Möglichkeiten zum Einsatz kommen, die sicherstellen, dass eine Kamera lediglich kurzzeitig und anlassbezogen aufzeichnet. Das heißt, dass rechtswidrig erlangte Dashcam-Aufnahmen unter Umständen zwar im Gerichtsprozess als Beweis verwertet werden dürfen, die Datenschutzaufsichtsbehörden können aber dennoch aufgrund solcher rechtswid-

rig erlangter Aufnahmen – unabhängig von der Verwertbarkeit im Zivilprozess – gegebenenfalls Verbote aussprechen oder Bußgelder verhängen.

Das Positionspapier zum Thema Dashcams ist abrufbar unter:

https://www.datenschutzkonferenz-online.de/media/oh/20190128_oh_positionspapier_dashcam.pdf

Kurzlink: *https://uldsh.de/tb38-544b*

Hinweise zu Kameradrohnen

Das Positionspapier zur Nutzung von Kameradrohnen durch Private zeigt, was beim Fliegen mit einer Videodrohne aus datenschutzrechtlicher Sicht beachtet werden muss. Verständlicherweise begeistert das Fliegen mit der Drohne immer mehr Hobbypiloten, die Luftperspektive ermöglicht ungewöhnliche Bildaufnahmen. Dennoch gibt es auch beim Fliegen Grenzen, um den Schutz der Privatsphäre der Menschen am Boden zu gewährleisten. Es ist nämlich möglich, mit der Drohne unbeobachtet Blicke in den Garten seines Nachbarn zu werfen oder gar in die Fenster von fremden Wohnungen oder Häusern zu schauen. Das ist selbstverständlich unzulässig.

Für Betroffene solcher Aktionen ergibt sich häufig das Problem, dass sie zwar die Drohne bemerken, diese aber nicht einer Person zuordnen können. Vom Boden aus kann man oft nicht einmal erkennen, ob es sich um eine Drohne mit Kamera handelt, geschweige denn ob die verbaute Kamera gerade bestimmte Bereiche erfasst oder heranzoomt. Im Ergebnis wird durch Kameradrohnen eine heimliche Beobachtung aus der Ferne ermöglicht, die nicht zulässig ist. Wenn höchstpersönliche Lebensbereiche verletzt werden, kann dies sogar eine Straftat sein.

Beim Einsatz von Drohnen ist die Luftverkehrsverordnung zu beachten, die im April 2017 um Regelungen zum Betrieb von unbemannten Fluggeräten erweitert wurde. Es gibt Bereiche, wie z. B. Wohnbereiche, Bereiche von Justizvollzugsanstalten, Unfallorte oder Menschenansammlungen, in denen Drohnen überhaupt nicht aufsteigen dürfen.

In den Bereichen, in denen das Fliegen erlaubt ist, sollten Drohnenpiloten darauf achten, dass niemand, der dies nicht möchte, mit einer Drohne gefilmt wird. Es sollte bedacht werden, ob sich jemand im näheren Umkreis durch die Drohne gestört fühlen könnte. Es empfiehlt sich immer, diese Personen über den geplanten Drohnenflug und den Zweck des Drohnenflugs zu informieren.

Das Positionspapier zum Thema Drohnen ist abrufbar unter:

https://www.datenschutzkonferenz-online.de/media/oh/20190116_oh_positionspapier_kameradrohnen.pdf

Kurzlink: *https://uldsh.de/tb38-544c*

Hinweise zur Videoüberwachung in Schwimmbädern

In der Orientierungshilfe zum Thema „Videoüberwachung in Schwimmbädern“ werden Hinweise gegeben, wie eine Videoüberwachung in Schwimmbädern im Einklang mit den Vorschriften der Datenschutz-Grundverordnung eingesetzt werden kann. Eine Kernaussage der Orientierungshilfe ist, dass Videoüberwachung den Einsatz von Aufsichtspersonal weder ersetzen kann noch darf. Auch ist Videoüberwachung grundsätzlich nicht erforderlich zur Verhinderung des unberechtigten Zutritts zu Bereichen, für die ein zusätzliches Entgelt (z. B. zum Saunabereich) zu entrichten ist. Dies kann in der Regel durch andere geeignete Maßnahmen, wie etwa ausreichend hohe Drehkreuze oder Schranken, ohne unverhältnismäßigen Aufwand verhindert werden. Zur Abwehr von den mit dem Baden verbundenen Gefahren ist eine Speicherung der Aufnahmen nicht geeignet und erforderlich. Im Ausnahmefall kann eine reine Beobachtung („verlängertes Auge“) zulässig sein, wenn sie der Unterstützung der Badeaufsicht an besonders gefährlichen oder unübersichtlichen Orten dient. Die allgemein erhöhte Unfallgefahr wegen des Aufenthalts im Wasser ist allerdings kein Grund für eine Videoüberwachung. Vielmehr muss sich die Gefährlichkeit

besonderer Bereiche aufgrund objektiver Anhaltspunkte ergeben.

Die Orientierungshilfe zum Thema „Videoüberwachung in Schwimmbädern" ist abrufbar unter: *https://www.datenschutzkonferenz-online.de/media/oh/20190108_oh_zusatz_videoueberwachung_schwimmbad.pdf*

Kurzlink: *https://uldsh.de/tb38-544d*

Was ist zu tun?

Verantwortliche, die Bodycams, Dashcams, Drohnen oder Kameras in Schwimmbädern einsetzen wollen, sollten sich die aktualisierten Orientierungshilfen ansehen und die darin enthaltenen Vorgaben berücksichtigen. Auch betroffene Personen, die z. B. unfreiwillig von einer Drohne gefilmt wurden oder sich fragen, was es mit den vielen Kameras im örtlichen Schwimmbad auf sich hat, können durch die Orientierungshilfen einen ersten Eindruck über die Zulässigkeit solcher Datenverarbeitungen erhalten.

5.4.5 Orientierungshilfe der Datenschutzkonferenz: biometrische Analyse

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat den Arbeitskreis „Technische und organisatorische Datenschutzfragen" damit beauftragt, sich gemeinsam mit dem Arbeitskreis „Videoüberwachung" mit dem Thema „Verarbeitung von Daten durch Sensorik und Videotechnik" und deren datenschutzrechtlicher Einordnung zu befassen. Das Ergebnis der Arbeitsgruppe ist das „Positionspapier zur biometrischen Analyse", das im April 2019 veröffentlicht wurde. Das Positionspapier beinhaltet neben Begriffsdefinitionen im Wesentlichen technische Beschreibungen der Funktionsweisen einzelner ausgewählter biometrischer Verfahren, mögliche Einsatzszenarien („Use Cases") sowie eine rechtliche Einordnung der Verarbeitung biometrischer Daten. Diese juristische Bewertung wurde einerseits generell und abstrakt vorgenommen, es finden sich aber auch ausgewählte Anwendungsfälle in dem Positionspapier wieder. Abschließend wird skizziert, wie das Standard-Datenschutzmodell (Tz. 6.2.3) dazu genutzt werden kann, die rechtlichen Anforderungen der Datenschutz-Grundverordnung bei der Verarbeitung biometrischer Daten in konkrete technische und organisatorische Maßnahmen zu überführen.

Als Anwendungsbeispiel wird in der Orientierungshilfe u. a. behandelt, ob

- die Bezahlung des Schulessens mithilfe des Fingerabdrucks zulässig ist,
- ein biometrischer Lichtbildabgleich durch einen Skiliftbetreiber durchgeführt werden darf,
- die zielgerichtete Außenwerbung durch biometrische Gesichtsanalyse erlaubt sein kann und
- bereits eine herkömmliche Videoüberwachung im Juweliergeschäft eine Verarbeitung biometrischer Daten darstellt.

Aus rechtlicher Sicht besonders spannend – und damit auch besonders umstritten – war bei der Erarbeitung des Positionspapiers die Frage, ob und ab welchem Zeitpunkt Bildaufnahmen von Gesichtern „biometrische Daten" sind und welche Voraussetzungen erfüllt sein müssen, damit sie als „besondere Kategorien personenbezogener Daten" gelten, deren Verarbeitung grundsätzlich untersagt und nur unter den engen Voraussetzungen des Art. 9 Abs. 2 DSGVO zulässig ist.

Biometrische Daten

Bei biometrischen Daten handelt es sich gemäß Art. 4 Nr. 14 DSGVO um mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

Das Positionspapier betrachtet das Gesichtsbild als ein biometrisches Datum im Sinne des Art. 4 Nr. 14 DSGVO. Im Gegensatz dazu sind Videoaufnahmen von Personen nicht per se biometrische Daten gemäß Art. 4 Nr. 14 DSGVO. Auf Lichtbildern oder Videoaufnahmen können aber biometrische Daten enthalten sein, wenn das Gesicht einer Person in entsprechender Auflösung, Ausrichtung und Größe auf dem Lichtbild oder der Videoaufnahme abgebildet wird.

Biometrische Daten zählen aufgrund ihrer Vielfältigkeit aber nur dann zu den sogenannten „besonderen Kategorien personenbezogener Daten", wenn sie mit besonderer Zweckbestimmung, nämlich zur eindeutigen Identifizierung, und damit in besonders risikobehafteter Weise verarbeitet werden. Dieses erhöhte Risiko besteht nur dann, wenn automatisierte biometrische Erkennungsverfahren eingesetzt werden. Eine herkömmliche Videoüberwachung kann also zwar biometrische Daten enthalten, verarbeitet nur deshalb aber nicht zwingend „besondere Kategorien personenbezogener Daten".

Das Positionspapier zur biometrischen Analyse ist auf der Webseite der Datenschutzkonferenz als Orientierungshilfe veröffentlicht worden und abrufbar unter:

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

Kurzlink: *https://uldsh.de/tb38-545*

06

KERNPUNKTE

Dokumentation von IT-Verfahren

Standard-Datenschutzmodell V2

Abschätzen des Datenschutzrisikos

6 Systemdatenschutz

6.1 Fokus Schleswig-Holstein

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

Wie in den Vorjahren war das ULD Gast bei den Sitzungen der ITBK (IT-Beauftragten-Konferenz), bei der die IT-Beauftragten der Ressorts zusammen mit dem ZIT SH die zentralen und dezentralen IT-Entwicklungen planen sowie Entscheidungen von ressortübergreifender Bedeutung treffen. Durch die Teilnahme wird das ULD über diese Entwicklungen informiert und kann auf datenschutzrechtliche Fallstricke hinweisen oder Empfehlungen zur technisch-organisatorischen Realisierung geben.

Zusätzlich wurde das ULD über einzelne IT-Vorhaben der Ressorts, die eine besondere Bedeutung oder eine große Reichweite haben, direkt durch das ZIT SH informiert.

Die Tendenz zur Zentralisierung von IT-Verfahren setzt sich weiter fort. Dies betrifft in erster Linie das Management der Standard-IT-Verfahren (z. B. für die Bürokommunikation) und die zentrale Bereitstellung von Fachverfahren und Diensten. Eine weitere Rolle spielt die Zentralisierung einzelner Verwaltungstätigkeiten bei gleichzeitig dezentraler Zuarbeit. Ein Beispiel hierfür ist der geplante Prozess der Genehmigung und Abrechnung von Dienstreisen, die nämlich dezentral genehmigt und zentral abgerechnet werden sollen. In einer papierbasierten Welt würden bei solchen Prozessen Schriftstücke zwischen Dienststellen ausgetauscht; in der digitalen Welt werden üblicherweise Plattformen oder Portale verwendet. In dem geschilderten Prozess besteht die Herausforderung darin, dass für die Genehmigungsprozesse in zahlreichen Dienststellen nahezu alle Beschäftigten einschließlich ihrer Vorgesetzten an die Plattform anzubinden wären, die ihrerseits wegen der Sensibilität der Daten und der unmittelbaren finanziellen Auswirkungen bei der Abrechnung besonders zu sichern ist. Dies ist nicht immer einfach, insbesondere wenn Beschäftigte keinen PC-Arbeitsplatz im Landesnetz haben.

Eine zentrale Bereitstellung von Verfahren und Diensten kann Vorteile für einen datenschutzgerechten Betrieb haben, weil die personellen Kapazitäten für die datenschutzgerechte Auswahl und Gestaltung konzentriert werden können. In der Praxis zeigen sich dann aber Probleme, wenn Anbieter von Lösungen oder Softwareprodukten nicht die Besonderheiten der Verwaltung in einer verteilten Umgebung berücksichtigen (können) – eine formelle Behördenhierarchie mit Dienst- und Fachaufsicht ist eben nicht damit gleichbedeutend, dass übergeordnete Behörden stets Zugriffsrechte auf sämtliche Unterlagen der nachgeordneten Behörden haben oder gar in deren Berechtigungsmanagement eingreifen.

6.1.2 Dokumentation von IT-Verfahren

Die Datenschutz-Grundverordnung erfordert von Verantwortlichen den Nachweis, dass die Verarbeitung personenbezogener Daten gemäß den rechtlichen Vorgaben erfolgt (Rechenschaftspflicht, Art. 5 Abs. 2 DSGVO). Eine Standardmaßnahme des Nachweises ist die Dokumentation der Verarbeitung.

In Artikel 30 DSGVO ist festgelegt, dass Verantwortliche ein Verzeichnis der Verarbeitungstä-

tigkeiten zu führen haben. Auch der (Mindest-) Inhalt ist dort festgeschrieben. Allerdings sind die dort verwendeten Begriffe hinsichtlich Art und Detaillierungstiefe interpretierbar, sodass Muster und Vorlagen bei den Aufsichtsbehörden nachgefragt werden.

Das ULD stellt auf seiner Webseite ein Muster für ein solches Verzeichnis sowie weitere Unterlagen zur Verfügung, die Verantwortliche bei der Zusammenstellung der Informationen in ihren Organisationen unterstützen (37. TB, Tz. 6.1.3): Eine der Herausforderungen der Praxis besteht nämlich darin, das an vielen Stellen (z. B. Fachabteilung, Organisationsabteilung, IT-Bereich) verteilte Wissen zusammenzuführen und passend zu den Anforderungen der DSGVO zu dokumentieren.

Nur ein Teil dieser Informationen fließt unmittelbar in das Verzeichnis der Verarbeitungstätigkeiten gemäß DSGVO. Viele weitere Aspekte sind ebenfalls zu dokumentieren: etwa die Rechtsgrundlagen der Verarbeitung, der Umgang mit zu löschenden bzw. zu archivierenden Daten bis hin zu technischen Details wie Hardware, Vernetzung oder Betriebssystemen. Hierbei ist der Verantwortliche in der Wahl des Dokumentationsformats frei.

Bei einer initialen Erhebung ist es sinnvoll, auch diese Informationen sofort strukturiert zu erfassen und dann in weiteren Dokumenten abzulegen. Die Herausforderung besteht darin, durch geschickte Verweisungen Dopplungen zu vermeiden, denn anderenfalls lassen sich die Dokumente nur mit großem Aufwand aktuell halten. Dazu dienen u. a. die vorgestellten Dokumentationsmuster. Im Berichtszeitraum gab es dazu mehrere Schulungen und Workshops mit öffentlichen Stellen sowie Prüferinnen und Prüfern, die positive Rückmeldungen über die Brauchbarkeit der Vorlagen gaben.

Im 37. Tätigkeitsbericht wurde die Veröffentlichung von Hinweisen des ULD zur Dokumentation angekündigt, die die zum 31.12.2018 außer Kraft getretene Datenschutzverordnung Schleswig-Holstein (DSVO) ersetzen. Sie nehmen über die reine Dokumentation eines bestehenden Verfahrens auch Aspekte der Planung (Spezifikation) und der Protokollierung auf. Diese Hinweise wurden Anfang des Jahres 2020 veröffentlicht. Anders als bei einer vergleichsweise statischen Landesverordnung können diese Hinweise bei Änderungsbedarfen auch kurzfristig angepasst werden. Daher sind Kommentare zur Praktikabilität sowie Änderungsbedarfe willkommen.

https://www.datenschutzzentrum.de/dokumentation/

6.2 Zusammenarbeit der Datenschutzbeauftragten zu Systemdatenschutz

Im Jahr 2019 hat der Arbeitskreis Technik der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Reihe von Anwendungshinweisen publiziert, an deren Erarbeitung das ULD vielfach beteiligt war. Drei Themenbereiche sind für die Praxis von besonderer Bedeutung: Windows 10 (Tz. 6.2.1), Messenger-Dienste im Krankenhaus (Tz. 6.2.2) und das Standard-Datenschutzmodell (Tz. 6.2.3).

Neben der Zusammenarbeit auf Bundesebene ist die Kooperation auf Landesebene mit den behördlichen Datenschutzbeauftragten hervorzuheben, beispielsweise zur Durchführung von Schwellwertanalysen und von Datenschutz-Folgenabschätzungen in der Verwaltung (Tz. 6.2.4).

6.2.1 Das Windows-10-Prüfschema

Der Arbeitskreis Technik hat unter dem Titel „Datenschutz bei Windows 10“ ein Prüfschema für Windows 10 publiziert, das inzwischen auch von der DSK verabschiedet wurde. Das Prüfschema „soll Verantwortliche, die Windows 10 bereits einsetzen oder dies beabsichtigen, in die Lage versetzen, eigenständig die Einhaltung der rechtlichen Vorgaben der DSGVO in ihrem konkreten Fall zu prüfen und zu dokumentieren“. Adressaten des Prüfschemas sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen. Zu berücksichtigen ist, dass diejenigen Stellen, die personenbezogene Daten mithilfe von Windows 10 verarbeiten, Verantwortliche im Sinne des Datenschutzrechts sind. Aber auch Microsoft selbst ist für einige Verarbeitungen Verantwortlicher.

In diesen Hinweisen zu Windows 10 wird betont, dass zum einen ein letztlich nicht kontrollierbares Abfließen zumindest von Telemetriedaten erfolgt und zum anderen durch den Umstand, dass Updates nicht unterbunden werden können, sich die Eigenschaften eines Windows-10-Systems vollständig ändern können. Daraus folgt auch, dass eine Aussage darüber, ob Windows 10 datenschutzkonform sei, nicht pauschal getroffen werden kann.

Nach einem Überblick in Kapitel A werden in Kapitel B mit Hinweisen für die rechtliche Prüfung drei Fallgruppen bezüglich der Übermittlung personenbezogener Daten unterschieden, wobei für eine Übermittlung von Daten an Microsoft eine Rechtsgrundlage im Kontext des internationalen Datenverkehrs bereitstehen muss. Im abschließenden Kapitel C sind die sieben zu durchlaufenden Prüfschritte aufgeführt.

Zu diesem 12-seitigen Text gibt es eine Anlage, in der sowohl allgemeine technische Aspekte als auch Windows-spezifische Sachverhalte angesprochen werden. Dazu gehört ein Überblick über die verschiedenen Editionen von Windows 10 und die jeweils integrierten Funktionen und Applikationen. Ein eigener Abschnitt zu Telemetriedaten beschreibt verschiedene Stufen der Datenübermittlungen an Microsoft. Dieser Abschnitt zeigt zudem auf, welche Maßnahmen getroffen werden können, um die Übermittlung personenbezogener Daten an Microsoft einzuschränken. Im Anschluss werden die verschiedenen Updatekonzepte beschrieben, wobei zu berücksichtigen ist, dass die Mehrzahl der Windows-10-Versionen (wie z. B. Windows 10 Version 1909) nur eine begrenzte Laufzeit von 18 bis 30 Monaten hat und danach nicht mehr mit Sicherheitspatches unterstützt wird. Somit sind Verantwortliche quasi gezwungen, Funktionsupdates in kurzen Zyklen einzuspielen und die Prüfschritte erneut zu durchlaufen.

