ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

TÄTIGKEITSBERICHT
2019

Tätigkeitsbericht 2019
des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

BERICHTSZEITRAUM: 2017/2018

REDAKTIONSSCHLUSS: 31.03.2019

LANDTAGSDRUCKSACHE 19/1430

(37. 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

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

Inhaltsverzeichnis

01

KERNPUNKTE

Datenschutz aus Europa

Die Dienststelle der Landesbeauftragten für Datenschutz

Digitalisierung in Schleswig-Holstein

1 Datenschutz und Informationsfreiheit

1.1 Die Zeitenwende – Datenschutz aus Europa

Datenschutz-Grundverordnung. Stichtag 25. Mai 2018. Alles neu? Eigentlich nicht. Das neue Datenschutzrecht weicht gar nicht so sehr von dem vorherigen ab. Wer vorher gut aufgestellt war, hat keinen großen Aufwand, um sich an die neuen Gegebenheiten anzupassen. Warum dann also die Hysterie, ja fast schon Panik? Wahrscheinlich liegt der Grund in der Angst vor hohen Geldbußen, die mit einem signifikant erweiterten Bußgeldrahmen erstmalig in der Geschichte des deutschen Datenschutzes Abschreckungscharakter haben. Art. 83 Abs. 1 DSGVO spricht daher auch davon, dass etwaige Geldbußen „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend" sein müssen. Man sieht aber an der Formulierung, dass sich diese Ängste relativieren, denn es ist – wie stets – geboten, dass solche Sanktionen verhältnismäßig sind. Es geht also nicht um ein unfaires Abstrafen.

Nun wollen die meisten Verantwortlichen es richtig machen und das Datenschutzrecht einhalten. Vielen ist dies kurz vor dem Wirksamwerden der DSGVO eingefallen, was dazu führte, dass im Unabhängigen Landeszentrum für Datenschutz die Telefone nicht mehr stillstanden, die E-Mail-Flut nicht mehr zu bewältigen war und bei Schulungen oder Präsentationen die Nachfrage auch zu Einzelthemen enorm war. Während wir zuerst in unseren Hinweisen und Vorträgen aufgezeigt haben, wie man sich mit wenig Aufwand von den Regelungen des Bundesdatenschutzgesetzes (BDSG) an die DSGVO anpassen kann, stellte sich immer mehr heraus, dass viele Anfragende sich anscheinend vorher um Datenschutz noch gar nicht gekümmert hatten und gar nicht wussten, dass sie auch vor Mai 2018 viele Datenschutzpflichten hätten einhalten müssen. Datenschutz war sicher kein Geheimthema gewesen, das nur Spezialisten bekannt war. Und doch haben erst die DSGVO und der Presse-Hype dazu geführt, dass das Thema ernst genommen wurde.

Die starke Verunsicherung wurde noch angeheizt mit Gerüchten, dass so ungefähr jede Datenverarbeitung nun verboten sei, mit Fällen von Überreaktionen oder Halbwahrheiten, die auf Titelseiten der Boulevardpresse zelebriert wurden (z. B. die Klingelschildposse „Ding Dong Datenschutz", Tz. 5.4.6), und von mehr oder weniger fragwürdigen Dienstleistern, die sich kleinen Firmen aufdrängten und ihnen nahelegten, dass man sie anheuern müsse, um Strafen und die prognostizierte Abmahnwelle zu vermeiden.

Im öffentlichen Bereich war es etwas ruhiger, obwohl die schleswig-holsteinischen Verwaltungen nicht schon – wie bei der DSGVO – für eine zwei Jahre lange Übergangszeit auf den veröffentlichten Gesetzestext zurückgreifen konnten, sondern das neue Landesdatenschutzgesetz und viele andere Datenschutzregeln erst kurzfristig in der finalen Version vorlagen und am 27. April 2018 von dem Schleswig-Holsteinischen Landtag beschlossen wurden (Tz. 4.1.1). Die neue Pflicht zur Benennung der behördlichen Datenschutzbeauftragten (Tz. 4.1.2) ergab sich bereits aus der DSGVO und war bekannt, aber die notwendigen Anpassungen in Abläufen und technischer Gestaltung, die Nacharbeiten bei Informationspflichten und die erforderlichen Aktualisierungen von Satzungen sind teilweise immer noch nicht abgeschlossen.

Im Ergebnis ist der gewünschte Effekt der DSGVO, dass EU-weit schnell und flächendeckend ein gutes Datenschutzniveau erreicht wird, noch nicht eingetreten. Ab dem ersten Geltungstag der DSGVO taten einige große außereuropäische Anbieter so, als wäre nun der Datenschutz viel laxer zu handhaben. Gerichtliche Untersagungen gegen eine invasive Datenverarbeitung wurden nicht mehr als bindend angesehen, da das neue Datenschutzrecht die entsprechende Verarbeitung angeblich erlauben würde. Zwar gibt es bei allen Aufsichtsbe-

hörden zahlreiche Beschwerden, die sich gegen solche Datenverarbeitungen richten, aber die Aufklärung und Bewertung der Sachverhalte ist nicht leicht bei weiterhin stark beschränkten Ressourcen der Aufsichtsbehörden und vielfach vorhandenen Defiziten in Transparenz und Kooperation dieser Datenverarbeitungskonzerne bei gleichzeitig sich ständig ändernden Diensten und Produkten.

Auch waren anscheinend viele Bürgerinnen und Bürger enttäuscht, weil nicht gleich die erwarteten großen Bußgelder verhängt wurden. Dies ist natürlich kein Wunder: Die Datenschutzaufsichtsbehörden sind nicht als schnelle Eingreiftruppe aufgebaut, sondern bearbeiten sukzessive und rechtskonform die eintreffenden Beschwerden, wie es das nationale Verwaltungsverfahrensrecht der einzelnen Staaten vorsieht. Dazu gehören bei mutmaßlichen Verstößen eine sorgfältige Aufklärung der Sachverhalte und Anhörungsverfahren zu den aufsichtsbehördlichen Bewertungen der Aufsicht, bevor Entscheidungen über etwaige Sanktionen getroffen werden.

Diejenigen, die es richtig machen wollten, waren auch nicht glücklich, weil sie feststellten, dass Hersteller von Produkten und Anbieter von Dienstleistungen ihnen oft keine Hilfe waren und es damit schwierig war, die eigene Rechenschaftspflicht zu erfüllen. Es wäre gut gewesen, wenn von Anfang an Beipackzettel von Produkten oder Informationsblätter und Verträge von Anbietern mit der nötigen Transparenz und den geeigneten Garantien für eine rechtskonforme Verarbeitung hätten aufwarten können. Stattdessen ist dieser Zustand noch immer nicht im grünen Bereich, denn Verantwortliche müssen weiterhin den Informationen hinterherlaufen, wenn sie ihre Verarbeitungstätigkeiten dokumentieren und die Risiken abschätzen. Eingebauter Datenschutz ist Mangelware, Voreinstellungen sind oft nicht datenschutzfreundlich (Tz. 2.3.2).

Die DSGVO verlässt sich an dieser Stelle darauf, dass der Markt diesen Anforderungen irgendwie nachkommen wird, denn Hersteller sind nicht unmittelbar verpflichtet, ihre Produkte auf einen datenschutzkonformen Einsatz auszurichten, wenn sie selbst keine personenbezogenen Daten verarbeiten und weder Verantwortlicher noch Auftragsverarbeiter sind. Selbst wenn auf lange Sicht die Nachfrage der Anwender zu einem Angebot führt, mit dem Datenschutzkonformität üblich und nicht die Ausnahme ist, bleibt der heutige Zustand unbefriedigend. Solange nur die Verantwortlichen und die Auftragsverarbeiter von der DSGVO verpflichtet sind und sich nicht darauf verlassen können, dass die Produkte auf dem europäischen Markt DSGVO-konform sind, fehlt ein großes Puzzleteil für einen effektiven Datenschutz.

Hilfen gab es für einige Bereiche von Branchenverbänden, von Kammern und von Berufsverbänden, da dort die jeweils typischen Verarbeitungstätigkeiten, Abläufe und oft auch die eingesetzte Informationstechnik bekannt sind und daher Musterlösungen übernommen oder angepasst werden können.

Auch die Aufsichtsbehörden haben schon vor Geltung der DSGVO mit einem über die Zeit erweiterten Portfolio an bundesweit abgestimmten Kurzpapieren und mit europäischen Leitlinien zu wichtigen Themen, an denen sich das ULD beteiligt hat, die Anwender unterstützt.

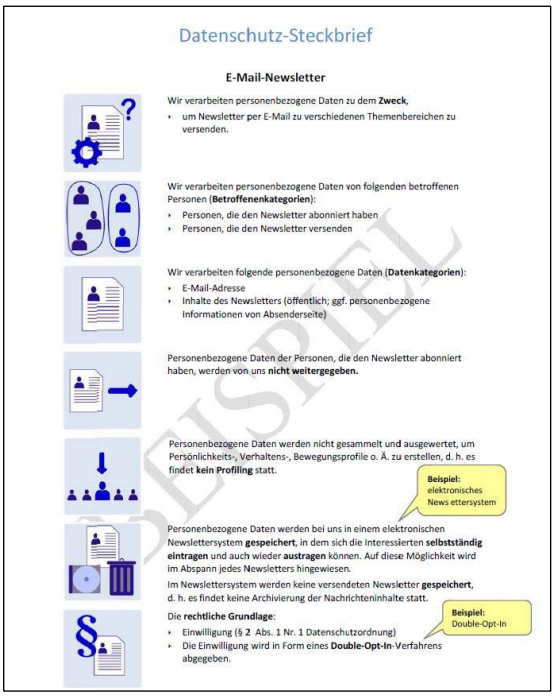


Abbildung: Illustrierter Datenschutz-Steckbrief

In Schleswig-Holstein haben wir außerdem die neue Praxis-Reihe „Datenschutzbestimmungen

praktisch umsetzen“ eingeführt, stellen Vorlagen für die Dokumentation mit Ausfüllanleitungen zur Verfügung und zeigen anschaulich, wie man die Informationspflichten erfüllen kann (Datenschutz-Steckbrief, Tz. 6.1.4).

Hilfen gibt es hier:

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

Datenschutz darf sich nicht zu einer Spezialwissenschaft im Elfenbeinturm des akademischen Diskurses entwickeln, sondern muss mindestens für typische Verfahren ohne großen Aufwand rechtssicher realisierbar sein und in die Praxis gebracht werden. Dafür müssen allerdings viele Standardanwendungen geändert werden, die bisher Datenschutzanforderungen ignoriert haben – es liegt also noch viel Arbeit vor uns.

Was ist zu tun?

Der Schlüssel liegt in der Gestaltung: Wenn gute Musterlösungen mit eingebautem Datenschutz bekannt sind, muss kein Anwender für sich allein das Rad neu erfinden.

1.2 Die Dienststelle der Landesbeauftragten für Datenschutz

Im letzten Bericht im Jahr 2017 konnten wir einen kleinen Stellenzuwachs vor allem für den Bereich der Prüfungen vermelden (36. TB, Tz. 1.4). Dazu gehören auch die gesetzlichen Pflichtprüfungen der Verarbeitung von personenbezogenen Daten durch die Polizei und die Verfassungsschutzbehörde (Tz. 4.2.1). Was keiner vorab verlässlich prognostizieren konnte, war das Mehr an Arbeitslast durch die europäische Datenschutzreform. Zur Vorbereitung waren dem ULD zwei bis Ende 2019 befristete Stellen gewährt worden. Damit standen dem ULD im Berichtszeitraum 32 Stellen zur Verfügung, um die vielfältigen Aufgaben des Datenschutzes und der Informationsfreiheit zu erledigen. Allein die Datenschutz-Grundverordnung listet 22 Aufgaben auf (Art. 57 Abs. 1 DSGVO) – von „a) Anwendung der Verordnung überwachen und durchsetzen“ bis „v) jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen“. Das Landesdatenschutzgesetz ergänzt das Aufgabenspektrum noch (§ 62 LDSG-neu).