Zum Schluss finden sich Referenzen auf weitere, vor allem sicherheitstechnische Untersuchungen zu Windows 10, wie die des Bundesamts der Sicherheit in der Informationstechnik (BSI) und der niederländischen Datenschutzaufsichtsbehörde.

https://www.datenschutzkonferenz-online.de/media/ah/20191106_win10_pruefschema_dsk.pdf

Kurzlink: *https://uldsh.de/tb38-621*

6.2.2 Messenger-Dienste im Krankenhaus

Aufgrund der im privaten Bereich weitverbreiteten und etablierten Nutzung wird auf Messenger-Dienste zunehmend auch im Gesundheitsbereich zurückgegriffen, häufig verbunden mit der Nutzung eines privaten Endgeräts. Der berufliche oder gewerbliche Einsatz von Messenger-Diensten unterliegt gesetzlichen Datenschutzvorgaben, denen gängige Messenger-Dienste bislang nicht oder nur bedingt entsprechen. Insbesondere der vielfach genutzte Dienst WhatsApp führt bei einer geschäftlichen Nutzung zu einer Reihe von Problemen, die einen Einsatz im Krankenhaus weitgehend ausschließen. Das sieben Seiten umfassende White

Paper „Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich" der DSK formuliert konkrete funktionale Anforderungen zu den Themen Messenger-Applikation, zur Sicherung der Kommunikation, zur Sicherheit der Endgeräte sowie zur Sicherung der Plattform und des Betriebs.

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

Kurzlink: *https://uldsh.de/tb38-622*

6.2.3 Standard-Datenschutzmodell V2: das SDM wird erwachsen

Die DSK hat im November 2019 das Standard-Datenschutzmodell in der Version 2.0 (SDM-V2) verabschiedet. Das SDM stellt mit einem Umfang von 68 Seiten ein Werkzeug bereit, „[…] mit dem die Auswahl und Bewertung technischer und organisatorischer Maßnahmen unterstützt wird, die sicherstellen und den Nachweis dafür erbringen, dass die Verarbeitung personenbezogener Daten nach den Vorgaben der DSGVO erfolgt". Es ist nicht mehr wie bisher als Erprobungsfassung ausgewiesen, sondern gilt nunmehr als praxiserprobt und stabil.

Die Entwicklung des SDM begann 2012 im ULD. Bis heute besteht das Modell aus drei wesentlichen Elementen:

1. Gewährleistungsziele:

Normative Anforderungen aus dem Datenschutzrecht werden durch Gewährleistungsziele aufgenommen, die ihrerseits mit konkreten Maßnahmen hinterlegt sind. So beschreibt das Gewährleistungsziel „Intervenierbarkeit" in SDM-V2 die Anforderung an einen Verantwortlichen, die Rechte von Betroffenen (u. a. Auskunft, Löschung, Berichtigungen, Einschränkungen) auch praktisch umsetzen zu können. Maßnahmen hierzu sind beispielsweise interne Prozesse für die Bearbeitung der Kommunikation mit Betroffenen sowie eine geeignete Gestaltung der Verfahren bis hin zu der Möglichkeit, einzelne Datenfelder oder Verarbeitungsschritte deaktivieren zu können.

2. Risikostufen:

Die Risiken, die von einer Verarbeitungstätigkeit mit personenbezogenen Daten ausgehen, werden in Stufen unterschieden. Die DSGVO gibt hier zwei Stufen vor: geringes/normales Risiko für die Rechte und Freiheiten natürlicher Personen, die grundsätzlich immer bestehen, und hohes Risiko. Diese Abstufung hilft insbesondere, um bei hohem Risiko die Schutzmaßnahmen besonders wirksam auszugestalten. So sollten Protokolldaten, die Inhaltsdaten oder Verfahren mit einem hohen Risiko betreffen, zunächst inhaltlich auf ihre Erforderlichkeit hin überprüft und dann revisionsfest und verschlüsselt gespeichert werden.

3. Daten, IT-Systeme und Prozesse:

Als dritte Komponente empfiehlt das Modell, bei personenbezogenen Verarbeitungstätigkeiten die dafür erforderlichen Daten, die dafür genutzten IT-Systeme und die darin genutzten Teilprozesse einzelner Verarbeitungsschritte zu unterscheiden. Alle Maßnahmen sollten entsprechend ihrer Risikostufe auf jeweils diese Komponenten spezifisch bezogen werden. So sollten Protokolldaten von Programmen und IT-Systemen sowie von unterschiedlichen Teilaktivitäten eines Verfahrens (z. B. inhaltliche Verarbeitungen) für Prüfungen gespeichert werden.

Was ist in der Version V2 neu hinzugekommen?

Der Text wurde neu gegliedert, er umfasst fünf Hauptkapitel: Kapitel A weist den Zweck und den Anwendungsbereich des SDM aus, Kapitel B versammelt die wesentlichen operativen Anforderungen der DSGVO und Kapitel C bildet die über die DSGVO verstreuten normativen Anforderungen systematisch auf den sieben Gewährleistungszielen ab. Kapitel D listet generische Maßnahmen auf und erläutert darüber

hinaus die Abgrenzung von Verarbeitungstätigkeiten, die Bestimmung der Risikostufe und die Struktur eines Datenschutzmanagements. Im Kapitel E wird u. a. der Bezug zum IT-Grundschutz des BSI hergestellt und das Verfahren beschrieben, mit dem Änderungen am Modell initiiert werden können.

Wesentliche Anforderungen aus der DSGVO

In Abschnitt B wurden dreiundzwanzig wesentliche operative Anforderungen zusammengetragen, die sich in der DSGVO, teils wiederholt, an verschiedenen Stellen finden. Beispielhaft sei hier das „Einwilligungsmanagement" genannt. Es besagt, dass bei der Gestaltung einer Verarbeitung darauf zu achten ist, dass Einwilligungen einzuholen und diese zu speichern sind, dass sie dem Nachweis dienen und vor allem dass sie von den Betroffenen widerrufen werden können. Auf die Umsetzung der Anforderungen ist während der Spezifikationsphase einer Verarbeitung bzw. beim Kauf eines Fachprogramms zu achten.

Katalog generischer Maßnahmen

Der bestehende Katalog mit generischen Maßnahmen wurde um weitere Maßnahmen ergänzt. Verantwortliche sollten sich an diesen Maßnahmen orientieren und diese auf die spezifischen Umstände ihrer Verarbeitungstätigkeiten anpassen.

Die generischen Maßnahmen werden in sogenannten Bausteinen weiter erläutert und in kleinteilige Referenzmaßnahmen zerlegt. So wird beispielsweise die generische Maßnahme „Protokollierung" im Baustein weiter spezifiziert, und es werden Teilmaßnahmen (etwa Festlegungen der zu protokollierenden Daten, Zugriffsberechtigungen, Auswertungskonzepte bis hin zur Löschung) beschrieben. Eine Unterarbeitsgruppe des AK Technik arbeitet daran, zu den bislang publizierten sieben Bausteinen, die von einigen Bundesländern sowie der Evangelischen Kirche Deutschland publiziert wurden, weitere Bausteine zu veröffentlichen.

Verarbeitungstätigkeit und Zweck

Das für die DSGVO zentrale Konzept der personenbezogenen „Verarbeitung" oder „Verarbeitungstätigkeit" wurde mit Bezug zum Zweck praxisnäher erläutert (siehe zur Definition die 14 Subprozesse in Art. 4 Abs. 2 DSGVO).

Wesentlicher Kern zur Beschreibung einer Verarbeitungstätigkeit ist die eng beschränkte Bestimmung des Zwecks. Mit Bezug zum Zweck sind vier Aspekte zu unterscheiden: die Zwecksetzung, die Zweckbeschreibung, die Zwecktrennung und die Zweckbindung. Die Zwecksetzung einer Verarbeitung muss legitim sein. Die Zweckbeschreibung berücksichtigt die Rechtskonformität und idealerweise die Umsetzung der Grundsätze aus Artikel 5 DSGVO. Die Ausführungen zur Zwecktrennung begegnen den absehbaren zweckändernden oder zweckdehnenden Begehrlichkeiten aus benachbarten Bereichen der Verarbeitung. Abschließend ist in Bezug zur Zweckbindung darauf zu achten, dass mit der Nutzung von IT-Komponenten die begrenzenden Eigenschaften, die Teil der Beschreibung des Zwecks und der Trennung zu anderen Zwecken sind, nicht unterlaufen werden.

Risikotypisierung

Von besonderem Wert für die Praxis sind sicher auch die Ausführungen zum „Risiko" von Verarbeitungstätigkeiten. Hier wurden insbesondere die Ende 2018 von der DSK verabschiedeten Risikopapiere Nr. 5 („Datenschutz-Folgenabschätzung") und Nr. 18 („Risiko") sowie das Working Paper 248 („WP 248") des Europäischen Datenschutzausschusses zur Datenschutz-Folgenabschätzung berücksichtigt. Im Wesentlichen formulieren die Grundsätze aus Artikel 5 der DSGVO die Risiken des Datenschutzes: Wenn die Verarbeitung diesen Grundsätzen nicht oder nicht zumindest ausreichend folgt, resultiert daraus ein Risiko. Drei Konzepte zur Erfassung und Bearbeitung von Risiken sind hervorzuheben: (a) die Typisierung der Risiken, (b) die Einschätzung der Risikohöhe und (c) die Strategie zur Risikominimierung.

(a) Risikotypisierung:

- Risikotyp 1: Der Grundrechtseingriff wird nicht so milde, wie vom Zweck her bestimmbar, gestaltet. Dieses Risiko wird durch die Ausgestaltung der Verarbeitungstätigkeit und der Vorgaben des

Datenschutzes „by Design“ und Datenschutzes „by Default“ (vgl. Artikel 25 DSGVO) primär bearbeitet.

- Risikotyp 2: Schutzmaßnahmen zur Milderung des Grundrechtseingriffs werden gar nicht, nicht hinreichend oder falsch bestimmt, betrieben und überwacht. Dieses Risiko kann durch ein reifes Datenschutzmanagement verringert werden.
- Risikotyp 3: Schutzmaßnahmen der IT-Sicherheit werden gar nicht, nicht hinreichend oder falsch betrieben und überwacht. Dieses Risiko kann in Zusammenarbeit mit der IT-Sicherheit verringert werden. Zu beachten ist dabei, dass die Schutzmaßnahmen der IT-Sicherheit ihrerseits datenschutzgerecht umgesetzt werden.

(b) Einschätzung der Risikohöhe:

Zur Einschätzung der Risikohöhe einer Verarbeitungstätigkeit empfiehlt das SDM-V2 eine Abfolge von vier Prüfschritten:

- die „Muss-Liste“ für Datenschutz-Folgenabschätzungen gemäß Art. 35 Abs. 4 DSGVO,
- die Kriterien von Art. 35 Abs. 3 DSGVO,
- die Hinweise des Working Paper 248 zu Datenschutz-Folgenabschätzungen sowie
- die Anhaltspunkte aus dem Erwägungsgrund 76 der DSGVO.

(c) Strategie zur Risikominimierung:

Zur Bestimmung der Schutzmaßnahmen zur Risikominimierung empfiehlt das SDM-V2 folgende Strategie: Das Risiko der Verarbeitungstätigkeit wird zunächst unter der Annahme betrachtet, dass es keinerlei Schutzmechanismen gibt – das SDM spricht vom Ausgangsrisiko, das die „reine Verarbeitungstätigkeit“, die von einer Organisation zumeist mit IT-Unterstützung betrieben wird, für die Freiheiten und Rechte betroffener Personen erzeugt. Dieses Risiko hat einen Schutzbedarf bei der betroffenen Person zur Folge, der sich aus dem Risiko der Verarbeitungstätigkeit ergibt, bevor technische und organisatorische Maßnahmen bestimmt und umgesetzt werden. Wenn sich in der Schwellwertanalyse herausstellt, dass ein normales Risiko von einer Verarbeitungstätigkeit ausgeht, ist auch der Schutzbedarf der Person normal, ein hohes Risiko erzeugt entsprechend einen hohen Schutzbedarf.

Während der Schutzbedarf der betroffenen Personen im Hinblick auf die Verarbeitungstätigkeit konstant bleibt, können die Risiken der Verarbeitungstätigkeit durch die Gestaltung der Verarbeitung und den Betrieb von Schutzmaßnahmen verringert werden. Die (Rest-)Risiken müssen so weit verringert werden, bis sich ein angemessenes Schutzniveau ergibt, das die Anforderungen der DSGVO erfüllt.

Besteht ein hoher Schutzbedarf, können zusätzliche Schutzmaßnahmen erforderlich sein. Das Modell empfiehlt folgendes Vorgehen:

1. Es sind die Maßnahmen des Referenzmaßnahmenkatalogs umzusetzen, die bei normalem Ausgangsrisiko bzw. normalem Schutzbedarf zu ergreifen sind.
2. Zusätzliche Maßnahmen aus dem Referenzmaßnahmenkatalog sind umzusetzen.
3. Zusätzlich sind individuelle Maßnahmen auszuwählen, etwa bestimmte Vorgänge einer Verarbeitungstätigkeit nur auf Antrag bzw. nach einer expliziten Prüfung freizugeben und diese Tätigkeit dann im Betrieb zu überwachen.
4. Die Wirksamkeit einer Maßnahme kann erhöht werden, indem Skalierungsmöglichkeiten genutzt werden. Ein Beispiel wäre der Betrieb dedizierter Protokollserver, die an zentraler Stelle sämtliche Protokolldaten speichern und den Zugriff durch Administratoren einschränken.
5. Auf die getroffenen Maßnahmen können ihrerseits besonders wirksame technische und organisatorische Schutzmaßnahmen (etwa zum Schutz von Trennung, Transparenz, Integrität oder Vertraulichkeit) angewendet werden.

Datenschutzmanagement

Als Datenschutzmanagementsystem bezeichnet man das systematische und organisationsweite Zusammenspiel von Planung, Betrieb und Überwachung von Datenschutzanforderungen

und Datenschutzmaßnahmen (vgl. Art. 32 Abs. 1 Buchst. d DSGVO). Es lassen sich vier Komponenten des Datenschutzmanagements identifizieren, die an das Vorgehen beim Qualitätsmanagement (sogenannter PDCA-Zyklus) angelehnt sind:

- Plan – Es sind Schutzmaßnahmen zu bestimmen, deren Prüffähigkeit zu spezifizieren ist. Das Produkt dieser Phase ist eine Spezifikation bzw. ein Plan, oder es sind Konzepte auf Maßnahmenebene.
- Do – Die Verarbeitungstätigkeit ist anhand der geplanten Komponenten und Aktivitäten zu gestalten, dabei sind die Schutzmaßnahmen einschließlich deren Prüfbarkeit zu implementieren. In dieser Phase werden Prüfergebnisse erzeugt.
- Check 1 – Prüfergebnisse funktionaler Soll-Ist-Differenzen werden so aufbereitet, dass sie rechtlich beurteilt werden können.
- Check 2 – Rechtliche Beurteilungen der funktionalen Prüfergebnisse erzeugen begründete Änderungsbedarfe.
- Act – Aus diesen Änderungsbedarfen sind Maßnahmen zu erarbeiten und umzusetzen, sodass zyklisch wieder in die konkrete Planung von Verarbeitungstätigkeiten oder von deren gemeinsamen Infrastrukturen eingestiegen werden kann.

Die Teilprozesse „Plan", „Do" und „Check" können für eine einzelne Verarbeitungstätigkeit mit einer Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO weitgehend zusammenfallen. Das Umsetzen der Schutzmaßnahmen („Act") würde auf eine positiv beendete DSFA folgen.

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

https://www.datenschutzkonferenz-online.de/media/ah/20191209_sdm-methode_v2.0a.pdf

Kurzlink: *https://uldsh.de/tb38-623*

6.2.4 Das Datenschutzrisiko systematisch abschätzen und beurteilen

2019 haben die Kommunen, Kreise und Ministerien damit begonnen, systematisch Schwellwertanalysen durchzuführen. Nach diesen Schwellwertanalysen, die für jede Verarbeitungstätigkeit obligatorisch sind, mussten in den Fällen mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen Datenschutz-Folgenabschätzungen (DSFA) gemäß Artikel 35 DSGVO durchgeführt werden. Eine DSFA dient der Bestimmung von angemessenen Schutzmaßnahmen für eine (geplante) Verarbeitungstätigkeit. Artikel 35 DSGVO verlangt neben einem DSFA-Bericht vom Verantwortlichen auch den Nachweis über die Wirksamkeit der aufgrund des Berichts umzusetzenden Schutzmaßnahmen zur Eindämmung des Risikos.

Das ULD war an der Erarbeitung einer systematischen Vorgehensweise zur Durchführung von Schwellwertanalysen und zur methodischen Durchführung von Datenschutz-Folgenabschätzungen im Bereich der öffentlichen Verwaltungen beteiligt. Grundlegende Vorarbeiten wurden durch die DSK in Form der Kurzpapiere Nr. 5 („Datenschutz-Folgenabschätzung") und Nr. 18 („Risiko") sowie des Standard-Datenschutzmodells (SDM-V2) zur Bestimmung von Schutzmaßnahmen geleistet. An diesen Vorarbeiten war das ULD ebenfalls maßgeblich beteiligt.

Zusammen mit dem Zentralen IT-Management des Landes Schleswig-Holstein (ZIT SH) wurden Formulare zur Durchführung von Schwellwertanalysen für Verarbeitungstätigkeiten im Bereich der Ministerien erarbeitet. In Zusammenarbeit mit der Datenschutzbeauftragten des Kreises Stormarn wurden außerdem für die Kreise und Kommunen ein Konzept erstellt und ein Programm entwickelt, das Projektleitungen bei der vollständigen Durchführung einer DSFA unterstützt. Erprobt wurde dieses Programm im Rahmen von Datenschutz-Folgenabschätzungen für ein Bewerberportal sowie zur Durchführung von Wahlen (Kommunalwahlen bis zu EU-Wahlen) in den Kreisen Nordfriesland und Schleswig-Flensburg. Bei der DSFA für die Wahlverwaltung wurde methodisch, wie es das

Kurzpapier Nr. 5 vorsieht, in vier Phasen vorgegangen. Nach der Vorbereitung folgten eine Erhebungs- und eine Durchführungsphase, die mit dem DSFA-Bericht abschloss. Aktuell befindet sich das Projekt in der Umsetzungsphase.

In der Vorbereitungsphase ist eine Verarbeitungsdokumentation (Art. 5 Abs. 2 und Art. 24 Abs. 1 DSGVO) zu erstellen. Alle zur Bewertung erforderlichen Daten sollen sich aus dieser Dokumentation und dem Verzeichnis der Verarbeitungstätigkeit (Artikel 30 DSGVO) ergeben. In dem vorliegenden Fall war das Programm zur Verwaltung von Wahlverfahren bereits kurzfristig beschafft worden – nachzuholen waren daher die Dokumentation und Beteiligung der behördlichen Datenschutzbeauftragten (Art. 38 Abs. 1 DSGVO). Für die Durchführung der Schwellwertanalyse und der DSFA wurde ein Kernteam bestehend aus einer Moderatorin/Projektmanagerin, einer Anwenderin, Vertretern der Technik und der Datenschutzbeauftragten als Beraterin (Art. 39 Abs. 1 Buchst. a DSGVO) gebildet.

In der Erhebungsphase wurden neben dem Projektteam weitere Anwenderinnen und Anwender, interessierte betriebliche Datenschutzbeauftragte, Vertreter des Rechenzentrums sowie die Wahlleitung beteiligt. Gemeinsam erhoben die Mitwirkenden die datenschutzrechtlich bedeutsamen Eigenschaften anhand der Gewährleistungsziele des Standard-Datenschutzmodells mit Bezug auf Daten, IT-Systeme und Prozesse. Die Durchführungsphase begann mit der Schwellwertanalyse. Diese endete mit dem gemeinsamen Ergebnis, dass ein hohes Risiko der Verarbeitungstätigkeit vorliegt. Das zur Durchführung einer DSFA verwendete Programm erlaubte es zum Schluss, die Risiken der Verarbeitungstätigkeit einmal ohne Schutzmaßnahmen und einmal mit denkbaren Schutzmaßnahmen zu visualisieren, wodurch eine Priorisierung von zu treffenden Maßnahmen nahegelegt wurde („Quick Wins").

Das Kernteam erstellte den DSFA-Bericht und übergab ihn dem Verantwortlichen mit Empfehlungen für zu treffende Maßnahmen entsprechend dem SDM. Die Aufgabe der DSFA-Projektmanagerin war damit beendet.

Offengeblieben war vor allem der Aspekt der Klärung der Verwendung von Schnittstellen zu anderen Verarbeitungstätigkeiten. Die Aufgaben der Beratung und der Revision bezüglich der Bearbeitung offener Punkte und der Umsetzung der empfohlenen Maßnahmen durch die Datenschutzbeauftragte läuft gegenwärtig.

Als Fazit zeigte es sich, dass bei der Erhebung und Beurteilung der Risiken möglichst alle an der Verarbeitung beteiligten Institutionen bzw. Fachbereiche zusammenkommen sollten. Es bedarf dann einer erfahrenen Projektleitung, die idealerweise über Kenntnisse auch zur Verarbeitungstätigkeit verfügt, um eine DSFA effektiv und effizient durchführen zu können. Ein Programm kann hier unterstützend eingesetzt werden, um für das Team die aufgedeckten Schwächen bzw. die zu mindernden Risiken nachverfolgbar zu machen und die Ergebnisse festzuhalten. Schon in dieser Phase kann dann Einvernehmen darüber hergestellt werden, in welcher Reihenfolge die zu ergreifenden Maßnahmen geplant und umgesetzt werden. Das eingesetzte Programm zur Unterstützung der Durchführung einer DSFA ist darüber hinaus so gestaltet, dass es auch die Umsetzungsphase unterstützt, deren Ergebnisse dann wiederum typischerweise von der Datenschutzbeauftragten geprüft werden.

Was ist zu tun?

Die öffentlichen Verwaltungen in Schleswig-Holstein sollten einen Pool an Expertinnen und Experten zur Durchführung von Datenschutz-Folgenabschätzungen bilden, von denen sich die Verantwortlichen in den Kommunen, Kreisen und Landesverwaltungen unterstützen lassen können.

6.3 Ausgewählte Ergebnisse aus Beratungen und Prüfungen

6.3.1 Zusammenarbeit mit den Spitzenorganisationen der Gewerkschaften

Wie in den Vorjahren war auch im Berichtszeitraum das ULD in die Zusammenarbeit der Landesbehörden, insbesondere des ZIT SH, mit den Spitzenorganisationen der Gewerkschaften eingebunden.

An dieser Stelle geht es zum einen um die Information der Spitzenorganisationen über gegebenenfalls mitbestimmungspflichtige Datenverarbeitungen, zum anderen um die Formulierung sogenannter 59er-Vereinbarungen auf Landesebene, durch die eine Mitbestimmung erfolgen kann.

59er-Vereinbarung

Vereinbarungen gemäß § 59 Mitbestimmungsgesetz zwischen den Spitzenorganisationen der Gewerkschaften und der zuständigen obersten Landesbehörde, die als allgemeine Mitbestimmungsregelungen über den Geschäftsbereich einer obersten Landesbehörde hinausgehen („Dienstvereinbarung auf Landesebene").

Konkrete Fälle waren u. a. die landesweit zentralisierte Verarbeitung von Personaldaten und dort die zugrunde liegenden IT-Verfahren (KoPers, Permis-V) und ihr Zusammenspiel. Hier ging es um die Aktualisierung und Anpassung einer 59er-Vereinbarung an die tatsächlichen Gegebenheiten.

Ein weiterer Fall betraf die zentrale Organisation des IT-Managements durch das ZIT SH, das mit einem neuen IT-Verfahren die Zusammenarbeit zwischen Dienstleistern (in erster Linie Dataport), zentralen Stellen (z. B. ZIT SH), IT-Verantwortlichen der Ressorts bis hin zu IT-Verantwortlichen vor Ort steuern möchte. Im Mittelpunkt steht dabei die Kommunikation von Arbeitsaufträgen (Tickets) in einem sogenannten Ticketsystem, das den Beteiligten einen gemeinsamen Blick auf die Arbeitsaufträge und den Stand ihrer Erledigung ermöglichen soll.

Dabei stellen sich datenschutzrechtliche Fragen, etwa im Hinblick auf die Daten der handelnden Beschäftigten im IT-Bereich, deren Tätigkeiten in solchen Systemen protokolliert werden. Aber auch Daten von Nutzerinnen und Nutzern, etwa bei Fehlbedienungen von Geräten, finden ihren Weg in solche Systeme, wenn beispielsweise Fehler direkt durch die Nutzenden gemeldet werden oder Fehlerbehebungen oder Gerätetausche mit ihnen koordiniert werden. Die Herausforderung besteht darin, die technische Zusammenarbeit mehrerer Verantwortlicher zu organisieren und Auftraggebern eine Kontrolle über das Ob und Wie der Ausführung eines Auftrags zu erlauben, ohne gleichzeitig eine detaillierte Verhaltens- und Leistungskontrolle über die Beschäftigten der Auftragnehmer zu ermöglichen. Dies kann z. B. durch Beschränkungen von Einsichtsrechten oder Löschungen von nicht mehr erforderlichen Teilinformationen in Tickets erfolgen.

Ein dritter, derzeit laufender Fall betrifft die Vereinbarung zur privaten Nutzung von Internet und E-Mail am Arbeitsplatz. Hier sind keine inhaltlichen Änderungen der Verfahrensweise beim Umgang mit Missbrauchsfällen geplant, aber Anpassungen im Hinblick auf die Speicherdauer von Informationen über Internetzugriffe zu Sicherheitszwecken.

Was ist zu tun?

Die vertrauensvolle Zusammenarbeit mit den Spitzenorganisationen sollte fortgesetzt werden.

6.3.2 Transparenzportal

Zum Januar 2020 tritt im Informationszugangsgesetz (IZG-SH) eine neue Regelung in Kraft. Diese verpflichtet Landesbehörden nicht nur wie bisher, Informationen und Unterlagen auf Anfrage zugänglich zu machen, sondern diese zukünftig aktiv zu veröffentlichen. Einige Details zu den Veröffentlichungspflichten, z. B. welche Behörden verpflichtet sind und welche Art von Informationen zu veröffentlichen sind, finden sich in § 11 IZG-SH (siehe auch Tz. 12.5).

Das Zentrale IT-Management des Landes (ZIT SH) betreibt eine technische Plattform, mit der die Behörden bei ihrer Veröffentlichungspflicht unterstützt werden: das Transparenzportal. Das Portal ermöglicht eine gleichartige Bereitstellung von Informationen an einem Ort, die Durchsuchbarkeit der Informationen und auch eine gleichartige Anreicherung der Informationen durch Metadaten. So sollen beispielsweise Dokumente, die sich auf örtliche Informationen beziehen, so ergänzt werden, dass nicht nur nach Dokumentennamen, sondern auch nach Orten gesucht werden kann.

Das ULD nimmt beratend an einer Steuerungsgruppe des Projekts zum Transparenzportal teil. Aus Sicht des Datenschutzes und des Informationszugangs ist es wichtig, die gesetzlichen Beschränkungen zu beachten, d. h. insbesondere die personenbezogenen Daten sowie Betriebs- und Geschäftsgeheimnisse vom Informationszugang auszunehmen.

Dazu sind zum einen organisatorische Vorkehrungen und zum anderen technische Maßnahmen zu treffen, damit die jeweiligen Behörden die Veröffentlichungsfähigkeit ihrer Unterlagen prüfen und Teile von Informationen, die nicht zu veröffentlichen sind, mit geeigneten technischen Werkzeugen vor der Veröffentlichung schwärzen können.

Das Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung (MELUND) als derzeit zuständiges Ministerium beabsichtigt, die Details in einer Verordnung (Verordnung zur Errichtung des Transparenzportals – TraPortVO) zu regeln. Das ULD wurde zu dem Verordnungsentwurf um Stellungnahme gebeten und hat insbesondere geprüft, inwieweit durch das Transparenzportal personenbezogene Daten verarbeitet werden: In diesem Fall wären der Betreiber des Portals einerseits sowie die veröffentlichenden Behörden andererseits gemeinsam für die Datenverarbeitung verantwortlich und müssten daher datenschutzrechtliche Zuständigkeiten in einer Vereinbarung gemäß Artikel 26 oder einer weiteren Rechtsverordnung regeln (siehe dazu auch Tz. 4.1.2). Eine Verarbeitung personenbezogener Daten ist im Rahmen der Veröffentlichung im Transparenzportal aber nicht geplant, sodass es sich in der zurzeit geplanten Ausgestaltung nicht um ein gemeinsames Verfahren handelt.

6.3.3 Gemeinsame Prüfung des Zentralen Meldedatenbestandes (ZMB) – Update

Im letzten Tätigkeitsbericht (37. TB, Tz. 6.3.3) berichteten wir über eine gemeinsame Prüfung des Zentralen Meldedatenbestandes (ZMB), die die Datenschutzbeauftragten aus Hamburg, Sachsen-Anhalt, Schleswig-Holstein und – mit Gaststatus – auch Bremen durchführten. Gegenstand dieser gemeinsamen Prüfung ist der sogenannte Mehrländer-Meldedatenspiegel (MMS), in dem auf einer technischen Plattform die (Einwohner-)Meldedaten aus den drei Bundesländern Schleswig-Holstein, Sachsen-Anhalt und Hamburg verarbeitet werden.

Die genaue Fragestellung der Prüfung ist, ob die derzeitige technische und organisatorische Ausgestaltung einen getrennten Betrieb dreier landesindividueller Länderspiegeldatenbanken darstellt oder ob nicht durch die Art der Implementierung und der Steuerung des Gesamtverfahrens faktisch ein gemeinsames Verfahren

aller drei beteiligten Länder betrieben wird, das regelnder Dokumente über die Art der Zusammenarbeit bedarf.

ZMB

ZMB bezeichnet den Zentralen Meldedatenbestand, der bei Dataport als Spiegeldatei betrieben wird und der tagesaktuelle Kopien der örtlichen Meldedaten erhält. Diese können an zentraler Stelle von Verwaltungs- und Sicherheitsbehörden im Rahmen und im Umfang ihrer Aufgaben automatisiert abgefragt werden. Ebenso werden diese Daten für die einfache Melderegisterauskunft an Firmen und natürliche Personen genutzt.

Während zunächst die Absicht bestand, die Verfahren vollständig getrennt zu betreiben (was entsprechende technische und organisatorische Trennungsmaßnahmen erfordert), hat sich mittlerweile die Ansicht durchgesetzt, dass die gemeinsamen Aspekte überwiegen und eine gemeinsame Verantwortlichkeit gemäß Artikel 26 DSGVO vorliegt.

Die zuständigen Innenbehörden haben einen Entwurf einer Vereinbarung gemäß Art. 26 Abs. 1 DSGVO erstellt, in dem die jeweiligen Zuständigkeiten geregelt werden sollen. Dieser Entwurf wird derzeit mit den beteiligten Aufsichtsbehörden diskutiert.

Offen ist weiterhin die genaue Ausgestaltung der Protokollierungen von Abrufen durch Strafverfolgungs- und Sicherheitsbehörden, die gemäß § 40 Abs. 3 Bundesmeldegesetz (BMG) – anders als andere Behörden für deren Abrufe und anders als für die sonstigen Melderegisterauskünfte – die Protokollierung selbst vornehmen müssen. Diese speziellen Abrufe sollen nämlich den einzelnen Meldebehörden nicht bekannt werden. Technisch kann eine solche Protokollierung zwar ebenfalls bei Dataport geschehen – allerdings im Auftrag der jeweiligen Behörde und nicht im Auftrag der Meldebehörden.

6.3.4 Artikel-33-Meldungen im öffentlichen und nichtöffentlichen Bereich – die technische Sicht

Im Berichtszeitraum erreichten das ULD zahlreiche Meldungen über Datenschutzvorfälle nach Artikel 33 DSGVO (siehe beispielsweise Tz. 4.1.13 und Tz. 5.4). Meist wurde dazu das vom ULD veröffentlichte Meldeformular verwendet, das die zur Bearbeitung durch das ULD erforderlichen Informationen in strukturierter Form erfasst.

Im überwiegenden Teil der Meldungen, die das ULD erreichten, bestand durch die Datenschutzverletzung tatsächlich ein Risiko für die Betroffenen – es erfolgten also keine unnötigen Meldungen oder „Bagatellmeldungen".

Über die Anzahl der Vorfälle, die nach Artikel 33 meldepflichtig wären, aber fälschlicherweise dem ULD nicht gemeldet wurden (Dunkelziffer), liegen keine Erkenntnisse vor.

Datenschutzvorfall

Eine Meldung eines Datenschutzvorfalls an die zuständige Datenschutzaufsichtsbehörde ist nach Artikel 33 DSGVO erforderlich, wenn ein Risiko für Betroffene durch die Verletzung nicht ausgeschlossen werden kann. Besteht voraussichtlich ein hohes Risiko durch die Datenschutzverletzung, sind die Betroffenen gemäß Artikel 34 zu informieren.

Einige IT-Sicherheits- und Datenschutzvorfälle haben eine solche Tragweite, dass sie presseöffentlich werden. Vergleicht man diese Pressemeldungen mit den dem ULD gemeldeten

Vorfällen, so zeigt sich eine Diskrepanz insbesondere bei solchen Vorfällen, die vermeintlich „nur“ die Integrität oder Verfügbarkeit von Daten betreffen – etwa umfassende IT-Ausfälle, Störungen des Netzverkehrs oder festgestellte Fehlberechnungen von Programmen. Hier wurde von den Verantwortlichen wohl häufig entweder kein Risiko für die betroffenen Personen gesehen oder eine Meldung schlicht versäumt.

Derzeit bilden Meldungen über verlorene oder gestohlene Datenträger und IT-Systeme (etwa Smartphones, Notebooks oder externe Speichermedien), Fehlversendungen (Fax, E-Mail, Brief), interne Fehlkonfigurationen sowie Angriffe auf IT-Systeme (z. B. durch Viren, Ransomware) einen Schwerpunkt in technischer Hinsicht.

Ransomware

Mit den Begriffen Ransomware, Erpressungs- oder Verschlüsselungstrojaner bezeichnet man Schadprogramme, die einen Datenbestand so verschlüsseln, dass er für die Verantwortlichen nicht mehr nutzbar ist. Die Entschlüsselung wird gegen die Zahlung eines Lösegeldes versprochen.

Das tatsächliche Risiko für die Rechte und Freiheiten betroffener Personen ist für Verantwortliche nicht immer sofort ersichtlich, insbesondere bei einem Befall der IT-Systeme mit Schadcode: Hier kommt es darauf an, ob der Schadcode die Datenbestände z. B. „nur“ verschlüsselt oder ob es beim Schadcodebefall auch zu einem Datenabfluss oder einer Datenveränderung gekommen ist. Im ersten Fall ist die Verfügbarkeit der Daten betroffen, im zweiten Fall die Vertraulichkeit oder die Integrität. Um diese Frage seriös beantworten zu können, ist eine Bestimmung des Schadcodes oder die Analyse seiner Wirkungsweise und des Infizierungswegs erforderlich.

Bei der Bearbeitung von Meldungen prüft das ULD neben der Vollständigkeit der Meldung auch die Plausibilität der Risikoeinschätzung der Verantwortlichen, eine eventuelle Pflicht zur Information der betroffenen Personen sowie die Frage, ob die in der Meldung dargestellten technisch-organisatorischen Maßnahmen zur Risikoeindämmung und Verhinderung einer Wiederholung ausreichend sind.

In vielen Fällen sind die ersten Meldungen nicht vollständig. Dies ist häufig nachvollziehbar, da innerhalb der geforderten 72-Stunden-Frist der Meldung meist der Sachverhalt noch nicht vollständig aufgeklärt ist. Insbesondere im Fall einer Infizierung durch Ransomware werden zumeist strafrechtliche Ermittlungen eingeleitet, welche die eigene Analyse des Vorfalls verzögern. Eine Ergänzung der Informationen ist daher möglich und wird vom ULD auch häufig angefordert, um eine abschließende Bewertung des Vorfalls vornehmen zu können.

Bei der Beurteilung der Frage, ob durch die Datenschutzverletzung ein hohes Risiko für die betroffenen Personen besteht und diese folglich zu informieren sind, gibt es teilweise abweichende Bewertungen. In diesen Fällen weist das ULD die Verantwortlichen darauf hin, dass die betroffenen Personen zu informieren sind. Ebenso gibt es Abweichungen bei der Beurteilung, inwieweit technisch-organisatorische Maßnahmen zur Eindämmung des aktuellen Risikos ausreichend sind. Ein Beispiel hierfür ist die Ausbreitung von Schadcode, bei der es nicht genügt, den infizierten Arbeitsplatz-PC vom Schadcode zu säubern. Vielmehr ist zu prüfen, ob der Schadcode keine weiteren Veränderungen im Netz, etwa die unbefugte Einrichtung administrativer Konten, vorgenommen hat. In den recht häufig auftretenden Fällen, in denen eine Ransomware durch die Erlangung von administrativen Rechten des Gesamtsystems („Golden Ticket“) diese Systeme vollständig verschlüsselt, ist das System tief greifend kompromittiert. Daher ist bei der Wiederherstellung der Systeme sicherzustellen, dass dieses „Golden Ticket“ nicht mehr verwendet werden kann; eine Beschreibung der Maßnahmen, wie die Gültigkeit dieses „Golden Tickets“ aufgehoben wird, ist daher für das ULD zur Bewertung absolut erforderlich.