Den Schwerpunkt legt die DSGVO auf die Funktion der Aufsicht, nicht auf die Beratung. Der Begriff „Beratung“ kommt in Artikel 57 DSGVO nur bei den kritischen Fällen der vorherigen Konsultation nach Artikel 36 DSGVO vor – wenn sich vor einer Einführung einer Verarbeitung in der vom Verantwortlichen durchgeführten Datenschutz-Folgenabschätzung herausstellt, dass das Risiko für die Rechte und Freiheiten natürlicher Personen zu groß ist. Außerdem „beraten und unterstützen [die Aufsichtsbehörden] die Datenschutzbeauftragten mit Rücksicht auf deren typische Bedürfnisse“ (§ 40 Abs. 6 BDSG-neu).

Die Datenschutzbehörde ist also nicht nur „Bußgeldstelle“, sondern hat beispielsweise die Verpflichtung, die Verantwortlichen, die Auftragsverarbeiter und die Öffentlichkeit zu sensibilisieren (u. a. für Medienkompetenz, Tz. 13.1). Im Berichtszeitraum hat das ULD durch zahlreiche Vorträge und Schulungen Datenschutzbeauftragte ebenso wie Verantwortliche in Unternehmen und in der Verwaltung über Datenschutzrechte, Datenschutzpflichten und technisch-organisatorische Lösungsmöglichkeiten informiert (Tz. 13.1). Ein Schwerpunkt lag im Jahr 2018 auf Vorträgen bei kleinen und mittleren Unternehmen (KMU), die besonders viel Nachfragebedarf hatten, was die Umsetzung der DSGVO angeht. Mehr als 1.000 Personen konnten so einen der Vorträge hören und bei Bedarf auch Einzelfragen mit den Vortragenden klären. Die Veranstaltungen fanden mit verschiedenen Kooperationspartnern statt, z. B.

Industrie- und Handelskammern, Handwerkskammern, Kammern im ärztlichen Bereich oder Arbeitgeberverbänden.

Während die große Nachfrage erst im Jahr 2018 einsetzte, fanden die ersten Veranstaltungen zur DSGVO mit zeitlichem Vorlauf statt. So haben wir eine Übersicht über die wichtigsten Schritte für Unternehmen im November 2017 bereitgestellt:

https://datenschutzzentrum.de/artikel/1178-.html

Ein zusätzlicher Druck bei unserer Arbeit entsteht dadurch, dass in der täglichen Arbeit oft kurze Fristen eingehalten werden müssen. Nicht ganz so kurz, aber dennoch bei einem großen Aufkommen von Anfragen herausfordernd, sind die meisten gesetzlich vorgegebenen Fristen wie die 8-Wochen-Frist bei einer vorherigen Konsultation nach Artikel 36 DSGVO, bei der es in der Regel eher um besonders komplexe Sachverhalte geht. Eine engere Zeittaktung wird durch den Föderalismus auf EU-Ebene im Konzert mit allen europäischen Mitgliedstaaten verursacht, wofür die deutsche Auffassung zu den Fragen im Vorfeld gebildet werden muss – im Endeffekt ein doppelter Föderalismus, der den Landesdatenschutzbeauftragten eine doppelte Bearbeitungsgeschwindigkeit abverlangt. Ein Teil der Arbeit muss auf Englisch erfolgen; hilfreich sind daneben weitere Sprachkenntnisse, um Missverständnisse in der Interpretation von grenzüberschreitenden Fällen möglichst schnell ausräumen zu können.

Der europäische Rechtsrahmen soll den Vorteil bieten, dass die Rechtssicherheit für alle Verantwortlichen verbessert wird und datenschutzkonforme Produkte, Anwendungen und Dienste im Binnenmarkt problemlos einsetzbar sind. Die Aufsichtsbehörden müssen auf der einen Seite unabhängig sein, auf der anderen Seite sollen sie im Sinne der Rechtssicherheit mit einer Stimme sprechen. Dies muss kein unauflösbarer Widerspruch sein, bedeutet aber gerade in der Anfangszeit der DSGVO, dass national oder regional bisher akzeptierte Praktiken noch einmal auf den Prüfstand der DSGVO-Konformität kommen müssen, um dasselbe (gute) Datenschutzniveau in allen Mitgliedstaaten zu verlangen. Hier ist schnelles und gleichzeitig sorgfältiges Arbeiten vonnöten, um abgestimmte, nachhaltige und europarechtskonforme Bewertungen abzugeben.

Unterschiede gibt es allerdings doch: Zum einen ist das nationale Verwaltungsverfahrensrecht einzuhalten, zum anderen schaffen die national oder länderspezifisch genutzten Öffnungsklauseln der DSGVO ein Potenzial für abweichende Behandlungen ähnlicher Fälle. Von einer Vollharmonisierung kann daher in vielen Details noch keine Rede sein. Allerdings muss dies nicht zu Problemen führen, weil eben doch die Grundwerte in Europa und die Datenschutzgrundsätze in Artikel 5 DSGVO einheitlich sind.

Gute Lösungen für alle Konstellationen sind also in der Regel möglich, das ist unsere Überzeugung. Dies bedingt, dass insbesondere die Fachdisziplinen Jura und Technik zusammenwirken. Praxistaugliche Ausarbeitungen von Empfehlungen und nachhaltige Bewertungen von Sachverhalten erfordern zumeist Teamarbeit, so die Erfahrungen unserer Dienststelle. Dasselbe gilt für die Verpflichtung „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" (Artikel 25 DSGVO).

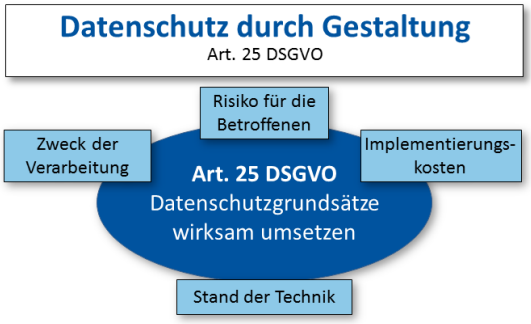


Abbildung: Kriterien in Art. 25 Abs. 1 DSGVO

Die Unabhängigkeit der Dienststelle wirkt sich auch darauf aus, dass sich das ULD informationstechnisch selbstständig verwaltet. Bei dem eigenen Betrieb der IT können wir Erfahrungen gewinnen, die andere Verantwortliche ebenfalls haben. Wir werden mit denselben Problemen konfrontiert, wir wissen um den Aufwand im täglichen Betrieb, bei der Einführung neuer Verfahren und beim Umgang mit unvorhergesehenen Ereignissen. Mit diesem Praxisbezug versuchen wir, unsere Lösungen weiter zu verbessern.

Mit Geltung der DSGVO haben wir auf unserer Webseite rechtzeitig Online-Formulare für eingehende Beschwerden betroffener Personen und zur Meldung von Datenschutzbeauftragten sowie Vorlagen zur Meldung von Datenpannen bereitgestellt.

Nicht vorhergesehen hatten wir, dass neben den etwa 4.000 Online-Meldungen mit den Namen der benannten Datenschutzbeauftragten auch etwa noch einmal 4.000 Faxe, Papierschreiben und E-Mail-Nachrichten mit der Bekanntgabe der Datenschutzbeauftragten eintrafen.

Unser Online-Beschwerdeformular wird im Durchschnitt mehrmals täglich genutzt. Weiterhin gehen Beschwerden auch in anderer Form, z. B. schriftlich oder per E-Mail, ein. Vom 25. Mai 2018 bis zum 31. Dezember 2018 wurden aufgrund der Beschwerden betroffener Personen etwa 500 Verfahren eingeleitet, weitere Fälle wurden aufgrund der fehlenden Zuständigkeit an andere Aufsichtsbehörden weitergegeben.

Bis Ende 2018 gingen 210 Meldungen von Datenpannen nach Artikel 33 DSGVO ein, der größte Teil aus dem nichtöffentlichen Bereich (für Einzelfälle siehe Tz. 5.6). Vor Geltung der DSGVO bestand auch schon eine Meldepflicht nach § 42a BDSG-alt und § 27a LDSG-alt für Vorfälle, in denen sensible Daten betroffen waren. Jedoch war die Anzahl der pro Jahr gemeldeten Fälle im unteren zweistelligen Bereich angesiedelt.

Bis Ende 2018 hatte die Landesbeauftragte für Datenschutz noch kein Bußgeld verhängt, jedoch verschiedentlich von den Mitteln der Verwarnung (für die Vergangenheit) und der Warnung (für die Zukunft) Gebrauch gemacht. Die meisten Verfahren nach der DSGVO, die im Berichtszeitraum eingeleitet worden waren, konnten allerdings bis Ende 2018 noch nicht beendet werden.

Auch fehlt es noch an einer Rechtsdurchsetzungsstelle. Das koordinierte und professionelle Vorgehen bei Sanktionen und Anordnungen gehört zu den wichtigsten Komponenten der Datenschutzreform, wie es auch im Gutachten des Rechtswissenschaftlers Prof. Dr. Alexander Roßnagel schon im Jahr 2017 mit einer optimalen Ausstattung von drei bis vier Personen beschrieben wurde:

https://datenschutzzentrum.de/artikel/1136-1.html

Dem ULD wurden ab 2019 insgesamt vier neue Stellen bewilligt: zwei Sachbearbeitungsstellen im primär juristischen Bereich, eine Technikstelle für Digitalisierung und eine Stelle für die Rechtsdurchsetzung, die jedoch noch mit einem Sperrvermerk versehen ist, d. h. zurzeit nicht besetzt werden darf, bis der Sperrvermerk vom Finanzausschuss aufgehoben wird. So kann sich die Dienststelle zunächst um drei Personen verstärken, die uns darin unterstützen werden, die zusätzlichen Anforderungen durch die europäische Datenschutzreform und die fortschreitende Digitalisierung zu erfüllen.

Was ist zu tun?

Datenschutz ist kein Randthema mehr, sondern wird verstärkt nachgefragt, sowohl von Anwendern als auch von betroffenen Personen. Die Digitalisierung in allen Lebensbereichen sorgt dafür, dass der Aufwand in der nächsten Zeit voraussichtlich wachsen wird, damit teure und risikoreiche Fehlentwicklungen vermieden werden. Die Dienststelle der Landesbeauftragten für Datenschutz muss ausreichend ausgestattet werden, um die gesetzlichen Aufgaben erfüllen zu können.

1.3 Digitalisierung in Schleswig-Holstein – mit Datenschutz die Segel setzen

Auch an Schleswig-Holstein geht die Digitalisierung nicht spurlos vorbei – im Gegenteil! Mit dem Digitalisierungsprogramm Schleswig-Holstein hat unser Bundesland einen klaren Kurs vorgelegt, um den neuen Herausforderungen nicht nur gewachsen zu sein, sondern durch aktive Gestaltung selbstbestimmt für den Weg in die Zukunft die Anker zu lichten. Dass Datenschutz und Informationsfreiheit tragende Säulen dieser Erneuerung sind, findet – wenig verwunderlich – natürlich die Zustimmung der Landesbeauftragten für Datenschutz Schleswig-Holstein und ihrer Dienststelle. Nun gilt es, den Weg von den ambitionierten Strategiepapieren in die Praxis zu bereiten, damit Digitalisierung aktiv zum Vorteil der Menschen und der Gesellschaft gestaltet wird.