Im Fall von verlorenen oder gestohlenen Geräten wird in den Meldungen zumeist angegeben, dass das entwendete Gerät bzw. die Daten verschlüsselt waren. Dabei ist zu bedenken, dass die Meldungen auch von Personen mit wenig

Bezug zur technischen Realisierung vorgenommen werden können, die möglicherweise einen einfachen Passwortschutz mit einer Verschlüsselung gleichsetzen. Diese Klarstellung sowie die Informationen zur Verschlüsselungsform (Datenbankfeld, Datei, Container, Partition, gesamtes System) und -qualität gehören zu den häufigsten Nachfragen des ULD.

Auch bei den technisch-organisatorischen Maßnahmen, welche die reguläre Verarbeitung absichern, gibt es in Teilen Nachholbedarf. So weist beispielsweise die Erkenntnis, dass zwar eine Datensicherung eingerichtet, diese aber seit Wochen nicht ausgeführt wurde, auf einen organisatorischen Mangel hin. Technisch-organisatorische Maßnahmen sind nicht nur einmalig einzurichten, sondern ihre Funktionsfähigkeit ist fortlaufend zu überprüfen.

In anderen Fällen waren angemessene Maßnahmen getroffen worden, die durch eine Verkettung von Zufällen im Einzelfall aber nicht ausreichten und zu einem Datenschutzvorfall führten, etwa bei Einbrüchen in gesicherte Büros. In diesen Fällen gab es manchmal keinen Nachholbedarf – es liegt schlicht in der Natur der Sache, dass bei risikobasierten Sicherheitsmaßnahmen, wie sie Artikel 32 DSGVO fordert, in Einzelfällen sich das Restrisiko manifestieren kann (zur Verschlüsselung mobiler Datenträger siehe Tz. 4.5.10 und 5.3.5).

Zusammenfassend lässt sich feststellen, dass das ULD durch die Meldepflicht gemäß Artikel 33 DSGVO weiter gehende Einblicke in die Risikostruktur erhält, die für die Beurteilung der Angemessenheit technisch-organisatorischer Maßnahmen wichtige Hinweise liefert.

07

KERNPUNKTE

Entscheidung des Bundesverwaltungsgerichts zu Facebook-Fanpages

Orientierungshilfe für Telemedienanbieter

7 Neue Medien

7.1 Entscheidung des Bundesverwaltungsgerichts zu Facebook-Fanpages

Nachdem der Gerichtshof der Europäischen Union (EuGH) mit Urteil vom 5. Juni 2018 eine gemeinsame datenschutzrechtliche Verantwortlichkeit von Facebook-Fanpage-Betreibern und Facebook angenommen hatte (37. TB, Tz. 7.1), wurde diese Beurteilung durch das Bundesverwaltungsgericht (BVerwG) in Leipzig mit Urteil vom 11. September 2019 bestätigt. Das BVerwG machte deutlich, dass sich das ULD zur Durchsetzung des vom europäischen Gesetzgeber intendierten hohen Datenschutzniveaus vom Gedanken der Effektivität leiten lassen durfte und dabei ermessensfehlerfrei entscheiden konnte, dass die Wirtschaftsakademie Schleswig-Holstein ihre Facebook-Fanpage deaktivieren muss.

Das ULD durfte nach den Ausführungen des Gerichts gerade auch die Wirtschaftsakademie Schleswig-Holstein zur Verantwortung ziehen. Ein Vorgehen gegen Facebook selbst oder gegen Untergliederungen von Facebook war demnach nicht geboten. Das Gericht sah in der Anordnung der Deaktivierung der Facebook-Fanpage ein verhältnismäßiges Mittel.

Das Oberverwaltungsgericht Schleswig hatte zunächst eine datenschutzrechtliche Verantwortung der Wirtschaftsakademie Schleswig-Holstein abgelehnt. Das BVerwG hat das entsprechende Berufungsurteil aufgehoben und den Rechtsstreit zur näheren Beurteilung der Rechtswidrigkeit der Datenverarbeitung und Aufklärung der tatsächlichen Umstände an das Oberverwaltungsgericht Schleswig zurückverwiesen. Die Beurteilung der Rechtswidrigkeit der Datenverarbeitung im Zusammenhang mit dem Betrieb der Facebook-Fanpage muss dabei nach den gesetzlichen Regelungen (insbesondere nach dem Telemediengesetz) erfolgen, die zum Zeitpunkt der letzten Behördenentscheidung im Jahr 2011 galten.

Die Pressemitteilungen des ULD und des BVerwG sind unter folgendem Link abrufbar:

www.datenschutzzentrum.de/artikel/1299-Rueckenwind-fuer-den-Datenschutz-Bundesverwaltungsgerichtsurteil-in-Sachen-Facebook-Fanpages.html

Kurzlink: *https://uldsh.de/tb38-71*

Weiterhin beschäftigen wir uns auch mit den Anforderungen, die im Bereich der sozialen Medien an die gemeinsam Verantwortlichen zu richten sind. Aus diesem Grund leiten wir auch die Taskforce Facebook Fanpages der Datenschutzkonferenz.

Als Zwischenergebnis ist festzuhalten, dass der aktuelle Zustand weiterhin problematisch ist: Bisher ist nicht ersichtlich, dass Facebook-Fanpage-Betreiber und Facebook die Anforderungen an die gemeinsame Verantwortlichkeit nach Artikel 26 DSGVO erfüllen. Es fehlen bisher transparente Vereinbarungen, wer welche Verpflichtungen nach der DSGVO wahrnimmt, insbesondere im Hinblick auf die Rechte der betroffenen Seitenbesucher.

Was ist zu tun?

Über die Beurteilung des BVerwG hinausgehend, erfüllen bisher weder die Betreiber von Facebook-Fanpages noch Facebook die Anforderungen der Datenschutz-Grundverordnung zur gemeinsamen Verantwortlichkeit. Die Pflicht zum Abschluss transparenter Vereinbarungen nach Maßgabe von Artikel 26 DSGVO trifft nicht allein Facebook. Auch die Seitenbetreiber sind aufgefordert zu handeln.

7.2 Veröffentlichung der Orientierungshilfe für Anbieter von Telemedien

Das ULD erhält eine Vielzahl von Beschwerden bezüglich der Gestaltung von Webseiten bzw. der durch den Aufruf von Webseiten ausgelösten Datenverarbeitungsvorgänge. Die Beschwerden richten sich in den meisten Fällen insbesondere gegen sogenannte Cookie-Banner, die bei einem ersten Aufruf der Seite eingeblendet werden. Häufig enthalten diese sinngemäß folgenden Text:

„Mit der Nutzung dieser Website erklären Sie sich damit einverstanden, dass wir Cookies verwenden."

Diese und ähnliche Cookie-Hinweise können lediglich mit einem Klick auf einem „Verstanden" oder „OK" bestätigt werden. Manchmal findet sich in der Nähe des Buttons ein mit „Mehr Informationen" o. Ä. bezeichneter Link, der dann zu den allgemeinen Datenschutzerklärungen der Verantwortlichen führt.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat sich bereits im Frühjahr 2019 in der „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien" mit der Thematik befasst. Die Orientierungshilfe kann abgerufen werden unter:

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

Kurzlink: *https://uldsh.de/tb38-72a*

Auszug aus der Orientierungshilfe (Hervorhebungen durch die Redaktion):

*„Durch eine vorgeschaltete Abfrage beim ersten Aufruf einer Website oder einer Web-App **kann** u. a. eine wirksame Einwilligung für **einwilligungsbedürftige**[1] Datenverarbeitungen eingeholt werden. Dabei sind jedoch folgende Anforderungen zu beachten:*

- *Beim erstmaligen Öffnen einer Webseite erscheint das Banner beispielsweise als eigenes HTML-Element. In der Regel besteht dieses HTML-Element aus einer Übersicht aller einwilligungsbedürftigen Verarbeitungsvorgänge, die unter Nennung der beteiligten Akteure und deren Funktion ausreichend erklärt werden und über ein Auswahlmenü aktiviert werden können. Aktivieren bedeutet in diesem Zusammenhang, dass die Auswahlmöglichkeiten nicht „aktiviert" voreingestellt sein dürfen.*
- *Während das Banner angezeigt wird, werden zunächst alle weiter gehenden Skripte einer Webseite oder einer Web-App, die potenziell Nutzerdaten erfassen, blockiert. Der Zugriff auf Impressum und Datenschutzerklärung darf durch Cookie-Banner nicht verhindert werden.*
- ***Erst wenn der Nutzer seine Einwilligung(en) durch eine aktive Handlung, wie z. B. das Setzen von Häkchen im Banner oder den Klick auf eine Schaltfläche, abgegeben hat, darf die einwilligungsbedürftige Datenverarbeitung tatsächlich (durch technische Maßnahmen sichergestellt) stattfinden.***
- *Zur Erfüllung der Nachweispflichten des Art. 7 Abs. 1 DSGVO ist es gemäß Art. 11 Abs. 1 DSGVO nicht erforderlich, dass die Nutzer dazu direkt identifiziert werden. Eine indirekte Identifizierung (vgl. Erwägungsgrund 26) ist ausreichend. Damit die Entscheidung des Nutzers für oder gegen eine Einwilligung bei einem weiteren Aufruf der Website berücksichtigt wird und das Banner nicht erneut erscheint, kann deren Ergebnis auf dem Endgerät des Nutzers ohne Verwendung einer User-ID o. Ä. vom Verantwortlichen gespeichert werden. Durch ein solches Verfahren kann der Nachweis einer vorliegenden Einwilligung erbracht werden.*
- *Da eine Einwilligung widerruflich ist, muss eine entsprechende Möglichkeit*

[1] *Die Nutzung von Cookies ist nicht per se einwilligungsbedürftig. Entsprechende Banner sollen daher nur eingesetzt werden, wenn tatsächlich eine Einwilligung notwendig ist.*

> *zum Widerruf implementiert werden. Der Widerruf muss so einfach möglich sein wie die Erteilung der Einwilligung, Art. 7 Abs. 3 Satz 4 DSGVO.*

Verantwortliche müssen sicherstellen, dass die Einwilligung nicht nur das Setzen von einwilligungsbedürftigen Cookies umfasst, sondern alle einwilligungsbedürftigen Verarbeitungstätigkeiten, wie z. B. Verfahren zur Verfolgung der Nutzer durch Zählpixel oder diverse Fingerprinting-Methoden, wenn diese nicht aufgrund einer anderen Rechtsgrundlage zulässig sind.

Auch genügt es für eine Einwilligung im Sinne der DSGVO nicht, wenn, wie bei vielen einfachen Cookie-Bannern im Web, ein Hinweis auf das Setzen von Cookies zusammen mit einem „OK"-Button erfolgt. In diesen Fällen fehlt es an der nach Artikel 7 DSGVO erforderlichen Freiwilligkeit, wenn die betroffenen Personen zwar „OK" drücken können, aber keine Möglichkeit erhalten, das Setzen von Cookies abzulehnen."

Der vollständige Text ist hier verfügbar:

https://www.datenschutzkonferenz-online.de/media/wp/20180410_wp259_rev01.pdf

Kurzlink: *https://uldsh.de/tb38-72b*

Nach Art. 5 Abs. 2 DSGVO sind Verantwortliche verpflichtet, die Einhaltung der datenschutzrechtlichen Vorschriften nachweisen zu können (Rechenschaftspflicht).

Die Vorgaben, denen eine wirksame Einwilligung nach Art. 6 Abs. 1 Buchst. a DSGVO genügen muss, werden in den Leitlinien des Europäischen Datenschutzausschusses zur Einwilligung dargestellt. Außerdem hat der Europäische Gerichtshofs (EuGH) mit seinem Urteil im Verfahren „Planet 49" klargestellt, welche Anforderungen an eine Einwilligung im Sinne der DSGVO zu stellen sind:

http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&doclang=DE

Kurzlink: *https://uldsh.de/tb38-72c*

Aufgrund einer Vielzahl von Anfragen, Beschwerden und Kontrollanregungen, insbesondere zur Einbindung von Analysediensten, hat die Landesbeauftragte für Datenschutz Schleswig-Holstein in einer Pressemitteilung vom November zudem darauf hingewiesen, dass Rechtsauffassungen, die unter Berücksichtigung der Rechtslage vor dem 25. Mai 2018 veröffentlicht wurden, wie z. B. die „Hinweise des HmbBfDI zum Einsatz von Google Analytics", überholt sind und von den Aufsichtsbehörden des Bundes und der Länder nicht mehr vertreten werden.

Besonders kritisch sind Analysedienste („Analytics", „Insights" oder Trackingdienste), die – wie oft bereits aus deren Nutzungsbedingungen ersichtlich – eine Verarbeitung personenbezogener Daten in einem Umfang vornehmen, der über das erforderliche Maß hinausgeht oder eigenen Zwecken des Analysediensteanbieters dient. Der Einsatz eines solchen Dienstes würde – vorbehaltlich einer konkreten Prüfung im Einzelfall – auf Grundlage der Kriterien, die in der Orientierungshilfe für Anbieter von Telemedien aufgestellt worden sind, den Spielraum überschreiten, den die Rechtsgrundlage des Art. 6 Abs. 1 Buchst. f DSGVO („berechtigte Interessen") bietet. In diesen Fällen wäre der Einsatz solcher Dienste – wenn überhaupt – nur auf Grundlage einer der anderen in Betracht kommenden Rechtsgrundlagen aus Art. 6 Abs. 1 DSGVO, wie z. B. einer wirksamen Einwilligung nach Art. 6 Abs. 1 Buchst. a DSGVO, denkbar.

Was ist zu tun?

Wir haben alle Webseitenbetreiber – ähnlich wie auch Kolleginnen und Kollegen des Bundes und anderer Bundesländer – per Pressemitteilung aufgefordert, die Einbindung von Analysediensten gemäß den kommunizierten Anforderungen zu überprüfen. Sind die Analysedienste nicht rechtskonform nutzbar, müssen sie deaktiviert werden.

08

KERNPUNKTE

Schutzräume für Kinder

Datenschutz und Cybersecurity

Transparenz und Usability

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 Rechte und Freiheiten natürlicher Personen bestehen.

Im Berichtszeitraum beteiligte sich das ULD an Projekten zu aktuellen Themen in den Bereichen Privatheit und selbstbestimmtes Leben (Tz. 8.1), Datenschutz für Smartphone-Anwendungen (Tz. 8.2), Datenschutz in digitalen Arbeitswelten (Tz. 8.3), Cybersicherheit und Datenschutz (Tz. 8.4), Transparenz- und Einwilligungsmanagement (Tz. 8.5) sowie zu Fragen der Nutzbarkeit (englisch: „Usability") und Datenschutz (Tz. 8.6).

8.1 Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt: Schutzräume nötig

Angesichts der kurzen Projektzyklen im Bereich der Digitalisierung fast schon ein Projekt der Großelterngeneration: das interdisziplinäre „Forum Privatheit" zur Gewährleistung und Weiterentwicklung informationeller Selbstbestimmung und des Privaten in der digitalen Welt, das bereits im Dezember 2013 gestartet ist und bis März 2021 laufen wird.

Forum Privatheit

Das „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt" ist ein vom BMBF gefördertes interdisziplinäres Projekt, das sich mit Fragen des Datenschutzes, der Privatheit, der Selbstbestimmung und digitalen Grundrechten beschäftigt. Das Projekt bringt Wissenschaftlerinnen und Wissenschaftler aus Disziplinen wie Technik, Recht, Soziologie, Psychologie, Politologie, Wirtschaftswissenschaften und Ethik zusammen.

Auch im Berichtsjahr wurde wieder an Veröffentlichungen für Akteure im politischen Bereich (Policy Paper) und für Forschung, Anwendung und Nutzende (White Paper oder Forschungsberichte) gearbeitet. Nachdem in den Vorjahren die Fokusthemen „Fortentwicklung des Datenschutzes" (2017) und „Zukunft der Datenökonomie" (2018) behandelt worden waren, ging es im Jahr 2019 um Inklusion und Exklusion. So beteiligte sich das ULD an der Jahreskonferenz zum Thema „Aufwachsen in überwachten Umgebungen – Wie lässt sich Datenschutz in Schule und Kinderzimmer umsetzen?". Das Forum Privatheit fordert einen digitalen Schutzraum für Kinder, denn bei ihnen handelt es sich um eine besonders vulnerable Gruppe, deren Schutz in der Online-Welt bisher nicht ausreichend gewährleistet ist.

Weiterhin wurde im Berichtsjahr eine Methode zur Dokumentation von Verarbeitungsvorgängen und Identifizierung von Risiken für Grundrechte und Grundfreiheiten entwickelt und im Rahmen der Veröffentlichung in einer Fachzeitschrift vorgestellt. Zwei Veröffentlichungen zur datenschutzrechtlichen Einwilligungserklärung wurden begonnen und werden im kommenden Jahr abgeschlossen sein.

Außerdem richtete das Projektteam zusammen mit anderen Partnern einen internationalen Workshop zu „Feminist Data Protection“ aus, bei dem Machtasymmetrien aus unterschiedlichen Perspektiven beleuchtet wurden. Überwachung in verschiedenen Ausprägungen (geschlechtsspezifische Stereotypen, DNA-Analysen oder Stalking und häusliche Gewalt in und mithilfe von Smart Homes) gehörte zu den Schwerpunkten der Diskussion:

https://www.forum-privatheit.de/veranstaltungen/workshop-feminist-data-protection/

Kurzlink: *https://uldsh.de/tb38-81*

Wie stets zielt das Forum Privatheit auf eine dynamische Vernetzung der verschiedenen Fach- und Praxis-Communities je nach Thema und Interessenschwerpunkten. Einige der Ergebnisse richten sich an den Gesetzgeber, andere an die Technikentwicklung, wieder andere stellen Best Practices vor, an denen man sich bei der Gestaltung und beim Einsatz von Verarbeitungsverfahren orientieren kann. Unsere Rolle besteht nicht nur darin, die Praxistauglichkeit der Ergebnisse zu prüfen, sondern der Austausch mit der Wissenschaft ist für alle Seiten befruchtend.

https://forum-privatheit.de

8.2 Projekt AppPETs – Datenschutz eingebaut in Smartphone-Anwendungen

Im Projekt „Datenschutzfreundliche Smartphone-Anwendungen ohne Kompromisse“ (AppPETs) (37. TB, Tz. 8.2.2) hatte das ULD die datenschutzrechtliche Themenbearbeitung übernommen. Im Berichtszeitraum galt es u. a. ein gesetzgeberisches Vorhaben zu bewerten, das für das Projekt AppPETs einige Relevanz haben könnte: Der Gesetzentwurf von März 2019 zur Ergänzung des § 126a StGB sieht vor, das Anbieten von Leistungen zur Ermöglichung von Straftaten unter Strafe zu stellen. Angesprochen werden sollen etwa Handelsplattformen für Drogen und Waffen im Darknet, z. B. Dienste im Tor-Netzwerk. Konkret lautet der Normentwurf zur Aufnahme in das Strafgesetzbuch: „§ 126a Anbieten von Leistungen zur Ermöglichung von Straftaten (1) Wer eine internetbasierte Leistung anbietet, deren Zugang und Erreichbarkeit durch besondere technische Vorkehrungen beschränkt und deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten im Sinne von Satz 2 zu ermöglichen oder zu fördern, wird mit [...] bestraft, [...].“

Die in der Norm beschriebenen Dienste erfassen vom Wortlaut auch solche, die als datenschutzfördernde Lösungen (PETs) den Schutz betroffener Personen erhöhen. Typische technische und organisatorische Maßnahmen im Datenschutz zielen gerade darauf ab, Zugang und Erreichbarkeit durch besondere technische Vorkehrungen zu beschränken, also etwa Inhalte zu verschlüsseln. Der Einsatz von Anonymisierungsdiensten sowohl auf Nutzer- als auch auf Anbieterseite („Hidden services“) ist zudem ein wichtiges Werkzeug für den Selbstdatenschutz.