Die Erfahrungen der Vergangenheit zeigen allerdings, dass solch ein Ansinnen kein Selbstgänger ist, sondern neben umfassendem und fundiertem Sachverstand insbesondere die Bereitschaft erfordert, sich neuen Lösungsansätzen zuzuwenden. Denn machen wir uns nichts vor – die heute verbreitete Informationstechnik erfüllt bei Weitem nicht die Mindestanforderungen an Datenschutz und Datensicherheit, stellt damit alles andere als ein verlässliches Fundament für darauf aufbauende Anwendungen und Verfahren dar. Kaum ein Tag im Berichtszeitraum verging, ohne dass neue Vorfälle zu datengierigen Anbietern, versteckten Datenabflüssen, versehentlichen Datenpannen, ja selbst zu Fehlern bei den absoluten Grundlagen, dem kleinen Einmaleins der Informationssicherheit, zutage traten.

Diese Sicherheitsmängel in der Informationstechnik legen nahe, dass „quick & dirty“, schnell und fehlerhaft, als Prinzip bei der Entwicklung noch viel zu oft die erforderliche Sorgfalt in den Hintergrund drängt. Noch ist es wichtiger, schnell am Markt zu sein, als eine gute Qualität abzuliefern. Bei der Problemanalyse wird häufig deutlich, dass eine datenschutzkonforme Realisierung, ein Einhalten der gesetzlichen Vorgaben anscheinend nie geplant war. Vielmehr werden absichtlich, übermäßig und oft auch heimlich Daten gesammelt, ausgewertet und sogar an Dritte durchgereicht, mit denen die Nutzenden nie etwas zu tun hatten (Tz. 2.3.2). Diese Ignoranz rechtlicher Vorgaben wird mittelfristig mehr als nur die informationelle Selbstbestimmung der Nutzenden gefährden.

Aus dem Digitalisierungsprogramm Schleswig-Holstein

„Der Datenschutz dient dem Schutz der Menschenwürde und ist wesentliche Bedingung für eine freiheitliche Demokratie in einer digitalen Welt.

Schleswig-Holstein soll auch diesbezüglich zu einem Vorzeigeland werden. Hohe Standards im Datenschutz haben für uns zentrale Bedeutung. Wir wollen unseren Datenschutz zu einem internationalen Wettbewerbsvorteil entwickeln und den Nachweis erbringen, dass ein hohes Datenschutzniveau kein Hindernis im Wettbewerb, sondern vielmehr ein Marktvorteil ist. Guter Datenschutz schafft Vertrauen bei den Bürgerinnen und Bürgern, nicht nur in die Angebote der Wirtschaft, sondern auch in die Datenverarbeitung durch staatliche Stellen, und gewährleistet somit eine nachhaltige Fortentwicklung digitaler Angebote und Dienstleistungen.“

Schleswig-Holstein steht den Herausforderungen der Digitalisierung zum Glück nicht allein gegenüber. Die anderen Bundesländer sehen sich genauso mit den gleichen Problemstellungen konfrontiert. Vielerorts arbeiten kluge Köpfe bereits an Konzepten und Realisierungen, um den Risiken zu begegnen. Mit den anderen Mitgliedern der Europäischen Union verbindet uns dabei ein gemeinsamer Rechtsrahmen und Wertekanon, zu dem eben auch Datenschutz und Transparenz gehören.

Leuchtturmprojekte in den verschiedenen Regionen können nun zeigen, welchen Nutzen sie bringen, wie sie dabei Grundwerte und Menschenrechte bewahren und schützen. Von den

gewonnenen Erkenntnissen und Erfahrungen können dann alle profitieren und die gefundenen Lösungen übernehmen – gegebenenfalls mit Anpassungen an lokale Bedürfnisse. Ein kleines Beispiel hierfür ist unser Vorschlag in Tz. 4.3.4, die Tauglichkeit einer Entwicklung des Landes Berlin, die mehr Transparenz bei Funkzellenabfragen bietet, für Schleswig-Holstein zu prüfen.

§ 17 Abs. 4 LDSG-neu

Die oder der Landesbeauftragte ist über Planungen des Landes zum Aufbau oder zur wesentlichen Änderung von Systemen zur automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten.

Neue Projekte allein reichen aber nicht aus, um die schon viel zu lange mitgeschleppten Defizite im technischen Unterbau der Informationsgesellschaft zu beseitigen. Abhängigkeiten von Quasi-Monopolisten und proprietären Lösungen prägen hier immer noch das Bild. Es ist schon skandalös, wenn per Unternehmensentscheidung beispielsweise Betriebssysteme oder Textverarbeitungen standardmäßig einen Teil ihrer Verarbeitung in die Cloud verschieben und man kaum einen ungewollten Abfluss von Daten an Anbieter unterbinden kann. Darf Verwaltung, will Wirtschaft solche Systeme einsetzen, in denen außereuropäische Anbieter zwangsweise Daten über die Nutzung sammeln und einen fremden Zugriff nicht ausschließen können? Souveränität bei der Datenverarbeitung ist nicht nur für die Bürgerinnen und Bürger, sondern auch für Verwaltung und Wirtschaft unbestreitbar wichtig. Dies gilt ganz deutlich auch bei Messenger-Diensten oder sozialen Medien, die übergriffig Daten sammeln und auswerten. Manchmal ist dies in den Nutzungsbedingungen immerhin angedeutet, aber manchmal noch nicht einmal das.

Müssen wir die Selbstbestimmung aufgeben? Sind wir als Nutzende, als Verwaltung, als Wirtschaft diesen Angriffen ausgeliefert?

Nö.

Die Datenschutz-Grundverordnung gilt für den gesamten europäischen Markt, selbst für Anbieter ohne Sitz in der Europäischen Union, wenn sie dort ihre Waren oder Services anbieten oder das Verhalten von Personen in der EU beobachten (Art. 3 Abs. 2 DSGVO). Wieder sind die Bedürfnisse in Europa ähnlich, sodass Verwaltung und Wirtschaft mit einem Schulterschluss gegenüber Anbietern auftreten können, um ihre Bedingungen – und dazu gehört selbstverständlich auch die Konformität mit dem Datenschutzrecht – einzufordern und geeignete Lösungen zu erwirken. Die Datenschützer werden ihren Sachverstand dazu gern beitragen, werden aber oft erst dann einbezogen, wenn das Kind längst in den Brunnen gefallen ist.

Dies ginge auch plietscher: Insbesondere öffentliche Anwender, aber auch die Wirtschaft wäre gut beraten (und würde damit eigene Haftungsrisiken minimieren), vor der Beschaffung und dem Einsatz von Produkten Garantien von Herstellern und Anbietern einzufordern. Klar, für jede einzelne Anfrage wäre dies kaum aussichtsreich. Aber ein koordiniertes, gemeinsames Vorgehen der Anwender in einem Bundesland, bundeslandübergreifend oder gemeinsam mit ganz Europa ermöglicht Verhandlungen auf Augenhöhe.

Platt – Hochdeutsch

aver	aber
denn man tau	frisch ans Werk
nö	nein
plietsch	pfiffig, aufgeweckt, schlau
van sülvst	von selbst
versteiht sik	versteht sich

Parallel können eben diese Koalitionen genutzt werden, um unzureichenden Produkten und Diensten, die mit hoher Abhängigkeit von einzelnen Anbietern einhergehen, gute Eigenentwicklungen entgegenzustellen. Der Schleswig-Holsteinische Landtag hat dies sehr gut erkannt und mit seinem Beschluss vom 14. Juni 2018 festgelegt, dass künftig die Nutzung quelltextoffener Software („Open Source") eine besondere Rolle spielen soll. Bei solcher Software wird

der Programmcode nicht verheimlicht und ist daher überprüfbar. Der Landtag hat das Ziel vorgegeben, „möglichst viele Verfahren bei wesentlichen Änderungen oder der Neuvergabe auf Open-Source-Software umzustellen".

Das ist ein wichtiger erster Schritt, um die Kontrolle über die Datenverarbeitung im Land abzusichern, der auch unserem Rat im letzten Bericht (36. TB, Tz 2.3) folgt und von uns sehr begrüßt wird. Nun muss es konsequent weitergehen: Nicht nur die Software von Fachverfahren, Office-Anwendungen, Betriebssystemen oder Lernumgebungen an Schulen muss besser kontrollierbar und überprüfbar sein, sondern auch Hardware und Dienstleistungen müssen transparenter werden.

Dasselbe gilt bei der Standardisierung, insbesondere wenn es darum geht, sensible Vorgänge im Alltagsleben der Menschen abzusichern. Beispielsweise dürfen Verschlüsselungsverfahren (Tz. 10.1) keine Hintertüren enthalten oder künstlich abgeschwächt werden. Die Eigenschaft „Open Source" allein garantiert natürlich noch keine Sicherheit, ist dafür aber eine wichtige Voraussetzung. Sicherzustellen ist weiter, dass die Verfahren vor dem Einsatz auch tatsächlich unabhängig geprüft werden. Insbesondere wenn komplexe Algorithmen und künstliche Intelligenz zum Einsatz kommen, sind Prüfverfahren unabdingbar, die die Beherrschbarkeit einer solchen Verarbeitung gewährleisten (Tz. 2.2.3).

Schleswig-Holstein schlägt einen sehr guten Weg ein, um das Potenzial der Digitalisierung verantwortungsvoll und zukunftssicher zu nutzen, wenn diese Aspekte bei der Ausgestaltung und Überprüfung der Systeme von vornherein beachtet werden.

Denn man tau!

Was ist zu tun?

Das ULD bietet weiterhin seine Expertise für die strategischen Digitalisierungsprojekte des Landes zu Fragen des Datenschutzes und der Informationsfreiheit an. Alle Entwicklungen sollten die rechtlichen Anforderungen ab Beginn der Planung und Konzeption berücksichtigen und in die Lösungen einbauen. Wo immer möglich, sollten dabei Synergien genutzt werden. Aver dat versteiht sik van sülvst.

02

KERNPUNKTE

Zusammenarbeit der Aufsichtsbehörden

Digitalisierung und Grundrechte

Informationsfreiheit und Datenschutz „by Design“

2 Datenschutz – global und national

2.1 Datenschutz aus Europa – erste Erfahrungen

2.1.1 Zusammenarbeit in Deutschland

Die Zusammenarbeit der Datenschutzaufsichtsbehörden in Deutschland wird primär durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) geleitet. Vor einigen Jahren hat es noch ausgereicht, dass sich die Behördenleitungen zweimal im Jahr zusammensetzten und die wichtigen Themen besprachen, die in den Arbeitskreisen und Arbeitsgruppen vorbereitet worden waren. Mittlerweile sind es sechs oder sieben persönliche Treffen pro Jahr in großer Runde, vielfältige E-Mail-Abstimmungen und zusätzliche „Taskforces" für spezielle Themen, damit die nötigen Entscheidungen möglichst schnell getroffen werden können.

Die Datenschutzkonferenz veröffentlicht nun zentral im eigenen Webauftritt die Entschließungen, Orientierungshilfen und weitere Informationen wie beispielsweise die abgestimmten Kurzpapiere zur DSGVO:

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

Sowohl der nationale als auch der europäische Rechtsrahmen erfordern eine Abstimmung der Aufsichtsbehörden im Sinne einer Rechtssicherheit. Bei der Gesetzgebung, die in die Zuständigkeit der Bundesländer fällt, wäre dies ebenfalls wünschenswert, stößt jedoch aufgrund der unterschiedlichen Detailregelungen an ihre Grenzen. Das betrifft nicht nur typische Landeszuständigkeiten wie Polizei oder Schule, sondern auch grundlegend die Umsetzung der DSGVO und der EU-Richtlinie 2016/680, die in den Bundesländern verschieden gehandhabt wurde.

2.1.2 Zusammenarbeit in Europa

Im Mai 2018 wurde die Artikel-29-Datenschutzgruppe mit Geltungserlangung und gleichzeitigem Außerkrafttreten der Datenschutzrichtlinie vom Europäischen Datenschutzausschuss (EDSA – englisch: European Data Protection Board, EDPB) abgelöst. Es handelt sich um eine Einrichtung der Union mit eigener Rechtspersönlichkeit, die aus den Leitern der Aufsichtsbehörden der Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern besteht. Zu den Aufgaben des Ausschusses gehört – wie schon zuvor für die Artikel-29-Datenschutzgruppe – neben der Beratung der Kommission in datenschutzrechtlichen Fragen u. a. die Bereitstellung von Leitlinien, Empfehlungen und bewährten Verfahren („guidelines, recommendations and best practices"). Im Rahmen der ersten Sitzung des Ausschusses hat der EDSA eine Reihe von Leitlinien der ehemaligen Artikel-29-Datenschutzgruppe mit Bezug zur DSGVO bestätigt und sich diese damit zu eigen gemacht.