Das Anbieten von Leistungen zur Ermöglichung von Straftaten kann in der Praxis zu weit verstanden werden. Es werden vielfältige internetbasierte Leistungen angeboten, deren Ziel nicht eine Straftat ist, aber die dennoch Straftaten im weitesten Sinne ermöglichen. Bleibt die Norm unverändert, erfasst der Wortlaut Betreiber technischer Infrastrukturen, die anonyme, verschlüsselte und zugangsbeschränkte Dienste anbieten, und erst durch die korrekte Auslegung des Zwecks des Betriebs entfällt die Tatbestandsmäßigkeit. Damit stehen Betreiber vor dem Risiko, sich ungerechtfertigter Maßnahmen von Strafverfolgungsbehörden ausgesetzt zu sehen, da subjektive Elemente wie die Intention des Betreibers kaum umfassend bei der Vorabprüfung eines Anfangsverdachts ermittelt werden können.

Im Ergebnis war damit zu dem Gesetzentwurf festzuhalten, dass dieser in unveränderter Form zunächst zu erheblicher Rechtsunsicherheit beiträgt. Dies steht im Gegensatz zur europaweiten Stärkung der Datenschutzrechte durch die DSGVO. So ist Selbstdatenschutz nicht nur

ein Element des Datenschutzes durch Technikgestaltung nach Artikel 25 DSGVO, sondern leitet sich schon aus dem Datenschutzgrundsatz der Fairness der Datenverarbeitung nach Art. 5 Abs. 1 Buchst. a DSGVO ab.

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

8.3 Projekt EMPRI-DEVOPS – Datenschutz in digitalen Arbeitswelten

Das Projekt „Employee Privacy in Software Development and Operations" (EMPRI-DEVOPS) (37. TB, Tz 8.3.1) beschäftigt sich seit November 2018 mit dem datenschutzkonformen Einsatz von Softwaretools in zunehmend digitalisierten Arbeitswelten. Projektziel ist die datenschutzfreundliche Gestaltung von Softwareprodukten, die typischerweise im Kontext der agilen Softwareprogrammierung und der Systemadministration zum Einsatz kommen.

Der Projektfokus gibt damit einen Vorgeschmack auf die sogenannte Arbeit 4.0, bei der der Einsatz von Softwareprodukten mit informations- und kommunikationstechnologischen Komponenten zunehmend Bedeutung erlangt. Bereits heute bedingen Heimarbeit bzw. mobiles Arbeiten in der Regel den Einsatz von Tools, etwa zum zeitnahen Austausch von Ergebnissen oder gemeinsamer Bearbeitung in Echtzeit.

Arbeit 4.0

Der Begriff Arbeit 4.0 umfasst den Veränderungsprozess der Arbeitswelt einschließlich der Chancen und Risiken im Zeitalter der Digitalisierung.

Um die Chancen der Digitalisierung auch im Erwerbsleben nutzen zu können, bedarf es intelligenter Softwarelösungen, die die datenschutzrechtlichen Vorgaben zum Schutz der Persönlichkeitsrechte von Beschäftigten und weiteren Mitarbeitenden (auch außerhalb eines Beschäftigungsverhältnisses) wirksam umsetzen.

Teils als Nebenfolge, teils beabsichtigt fallen bei der Toolnutzung zahlreiche Metadaten an. Werden diese strukturiert ausgewertet und analysiert, können weiter gehende personenbezogene Informationen über die einzelnen Nutzerinnen und Nutzer offenbart werden.

Inferenzrisiko

Ein Inferenzrisiko besteht, wenn sich aus vorhandenen Daten, etwa den bei der Nutzung von Kooperationstools anfallenden Metadaten, weitere sensible Informationen ableiten lassen. So können etwa Rückschlüsse auf Tagesabläufe und Arbeitsgewohnheiten aus Zeitstempeln der Aktivitäten (z. B. Bereitstellung von bearbeiteten Dokumenten) erlangt werden.

Mit zunehmender Softwarenutzung fallen auch mehr dieser digitalen Datenspuren an, die Rückschlüsse auf das Verhalten von Beschäftigten und weiteren Mitarbeitenden als Nutzende der Software ermöglichen und schnell das zulässige Maß an Leistungskontrolle oder Überwachung überschreiten können. Der Wandel in der Arbeitswelt und neue arbeitsteilige Gestaltungsformen, etwa projektbezogene Zusammenarbeit über Unternehmensgrenzen hinweg, machen zudem die Zuordnung und Zuständigkeit für Datenbestände schwer bestimmbar. Dies ermöglicht auch Externen Rückschlüsse auf Beschäftigtendaten oder interne Betriebsabläufe. Daher ist eine stärkere Beachtung des Schutzbedarfs dieser digitalen Datenspuren von Softwarenutzerinnen und -nutzern geboten.

Der Tooleinsatz im Beschäftigungskontext unterliegt aufgrund dieses Überwachungspotenzials regelmäßig der betrieblichen Mitbestimmung. Betriebs- und Personalräte müssen daher künftig auch die anfallenden Metadaten

und Zusatzfunktionalitäten von Softwareprodukten stärker in den Blick nehmen. Unternehmen müssen sich als Verantwortliche dieser Risiken bewusst sein.

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

Was ist zu tun?

Bei zunehmender Softwarenutzung im Beschäftigungskontext besteht die Gefahr übermäßiger Verhaltens- und Leistungskontrollen der Beschäftigten. Bei Auswahl, Konfiguration und Betrieb von Softwareprodukten sollten diese Risiken berücksichtigt werden.

8.4 Cybersicherheit und Datenschutz

Datenschutz und die effektive Gewährleistung von Cybersicherheit für Bürgerinnen und Bürger sowie die digitale Infrastruktur stehen in einem komplexen Verhältnis zueinander. Beide dienen dem Schutz der Menschen. Datenschutz in einer digitalisierten Welt kann nicht ohne technischen Schutz von Daten auskommen, der auch auf Infrastrukturebene gewährleistet sein muss. Umgekehrt ist für die Erkennung von Gefahren für kritische Infrastrukturen eine breite Datenbasis erforderlich. Hier bestehen einerseits berechtigte Bedarfe, andererseits aber auch darüber hinausgehende Begehrlichkeiten an Daten, auch an personenbezogenen oder personenbeziehbaren Daten. Hier gilt es im Einklang mit den Rechten und Freiheiten der betroffenen natürlichen Personen zu differenzieren und effektive technische und rechtliche Schutzmaßnahmen vorzusehen.

Gegenstand des EIDI-Projekts ist die effiziente Unterrichtung und Frühwarnung betroffener Personen über erfolgte Datenlecks und das Risiko von Identitätsdiebstählen (Tz. 8.4.1). Auf europäischer Ebene engagierte sich das ULD in den Projekten CANVAS (Tz. 8.4.2) mit Ausarbeitungen zum Spannungsverhältnis zu Recht und Ethik und PANELFIT (Tz. 8.4.3) mit Schwerpunkten im Bereich der Forschung von Informations- und Kommunikationstechnologien.

8.4.1 Projekt EIDI – verlässliche Benachrichtigung von Betroffenen nach Cybervorfällen

Identitätsmissbrauch ist für die betroffenen Personen im geringsten Fall lästig, oftmals jedoch eine Gefahr für die Reputation oder birgt handfeste finanzielle Risiken. Nutzerinnen und Nutzer haben nur eingeschränkte Möglichkeiten, sich dagegen zu wehren. Um Opfer zu werden, müssen sie in der Kette der Ereignisse auch nicht etwas falsch gemacht haben. Werden Zugangsdaten, etwa die Kombination von Nutzername und Passwort, bei Diensteanbietern nicht zuverlässig gegen externe oder interne Angreifer (etwa unzufriedene Beschäftigte) gesichert, können diese in falsche Hände geraten. Informationen aus solchen sogenannten „Leaks“ werden teilweise im Internet zum Kauf, Tausch oder frei angeboten. Bleibt der Sicherheitsvorfall unbemerkt, können solche Zugangsdaten sodann von Kriminellen unerkannt zur Nutzung des betreffenden Dienstes verwendet werden.

Oftmals ist das Risiko nicht nur auf einen Dienst beschränkt, denn es kommt gar nicht selten vor, dass Nutzerinnen und Nutzer aus Bequemlichkeit identische Zugangsdaten für mehrere Dienste gewählt haben. Angreifer probieren diese daher bei verschiedenen Diensten aus („Credential Stuffing“). Bei ausreichend großen

Datensammlungen ist dieses Vorgehen für die Kriminellen vergleichsweise Erfolg versprechend. Die Nutzenden selbst haben es nicht mehr in der Hand, dies zu erkennen oder hiergegen rechtzeitig vorzugehen. Haben die betroffenen Diensteanbieter den Anmeldeverkehr mit geeigneten Maßnahmen im Blick, können zumindest bestimmte Abweichungen oder Muster möglicherweise noch rechtzeitig erkannt und schützende Maßnahmen ergriffen werden.

Credential Stuffing

Nutzende verwenden oft dieselben Log-in-Daten für mehrere Dienste. Erlangen Kriminelle Listen von Zugangsdaten, probieren sie diese daher automatisiert bei diversen Online-Diensten aus.

In dem vom BMBF geförderten Projekt „Effektive Information nach digitalem Identitätsdiebstahl" (EIDI) (37. TB, Tz. 8.4.1) wurde erforscht, wie auf Grundlage veröffentlichter Datensammlungen Schutzmaßnahmen ergriffen und Betroffene zielführend unterrichtet werden können.

Aufbauend auf die im Projekt erlangten Erkenntnisse bietet die Universität Bonn als EIDI-Projektpartner einen Leak-Checker-Dienst an, der es gestattet zu prüfen, ob die eigene E-Mail-Adresse von den dort bekannten Datenlecks betroffen ist, und das Ergebnis per E-Mail an die getestete Adresse zu erhalten. Die mit dem Projekt kooperierenden Diensteanbieter haben zudem die Möglichkeit, proaktiv ihre Kundinnen und Kunden zu schützen, indem sie deren Daten mit denen der Leak-Datenbank abgleichen. Dabei dürfen die Informationen nicht etwa frei zwischen den Partnern zirkulieren. Vielmehr wurde ein datensparsames Verfahren entwickelt, bei dem die kooperierenden Diensteanbieter ausschließlich erfahren können, ob konkrete Zugangsdaten in einem bestimmten Leak enthalten waren und ob das darin enthaltene Passwort für den eigenen Dienst funktioniert. Umgekehrt erfährt auch die Stelle, die die Leak-Daten sammelt und für die Kooperationspartner aufbereitet, nichts über deren Kundenstamm.

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

Was ist zu tun?

Diensteanbieter können den Anmeldeverkehr auf ihren IT-Systemen datenschutzkonform im Blick behalten und vertrauenswürdige Leak-Checker-Dienste in Anspruch nehmen. Dann können betroffene Personen informiert und das Risiko eines Identitätsmissbrauchs eingedämmt werden.

8.4.2 Projekt CANVAS – Cybersicherheit zwischen Technik, Ethik und Recht

Das von der Europäischen Kommission geförderte Projekt „Constructing an Alliance for Value-driven Cybersecurity" (CANVAS) (37. TB, Tz. 8.4.2) zielte darauf ab, ein Expertennetzwerk für Cybersicherheit zu schaffen, in dem Technikentwicklerinnen und -entwickler mit Rechtsexpertinnen und -experten, Ethikerinnen und Ethikern sowie Sozialwissenschaftlerinnen und -wissenschaftlern zusammengebracht werden. Außerdem ging es darum, politische Entscheidungsträger über die wesentlichen Konfliktfelder und mögliche Lösungsansätze zu informieren.

Der zunehmende Einsatz von Informations- und Kommunikationstechnologien in allen Bereichen der modernen Welt macht oft das Leben leichter und kann Vielfalt, Kreativität und Interaktivität fördern. Zugleich jedoch wächst damit die Abhängigkeit von Menschen und Organisatio-

nen von diesen Technologien, die nie vollständig sicher und zuverlässig geschützt sein können. Daher ist die Cybersicherheit zu einer Angelegenheit von globalem Interesse und Bedeutung geworden. Dementsprechend ist der Cybersicherheitsdiskurs von der ständig wachsenden Vielfalt der Bedrohungsformen geprägt, die von einfachen Computerviren über Cyberkriminalität und Cyberspionageaktivitäten bis hin zu Cyberterror und Kriegsführung im digitalen Raum reichen.

Diese wachsende Komplexität des digitalen Ökosystems in Kombination mit zunehmenden globalen Risiken führt zu einem grundrechtlichen Zielkonflikt: Eine Überbetonung der Cybersicherheit kann Grundwerte wie Gleichheit, Fairness, Freiheit oder Privatsphäre verletzen. Andererseits könnte die Vernachlässigung der Cybersicherheit das Vertrauen der Bürgerinnen und Bürger in die digitale Infrastruktur untergraben und bei einem erfolgreichen Cyberangriff ganz konkrete Folgen für Gesundheit, Sicherheit und Grundversorgung der Bürgerinnen und Bürger bedingen. Um dieser Herausforderung zu begegnen, hat die Europäische Kommission das CANVAS-Projekt damit beauftragt herauszufinden, wie Cybersicherheit mit den Grundrechten und europäischen Werten in Einklang gebracht werden kann. Cybersecurity berührt nicht nur den technischen Bereich, sondern auch andere Domänen wie etwa Ethik, Recht oder Soziologie mit verschiedenen Forschungsmethoden. Daher war es wichtig, Expertinnen und Experten aus den unterschiedlichen Bereichen zusammenzubringen und gemeinsam nach Lösungen zu suchen, die als Fundament die europäischen Grundwerte, Grundrechte und Grundfreiheiten haben.

Das CANVAS-Projekt hat Vertreterinnen und Vertreter aus den Sektoren Gesundheit, Finanzen sowie nationale Sicherheit für Diskussionen über die sektorspezifischen Herausforderungen zusammengebracht. In themenbezogenen Workshops wurde gemeinsam nach geeigneten Lösungen gesucht, wobei ein besonderer Fokus auf ethischen Fragen aus Wissenschaft und Wirtschaft lag.

Die herausgearbeiteten Diskussionsergebnisse und Lösungsansätze wurden anschließend in vielfältiger Weise der Öffentlichkeit, der Forschung und Lehre sowie der Politik präsentiert und zur weiteren Verwendung aufbereitet. Dies wird in eine Buchveröffentlichung einfließen.

Das Material des europäischen Projektteams wurde vorwiegend in englischer Sprache erstellt, um zeitnah einen internationalen Diskurs zu ermöglichen. Es besteht aus:

- mehreren White Papers zur Cybersecurity jeweils in Relation zu Ethik, Recht bzw. technischen Herausforderungen sowie einer Darstellung der durch das Projekt ermittelten Haltungen und Meinungen zum Thema von Bürgerinnen und Bürgern auf der einen Seite und staatlichen Stellen auf der anderen Seite,
- „Briefing Packages“ als prägnante Kurzpapiere der Projektergebnisse für europäische und nationale Normgeber,
- einem Muster-Curriculum für die Ausbildung an Hochschulen im Cybersecurity-Bereich mit besonderem Augenmerk auf die Werteperspektive,
- einem zu dem Curriculum passenden „Massive Open Online Course (MOOC)“ mit Online-Schulungsmaterial, Tutorien und Videos.

Das Material ist frei auf der Webseite des CANVAS-Projekts verfügbar:

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

8.4.3 Projekt PANELFIT – Cybersicherheit und Datenschutz

Die Datenschutz-Grundverordnung und die weiterhin im Gesetzgebungsprozess befindliche E-Privacy-Verordnung sind mit wichtigen Änderungen und Weiterentwicklungen im Bereich Datenschutz verbunden. Das von der EU-Kommission geförderte Projekt „Participatory Approaches to a New Ethical and Legal Framework for ICT" (PANELFIT) (37. TB, Tz. 8.4.3) will dazu beitragen, dass solche Änderungen schnell und vollständig von allen europäischen Akteuren im Bereich der Technikforschung und Innovation aufgegriffen und umgesetzt werden. Während das Projekt auch ethische Aspekte betrachtet, konzentriert sich das ULD auf den Datenschutz. Das ULD stützt sich dabei auf seine jahrelange Erfahrung in nationalen und internationalen Forschungsprojekten. Auf dieser Basis gestaltet es Beiträge zu den praxisorientierten Richtlinien, die das PANELFIT-Projekt für in der Forschung Tätige zusammenstellt, und den Empfehlungen für Entscheidungsträger wie z. B. Förderträger im Bereich der Informations- und Kommunikationstechnologien.

Im Jahr 2019 hat das PANELFIT-Projekt mehrere Workshops mit externen Expertinnen und Experten veranstaltet, um herauszuarbeiten, an welchen Stellen in der Technikforschung und Innovation die neuen gesetzlichen Datenschutzregeln nicht ausreichend umgesetzt werden. Das ULD hat aktiv an der Organisation, Moderation und Diskussion mitgewirkt. Aufgrund dieses Inputs und weiterführenden Recherchen hat das PANELFIT-Projekt Herausforderungen und bisherige Defizite bei der Umsetzung des neuen Rechtsrahmens erkannt und aufgezeigt, teilweise konnten auch schon Lösungen vorgeschlagen werden.

Zu den Herausforderungen, die dem ULD besonders am Herzen liegen, gehört die durchaus wünschenswerte Initiative der Europäischen Kommission, in Europa Forschungsergebnisse und Daten frei zu teilen (sogenanntes „Open Access"). Dies kann jedoch im Konflikt mit Datenschutzanforderungen stehen. Eine Klärung, wie das faire Teilen personenbezogener Daten in der Forschung möglich wäre, soll hier Abhilfe schaffen. Das ULD hat gegenüber der Kommission die Notwendigkeit einer solchen Klärung begründet und erste Ansätze für datenschutzwahrende Teilungsstrategien erarbeitet.

Ein anderes Anliegen des ULD ist der Umgang mit unvorhergesehenen Situationen in der Forschung. Zum Beispiel kann ein Forschungsprojekt im Umfeld der geplanten Arbeit unerwartet größere Datenschutzproblemfelder aufdecken. Dies hat das ULD im Projekt iKoPA (zuletzt 37. TB, Tz. 8.6.1) auch wirklich erlebt, als klar wurde, dass die auf jedem Handy installierten „Location Services" alle Bewegungen von mit WLAN ausgerüsteten Fahrzeugen an zentrale Server melden (Stichwort „WiFi-Tracking").

https://uld-sh.de/LStrack

Aufgrund der eigenen Schwierigkeiten, wie man außerhalb der geplanten Projektarbeit und -dauer hinaus bewirken kann, dass solche Probleme nicht einfach unter den Tisch fallen, sondern von den relevanten Akteuren erkannt und gelöst werden, versucht das ULD Lösungsvorschläge für Forschungsprogramme zu erarbeiten.

Es gibt außerdem viele Fragen in der täglichen Arbeit der Forschenden. So besteht beispielsweise der Bedarf an praktischen und leicht verständlichen Anleitungen, wie man Cookies und Cookie Policies auf Projektwebseiten datenschutzgerecht handhabt.

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

8.5 Projekt SPECIAL – Transparenz- und Einwilligungsmanagement für das semantische Netz

In dem von der Europäischen Kommission geförderten Projekt „Scalable Policy-awarE linked data arChitecture for prIvacy, trAnsparency and compLiance“ (SPECIAL) (37. TB, Tz. 8.5.1) sind neue datenschutzfördernde Konzepte und Technologien entwickelt worden. Die Anforderungen der Datenschutz-Grundverordnung in Bezug auf eine einwilligungsbasierte Verarbeitung personenbezogener Daten lassen sich mit einem gut durchdachten Einwilligungsmanagement umsetzen, das hinreichende Transparenz, Information sowie die Inanspruchnahme der Betroffenenrechte unterstützt. Jedoch stellt gerade dies häufig die Anwenderinnen und Anwender von Big-Data-Technologien vor große Herausforderungen. Das Projekt SPECIAL hat daher verschiedene Lösungsansätze verfolgt, die einzeln oder in Kombination zu einer Verbesserung des Datenschutzes beitragen können:

- Die Entwicklung einer Managementumgebung für Verarbeitungsrichtlinien (Policy Management Framework), die dem Verantwortlichen eine bessere Kontrolle über die verarbeiteten personenbezogenen Daten ermöglicht. Dies umfasst maschinenlesbare Zugriffs- und Verarbeitungsrichtlinien, die zugleich eine Überprüfbarkeit der Verarbeitung gewährleisten.
- Die Entwicklung eines Transparenz- und Compliance-Frameworks, das den betroffenen Personen die notwendigen Informationen darüber vermittelt, wie Daten verarbeitet und wem sie übermittelt werden. Dies soll in einer Weise geschehen, dass betroffene Personen tatsächlich und ohne das Lesen sonst oft seitenlanger, für den Laien unverständlicher Datenschutzerklärungen in die Lage versetzt werden, vor Abgabe einer Einwilligung umfassend über die beabsichtigte Datenverarbeitung informiert zu sein.
- Die Entwicklung einer skalierbaren Architektur, die in der Lage ist, die Verarbeitungsrichtlinien zu unterstützen und so Berechtigungen auch computerauswertbar abzubilden.

Die entwickelten Lösungsansätze wurden in verschiedenen Testanwendungsfällen auch für Mobilgeräte evaluiert und verbessert. Die Umsetzung sollte zeigen, dass eine Wertschöpfung aus geteilten Daten bzw. Big Data unter Einhaltung datenschutzrechtlicher Belange möglich ist und zum Vertrauen der Nutzerinnen und Nutzer in digitale Dienste beiträgt. Zu diesem Zweck wurden Nutzerstudien durchgeführt, die mit ihren konstruktiven und positiven Ergebnissen eine Fortentwicklung der Umsetzung von Transparenz und Information für die betroffenen Personen ermöglichen. Des Weiteren hat sich das Projekt SPECIAL in der „W3C Data Privacy Vocabularies and Controls Community Group“ (DPVCG) engagiert, um die Standardisierung einer DSGVO-konformen Taxonomie zu unterstützen. Diese enthält Datenschutzbegriffe und Klassifizierungen z. B. für Kategorien personenbezogener Daten, Verarbeitungszwecke, Rechtsgrundlagen der DSGVO, Speicherfristen sowie Art und Umfang der Verarbeitung. Ziel ist, alle relevanten Umstände der Verarbeitung personenbezogener Daten in computerverwertbarer Form abbilden zu können:

https://www.w3.org/community/dpvcg/

Zentrales rechtswissenschaftliches Ergebnis sind schließlich die Ausarbeitungen zu dynamisch erteilten Einwilligungen („Dynamic Consent“). Statt betroffenen Personen lange, komplexe Einwilligungserklärungen vorzulegen wird eine Rahmenvereinbarung über die Datenverarbeitung getroffen. Sie gestattet, bei Bedarf weiter gehende Einwilligungen einzuholen. Daneben kann eine verlässliche digitale Kommunikationsmöglichkeit, etwa via App, bereitgestellt werden. Ergibt sich ein Rückfragebedarf, z. B. wenn der Verantwortliche aus einer Analyse der vorhandenen Daten neue Informationen erlangt oder beabsichtigt, vorhandene Daten zu geänderten Zwecken zu verarbeiten, kann die

betroffene Person auf diesem Wege erreicht werden. Verantwortliche erhalten so Rechtssicherheit und nachweisbare Compliance, für betroffene Personen gibt es ein Mehr an Transparenz feiner differenzierter Entscheidungsmöglichkeiten. Beides ist für vertrauenswürdige Big-Data-Anwendungen wünschenswert.

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

8.6 Projekt Privacy&Us – Usability für das Internet of Things

Das durch die Europäische Union geförderte Projekt „Privacy&Us – Usability für das Internet of Things" förderte junge Wissenschaftlerinnen und Wissenschaftlicher im Rahmen eines Forschungsnetzwerks aus Universitäten, Unternehmen und weiteren Stellen. Thematisch befasste sich das Netzwerk mit unterschiedlichen Aspekten des Datenschutzes unter dem Blickwinkel der Benutzerfreundlichkeit (Usability). Am ULD wurden etwa Vorschläge erarbeitet, wie im Internet der Dinge die nötige Transparenz über Datenverarbeitungsvorgänge hergestellt werden könne (37. TB, Tz. 8.6.3). Diese müsse sowohl für Endnutzer als auch für Verantwortliche verständlich und inhaltlich leicht zugänglich sein, um das jeweils mit der Datenverarbeitung verbundene Risiko beurteilen und die angemessenen technischen und organisatorischen Maßnahmen auswählen und umsetzen zu können. Die laufenden Forschungen wurden fortgesetzt.

Im Berichtszeitraum waren am ULD zudem zwei Nachwuchsforschende des Netzwerks zu Gast. In enger Zusammenarbeit mit dem Wissenschaftler aus Karlstad, Schweden, und dem SPECIAL-Projektteam am ULD (Tz. 8.5) entstand ein Beitrag mit Anregungen für die Gestaltung einer App für das Management von „Dynamic Consent", d. h. also Einwilligungserklärungen mit einer dynamischen Komponente. Eine solche App muss sowohl hinreichend informieren als auch individuelle Einstellungen ermöglichen, darf aber die Nutzenden zugleich nicht überfordern. Die gezielte Berücksichtigung von Gesichtspunkten der leichten und effizienten Nutzbarkeit und Benutzerfreundlichkeit ermöglicht hier den Brückenschlag.

Des Weiteren wurde im Rahmen der „Digitalen Woche Kiel" in Kooperation mit der Wirtschaftsuniversität Wien ein Vortrag über Datenschutzaspekte von Sprachassistenten angeboten.

09

KERNPUNKTE

Akkreditierungsregeln und Zusammenarbeit im AK Zertifizierung

Stand der Zertifizierung beim ULD

9 Zertifizierung: Audit und Gütesiegel

9.1 Akkreditierungsregeln und Zusammenarbeit im AK Zertifizierung

Das ULD hat auf Wunsch der Datenschutzkonferenz weiterhin den Arbeitskreis Zertifizierung (AK Zertifizierung) der Datenschutzaufsichtsbehörden in Deutschland geleitet. Kernaufgabe 2019 war es, zusammen mit der Deutschen Akkreditierungsstelle GmbH (DAkkS) das Akkreditierungswesen nach Artikel 42 und Artikel 43 DSGVO aufzubauen und in Betrieb zu nehmen. Hierzu hatte der AK Zertifizierung schon 2018 Akkreditierungskriterien erarbeitet, die von der Datenschutzkonferenz auch im August 2018 angenommen worden waren (37. TB, Tz. 9.1.2). Diese müssen nach Art. 64 Abs. 1 Buchst. c DSGVO dem Europäischen Datenschutzausschuss zur Stellungnahme übermittelt werden.

Leider waren unsere Bemühungen 2019 diesbezüglich nicht erfolgreich: Aufgrund noch fehlender Grundlagenpapiere auf europäischer Ebene wurden wir mehrfach vom Sekretariat des Ausschusses gebeten, diesen Antrag zurückzunehmen bzw. ruhen zu lassen. Als dann im Herbst 2019 die vollständigen grundlegenden Unterlagen des Ausschusses vorlagen, ergab sich ein kleiner Änderungsbedarf an unseren Akkreditierungskriterien. Die Datenschutzkonferenz gab daher dem AK Zertifizierung den Auftrag, diese Änderungen vorzunehmen. Es ist geplant, Anfang 2020 die neuen Akkreditierungskriterien beim Ausschuss einzureichen, sodass in der Folge Akkreditierungen vorgenommen werden können.

Weiterhin unklar ist in diesem Zusammenhang, wie viele Anträge auf Akkreditierung nach Art. 43 DSGVO in Verbindung mit § 39 BDSG (37. TB, Tz. 9.1.3) und auf Genehmigung von Kriterienkatalogen auf das ULD zukommen werden. Dieses Problem haben auch die anderen Bundesländer, sodass der AK Zertifizierung eine Kooperationsvereinbarung zwischen allen Aufsichtsbehörden und auch der DAkkS entworfen hat, die eine gegenseitige Unterstützung ermöglichen soll. Auch beinhaltet diese Vereinbarung Verfahrensabstimmungen zwischen den Datenschutzaufsichtsbehörden und der DAkkS. Diese Vereinbarung soll ebenfalls Anfang 2020 den Datenschutzaufsichtsbehörden zur Verabschiedung vorgelegt werden.

Was ist zu tun?

Sobald die endgültigen Kriterien für Akkreditierungen vorliegen, wird das ULD entsprechende Anträge aus Schleswig-Holstein zusammen mit der DAkkS bearbeiten.

9.2 Stand der Zertifizierung beim ULD

Das ULD kann nach Art. 42 Abs. 5 Satz 1 DSGVO selbst Zertifizierungen vornehmen. Nach den Erfahrungen der vergangenen Jahre mit Datenschutzaudit und Datenschutz-Gütesiegel planen wir weiterhin von diesem Recht Gebrauch zu machen. Die Erarbeitung eines entsprechenden Kriterienkatalogs wurde zunächst unterbrochen, bis vonseiten des Europäischen Datenschutzausschusses die nötigen Informationen vorliegen. Auch beschäftigte sich 2019 ein Unterarbeitskreis „Prüfkriterien" des AK Zertifizierung, in dem wir mitwirken, mit der Zusammenstellung von Vorgaben für entsprechende Zertifizierungsprogramme und Kriterien. Dessen Ergebnisse werden wir aufgreifen. Geplant ist dann, dass wir die Prüfungen und Zertifizierungen selbst vornehmen und nicht mehr, wie es noch beim Datenschutz-Gütesiegel bis 2018 der Fall war (37. TB, Tz. 9.2.2 und 9.2.3), die Prüfung von Gutachtern in eigener Verantwortung durchgeführt wird. Die Zertifizierung des ULD kann insbesondere ein Angebot für Antragsteller aus der öffentlichen Verwaltung in Schleswig-Holstein sein, die ihre Verarbeitungen nachweisbar konform zu den datenschutzrechtlichen Regelungen umgesetzt haben.

Was ist zu tun?

Das ULD wird ein Zertifizierungsprogramm erarbeiten und Kriterien für die Zertifizierung aufstellen.

10

KERNPUNKTE

Pseudonymisierung

Künstliche Intelligenz

DNS-over-HTTPS

10 Aus dem IT-Labor

10.1 Pseudonymisierungslösungen mit zahlreichen Facetten – nicht „One size fits all“

Ein in der DSGVO konkret genanntes Mittel für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen ist die Pseudonymisierung. Als einzige Maßnahme wird sie mit einer Begriffsbestimmung (Art. 4 Nr. 5 DSGVO) hervorgehoben. Pseudonymisierung kann als datenschutzfördernde Maßnahme dienen, indem die Identität eines Individuums in einem spezifischen Zusammenhang verborgen wird. Gerade bei der Verarbeitung einer großen Zahl oder besonders sensibler personenbezogener Daten ist die Pseudonymisierung oft eine empfehlenswerte ergänzende Maßnahme.

Pseudonymisierung

Pseudonymisierung ist eine Verarbeitung von personenbezogenen Daten, bei der das Resultat ohne Hinzuziehen von zusätzlichen Informationen nicht mehr einer spezifischen Person zugeordnet werden kann. Nur diese zusätzlichen Informationen ermöglichen es, die pseudonymisierten Daten einem Individuum zuzuordnen – beispielsweise in Form einer Tabelle oder Berechnungsfunktion.

Beim Einsatz einer datenschutzkonformen Pseudonymisierung sind zahlreiche technische und organisatorische Anforderungen zu berücksichtigen, damit das Pseudonymisierungsverfahren zuverlässig und sicher eingesetzt werden kann, aus den pseudonymisierten Daten keine Rückschlüsse auf einzelne Personen gezogen werden können und auch weiterhin alle Betroffenenrechte der betroffenen Personen gewahrt bleiben.

Die Fokusgruppe Datenschutz der Plattform „Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft“ hat im Rahmen des Digital-Gipfels der Bundesregierung 2018 eine umfangreiche Beschreibung all dieser Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen vorgelegt. An dieser Arbeitsgruppe wirken Vertreterinnen und Vertreter von Unternehmen, aus Hochschulen, von Unternehmensverbänden sowie von zivilgesellschaftlichen Institutionen mit. Die Datenschutzaufsichtsbehörden sind über den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie über das ULD vertreten.

Als nächsten Schritt plant die Fokusgruppe die Finalisierung von Verhaltensregeln („Code of Conduct“) für Pseudonymisierung; ein Entwurf wurde schon beim Digital-Gipfel 2019 vorgelegt.

Die Verhaltensregeln sollen Verantwortlichen die Möglichkeit bieten, praxisorientiert passende organisatorische und technische Maßnahmen auszuwählen, Zuständigkeiten festzulegen und notwendige Prozesse einzuführen. Anhand von zwei Anwendungsbeispielen werden die Vorgaben und Fragestellungen näher erläutert. Der Entwurf soll in einem nächsten Schritt um sektorspezifische Good-Practice-Beispiele ergänzt werden. Vor der Genehmigung eines „Code of Conduct“ gemäß Art. 40 Abs. 2 Buchst. d DSGVO durch eine Aufsichtsbehörde müssen zudem Prozesse zur Kontrolle der Einhaltung des Codes festgelegt werden.

Der Entwurf für einen „Code of Conduct“ zum Einsatz DSGVO-konformer Pseudonymisierung ist unter folgendem Link abrufbar:

https://www.de.digital/DIGITAL/Redaktion/DE/Textsammlung/digital-gipfel-plattform-sicherheit-schutz-vertrauen-fg3.html

Kurzlink: *https://uldsh.de/tb38-101a*

Auch auf europäischer Ebene wird der datenschutzfördernde Einsatz von Pseudonymisierung diskutiert. Mit einem gemeinsamen Workshop der Agentur der Europäischen Union für Cybersicherheit (ENISA) und des ULD am 12. November 2019 in Berlin konnte die aktuelle

Debatte in verschiedenen Sektoren und Ländern gebündelt werden.

Im Rahmen des Workshops gelang ein interdisziplinärer Austausch zu erprobten Techniken für Pseudonymisierung und über verschiedene Erfahrungen. Eines der Hauptergebnisse des Workshops war, dass es nicht eine einzige Pseudonymisierungslösung gibt, die in allen Fällen angewendet werden kann. „One size fits all" funktioniert hier nicht. Obwohl heute mehrere verschiedene technische Ansätze zur Verfügung stehen, sollte ein Risikobewertungsprozess – basierend auf dem Kontext und dem gewünschten Nutzungsgrad – für jeden einzelnen Fall das bestmögliche Verfahren vorsehen.

Daher sind weitere Arbeiten an praktischen Beispielen und realen Umsetzungsszenarien sowohl auf der technischen als auch auf der rechtlichen Seite erforderlich.

Die Materialien des Workshops sowie der ENISA-Report „Pseudonymisation Techniques and Best Practices" stehen online zur Verfügung:

https://www.enisa.europa.eu/events/uld-enisa-workshop/uld-enisa-workshop-pseudonymization-and-relevant-security-technologies

Kurzlink: *https://uldsh.de/tb38-101b*

10.2 Ergebnisse der Datenschutz-Taskforce „Künstliche Intelligenz"

Künstliche Intelligenz (KI) hat in den letzten Jahren permanent an Bedeutung gewonnen. Dabei ist KI nicht nur eine technische Zukunftsvision, sondern KI-Systeme sind im Alltag angekommen, beispielsweise als unterstützende Systeme in der Forschung und Medizin, aber auch in Suchmaschinen, Sprachassistenten oder Online-Shops. Um eine rechtlich zulässige Verarbeitung von personenbezogenen Daten in KI-Systemen sicherzustellen und Akzeptanz bei den Betroffenen zu erzeugen, müssen bei der Entwicklung und Anwendung von KI hohe Anforderungen an technisch-organisatorische Maßnahmen und Standards in Bezug auf Datenschutz und Datensicherheit gestellt werden.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat Anfang 2019 eine Taskforce „KI" ins Leben gerufen, die in einem ersten Schritt die grundsätzlichen Anforderungen an KI-Systeme erarbeitet hat. Diese Grundsatzerklärung wurde am 3. April 2019 von der DSK als „Hambacher Erklärung zur Künstlichen Intelligenz" verabschiedet. Kernpunkte der Hambacher Erklärung sind sieben Datenschutzanforderungen an KI-Systeme:

(1) KI darf Menschen nicht zu Objekten machen.

Die Würde des Menschen gebietet, dass Entscheidungen mit rechtlicher Wirkung oder ähnlicher Beeinträchtigung nicht allein Maschinen überlassen werden. Betroffene müssen einen Anspruch auf das Eingreifen einer Person haben (Intervenierbarkeit).

(2) KI muss Diskriminierungen vermeiden.

Lernende Systeme sind im hohen Maße abhängig von den eingegebenen Daten. Durch unterschiedliche Faktoren können Algorithmen in KI-Systemen die zugrunde liegenden Daten so bewerten, dass Diskriminierungen erlernt und sogar verstärkt werden können. Es muss eine Risikoüberwachung installiert werden, die sowohl offensichtliche als auch verdeckte Diskriminierungen erkennen kann.

(3) KI muss transparent, nachvollziehbar und erklärbar sein.

Werden personenbezogene Daten durch KI-Systeme verarbeitet, dann gilt die Rechen-

schaftspflicht des Verantwortlichen. Die Nachvollziehbarkeit und Erklärbarkeit des KI-Systems muss nicht nur im Hinblick auf das Ergebnis gewährleistet sein, sondern auch auf die Trainingsdaten, die Prozesse und das Zustandekommen von Entscheidungen.