Dem Ausschuss kommt entscheidende Bedeutung in Fällen der Zusammenarbeit und Kohärenz zu. In Angelegenheiten mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat haben Aufsichtsbehörden, die hierzu beabsichtigen, Maßnahmen zu erlassen, dem Ausschuss vorab entsprechende Beschlussentwürfe vorzulegen. Der Ausschuss gibt dann eine Stellungnahme ab, die mit einfacher Mehrheit der Mitglieder des Ausschusses angenommen werden kann.

Dieser Stellungnahme soll die vorlegende Aufsichtsbehörde weitestgehend Rechnung tragen. Beabsichtigt sie stattdessen, der Stellungnahme

des Ausschusses insgesamt oder teilweise nicht zu folgen, ist dies dem Ausschuss mitzuteilen. Dieser erlässt dann im sogenannten Streitbeilegungsverfahren einen rechtsverbindlichen Beschluss, der grundsätzlich mit einer Zweidrittelmehrheit angenommen werden muss.

Auch bei sonstigen Angelegenheiten mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat besteht die Möglichkeit, eine Stellungnahme des Ausschusses einzuholen.

Die Vertretung der deutschen Aufsichtsbehörden im EDSA regelt das Bundesdatenschutzgesetz (BDSG). Danach ist die oder der Bundesbeauftragte (gemeinsamer Vertreter) gemeinsamer Vertreter im Europäischen Datenschutzausschuss. Als Stellvertreterin oder Stellvertreter des gemeinsamen Vertreters wählt der Bundesrat eine Leiterin oder einen Leiter der Aufsichtsbehörde eines Landes (Stellvertreter).

Der EDSA unterhält, wie schon zuvor die Artikel-29-Datenschutzgruppe, eine Reihe an Arbeitsgruppen, die die Entscheidungen des EDSA vorbereiten. In mehreren dieser sogenannten Expert Subgroups ist das ULD als Vertretung der Bundesländer tätig. Dies sind die Key Provisions Expert Subgroup, die Technology Expert Subgroup und bis vor Kurzem auch die Enforcement Expert Group. Aufgabe der Ländervertretungen ist es unter anderem, die Auffassungen der Landesdatenschutzbehörden in die Expert Subgroups zu tragen und dort gemeinsam mit den Vertreterinnen und Vertretern der anderen mitgliedstaatlichen Aufsichtsbehörden Leitlinien und Empfehlungen zu erarbeiten.

Die ersten Leitlinien, die nach Geltungserlangung der DSGVO vom EDSA verabschiedet wurden, waren die „Guidelines 1/2018 on certification and identifying certification criteria“, bei denen das ULD als Berichterstatter (Rapporteur) fungiert hat. Gleiches gilt für die „EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)“ (zur Zertifizierung siehe Tz. 9.1).

Bei der Erklärung des Europäischen Datenschutzausschusses zur Überarbeitung der E-Privacy-Verordnung und zu den Auswirkungen auf den Schutz der Privatsphäre von Personen im Hinblick auf die Geheimhaltung und die Vertraulichkeit ihrer Kommunikation war das ULD ebenfalls beteiligt (Tz. 11.2).

Neben der Koordination der Rechtsauffassungen unter den europäischen Aufsichtsbehörden bei der Erstellung von Leitlinien und Empfehlungen bedarf es unter Geltung der DSGVO stärker als zuvor einer Abstimmung bei der Fallbearbeitung von Beschwerden. In grenzüberschreitenden Fällen bedarf es der Koordination, welche Behörde das jeweilige Verfahren führt und welche anderen Behörden gegebenenfalls noch betroffen und daher am Verfahren zu beteiligen sind. Um diese Abstimmung vornehmen zu können, haben sich die europäischen Aufsichtsbehörden an das Binnenmarktinformationssystem der Europäischen Kommission angeschlossen, um die Abstimmungsprozesse dort durchzuführen.

2.2 Digitalisierung und Grundrechte

2.2.1 Informationelle Fremdbestimmung

Im Jahr 2017 haben wir unsere Sommerakademie dem Thema „Herausforderung ‚Informationelle Nichtbestimmung‘“ gewidmet. Schwerpunkt waren gesellschaftspolitische Fragen zur informationellen Selbstbestimmung, Fremdbestimmung und Nichtbestimmung. Basis der Debatte ist die Forderung des Datenschutzes, dass die Menschen keiner unkontrollierten Fremdbestimmung ausgesetzt werden. Daher ist das Recht auf informationelle Selbstbestimmung seit mehreren Jahrzehnten das Fundament des Datenschutzes in Deutschland. Nur:

Was ist, wenn Menschen sich für eine „Nichtbestimmung" entscheiden – weil sie Datenschutz nicht interessiert oder sie sich ohnmächtig fühlen angesichts einer Übermacht der Datenverarbeiter, die über die Regeln entscheiden? Und was passiert in der Welt des „Internet of Things", wenn alle Geräte miteinander vernetzt sein können und sich austauschen, ohne Entscheidungen ihrer Nutzerinnen und Nutzer abzuwarten? Wenn Smart Homes und Smart Cars und ganze Smart Cities automatisch funktionieren und Verbesserungen im Komfort oder in der Sicherheit versprechen? Können Menschen dann noch eingreifen, oder sind sie zur Nichtbestimmung verdammt?

Viele Gründe könnten zu einer faktischen „informationellen Nichtbestimmung" führen: Überlastung, Bequemlichkeit, zu hoher Aufwand, Hilflosigkeit oder Resignation. In der heutigen Realität ist „eingebauter Datenschutz" leider keineswegs eine Selbstverständlichkeit, stattdessen sind Verkettbarkeit und Identifizierbarkeit in der Technik implementiert, gegen die sich Nutzende kaum wehren können (siehe auch Tz. 10.3 und Tz. 10.4). Zu kritisieren ist auch das Prinzip „Take it or leave it" („Nimm es, wie es ist, oder lass es bleiben"), mit dem datenhungrige Apps auf dem Smartphone alle möglichen Zugriffsberechtigungen begehren. Oft kann man sich nicht ausreichend gegen zu weitgehende Zugriffe der Apps schützen.

Bei dieser Sommerakademie richtete sich der Blick einerseits auf die aktuelle Technikentwicklung, andererseits auf die zu diesem Zeitpunkt noch nicht geltende Datenschutz-Grundverordnung. Nichtbestimmung im Sinne eines Ausgeliefertseins entspricht nicht dem Menschenbild der aufgeklärten und demokratischen Gesellschaft. Alle Verantwortlichen müssen in ihrem jeweiligen Bereich dafür Sorge tragen, dass die datenschutzrechtlichen Anforderungen erfüllt sind. Das Herausstellen der Selbstbestimmung darf auch nicht dazu führen, dass nur noch diejenigen einen Schutz ihrer Persönlichkeitsrechte erhalten, die sich selbst darum kümmern. Es reicht selbstverständlich nicht aus, auf Möglichkeiten des Selbstdatenschutzes zu verweisen. Stattdessen spielen datenschutzfreundliche Voreinstellungen eine wesentliche Rolle („Data Protection by Default"), wie dies in Art. 25 Abs. 2 DSGVO gefordert ist (Tz. 2.3.2), die mit der DSGVO nun eingefordert werden können.

Was ist zu tun?

Informationelle Nichtbestimmung bedeutet Fremdbestimmung. Grundlage der Selbstbestimmung muss eine faire Gestaltung von Gesetzen, Standards, Prozessen und Informationstechnik sein.

2.2.2 Beschäftigtendatenschutz 4.0

Der Beschäftigtendatenschutz gehört zu den wichtigen Themen, die bereits seit Jahrzehnten immer wieder Aufmerksamkeit erlangen. Dies wird sich auch für die nahe Zukunft nicht ändern. Die Datenschutz-Grundverordnung lässt für diesen Bereich eigene Konkretisierungen der Mitgliedstaaten zu (Artikel 88 DSGVO). Aus diesem Grund hat die Sommerakademie 2018 die aktuellen Fragen und einen etwaigen Regelungsbedarf zum Thema „Update nötig: Beschäftigtendatenschutz im digitalen Zeitalter 4.0" näher unter die Lupe genommen.

Besonders die Digitalisierung bringt neue Brisanz in den Beschäftigtendatenschutz. Denn ähnlich grundlegend wie die industrielle Revolution vor 200 Jahren wird sich die digitale Revolution unserer heutigen Zeit auswirken, wenn „intelligente" Technik Einzug in Bewerbungsverfahren und Arbeitsplatzgestaltung hält: Eine automatische Auswertung der Stimme soll helfen, die geeigneten Personen für einen Job auszufiltern. Einige Arbeitgeber locken mit einem Bonus, wenn Fitness- und Schlafanalysetools einen gesunden Lebensstil unter Beweis

stellen. Kontrolle und Tracking von Beschäftigten sollen zu mehr Leistung führen.

In Deutschland sind die Vorschriften für Datenschutz im Beschäftigtenkontext bislang recht mager. In Ermangelung eindeutiger Regelungen müssen die Grenzen der Überwachung von Beschäftigten in vielen Einzelfällen arbeitsgerichtlich geklärt werden. Dies bedeutet gleichzeitig, dass viele Sachverhalte nicht gerichtlich geklärt werden, weil die betroffenen Personen sich keinen zeitraubenden Gang durch die gerichtlichen Instanzen leisten wollen oder können. Auch endet der Großteil der Verfahren mit einem arbeitsgerichtlichen Vergleich, sodass die Grundfragen nicht entschieden werden. Aus diesem Grund spricht viel für ein Beschäftigtendatenschutzgesetz, das die Rechte und Pflichten der Arbeitgeber und der Beschäftigten rechtssicher festschreibt. Dazu gehört auch die Frage, unter welchen – stark eingeschränkten – Bedingungen von einer Freiwilligkeit einer Einwilligung der Beschäftigten ausgegangen werden kann und wo gar das Instrument der Einwilligung definitiv nicht infrage kommt.

Was ist zu tun?

Die Entwicklung eines Beschäftigtendatenschutzgesetzes ist die Aufgabe des Bundesgesetzgebers. Im täglichen Miteinander können sich Betriebs- und Personalräte für den Datenschutz der Beschäftigten starkmachen und auch mit den jeweiligen Datenschutzbeauftragten zusammenarbeiten. Zusätzlich besteht ein Bedarf im Bereich der Technikentwicklung, damit Arbeitgebern faire und maßvolle Kontrollmöglichkeiten an die Hand gegeben werden können, ohne dass die Beschäftigten bei der Arbeit standardmäßig einer Vollüberwachung ausgesetzt sind.

2.2.3 Algorithmen und künstliche Intelligenz

In der öffentlichen Debatte über die Digitalisierung vieler Lebens- und Wirtschaftsbereiche wird zunehmend über neue Möglichkeiten und Gefahren des Einsatzes von Algorithmen und künstlicher Intelligenz (kurz KI) diskutiert. Diverse KI-Strategien werden erarbeitet und verfolgt und die ethischen Aspekte in unterschiedlichen Anwendungsszenarien beleuchtet.

Werden Systeme der künstlichen Intelligenz unter Verwendung personenbezogener Daten erstellt oder werden mit ihnen Entscheidungen getroffen, die natürliche Personen betreffen, so sind die datenschutzrechtlichen Anforderungen zu berücksichtigen. Auch für das Grundrecht auf Informationsfreiheit kann der Einsatz von KI-Systemen Auswirkungen haben. Daher beschäftigt sich das ULD im Austausch mit anderen intensiv mit den neuen Fragestellungen.

Vielfach werden die Begriffe dieses Themenbereichs unscharf verwendet, da es bisher noch kaum allgemein anerkannte Definitionen gibt. Von Bedeutung ist jedoch, dass KI-Systeme in Abgrenzung zu klassischen Algorithmen Regeln anwenden, die nicht explizit programmiert, sondern auf Grundlage des sogenannten maschinellen Lernens erstellt wurden. Oftmals ändern sich die „erlernten" Regeln auch noch im Betrieb eines KI-Systems, sodass zwei identische Eingaben zu unterschiedlichen Zeitpunkten zu unterschiedlichen Ausgaben führen können.

Aufgrund dieser Dynamik und der Komplexität spricht man beim Einsatz von Methoden der künstlichen Intelligenz nicht von (einzelnen) Algorithmen, sondern von KI-Systemen, bei denen verschiedene algorithmische Strukturen zusammenwirken: beim Trainieren eines KI-Systems mit Trainingsdaten und/oder Eingaben im laufenden Betrieb, bei der Bewertung der Ergebnisse und bei der Anpassung aufgrund von Interaktionen mit der Außenwelt. Daten- und Algorithmenstrukturen sind nicht mehr

unabhängig zu betrachten und verändern sich gegebenenfalls stetig.

Künstliche Intelligenz

„Wir verstehen ‚künstliche Intelligenz' […] als Sammelbegriff für diejenigen Technologien und ihre Anwendungen, die durch digitale Methoden auf der Grundlage potenziell sehr großer und heterogener Datensätze in einem komplexen und die menschliche Intelligenz gleichsam nachahmenden maschinellen Verarbeitungsprozess ein Ergebnis ermitteln, das gegebenenfalls automatisiert zur Anwendung gebracht wird. Die wichtigsten Grundlagen für KI als Teilgebiet der Informatik sind die subsymbolische Mustererkennung, das maschinelle Lernen, die computergerechte Wissensrepräsentation und die Wissensverarbeitung, welche Methoden der heuristischen Suche, der Inferenz und der Handlungsplanung umfasst."
(Definition der Datenethikkommission)

Diese Eigenschaften werden oft damit zusammengefasst, dass KI-Systeme als „Blackbox" zu betrachten sind, deren Berechnungswege nicht nachvollzogen werden können. Eine Verarbeitung personenbezogener Daten oder ein Einsatz mit Auswirkungen auf die Rechte und Freiheiten von betroffenen Personen ist unter dieser Voraussetzung in der Regel nicht zulässig. Und auch bei der Verarbeitung von nicht personenbezogenen Daten müssen KI-Systeme in der öffentlichen Verwaltung mit Blick auf das Grundrecht der Informationsfreiheit Auskunftsansprüche erfüllen. In der aktuellen Forschung werden nun erklärbare KI-Systeme entwickelt, die mehr Transparenz schaffen sollen.

Weitere Risiken für die Rechte und Freiheiten betroffener Personen können sich bei dem Einsatz von KI-Systemen beispielsweise ergeben, weil die Ergebnisse diskriminierend sein können, die Systeme manipuliert werden oder widerrechtlich Daten verarbeitet werden, wie z. B. Verhaltens- oder Bewegungsdaten.

Für die Entwicklung und den Einsatz von KI-Systemen gibt es in der DSGVO bereits wichtige rechtliche Vorgaben. Das ULD setzt sich mit diesen Fragestellungen in Vorträgen, Publikationen und den Gremien der Datenschutzkonferenz auseinander und begleitet engagiert die öffentliche Diskussion.

Auch aus Sicht der Informationsfreiheit ist Transparenz von Algorithmen und KI in verstärktem Maße notwendig:

https://www.datenschutzzentrum.de/artikel/1255-.html

Was ist zu tun?

Für den datenschutzkonformen Einsatz von KI-Systemen gibt es gegenwärtig noch keine speziellen Standards oder detaillierte Anforderungen an technische und organisatorische Maßnahmen. Die Erkenntnisse in diesem Bereich zu mehren und Best-Practice-Beispiele zu entwickeln, ist eine wichtige Aufgabe von Wirtschaft und Wissenschaft.

2.2.4 Informationsfreiheit „by Design“

Datenschutz „by Design“ ist eine Anforderung der DSGVO. Das Informationszugangsgesetz formuliert nicht unmittelbar eine ähnliche Gestaltungsanforderung. Dennoch gilt auch für den Bereich der Informationsfreiheit: Wenn von Anfang an bei der Konzeption von Prozessen und Informationstechnik die Anforderungen der Informationsfreiheit einfließen, profitieren die Anwender davon, weil sie in ihren Pflichten als informationspflichtige Stellen unterstützt werden. Zusätzlich fördert eingebaute Informationsfreiheit die Transparenz des Verwaltungshandelns für die Anfragenden. Außerdem lässt sich das Recht auf Informationszugang auf dieser Grundlage weiterentwickeln.

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.

Zurzeit erhält die Digitalisierung stärker Einzug in die Verwaltung, beispielsweise aufgrund des Onlinezugangsgesetzes. Dies ist eine gute Gelegenheit, Informationsfreiheitsanforderungen parallel zum Datenschutz zu implementieren.

Über die Grundsätze ordnungsgemäßer Aktenführung hinaus können informationspflichtige Stellen beispielsweise schon in ihrer Aktensystematik durch das Führen von Teilakten oder die Kennzeichnung sensibler Abschnitte bzw. Aktenteile eine schnellere Bearbeitung von Auskunftsersuchen erreichen. Technisch unterstützt werden kann der Ansatz mit einer Suchfunktion und mit Anwendungen, die für die Daten eine barrierefreie und maschinenlesbare digitale Veröffentlichung anbieten. Auch Methoden zur Anonymisierung oder zur Schwärzung sensibler Daten, die nicht herausgegeben werden dürfen, können zum Einsatz kommen – in diesem Fall sowohl im Sinne der Informationsfreiheit als auch des Datenschutzes.

Auch die Konferenz der Beauftragten für Informationsfreiheit des Bundes und der Länder beschäftigt sich mittlerweile mit dem Thema „Informationsfreiheit by Design“.

Was ist zu tun?

Alle, die Digitalisierung gestalten, sollten sowohl Datenschutz als auch Informationsfreiheit von Anfang an berücksichtigen und „by Design“ in die Prozesse und IT-Systeme einbauen.

2.3 Datenschutz durch Gestaltung

2.3.1 Datenschutz „by Design“ – schon in der Softwareentwicklung

Mit der Datenschutz-Grundverordnung (DSGVO) sind einige neue Verpflichtungen in den Fokus gerückt. Dazu gehört die neue Anforderung „Datenschutz durch Technikgestaltung“ bzw. „Data Protection by Design“. Diese Anforderung umfasst dabei fast alle Vorgaben der DSGVO, sodass eine Verfolgung des damit verbundenen Ansatzes eine strukturierte und organisierte Umsetzung verspricht.

Allerdings ist die Anforderung „Datenschutz durch Technikgestaltung“ in Artikel 25 der DSGVO nur allgemein formuliert und der Gesetzestext bietet zu wenig Orientierung für die Praxis. Hinzu kommt die besondere Konstellation, dass die Anforderung an die Verantwortlichen einer Verarbeitung personenbezogener Daten gerichtet ist und nicht an die Entwicklerinnen und Entwickler von Software.

Vor diesem Hintergrund hat das ULD mit dem Kompetenzverbund Software Systems Engineering (KoSSE) und dem Clustermanagement Digitale Wirtschaft Schleswig-Holstein (DiWiSH) einen Workshop für Interessierte aus Unternehmen, Verwaltungen und Hochschulen angeboten, in welchem über die neue Anforderung diskutiert werden konnte.

Unter dem Titel „Wie baut man Datenschutz in Software ein?“ haben hochkarätige Vortragende aus unterschiedlichen Perspektiven über den aktuellen Stand der Forschung und praktische Lösungsansätze informiert. Dazu gehört auch eine Softwareunterstützung zur Umsetzung des Standard-Datenschutzmodells, an dem die Universität Hamburg forscht. Die Diskussionen im und am Rande des Workshops haben gezeigt, dass es einige offene Fragen gibt und das Interesse an einem weiteren Austausch in einem ähnlichen Format sehr groß ist.

KoSSE

Der Kompetenzverbund Software Systems Engineering besteht aus mehreren Verbundprojekten zwischen Wirtschaft und Wissenschaft, die durch den Transfer von Forschungs- und Entwicklungsergebnissen in marktfähige Produkte die beteiligten Unternehmen stärken. Die Sprecher des Verbunds sind zwei Professoren an den Universitäten zu Kiel und zu Lübeck.

Die Vortragsfolien und ein Graphical Recording des Workshops sind unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/artikel/1266-.html

Was ist zu tun?

Es gibt noch nicht viele praktische Erfahrungen bei der Umsetzung der Anforderung „Datenschutz durch Technikgestaltung“. Forschungsprojekte von Hochschulen und Unternehmen, mit denen Werkzeuge entwickelt oder Best-Practice-Beispiele geschaffen werden, sollten unterstützt werden. Der Austausch von Forschung, Wirtschaft und Aufsichtsbehörden soll fortgeführt werden.

2.3.2 Die Macht von Datenschutz „by Default“

Die Vorschriften in der DSGVO zur Technikgestaltung beginnen mit „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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen [...]“ – das sind also die Vorbedingungen, die Kriterien, die der Verantwortliche in die Abwägung einbeziehen muss, um die geeigneten technischen und organisatorischen Maßnahmen für technischen Datenschutz auszuwählen und zu implementieren. Jede Abwägung bezieht sich auf den individuellen Einzelfall. Jeder Verantwortliche mag die Kriterien unterschiedlich auslegen, solange es noch keine verbindlichen Aussagen dazu gibt. Dies könnte dazu führen, dass die Vorschrift zu Datenschutz

durch Technikgestaltung noch einige Zeit lang zu wenig in der Praxis umgesetzt wird.

Ganz anders ist dagegen Art. 25 Abs. 2 DSGVO aufgebaut: Keine Kriterien für eine Abwägung, sondern ganz direkt die Forderung, dass der Verantwortliche die Maßnahmen für datenschutzfreundliche Voreinstellungen trifft.

Art. 25 Abs. 2 Satz 1 DSGVO

Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung ~~grundsätzlich~~*) nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

*) Zunächst ein Fehler in der deutschen Sprachversion; im Corrigendum vom 19. April 2018 wurde der Begriff „grundsätzlich" aus dem DSGVO-Text gelöscht.

Dies ist zwar nicht überraschend, weil Art. 25 Abs. 2 DSGVO ohnehin nur das Erforderlichkeitsprinzip betont, die in den Datenschutzgrundsätzen Datenminimierung und Speicherbegrenzung enthalten sind. Aber angesichts der Realität, in der datenschutzfreundliche Voreinstellungen, Datenminimierung und Speicherbegrenzung nicht der Standard sind, ist dies doch eine beinahe revolutionäre Regelung.

Art. 25 Abs. 2 Satz 2 DSGVO konkretisiert, worauf sich die Anforderung bezieht: auf „die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit". Das bedeutet u. a.: Es dürfen von Anfang an nicht mehr Daten erhoben, gespeichert oder anders verarbeitet werden als für den Zweck erforderlich. Auch die Verarbeitungsarten müssen auf das für den Zweck notwendige Maß beschränkt sein. Die Daten dürfen nicht länger als nötig gespeichert sein. Und bei der Zugänglichkeit der Daten muss ebenfalls minimiert werden – das kann z. B. die Speicherung von unverschlüsselten Daten in einer Cloud ausschließen, wenn eine lokale Verarbeitung mit weniger Zugänglichkeit (nämlich nur für die betroffene Person selbst) ausreicht. Auch ein Aussenden von Daten, wie dies bei vernetzten Autos der Fall ist, muss als Voreinstellung in der Zugänglichkeit beschränkt sein, solange dies für den Zweck ausreicht.