(4) KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben.

Bei dieser Anforderung ist besonders zu beachten, dass sie sowohl die personenbezogenen Daten berücksichtigt, die mit dem entsprechenden KI-System verarbeitet werden, als auch die (personenbezogenen) Trainingsdaten, mit denen das entsprechende KI-System trainiert wurde.

(5) Für KI gilt der Grundsatz der Datenminimierung.

Insbesondere für das Training von KI-Systemen werden große Bestände an Trainingsdaten benötigt. Für personenbezogene Trainingsdaten gilt, dass sie stets auf das notwendige Maß beschränkt sein müssen.

(6) KI braucht Verantwortlichkeit.

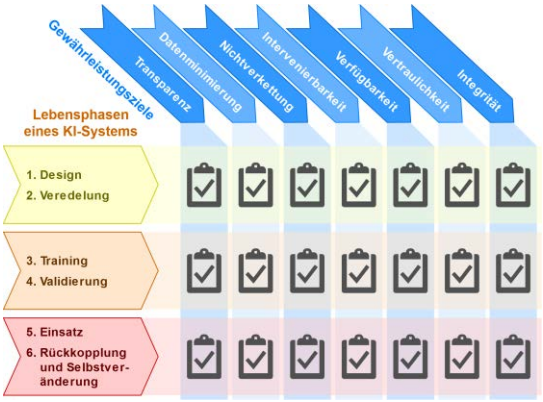
Der Verantwortliche muss dafür sorgen, dass die rechtmäßige Verarbeitung, die Sicherheit der Verarbeitung, die Beherrschbarkeit des KI-Systems und die Wahrung der Betroffenenrechte gewährleistet werden.

(7) KI benötigt technische und organisatorische Standards.

Für KI-Systeme gibt es gegenwärtig noch keine speziellen Standards. Hier ist die Entwicklung von Best Practices durch Wirtschaft und Wissenschaft mit der Begleitung der Datenschutzaufsichtsbehörden wünschenswert. Die weitere Entwicklung muss allerdings auch politisch gesteuert werden, um den Schutz der Grundrechte zu gewährleisten.

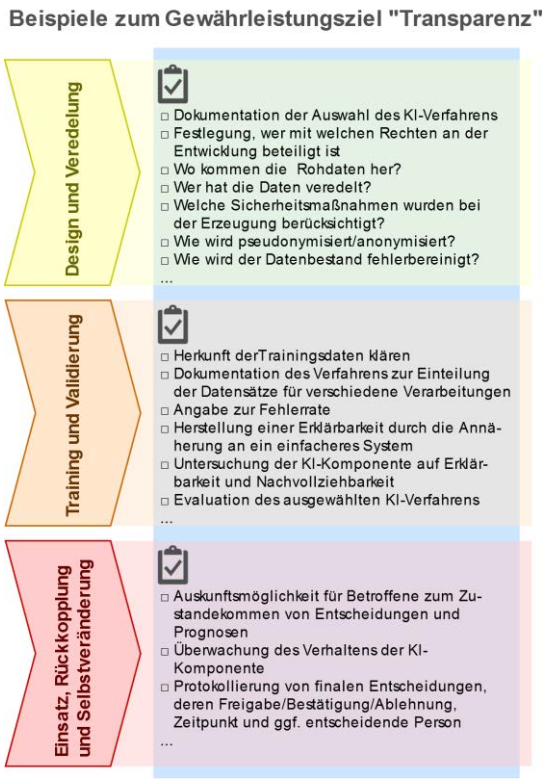
Die „Hambacher Erklärung zur Künstlichen Intelligenz" ist als Leitdokument zum Einsatz von KI-Systemen zu verstehen, das die grundsätzlichen Anforderungen an ein KI-System definiert, ohne Details oder konkrete Maßnahmen zur Umsetzung zu nennen. Um Verantwortlichen und Entwicklern detailliertere technische und organisatorische Maßnahmen zum Einsatz von KI-Systemen an die Hand zu geben, hat die DSK das „Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen" entwickelt, das am 6. November 2019 durch die DSK beschlossen wurde.

In dem Positionspapier werden verschiedene Lebensphasen eines KI-Systems (Design & Veredelung der Daten, Training & Validierung sowie Einsatz & Rückkopplung) unterschieden. Die sieben Datenschutzanforderungen aus der Hambacher Erklärung werden aufgegriffen und unter Berücksichtigung des Lebenszyklus und mithilfe der Gewährleistungsziele des Standard-Datenschutzmodells (Tz. 6.2.3) konkretisiert. Das Ergebnis ist eine Matrix, in der pro Lebensphase und Gewährleistungsziel konkrete Anforderungen und Risiken definiert sind.



Durch diese Matrixsystematik ist eine ganzheitliche Sicht auf ein KI-System gelungen, die aufgrund der rasanten Entwicklungen nicht den Anspruch auf Vollständigkeit erheben kann, aber einen Weg aufzeigt, die komplexen Strukturen eines KI-Systems zu berücksichtigen.

Betrachtet man die unterschiedlichen „Felder" der Matrix, z. B. das Gewährleistungsziel „Transparenz", in den verschiedenen Phasen des Lebenszyklus eines KI-Systems, dann zeigen sich in jeder Phase die unterschiedlichen Fragestellungen zur Transparenz.



Neben der ausführlichen Beschreibung der technischen und organisatorischen Maßnahmen in Textform ist dem Positionspapier eine übersichtliche Tabelle als Anhang beigefügt, die die Maßnahmen in Kurzform den einzelnen Phasen und Gewährleistungszielen zuordnet.

Die „Hambacher Erklärung zur Künstlichen Intelligenz" und das „Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen" sind unter den folgenden Links abrufbar:

Hambacher Erklärung:

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

Kurzlink: *https://uldsh.de/tb38-102a*

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

Kurzlink: *https://uldsh.de/tb38-102b*

Was ist zu tun?

Anwender und Entwickler von KI-Systemen sollten die Hinweise aus der „Hambacher Erklärung zur Künstlichen Intelligenz" und aus dem Positionspapier berücksichtigen. Zudem sollte im KI-Bereich ein Schwerpunkt der Forschung auf Realisierungen und Verbesserungen von KI-Systemen im Sinne der Grundrechte und Werte gelegt werden – hierfür könnten Fördergeber Anreize bieten.

10.3 Nutzung von DNS-over-HTTPS

Neuere Browserversionen enthalten Funktionen, die eine Namensauflösung durch das Domain Name System (DNS) mittels kryptografisch gesicherter Verbindungen (TLS) ermöglichen. Während dieser Ansatz einerseits eine bekannte Schwachstelle der Internetnutzung anpackt, können andererseits neue Probleme entstehen.

In der Vergangenheit kam beim DNS wenig kryptografische Sicherheit zum Einsatz, was Angreifende aller Couleur immer wieder ausnutzen, um beispielsweise zu überwachen, mit welchen Diensten Nutzerinnen und Nutzer kommunizieren, oder um ihnen für Betrugs- oder Zensurversuche manipulierte Daten unter-

zuschieben. In einigen Ländern werden auf diese Weise Netzsperren versucht. Manche Provider nutzen diese Angriffsmöglichkeit gar, um ihren Kundinnen und Kunden Werbung aufzudrängen. Umgekehrt können Nutzende eigene (lokale) DNS-Server betreiben, um damit potenziell schädliche Dienste, die etwa Viren verbreiten oder User-Tracking betreiben, für das komplette Heimnetz zu unterdrücken: Dazu werden lokale DNS-Anfragen von Clients vom eigenen DNS-Server mit Sperrlisten abgeglichen. Befindet sich ein angefragter Server auf dieser Liste, so erhält der Client eine „Nullantwort" und der Verbindungsaufbau unterbleibt. Technisch sind diese Mechanismen ähnlich wie die oben genannten Netzsperren oder Umleitungen durch Provider – mit dem Unterschied, dass hier die Nutzenden selbst entscheiden.

Domain Name System (DNS)

DNS ist der zentrale Dienst im Internet, der es ermöglicht, Namen wie z. B. www.datenschutzzentrum.de in IP-Adressen aufzulösen, sodass Datenpakete an das richtige Ziel versendet werden können. DNS ist vorrangig auf Robustheit ausgelegt. Unzählige Server bieten den Dienst an und gleichen sich asynchron miteinander ab. Dadurch verbreiten sich geänderte Einträge zwar mit einer gewissen Trägheit, dafür erhält man aber eine hohe Verfügbarkeit. Fällt ein DNS-Server aus, kann auf andere DNS-Server ausgewichen werden.

Mit DNS-over-TLS (DoT) und DNS-over-HTTPS (DoH) wurden zwei Standards vorgeschlagen, um DNS-Anfragen durch verschlüsselte Übertragung gegen Ausspähung und Manipulation zu schützen. Bei DoT wird das bisherige DNS-Protokoll – vereinfacht ausgedrückt – lediglich um die Verwendung von TLS für die Verbindung erweitert (kryptografische Absicherung der Netzpakete). Bei DoH wird eine HTTPS-Verbindung aufgebaut, wie sie auch zum Abruf von Webseiten genutzt wird. Dies hat den zusätzlichen Vorteil, dass für Angreifer mit lesendem Zugriff die Namensauflösung nicht von anderen Datentransfers im Web unterscheidbar ist. Durch den zusätzlich zum DNS zu betreibenden Webserver, um DoH als Dienst anzubieten, eröffnen sich aufgrund der zusätzlichen Komplexität dabei allerdings neue Angriffsmöglichkeiten, sodass ein erhöhter Aufwand für eine fortwährende Absicherung im Betrieb zu erwarten ist.

Während die Namensauflösung per DNS üblicherweise durch das Betriebssystem erfolgt, wird DoH derzeit in Browsern implementiert. Dies bietet den Vorteil, dass auch in Umgebungen mit zensierenden DNS-Servern, die einem (Betriebs-)System zwangsweise zugewiesen werden, ein unmanipulierter DNS-Server durch den Browser leichter anzusprechen ist. Damit sollen Zensurmaßnahmen, wie man sie in autoritären Staaten findet, leichter umgehbar sein.

Werden Browser allerdings so ausgeliefert, dass sie als Voreinstellung DoH nutzen, erschwert dies eine Integration in lokalen Netzen, da lokale Servernamen dann nicht in IP-Adressen aufgelöst werden können. Auch die beschriebenen Schutzmaßnahmen vor Schadsoftware und User-Tracking durch lokale DNS-Server greifen dann nicht mehr. Insbesondere dann, wenn alle Browser auf einen einzigen DoH-Server verwiesen werden, ergeben sich sogar deutliche Vertraulichkeitsprobleme. Denn es fallen sehr viele Informationen darüber, welche Systeme mit welchen Diensten kommunizieren, an wenigen zentralen Stellen an. Nicht alle Nutzenden sind in der Lage, diese Problematik zu überblicken, geschweige denn selbst technisch Abhilfe zu schaffen. Die bisherige DNS-Landschaft mit vielen verteilten Systemen bietet daher klare Vorteile. Wichtig ist hier, dass auch künftig die Wahl des DNS-Servers in der Hand der Nutzenden bzw. der Geräteadministration bleibt. Keinesfalls sollte eine DNS-Vorauswahl fest im Betriebssystem verankert werden. Dies ist gerade im Hinblick auf das Unternehmen Google relevant, das als Anbieter sowohl eines Betriebssystems als auch eines DNS-Dienstes eine solche Kopplung in Erwägung ziehen könnte.

Sofern Browser und Betriebssystem (bzw. andere Anwendungen auf dem System) jeweils unterschiedliche DNS-Server nutzen, kann dies nicht nur zu deutlicher Verwirrung bei den Nutzenden führen; auch die Funktionen von Sicher-

heitssoftware bzw. anderen Schutzmaßnahmen könnten dadurch beeinträchtigt werden.

Andere Erweiterungen des DNS sind schon etwas länger verfügbar, haben sich aber auch noch nicht flächendeckend durchgesetzt. Mit den „Domain Name System Security Extensions" (DNSSEC) sowie ergänzend „DNS-based Authentication of Named Entities" (DANE) stehen Hilfsmittel bereit, um die Einträge im DNS mit digitalen Signaturen zu versehen, sodass Manipulationen bemerkbar werden. Auf diese Weise können auch TLS-Zertifikate an Domain-Namen gebunden und gegen unbefugte Austausche gesichert werden (37. TB, Tz. 10.1). Leider werden diese Verfahren noch nicht von allen Domain-Anbietenden unterstützt. Zudem sind noch nicht alle DNS-nutzenden Instanzen in der Lage, Einträge darüber zu validieren. Auch die Signalisierung an die Nutzenden, wenn eine Manipulation erkannt wird, ist noch eine Baustelle.

Was ist zu tun?

Die DNS-Nutzung und damit auch deren verschlüsselnde Abwicklung sollten nicht auf Browser-, sondern auf Systemebene erfolgen. Die Hersteller von Betriebssystemen sind daher aufgefordert, DoT und DoH zu implementieren (sofern nicht schon geschehen). Browser sollten nicht auf wenige zentrale DoH-Server voreingestellt sein. Die Betreiber von DNS-Resolvern sollten zeitnah auf verschlüsselnde Dienste umstellen. Domain-Anbietende sollten DNSSEC und DANE unterstützen.

10.4 Verschlüsselte Kommunikation mit Behörden

Immer noch ist die verschlüsselte Kommunikation mit Behörden ein schwieriges Pflaster, da es weiterhin an der Etablierung von Verschlüsselungsstandards fehlt bzw. etablierte Standards aus verschiedenen Gründen nicht genutzt werden.

Ein weiteres Problem ist häufig die Eilbedürftigkeit. Zwar kann man zu Recht von Behörden und anderen öffentlichen Stellen verlangen, eine regelmäßige Kommunikation untereinander adäquat durch Verschlüsselungsverfahren abzusichern, etwa durch den Austausch von Zertifikaten oder PGP-Schlüsseln oder über die Bereitstellung von Webportalen über HTTPS-Verbindungen und Zugriffskontrollen. Dies gilt auch für die Kommunikation von Behörden mit Personen oder Organisationen, die im Auftrag oder für Behörden tätig sind und dabei eigene Technik verwenden, etwa Betreuungspersonen für Jugendliche oder Lehrkräfte. Zwar wären übergreifende sichere Kommunikationsverfahren gut, doch in der Praxis sind heutzutage meist individuelle Absprachen und Lösungen nötig.

Doch wie kann man vorgehen, wenn spontan eine dringende Kommunikation mit einem Partner notwendig ist, mit dem noch kein Verfahren etabliert wurde, etwa die Verwaltung dringend Hilfe leisten muss oder will und es einer eiligen Klärung etwa bei einem Rentenversicherungsträger bedarf? Ebenso wie man bedenkenlos zum Telefon greift oder sich bei der Briefpost auf die Sicherheit der Infrastruktur verlässt, liegt die Nutzung von Messengern, E-Mail oder cloudbasierten Datei-Sharingdiensten nahe. In diesen Fällen sind häufig Dienstleister außerhalb des Geltungsbereichs der DSGVO und des Telekommunikationsgesetzes beteiligt, die zumindest teilweise auch Inhaltsdaten analysieren. Daher sind diese Verfahren trotz ihrer technischen Einfachheit ohne datenschutzrechtliche Analyse nicht geeignet, spontan ausgewählt zu werden.

Ein Ausweg besteht darin, zumindest vorab einige dieser Verfahren zu sichten und zu prüfen – dann kann man im Bedarfsfall auf ein Portfolio zurückgreifen und findet vielleicht ein Verfahren, dass für beide Kommunikationspartner nutzbar ist. Kommen dabei webbasierte Dienste zum Einsatz, dürften diese für die Kommunikationspartner zumindest aus technischer Sicht leicht nutzbar sein, ohne dass die Installation von Apps oder Programmen notwendig ist. Oder es finden sich Verfahren, die vielleicht nicht von jedem Arbeitsplatz aus nutzbar sind, aber dennoch eine höhere Sicherheit aufweisen als eine unverschlüsselte E-Mail: So sind beispielsweise viele öffentliche Stellen über De-Mail oder das elektronische Behördenpostfach erreichbar.

Perspektivisch sind Multikanallösungen geeignet, die den Beschäftigten in den Behörden Empfang und Versand von Nachrichten am Arbeitsplatz erlauben – losgelöst von den Details des elektronischen Transports und der Verschlüsselung.

11

KERNPUNKTE

Guidelines aus Europa – Verantwortlicher und Auftragsverarbeiter

Guidelines aus Europa – der Vertrag als Rechtsgrundlage

11 Europa und Internationales

Eine Harmonisierung des Datenschutzes in Europa kann nur gelingen, wenn die Normen der DSGVO einheitlich ausgelegt und angewendet werden. Die Guidelines des Europäischen Datenschutzausschusses (EDSA), dem Gremium der Aufsichtsbehörden in Europa, geben die wichtigsten Übereinkünfte der europäischen Aufsichtsbehörden wieder. Die Guidelines werden in Arbeitsgruppen (Expert Subgroups) erarbeitet. Das ULD ist als Vertreter der Datenschutzaufsichtsbehörden der Länder Mitglied in der Key Provisions Expert Subgroup, wo Grundsatzfragen geklärt werden. Als stellvertretender Ländervertreter arbeitet das ULD in der Technology Expert Subgroup mit, die den Fokus auf Informations- und Kommunikationstechnologien und verwandte Themen legt. Darüber hinaus beteiligt sich das ULD in Unterarbeitsgruppen und entsendet zu Einzelfragen Vertreterinnen und Vertreter in die Arbeitsgruppen des EDSA.

11.1 Guidelines aus Europa – Verantwortlicher und Auftragsverarbeiter

Das ULD war an einer Stellungnahme (englisch: „Guidelines“) zu den Anforderungen an Verantwortliche und Auftragsverarbeiter in der Key Provisions Expert Subgroup des EDSA beteiligt. Zur Vorbereitung der Stellungnahme wurde eine Anhörung in Brüssel begleitet, bei der Vertreterinnen und Vertreter der Wirtschaft, von Verbänden und von Nichtregierungsorganisationen die Möglichkeit erhielten, ihre Erfahrungen und Erwartungen an diese Guidelines einzubringen.

Die Guidelines, an denen im Berichtsjahr intensiv gearbeitet wurde und die im Jahr 2020 im EDSA abgestimmt und veröffentlicht werden sollen, werden die Vorgaben der DSGVO zum Verantwortlichen, zum Auftragsverarbeiter und zur gemeinsamen Verantwortlichkeit präzisieren. Anhand von Fallbeispielen werden die weiteren Anforderungen erläutert.

Key Provisions Expert Subgroup

Die Key Provisions Expert Subgroup des Europäischen Datenschutzausschusses (EDSA) befasst sich mit grundlegenden Themen und Begriffen der DSGVO und bereitet dazu Stellungnahmen (Guidelines) des EDSA vor.

11.2 Guidelines aus Europa – der Vertrag als Rechtsgrundlage

Als Vertreter der deutschen Bundesländer in der Key Provisions Expert Subgroup hat das ULD als Co-Berichterstatter die Guidelines des EDSA zur Rechtsgrundlage aus Art. 6 Abs. 1 Buchst. b DSGVO mitverfasst.