Für Entwicklerinnen und Entwickler ist die „Datenschutz by Default"-Anforderung neu. Bisher wurden die Voreinstellungen vielfach anders gewählt, sodass erheblicher Nachbesserungsbedarf in der heutigen Informationstechnik besteht.

Was ist zu tun?

Die Verantwortlichen müssen die Anforderung „Datenschutz by Default" ernst nehmen und in ihrem Verantwortungsbereich darauf hinwirken, dass tatsächlich datenschutzfreundliche Voreinstellungen Startpunkt einer jeden Verarbeitung werden.

2.3.3 Anforderungen und Standards der Pseudonymisierung

Die DSGVO nennt einige konkrete Maßnahmen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen. Eine dieser Maßnahmen ist die Pseudonymisierung, die als einzige mit einer Begriffsbestimmung (Art. 4 Nr. 5 DSGVO) hervorgehoben wird. Pseudonymisierung kann als datenschutzfördernde Maßnahme dienen, indem die Identität eines Individuums in einem spezifischen Zusammenhang verborgen wird.

Pseudonymisierung

Pseudonymisierung ist gemäß Art. 4 Nr. 5 DSGVO 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. Ein konkretes Beispiel ist die Verwendung von Patienten- und Kontrollnummern (anstelle von Namen) im Krebsregister des Landes Schleswig-Holstein (vgl. dazu § 5 Krebsregistergesetz – KRG SH).

Im Detail gibt es eine Reihe von Voraussetzungen, die ein rechtssicheres Pseudonymisierungsverfahren erfüllen muss, z. B. hinsichtlich der rechtlichen Zulässigkeit, der Betroffeneninformation oder der Regelungen für die Zuordnung pseudonymisierter Daten zu Personen. Darüber hinaus bestehen technische und organisatorische Anforderungen für eine geeignete Pseudonymisierung.

Mit diesen Fragestellungen beschäftigt sich die Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels der Bundesregierung. In dieser Gruppe arbeiten Vertreterinnen und Vertreter von Unternehmen, aus Hochschulen, von Unternehmensverbänden und zivilgesellschaftlichen Institutionen an gemeinsamen Positionen. Als Datenschutzaufsichtsbehörden sind der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sowie das ULD vertreten.

Im Jahr 2017 hat die Fokusgruppe bereits ein viel beachtetes „Whitepaper zur Pseudonymisierung“ veröffentlicht, anlässlich des Digital-Gipfels im Dezember 2018 ist ein Arbeitspapier der Fokusgruppe erschienen, in welchem die „Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen“ umrissen werden. Es ist unter folgendem Link abrufbar:

https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p9-datenschutzkonformer-einsatz-von-pseudonymisierungsloesungen.pdf

Die Fokusgruppe Datenschutz will sich in einem nächsten Schritt mit der Standardisierung von Pseudonymisierungsverfahren beschäftigen.

Was ist zu tun?

Die Arbeit zur Standardisierung von Pseudonymisierungsverfahren soll fortgesetzt werden. Best-Practice-Beispiele können den praktischen Nutzen bei gleichzeitiger Eindämmung des Risikos für die betroffenen Personen zeigen.

03

KERNPUNKTE

Parlamentarische Tätigkeiten

Datenschutz und Informationsfreiheit für Abgeordnete

3 Landtag

3.1 Parlamentarische Tätigkeit in eigener Datenschutzkontrolle der Abgeordneten

Das Landesdatenschutzgesetz Schleswig-Holstein sieht sowohl in alter als auch neuer Fassung eine Bereichsausnahme für die „Wahrnehmung parlamentarischer Aufgaben" vor. Parlamentarische Aufgaben unterfallen auch nicht dem Unionsrecht. Dies bedeutet, dass ein Großteil der Tätigkeit im Landtag nicht unter die Kontrolle der Landesbeauftragten für Datenschutz fällt und weder DSGVO noch LDSG gelten. Stattdessen hat sich der Landtag schon vor vielen Jahren unter Berücksichtigung seiner verfassungsrechtlichen Stellung und der Grundsätze des Landesdatenschutzgesetzes eine Datenschutzordnung für die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben gegeben. Darin werden auch die Zusammensetzung und die Aufgaben des Datenschutzgremiums geregelt. Die Landesbeauftragte für Datenschutz kann beratend tätig werden.

§ 2 Abs. 3 LDSG-neu

(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.

Mit der DSGVO ist die bisherige Datenschutzordnung nicht hinfällig geworden, sondern gilt weiterhin. Es ist eine Aktualisierung mit einigen Anpassungen geplant.

Zu berücksichtigen ist auch, dass der Landtag neben den parlamentarischen Aufgaben auch Verwaltungsaufgaben wahrnimmt und insoweit DSGVO und LDSG einschlägig sind. Generell bietet sich eine Orientierung an DSGVO und LDSG an, besonders bei der Gestaltung von Technik und Organisation.

§ 62 Abs. 1 Nr. 3 LDSG-neu

(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; [...]

In diesem Kapitel wurde in früheren Tätigkeitsberichten auch über erfolgreiche Datenschutzaudits des Landtages berichtet. Das Instrument des Audits gibt es jedoch seit dem 25. Mai 2018 mit Wegfall des vorherigen LDSG nicht mehr (Tz. 9.3). Stattdessen könnte man sich um eine Zertifizierung nach Artikel 42 DSGVO bemühen (Tz. 9.1), sobald das Instrument in der Praxis nutzbar ist.

3.2 Service – Datenschutz und Informationsfreiheit für Abgeordnete

Die Datenschutz-Grundverordnung hat überall für Aufmerksamkeit für das Thema Datenschutz gesorgt, auch bei den Abgeordneten des Schleswig-Holsteinischen Landtages. Daher hat das ULD die Abgeordneten im Februar 2018 zu einem Datenschutzabend eingeladen und vorgestellt, womit sich die Dienststelle täglich beschäftigt, wer die Ansprechpersonen für die vielfältigen Themen sind und wie die Abgeordneten sich beraten lassen können, wenn Fragen zum Datenschutz oder auch zur Informationsfreiheit auftauchen. Auch aktuelle Risiken in der Technik wurden vorgestellt, so die „Yellow Dots", die Farbdrucker in Ausdrucken encodieren (Tz. 10.4) oder das Ultraschall-Tracking (Tz. 10.3), das vom ULD in einer kleinen Demoinstallation vorgeführt wurde.

Während an dem Datenschutzabend nur ein grober Überblick gegeben werden konnte, zeigte sich mit dem Wirksamwerden der DSGVO, dass ein konkreter Bedarf an Unterstützung für die Abgeordneten bestand. An mehreren Terminen waren daher ULD-Mitarbeiterinnen und -Mitarbeiter vor Ort, um den interessierten Abgeordneten aller vertretenen Parteien Rede und Antwort zu stehen. Viele Themen betrafen alle Teilnehmenden in ihrer täglichen Arbeit. Einige Abgeordnete nutzten darüber hinaus die Möglichkeit, sich bei Spezialfragen und individuellen Einzelfällen beraten zu lassen.

Eine besondere Schwierigkeit ergibt sich aus der Tatsache, dass Abgeordnete in vielfältigen Rollen personenbezogene Daten verarbeiten können: als Einzelperson, als Verantwortliche in den Fraktionen und Gruppen im Landtag, als Parteimitglieder mit unterschiedlicher Verantwortung auf Orts-, Landes- und Bundesebene und schließlich auch als Kontakt für die Wählerinnen und Wähler in den Wahlkreisen, die sich auch zu Datenschutzthemen mit der Bitte um Rat und Tat an ihre Abgeordneten wandten. Gar nicht so einfach, sich jeweils die eigene Rolle bewusst zu machen, in der man gerade agiert, denn davon hängt auch ab, welche rechtlichen Datenschutzregeln gelten. Zum Glück bedeutet dies im Ergebnis aber nicht, dass die datenschutzkonformen Lösungen für die einzelnen Verarbeitungstätigkeiten jeweils einzeln und immer wieder von vorn erarbeitet werden müssen. Hat man einmal die Zwecke der Verarbeitung bestimmt und die zugehörigen Standardprozesse überlegt, fällt auch die Umsetzung nicht mehr schwer. Eine Hilfestellung besteht darin, dass man sich in die Position derjenigen hineinversetzt, deren personenbezogene Daten verarbeitet werden: Sind sie wohl damit einverstanden, oder empfinden sie dies als unfair? Ist ihnen bewusst, dass und welche Datenverarbeitungen stattfinden? Wissen sie, an wen Daten weitergegeben werden können?

Und wieder gilt, was wir schon in Tz. 1.1 geschrieben haben: Bei der Auswahl von Produkten und Dienstleistungen Datenschutz-Compliance einfordern!

Was ist zu tun?

Die Abgeordneten des Schleswig-Holsteinischen Landtages und ihre Teams können sich gerne bei Fragen zu Datenschutz und Informationsfreiheit an die Landesbeauftragte für Datenschutz und ihre Dienststelle wenden.

04

KERNPUNKTE

Neues Landesdatenschutzgesetz

Behördliche Datenschutzbeauftragte

Prüfungen in den Bereichen Polizei und Verfassungsschutz

Neue Rolle des ULD im Schulbereich

4 Datenschutz in der Verwaltung

4.1 Allgemeine Verwaltung

4.1.1 Neues Landesdatenschutzgesetz

Bis zum 25. Mai 2018 waren die Vorschriften zum Datenschutz für den öffentlichen Bereich im Land Schleswig-Holstein einfach zu verorten: Entweder gab es bereichsspezifisches Recht, das sich in Bundes- oder Landesgesetzen und Verordnungen fand. Oder – soweit dies nicht der Fall war – man griff auf die Vorschriften des Landesdatenschutzgesetzes (LDSG) vom 9. Februar 2000 zurück.

Seit dem 25. Mai 2018 gilt die DSGVO (EU-Verordnung 2016/679), die in allen Mitgliedstaaten der EU direkt anwendbar ist. Gleichwohl ist im Mai auch ein vom Landtag im April 2018 verabschiedetes neues Landesdatenschutzgesetz in Kraft getreten, das sogar deutlich umfangreicher ist als das alte LDSG. War das nötig?

Das neue LDSG dient zwei Zwecken. Der erste Zweck besteht darin, dass sogenannte Öffnungsklauseln in der DSGVO wahrgenommen werden. Diese erlauben es dem nationalen Gesetzgeber, eigene Regelungen zu treffen, z. B. zur Einschränkung der Rechte der betroffenen Personen. Zum Teil werden die Mitgliedstaaten auch verpflichtet, eigene Vorschriften zu erlassen. Dies betrifft vor allem die Rechtsgrundlagen für die Datenverarbeitung im öffentlichen Bereich. Im Abschnitt 2 des neuen LDSG (§§ 3-19) werden diese Öffnungsklauseln wahrgenommen und entsprechende Regelungen erlassen.

Der weitere Zweck des neuen LDSG steht im Zusammenhang mit der „Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates“, der sogenannten JI-Richtlinie, die zeitgleich mit der DSGVO im EU-Amtsblatt veröffentlicht wurde. Da es sich um eine Richtlinie handelt, war es erforderlich, dass der nationale Gesetzgeber sie in eine gesetzliche Vollregelung umsetzt. Dies ist für das Land Schleswig-Holstein mit dem Abschnitt 3 des neuen LDSG (§§ 20-68) erfolgt. Offensichtlich gelten diese Vorschriften für den Bereich der Strafverfolgung durch die Polizei und die Justiz sowie der Gefahrenabwehr durch die Polizei. Wegen der Nähe zur Strafverfolgung fällt allerdings auch die Verfolgung von Ordnungswidrigkeiten unter die Richtlinie. Dies ist von Bedeutung für alle Bußgeldverfahren, die von öffentlichen Stellen betrieben werden. Namentlich im Bereich der Verfolgung von Verkehrsordnungswidrigkeiten, wo es in den Fachgesetzen an konkreten Vorgaben zur Verarbeitung personenbezogener Daten fehlt, werden die Vorschriften im Abschnitt 3 des LDSG zur Anwendung kommen. Bei der Gefahrenabwehr, die durch sonstige, z. B. kommunale Ordnungsbehörden betrieben wird, bleibt es bei der Anwendung der DSGVO und der ergänzenden Regelungen im Abschnitt 2 des LDSG.

Der Vollständigkeit halber sei noch erwähnt, dass sich in Abschnitt 1 des LDSG (§§ 1-2) die Vorschriften zum Gesetzeszweck und zum Anwendungsbereich finden. Die Vorschriften zur Organisation des Unabhängigen Landeszentrums für Datenschutz (ULD) als Anstalt öffentlichen Rechts wurden in ein separates Gesetz ausgegliedert. Darin wurde insbesondere die Amtszeit der oder des Landesbeauftragten für Datenschutz auf sechs Jahre ausgedehnt, allerdings die Wiederwahl erneut auf eine weitere Amtsperiode begrenzt. Aufsichtsbehörde ist die oder der Landesbeauftragte für Datenschutz, die oder der zugleich Leiter(in) des ULD ist. Zusammen mit dem Neuerlass des LDSG wurden knapp 40 Landesgesetze geän-

dert. Dabei ging es in erster Linie um begriffliche Anpassungen an die DSGVO.

Das ULD hatte im Vorfeld der Verabschiedung des LDSG ausführliche Stellungnahmen abgegeben. Viele unserer Vorschläge wurden schließlich berücksichtigt. Doch auch einige kritikwürdige Formulierungen fanden ihren Weg in die verabschiedete Fassung, wie z. B. die Vorschrift zur Videoüberwachung, die als Erlaubnis zur Nutzung biometrischer Überwachungssysteme missverstanden werden könnte. Alles in allem liegt mit dem LDSG aber ein brauchbares Gesetz vor, das jetzt durch Anwendung und Auslegung mit Leben gefüllt werden muss. Bereits nach einem Jahr soll das Gesetz evaluiert werden, sodass sich bereits im Jahr 2019 die Gelegenheit zur weiteren Verbesserung des LDSG bietet.

Was ist zu tun?

Um sich mit dem neuen Datenschutzrecht in Schleswig-Holstein vertraut zu machen, sollten die zuständigen Mitarbeiterinnen und Mitarbeiter der öffentlichen Stellen geeignete Veranstaltungen, z. B. der DATENSCHUTZAKADEMIE Schleswig-Holstein, besuchen. Ergeben sich Probleme oder Widersprüche bei der Anwendung des LDSG, sollte dies dem ULD mitgeteilt werden, damit der entsprechende Punkt in den Prozess der Evaluierung eingebracht werden kann.

4.1.2 Benennung behördlicher Datenschutzbeauftragter

Unter dem früheren Landesdatenschutzgesetz (LDSG-alt) vom 9. Februar 2000 bestand zwar die Möglichkeit für öffentliche Stellen, eine oder einen behördliche(n) Datenschutzbeauftragte(n) zu bestellen, aber keine Pflicht. Das hat sich mit dem vollständigen Inkrafttreten der DSGVO geändert. Diese schreibt vor, dass Verantwortliche und Auftragsverarbeiter in jedem Fall eine(n) Datenschutzbeauftragte(n) (DSB) zu benennen haben, wenn die Verarbeitung der Daten von einer Behörde oder öffentlichen Stelle durchgeführt wird. Ausgenommen sind nur Gerichte, die im Rahmen ihrer justiziellen Tätigkeit handeln. An dieser Stelle sei angemerkt, dass das ULD die Begriffe „Benennung" (wie es die DSGVO bezeichnet) und „Bestellung" von DSB (Bezeichnung im deutschen Datenschutzrecht vor Geltung der DSGVO) als deckungsgleich ansieht.

Damit trifft die Benennungspflicht alle öffentlichen Stellen, unabhängig von der Größe, namentlich die Landesbehörden und Kommunen und die von den letzteren gegründeten Zweckverbände und gemeinsamen Kommunalunternehmen. Erfasst sind z. B. aber auch kleine, ehrenamtlich arbeitende Wasser- und Bodenverbände, denn diese sind nach § 1 Wasserverbandsgesetz Körperschaften des öffentlichen Rechts. Die Benennungspflicht trifft auch Private, die aufgrund einer Beleihung hoheitliche Tätigkeiten ausüben, wie z. B. bevollmächtigte Bezirksschornsteinfeger.

Eigenbetriebe zählen als Teil der Kommune. Daher geht das ULD davon aus, dass ein von der Kommune bestellter DSB auch für den Eigenbetrieb zuständig ist, soweit nicht der Eigenbetrieb einen eigenen DSB bestellt hat. Entsprechendes gilt für kommunale Kindertagesstätten (Kitas) und für Feuerwehren.

§ 5 Abs. 2 Brandschutzgesetz Schleswig-Holstein

Die öffentlichen Feuerwehren sind gemeindliche Einrichtungen ohne eigene Rechtspersönlichkeit.

Werden Aufgaben auf privatrechtlich konstituierte Träger (z. B. den Kommunen gehörende GmbHs) ausgelagert, so richtet sich die Benennung eines DSB bei diesen Stellen nach dem Bundesdatenschutzgesetz.

Anders als unter dem früheren LDSG ist nicht nur die Benennung von eigenen Beschäftigten als DSB möglich. Die DSGVO lässt es ausdrücklich zu, auch Externe zu benennen. In beiden Fällen ist jedoch die erforderliche Qualifikation sicherzustellen.

Art. 37 Abs. 5 DSGVO

Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.

Aus dem Erwägungsgrund 97 zur DSGVO ergibt sich, dass das Fachwissen umso ausgeprägter sein muss, je umfangreicher die Datenverarbeitung und der damit gebotene Schutz der Daten ausfallen. Insbesondere für die große Zahl der im Zusammenhang mit der DSGVO neu benannten DSB ist es daher entscheidend, an geeigneten Fortbildungsveranstaltungen teilzunehmen, um möglichst schnell eine solide Kenntnis von Datenschutzrecht und -technik zu erwerben.

Dabei ist gerade bei der Benennung eigener Beschäftigter als DSB zu beachten, dass die Stelle angemessen dotiert ist. Eine Vergütung unterhalb E 11/A 12 ist nicht angemessen, da die Aufgabe der behördlichen DSB von einer erheblichen Komplexität ist. Diese ergibt sich z. B. aus einem Urteil des Finanzgerichts München vom 25. Juli 2017 (das allerdings noch auf die alte Rechtslage und den Privatbereich abstellt):

uldsh.de/fg-muenchen-dsb

Die DSGVO sieht auch vor, dass mehrere öffentliche Stellen eine(n) gemeinsame(n) DSB benennen können. Gerade bei Kommunen bietet sich dies unter Ausnutzung des Instrumentariums des Gesetzes über die kommunale Zusammenarbeit an. Hierbei ist zu beachten, dass ein realistischer Personalschlüssel zugrunde gelegt wird. Die Bundesbeauftragte für den Datenschutz (BfDI) hatte im Hinblick auf die Bundesverwaltung ein Verhältnis von 1.000 Beschäftigen auf eine Vollzeitstelle einer DSB angemahnt. Nach vollständiger Geltung der DSGVO hat die BfDI den Schlüssel auf eine Stelle je 500 Beschäftige herabgesetzt.

uldsh.de/dsgvo-bundesverwaltung
(S. 29 f. der PDF-Datei)

Vor diesem Hintergrund und aufgrund der in der Vergangenheit mit den bereits unter dem früheren LDSG bestellten DSB gemachten Erfahrungen geht das ULD derzeit davon aus, dass auch bei Kommunen eine Obergrenze von 1.000 Beschäftigten pro Vollzeitstelle einer oder eines DSB gilt. Dies ist auch bei der Benennung von gemeinsamen DSB zu beachten. Hat ein Kreis z. B. etwa 700 Beschäftigte, so dürfen die von der oder dem gemeinsam bestellten DSB betreuten Kommunen oder Zweckverbände zusammen nicht mehr als 300 Beschäftigte haben. Wird diese Anzahl überschritten, ist in der Regel die Schaffung einer weiteren (gegebenenfalls anteilsmäßigen) Stelle erforderlich.

Bei kleineren öffentlichen Stellen kann die oder der DSB auch mit anderen Aufgaben betraut werden. Diese dürfen jedoch nicht zu einem Interessenkonflikt führen. Damit scheidet die Benennung von leitenden Mitarbeiterinnen und Mitarbeitern der öffentlichen Stelle oder auch der IT-Abteilung aus.

Die Kontaktdaten der oder des DSB sind zu veröffentlichen. Die Veröffentlichung hat regelmäßig auf der Homepage der öffentlichen Stelle zu erfolgen. Dabei ist es nicht zwingend erforderlich, dass der Name der oder des DSB genannt wird. Es muss mindestens eine postalische und elektronische Kontaktadresse angegeben werden, letztere z. B. nach dem Schema: datenschutz@behoerde.de. Für die ebenfalls verpflichtende Meldung der DSB an die Aufsichtsbehörde hat das ULD ein Meldeportal zur Verfügung gestellt unter:

uldsh.de/dsb-meld

Die oder der DSB berichtet unmittelbar der höchsten Managementebene – es handelt sich also um eine Stabsstellenfunktion. Es besteht Weisungsfreiheit bei der Ausübung der Aufgaben als DSB; die Dienststellenleitung darf z. B. nicht anordnen, dass eine bestimmte Kontrolle durch die oder den DSB vorrangig durchzuführen sei. Weiterhin muss die oder der DSB frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden werden. Dazu gehört eine Informationspflicht der öffentlichen Stelle gegenüber der oder dem DSB z. B. bei der Einführung neuer IT-Verfahren. Dies betrifft sowohl die Verarbeitung der personenbezogenen Daten von Bürgerinnen und Bürgern als auch die Verarbeitung von Beschäftigtendaten.

Die DSGVO legt fest, dass die oder der DSB wegen der Erfüllung der gesetzlichen Aufgaben nicht abberufen oder benachteiligt werden darf. Anders als im BDSG finden sich im LDSG keine weiter reichenden Regelungen zum Kündigungsschutz. Daher wäre es z. B. zulässig, wenn die oder der DSB einer öffentlichen Stelle von der Position abberufen wird, weil die Stelle die Aufgabe aus wirtschaftlichen Erwägungen an Externe vergeben will.

Der oder dem DSB müssen alle notwendigen Ressourcen zur Verfügung gestellt werden. Dazu gehört, dass die öffentliche Stelle

- eine Arbeitsumgebung zur Verfügung stellt, die es der oder dem DSB ermöglicht, seine Aufgaben mit dem jeweils nötigen Grad an Vertraulichkeit zu erfüllen; dazu gehört die Nutzungsmöglichkeit von entsprechenden Räumlichkeiten (z. B. ein Einzelbüro oder ein Besprechungszimmer), ein abgesicherter E-Mail-Zugang oder abschließbare Behältnisse für Dokumente,
- die Teilnahme an Fortbildungen ermöglicht und Fachliteratur finanziert,
- die Teilnahme an Sitzungen mit anderen DSB ermöglicht und die erforderlichen Reisekosten übernimmt.

Dabei kann es sinnvoll sein, der oder dem DSB für die Erfüllung der Aufgaben ein angemessenes Budget zur Verfügung zu stellen, sodass die oder der DSB selbst priorisieren kann, wofür die vorhandenen Mittel ausgegeben werden.

Zu den Aufgaben der oder des DSB gehören die Beratung der öffentlichen Stelle und die Schulung der Beschäftigten sowie die Kontrolle der Einhaltung der Vorschriften über den Datenschutz. Für die Aufsichtsbehörde, in Schleswig-Holstein also die Landesbeauftragte für Datenschutz mit ihrer Dienststelle, dem ULD, dient sie oder er als Kontaktperson.