Die Guidelines wurden in der 14. Sitzung des EDSA-Plenums im Oktober 2019 verabschiedet, nachdem sie im Rahmen einer Konsultation der Öffentlichkeit im April 2019 vorgestellt worden waren.

Vertragliche Rechtsgrundlage

Gemäß Art. 6 Abs. 1 Buchst. b DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn diese für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen.

Die Guidelines beschäftigen sich mit der Frage, unter welchen Bedingungen eine Verarbeitung von personenbezogenen Daten für die Erfüllung eines Vertrags erforderlich ist. Anlass ist der Umstand, dass Unternehmen insbesondere bei Online-Angeboten dazu neigen, mehr personenbezogene Daten zu erheben und weiterzuverarbeiten, als dies unbedingt für die Erbringung der von ihnen angebotenen Leistung notwendig ist. Oft werden dafür Verträge künstlich erweitert, oder es wird die Erteilung einer Einwilligung vom Betroffenen anstelle einer Geldzahlung als Gegenleistung erwartet.

Die Guidelines stellen klar, dass nur solche Verarbeitungen durch Art. 6 Abs. 1 Buchst. b DSGVO gerechtfertigt werden können, die bei einer objektivierten Betrachtung des geschuldeten Vertragsgegenstands erforderlich sind. Verarbeitungen, die dazu nicht erforderlich sind, deren Zwecke aber im Vertrag aufgeführt werden, müssen durch eine andere Rechtsgrundlage gerechtfertigt sein.

Die „Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects" liegen bislang nur in englischer Sprache vor:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

Kurzlink: *https://uldsh.de/tb38-112*

12

KERNPUNKTE

Geschäftsgeheimnisse europäisch definiert

Eigenverantwortlichkeit bei erlangten Informationen

Transparenzportal

12 Informationsfreiheit

12.1 Geschäftsgeheimnisse europäisch definiert

Mit dem Gesetz zum Schutz von Geschäftsgeheimnissen hat der Bundesgesetzgeber in Umsetzung einer europäischen Richtlinie auch die Begriffsbestimmung für die Geschäftsgeheimnisse neu geformt. Demnach gilt:

„Geschäftsgeheimnis ist eine Information,

- die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und
- die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und
- bei der ein berechtigtes Interesse an der Geheimhaltung besteht."

Die Einschätzung, inwieweit Geschäftsgeheimnisse bei der Gewährung eines Informationszugangs durch informationspflichtige Stellen bereitzustellen sind, ist Gegenstand einer Prüfung von § 10 Satz 1 Nr. 3 Informationszugangsgesetz Schleswig-Holstein (IZG-SH). Nach dieser Vorschrift ist der Antrag u. a. abzulehnen, soweit durch die Bekanntgabe der Informationen Betriebs- oder Geschäftsgeheimnisse zugänglich gemacht würden. Dies bedingt eine Untersuchung, ob die begehrten Informationen überhaupt ein Geschäftsgeheimnis darstellen.

Mit der neuen Begriffsbestimmung werden zunächst die bisher verwendeten Kriterien berücksichtigt, wie etwa das berechtigte Interesse an einer Geheimhaltung, das auch mit der Wettbewerbsrelevanz der Geschäftsgeheimnisse im Zusammenhang steht.

Besondere Bedeutung hat jedoch das neu geschaffene Merkmal, wonach die schutzbedürftigen Informationen Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen sein müssen. Dabei fehlen nähere Hinweise des Gesetzgebers, was konkret angemessene Geheimhaltungsmaßnahmen sein können. Es liegt aber nahe, dass der Geheimnischarakter und damit auch die Qualität der Informationen als Geschäftsgeheimnis verloren gehen, wenn angemessene Sicherheitsmaßnahmen fehlen. Für jedermann zugängliche Informationsquellen im Internet oder frei zugängliche Räume mit dort gelagerten schutzbedürftigen Unterlagen würden keine angemessenen Geheimhaltungsmaßnahmen darstellen. Unternehmen sollten im Fall von Geschäftsgeheimnissen weitere Sicherheitsmaßnahmen erwägen, wie etwa eine Verschlüsselung von Datenträgern und eine probate Benutzer- und Rechteverwaltung.

Was ist zu tun?

Für die geheimhaltungsbedürftigen Informationen, die inhaltlich den Charakter eines Geschäftsgeheimnisses erfüllen, müssen angemessene Sicherheitsmaßnahmen getroffen werden. Hiervon kann für die Beurteilung nach § 10 Satz 1 Nr. 3 IZG-SH abhängen, inwieweit ein Geschäftsgeheimnis vorliegt.

12.2 Erforderlichkeit zur Angabe einer Postadresse

In einer Angelegenheit ist ein Bürger an uns herangetreten, weil die informationspflichtige Stelle von ihm die Angabe seiner postalischen Anschrift forderte.

Vorausgegangen war ein per E-Mail gestellter IZG-SH-Antrag des Bürgers bei der informationspflichtigen Stelle. Diese verlangte von dem Antragsteller vor der Bearbeitung seines Antrags die Angabe seiner vollständigen postalischen Anschrift. Begründet wurde diese Forderung damit, dass dies für den Erlass eines rechtsmittelfähigen Bescheids erforderlich sei und der Antragsteller zudem identifiziert werden müsse.

Das ULD konnte sich dieser Rechtsauffassung nicht anschließen. Die Aufforderung an den Antragsteller, seine postalische Anschrift bekannt zu geben, liefe darauf hinaus, eine bestimmte Form des Antrags zu verlangen. Bereits hierzu fehlt im IZG-SH eine entsprechende Verpflichtung. Der Gesetzgeber hat vielmehr ausdrücklich von einem Formerfordernis abgesehen. Anträge können schriftlich, mündlich oder elektronisch gestellt werden. Die Angabe einer Postanschrift wird nicht gefordert.

Sofern die anstehende Informationserteilung personenbezogene Daten Dritter berühren würde, ist die Datenübermittlung an den Empfänger nach Art. 5 Abs. 2 in Verbindung mit Art. 24 DSGVO zu protokollieren und im Rahmen eines etwaigen Auskunftsverlangens an den betroffenen Dritten nach Art. 15 Abs. 1 Buchst. c DSGVO zu berücksichtigen. Daraus folgt, dass die zu Protokollzwecken vorzunehmende Abfrage der postalischen Anschrift so lange unzulässig bleibt, wie die Übermittlung der personenbezogenen Daten des Dritten nicht unmittelbar bevorsteht. Die postalische Anschrift wäre im Übrigen auch nicht für die Durchführung eines Anhörungsverfahrens nach § 10 Satz 3 IZG-SH notwendig.

Grundsätzlich ist es nach Auffassung des ULD weder aus Bestimmtheitsanforderungen noch aus Gründen der wirksamen Bekanntgabe eines Verwaltungsaktes erforderlich, dass der per E-Mail anfragende Antragsteller seine postalische Anschrift nennt. Sollten für die Bereitstellung der Informationen Kosten anfallen, wäre dies für den vorliegenden Fall zu prüfen.

Entgegen der im geführten Verfahren vorgebrachten Ansicht der informationspflichtigen Stelle ist der Antragsteller aber nicht verpflichtet, mittels Angabe der Postanschrift eine Anspruchsberechtigung nachzuweisen.

12.3 Eigenverantwortlichkeit bei der Weiterverwendung der erlangten Informationen

Erhält die antragstellende Person auf den Antrag nach dem IZG-SH die begehrten Informationen, möchte sie die Informationen meist auch weiterverwenden. Mitunter ergeben sich sogar bereits in der Anfrage Anhaltspunkte dafür, dass eine Veröffentlichung der erlangten Informationen durch die antragstellende Person im Internet geplant ist.

Dabei ist zu beachten, dass das IZG-SH keine Regelungen dazu enthält, wie die durch dieses Gesetz erlangten Informationen weiterverwendet werden dürfen. Die antragstellende Person handelt bei der Weiterverwendung der erlangten Informationen daher in voller Eigenverantwortung. Das bedeutet, dass von der antragstellenden Person verschiedene Aspekte, wie etwa die Persönlichkeitsrechte anderer Personen oder andere Rechte Dritter, zu prüfen und zu berücksichtigen sind. Auch sind etwaige zivilrechtliche Forderungen der von der Übermittlung betroffenen Dritten wegen Verletzung von deren Rechten (z. B. Betriebs- und Geschäftsgeheimnisse) in Betracht zu ziehen. Nichts anderes ergibt sich aus dem Informationsweiterverwendungsgesetz (IWG).

Die informationspflichtige Stelle, welche die Informationen herausgibt und z. B. Anhaltspunkte dafür hat, dass von der antragstellenden

Person eine Veröffentlichung im Internet geplant ist, darf die Verwendung der Informationen aus diesem Grund nicht einschränken. Das IZG-SH enthält dafür keine Rechtsgrundlage. Die informationspflichtige Stelle kann und sollte aber einen Hinweis auf die Eigenverantwortlichkeit der antragstellenden Person erteilen.

Was ist zu tun?

Die antragstellende Person muss eigenverantwortlich prüfen, ob eine beabsichtigte Weitergabe der von der informationspflichtigen Stelle erlangten Informationen zulässig ist. Auf diesen Umstand sollten die informationspflichtigen Stellen hinweisen.

12.4 Kosten bei der Erteilung des Informationszugangs in Selbstverwaltungsangelegenheiten

Wiederholt wurde an das ULD die Frage herangetragen, ob die informationspflichtige (kommunale) Stelle in Selbstverwaltungsaufgaben Kosten für die Erteilung der Informationen, die nach dem IZG-SH herausgegeben wurden, nach einer kommunalen Satzung oder nach der Landesverordnung über Kosten nach dem Informationszugangsgesetz (IZG-SH-KostenVO), die eine Beschränkung der Gebühren vorsieht, verlangen darf.

Das ULD vertritt die Auffassung, dass auch in diesen Fällen die IZG-SH-KostenVO als Rechtsgrundlage für die Erhebung und Bemessung von Kosten heranzuziehen ist. Ableitbar ist dies aus den Gesetzesmaterialien zum IZG-SH. Der Gesetzgeber wollte bereits im Rahmen der früheren Regelung mit der Kostenregelung sicherstellen, dass die antragstellende Person nicht durch zu hohe Kosten abgeschreckt wird. Dies würde dem Grundcharakter dieses Gesetzes, das den Zugang zu Informationen unabhängig von einem bestehenden Interesse ermöglichen will, zuwiderlaufen. In den Gesetzesmaterialien findet sich zwar des Weiteren der Hinweis, dass sich die in dem weggefallenen Umweltinformationsgesetz Schleswig-Holstein (UIG-SH) enthaltene Ermächtigung zur Gebührenerhebung u. a. auch an die kommunalen Gebietskörperschaften richtet, wenn sie für Informationserteilungen in Selbstverwaltungsangelegenheiten Kosten nach dem Kommunalabgabengesetz erheben (Schleswig-Holsteinischer Landtag, Drs. 16/722, Seite 37 zu § 9).

Unter Berücksichtigung der weiteren Gesetzesmaterialien (Drs. 17/171, Seite 24 zu § 9) kann dieser Hinweis jedoch nicht so verstanden werden, dass Satzungen anstelle der IZG-SH-KostenVO anwendbar sind. Der Gesetzgeber weist eindeutig auf „speziellere Vorgaben" des damaligen UIG-SH (Drs. 17/171, Seite 24 zu § 9) bzw. auf eine „spezifische Kostenregelung" im Verordnungswege hin (Drs. 17/1610, Seite 25 zu § 12). Hätte der Gesetzgeber eine Öffnungsklausel gewollt, die weiter gehende satzungsrechtliche Vorschriften zulässt, hätte er dies ausdrücklich geregelt – beispielsweise entsprechend § 10 Abs. 3 Satz 1 des Akteneinsichts- und Informationsgesetzes des Landes Brandenburg, der eine Befugnis, die Erhebung von Gebühren und Auslagen auch durch Satzung regeln zu können, enthält.

Was ist zu tun?

Werden Informationen nach dem IZG-SH bereitgestellt, die Selbstverwaltungsangelegenheiten der informationspflichtigen Stelle betreffen, sind etwaige Kosten nach der IZG-SH-KostenVO zu erheben.

12.5 Transparenzportal – Veröffentlichungspflichten der Landesbehörden

Unter der Überschrift „Transparenzgesetz Schleswig-Holstein" wurde das IZG-SH vor einigen Jahren reformiert (36. TB, Tz. 12.1). In einer ersten Stufe ist die Veröffentlichungspflicht für Landesbehörden ab dem 01.01.2020 dort geregelt (§ 11 IZG-SH in neuer Fassung). Hierbei entsteht die Verpflichtung für die genannten Stellen, Richtlinien, Runderlasse an andere Behörden, amtliche Statistiken, öffentliche Tätigkeitsberichte und Broschüren, Haushaltspläne, Stellenpläne und Wirtschaftspläne sowie Vorlagen der Landesregierung nach Beschlussfassung und Mitteilung an den Landtag aktiv zu veröffentlichen.

Das Land richtet hierzu ein zentrales elektronisches Informationsregister und Informationsregisterstellen ein, um das Auffinden der Informationen zu erleichtern und interessierte Personen zu beraten. Aus diesem Grund wurde das Transparenzportal Schleswig-Holstein in Betrieb genommen, in dem Bürgerinnen und Bürger nach Informationen suchen können (siehe auch Tz. 6.3.2).

Einzelheiten, insbesondere die organisatorischen Zuständigkeiten und Pflichten der einzelnen Behörden zur Erfüllung der Veröffentlichungspflichten, regelt die Landesregierung nach § 11 Abs. 5 IZG-SH in einer Rechtsverordnung.

Das Transparenzportal ist erreichbar unter:

https://transparenz.schleswig-holstein.de/

Was ist zu tun?

Landesbehörden sind nach § 11 Abs. 3 IZG-SH verpflichtet, die im IZG-SH näher bestimmten Informationen mit einheitlichen Metadaten zu registrieren. Dafür müssen sie die organisatorischen Voraussetzungen schaffen.

13

KERNPUNKTE

Datenschutzbildung und -fortbildung

DATENSCHUTZAKADEMIE

Sommerakademie

13 DATENSCHUTZAKADEMIE Schleswig-Holstein

Die Datenschutz-Grundverordnung betont die Wichtigkeit des Fachwissens bei den behördlichen und betrieblichen Datenschutzbeauftragten. Hierzu besteht das Angebot der DATENSCHUTZAKADEMIE Schleswig-Holstein, die seit 1993 die Konzeption und Organisation der Fortbildungsveranstaltungen zu Datenschutz und Informationsfreiheit leistet.

Als verpflichtende Aufgabe muss jede Datenschutzaufsichtsbehörde außerdem „die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären" (Art. 57 Abs. 1 Buchst. c DSGVO) und „die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten sensibilisieren (Art. 57 Abs. 1 Buchst. e DSGVO) – auch dafür werden Veranstaltungen angeboten.

13.1 Fortbildungsveranstaltungen im Programm der DATENSCHUTZAKADEMIE

Die Nachfrage nach qualitativ hochwertigen Fortbildungsveranstaltungen im Bereich Datenschutz und Datensicherheit ist weiterhin ungebrochen. Im Schulungsjahr 2019 hat die DATENSCHUTZAKADEMIE mehr als 60 Fortbildungsveranstaltungen durchgeführt. Dabei ließen sich über 1.000 Teilnehmende von den Dozentinnen und Dozenten der DATENSCHUTZAKADEMIE zu dem vielfältigen Themenbereich von Datenschutz, Datensicherheit und Informationsfreiheit fortbilden.

Die seit Jahren durchgeführten behördlichen und betrieblichen Grundlagenkurse der DATENSCHUTZAKADEMIE werden kontinuierlich gut angenommen und bilden damit eine solide Grundlage für datenschutzkonformes Handeln in schleswig-holsteinischen Landesbehörden, kommunalen Verwaltungen und Unternehmen.

Aufgrund der neuen gesetzlichen Regelungen ist die Nachfrage nach Fortbildungsveranstaltungen im Bereich Informationszugangsgesetz und Transparenzgesetz im Vergleich zu den Vorjahren besonders hoch.

Neben dem rechtlichen Fortbildungsangebot bestand zum Themenschwerpunkt „Technischer Datenschutz und Datensicherheit" eine hohe Nachfrage. Zunehmende Digitalisierung und eine Vielzahl neuer technischer Verarbeitungsverfahren führen zu einem Bedarf nach entsprechenden Fortbildungsangeboten.

Wie auch in den vorangegangenen Jahren wurde eine Vielzahl von Sonderkursen mit speziell auf den Auftraggeber zugeschnittenen Themen im Bereich Datenschutz und Datensicherheit durchgeführt.

Die Schülerkurse „Entscheide DU – sonst tun es andere für dich!" erfreuten sich im Berichtszeitraum weiterhin großer Beliebtheit. Fast 2.000 Schülerinnen und Schülern aller Schultypen (ab Klassenstufe 5) wurde vor Ort in ihren Schulen Datenschutz- und Medienkompetenz, besonders mit Fokus auf den Umgang mit ihren eigenen Daten im Internet und in sozialen Medien, vermittelt.

Das Jahresprogramm der DATENSCHUTZAKADEMIE finden Sie unter:

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

13.2 Sommerakademie – jährliche Datenschutzkonferenz in Kiel

Die alljährlich an einem Montag im Spätsommer stattfindende Sommerakademie der DATENSCHUTZAKADEMIE zog auch im Jahr 2019 Datenschutzexpertinnen und -experten sowie Interessierte aus dem gesamten Bundesgebiet und darüber hinaus nach Kiel.

Unter dem Thema „Verbraucher im Fokus'" wurden gesellschaftspolitische Fragen zu den Stellschrauben für den Verbraucherdatenschutz im Internet diskutiert. Das Problem: Umfassendes Tracking und Analyse des Nutzungsverhaltens im Internet, eine darauf aufbauende Kategorisierung der Menschen sowie eine manipulative Gestaltung von Angeboten (sogenannte „Dark Patterns") führen zu unfairer Behandlung der Verbraucherinnen und Verbraucher in der Online-Welt. Vorträge aus Wissenschaft und Praxis gaben interessante Einblicke darin, wo die Probleme in der Realität liegen und welche Lösungsansätze zielführend sein können, z. B. bei dem Auskunftsanspruch der betroffenen Personen, alternativen Social-Media-Modellen ohne Werbung, digitaler Souveränität für die Nutzenden, cleverem Einwilligungsmanagement und anderen Assistenzsystemen sowie dem proaktiven Wahrnehmen von Verantwortung durch Unternehmen im digitalen Bereich (Stichwort „Corporate Digital Responsibility").

Die Präsentationen der Vortragenden sind ebenso wie die visuellen Protokolle („Graphical Recordings"), in denen wichtige Aussagen während des Vortrags zeichnerisch aufgegriffen und grafisch in Beziehung gesetzt werden, auf unserer Webseite verfügbar:

https://www.datenschutzzentrum.de/sommerakademie/2019/

Dort findet man auch Material zu den Themen aus den Praxis-Infobörsen am Nachmittag, die nicht nur für behördliche oder betriebliche Datenschutzbeauftragte interessant sind.

Index

K

L

M

N

O

P

R

S

T

U

V

W

Z