Die betroffenen Personen können sich in allen Fragen der Datenverarbeitung direkt an die oder den DSB wenden. Die oder der DSB ist zum Stillschweigen über die Sachverhalte verpflichtet, die ihr oder ihm in dieser Eigenschaft bekannt werden.

Es ist wichtig zu betonen, dass die oder der DSB keinesfalls selbst die Verantwortung für die Datenverarbeitung trägt. Diese verbleibt bei der Leitung der öffentlichen Stelle.

Für den Anwendungsbereich der JI-Richtlinie (dazu siehe oben unter Tz. 4.1.1) finden sich in den §§ 58-60 LDSG-neu Regelungen zur Benennung von Datenschutzbeauftragten, die im Wesentlichen mit den Artikeln 37-39 der DSGVO übereinstimmen. Diese gelten für Behörden, die ausschließlich oder vornehmlich diesen Teil des LDSG anwenden, also in erster Linie für die Polizei. Das ULD geht insoweit von einer einheitlichen Benennung von DSB bei einer öffentlichen Stelle entweder nach Artikel 37 DSGVO oder nach § 58 LDSG-neu aus. Das bedeutet: Soweit öffentliche Stellen das jeweils andere Rechtsregime anwenden (z. B. Kommunen als Ordnungswidrigkeitenbehörden den Abschnitt 3 des LDSG-neu oder die Polizei in Personalangelegenheiten die DSGVO und den Abschnitt 2 des LDSG-neu), ist insoweit keine erneute oder gesonderte Benennung einer oder eines DSB nach jenem Rechtsregime erforderlich. Die oder der DSB wird immer nach dem Rechtsregime benannt, das vorrangig anwendbar ist, bei den allermeisten öffentlichen Stellen also nach Artikel 37 DSGVO, bei der Polizei nach § 58 LDSG-neu.

Was ist zu tun?

Alle öffentlichen Stellen haben eine oder einen Datenschutzbeauftragten zu benennen. Diesen sind angemessene Ressourcen und die Gelegenheit zur Fortbildung zu gewähren, damit sie ihre Aufgaben erfüllen können.

4.1.3 Versand von personenbezogenen Informationen per E-Mail innerhalb und außerhalb des Landesnetzes

Im Berichtszeitraum traten mehrere öffentliche Stellen des Landes an das ULD heran und baten um Bewertung der Frage, unter welchen Bedingungen personenbezogene Informationen per E-Mail versandt werden dürfen. Von Bedeutung ist dies vor allem in Massenverfahren, in denen große Zahlen von Adressaten erreicht werden müssen. In diesen Verfahren kann der Versand von Informationen per E-Mail zu erheblichen Kosteneinsparungen führen. Gleichwohl sind die Anforderungen des Datenschutzrechts an die erforderliche Datensicherheit zu beachten.

Wenn sich Versender und Adressat im Landesnetz befinden, bestehen insoweit keine Probleme. Das Landesnetz ist vom allgemeinen Internet abgeschottet und gilt aktuell als hinreichend sicher, sodass innerhalb des Landesnetzes auch personenbezogene Daten per E-Mail versandt werden können. Auf diese Weise kann z. B. das Dienstleistungszentrum Personal (DLZP) mit den allermeisten aktiven Beschäftigten kommunizieren, da diese E-Mail-Adressen innerhalb des Landesnetzes haben. Gefahren für die Vertraulichkeit entstehen jedoch dann, wenn E-Mails automatisiert weitergeleitet werden (Urlaub/Vertretung) oder Postfächer für die Einsicht Dritter, etwa innerhalb einer Arbeitsgruppe, geöffnet wurden.

Schwieriger wird die Lage, wenn E-Mails nach außerhalb des Landesnetzes versandt werden sollen. Dies betrifft z. B. die etwa 30.000 Ruhegehaltsempfängerinnen und -empfänger, die vom DLZP ebenfalls betreut werden. Ein anderer Anwendungsfall ist die Kommunikation mit Bewerberinnen und Bewerbern auf Stellen im öffentlichen Dienst, die im Rahmen des Bewerbungsverfahrens bestimmte Nachrichten erhalten sollen.

Nach wie vor gilt, dass das Versenden von E-Mails im öffentlichen Internet unsicher ist. Zwar wird zum Teil eine sogenannte Transportverschlüsselung verwendet, die die E-Mail bei ihrem Transport zwischen E-Mail-Servern verschlüsselt. Allerdings wird diese Transportverschlüsselung bei der Zwischenspeicherung auf dem E-Mail-Server wieder entfernt, sodass jedenfalls für die Betreiber der Server die E-Mail-Nachricht und etwaige Anhänge ohne Weiteres lesbar sind. Vorzuziehen wäre eine sogenannte Ende-zu-Ende-Verschlüsselung, wie sie beispielsweise durch den OpenPGP-Standard oder bei der Verwendung von S/MIME sichergestellt werden kann: Hier erfolgen Ver- und Entschlüsselung direkt bei den Absendern bzw. Empfängern auf deren Endgeräten. Allerdings gibt es leider nach wie vor nur eine relativ geringe Zahl von Versendern bzw. Empfängern von E-Mails, die an diesem Verfahren teilnehmen. Um gleichwohl zu einem angemessenen Schutz im Sinne von Artikel 32 DSGVO zu kommen, hält das ULD die folgenden Maßgaben für geeignet:

Die Versendung von personenbezogenen Daten per E-Mail ist ausnahmsweise dann auch außerhalb des Landesnetzes zulässig, wenn die oder der Betroffene ihre oder seine Einwilligung dazu gegeben hat. Dazu muss sie oder er über die Risiken adäquat aufgeklärt worden sein. Die Einwilligung kann auch jederzeit mit Wirkung für die Zukunft widerrufen werden.

Eine solche Einwilligung darf sich jedoch nur auf Daten beziehen, die nicht dem besonderen Schutz des Art. 9 Abs. 1 DSGVO unterliegen. Im Hinblick auf den rechtlich gebotenen Schutz dieser besonders sensiblen Daten kommt eine unverschlüsselte Versendung über offene Netze nicht infrage.

Art. 9 Abs. 1 DSGVO

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

Konkret wurde dies beispielsweise für das Management von Bewerberdaten im Landesbereich mit dem Finanzministerium abgestimmt, das den Einsatz des dafür vorgesehenen Systems KoPers organisiert. In Massenbewerbungsverfahren, wie z. B. bei der Polizei, können allgemeine Verfahrensnachrichten per E-Mail versandt werden, wenn die Betroffenen darin eingewilligt haben. Dies betrifft beispielsweise die Nachricht, dass die Bewerbung erfolgreich eingegangen ist. Weiterhin dürfen auch Mitteilungen über die Erfolglosigkeit der Bewerbung versendet werden, wenn sie keine Daten im Sinne von Artikel 9 DSGVO oder vergleichbar sensible Daten enthalten. Zu den vergleichbar sensiblen Daten sind beispielsweise auch Daten über die Körpergröße zu zählen, deren Nichterreichen zur Zurückweisung einer Bewerbung führt. In solchen Fällen ist ein Schreiben auf dem Postweg zu versenden.

Was ist zu tun?

Die öffentlichen Stellen im Land Schleswig-Holstein sollten vorrangig darum bemüht sein, mit ihren Kommunikationspartnern verschlüsselte E-Mails auszutauschen, wenn personenbezogene oder andere schutzwürdige Daten enthalten sind. Ohne ausreichenden Schutz dürfen besonders sensible personenbezogene Daten (Artikel 9 DSGVO) nicht per E-Mail versandt werden.

4.1.4 E-Mails mit nachgesandtem Passwort führen nicht zu Sicherheit von Meldedaten

Im Berichtszeitraum wandte sich das Ministerium für Inneres, ländliche Räume und Integration an das ULD und bat um datenschutzrechtliche Beratung im Zusammenhang mit der Durchführung einer Befragung. Mit Beschluss vom 4. Oktober 2017 hatte der Schleswig-Holsteinische Landtag die Landesregierung beauftragt, eine wissenschaftlich begleitete Sportentwicklungsplanung für das Land Schleswig-Holstein durchzuführen; Teil davon sollte auch die Befragung der Bevölkerung zu ihren Sportgewohnheiten und zu Anforderungen z. B. im Hinblick auf Vereine und Sportstätten sein. Das Innenministerium bat das ULD insbesondere um Beratung dazu, in welcher Weise auch Minderjährige in datenschutzkonformer Weise in die Befragung einbezogen werden können. Das ULD hat dazu Empfehlungen abgegeben, die – soweit ersichtlich – vom Innenministerium auch umgesetzt wurden.

Bei der Durchführung sorgte dann allerdings die sogenannte Stichprobenziehung für einige Nachfragen beim ULD. Die Befragungsunterlagen sollten an eine möglichst repräsentative Auswahl von Einwohnern des Landes geschickt

werden. Dazu hatte das Innenministerium die Meldebehörden in den Kommunen angewiesen, eine bestimmte Anzahl von Datensätzen aus dem jeweiligen Melderegister zu ziehen. Diese Stichprobe sollte sodann als Excel-Tabelle per E-Mail an das Innenministerium übersendet werden. Dazu sollte die Excel-Datei verschlüsselt und mit einem Kennwort gegen unerlaubten Zugriff gesperrt werden, was innerhalb des Programms selbst möglich ist. Sodann sollte die Datei mittels E-Mail an das Innenministerium übersandt werden. Um die Datei auf der Empfängerseite zu entschlüsseln, wurden die Meldebehörden aufgefordert, das Passwort, mit dem die Excel-Datei gesperrt ist, in einer zweiten E-Mail an denselben Empfänger im Innenministerium zu übersenden.

Dieses Vorgehen rief die Kritik einiger kommunaler Datenschutzbeauftragter hervor. Diese wiesen darauf hin, dass die Übersendung des Passworts auf demselben Kanal wie die mit diesem Passwort geschützten Informationen nur unwesentlich zur Erhöhung der Sicherheit beiträgt. Die Datenschutzbeauftragten schlugen vielmehr vor, das Passwort auf einem anderen Kanal, z. B. telefonisch, an den Empfänger im Innenministerium durchzugeben, um so für eine erhöhte Sicherheit zu sorgen.

Das Innenministerium war mit diesem Vorgehen nicht einverstanden. Mit einer E-Mail an alle Meldebehörden erklärte es, dass der getrennte Versand der Excel-Datei und des Passworts jeweils per E-Mail sicher sei und datenschutzrechtlich nicht beanstandet werden könne. Es handele sich hierbei um eine „Zwei-Faktor-Verschlüsselung“, die den inhaltlichen Vorgaben von Art. 32 Abs. 1 DSGVO (Datensicherheit) entspreche. Soweit sich einige Meldebehörden gleichwohl darum bemühten, das Passwort telefonisch durchzugeben, wurde dieses dem Vernehmen nach aufseiten des Innenministeriums nicht angenommen.

Das ULD sah sich gezwungen, in einer eigenen Mitteilung an die Meldebehörden klarzustellen, dass mit der vom Innenministerium vorgeschlagenen Versandart keine ausreichende Sicherheit hergestellt werden könne. Es handelt sich gerade nicht um ein Zwei-Faktor-Verfahren, wenn die verschlüsselte Datei und das Passwort über dasselbe Medium (E-Mail) versendet werden. Gerade weil der Versand von personenbezogenen Informationen per E-Mail keine ausreichende Sicherheit der Daten gewährleistet, werden diese verschlüsselt. Dann das Passwort über ebenjenen unsicheren Übertragungsweg zu versenden, erhöht die Datensicherheit allenfalls marginal; jedenfalls wird nicht das dem Risiko angemessene Schutzniveau gewährleistet.

Aus Sicht des ULD ist es daher geboten, für die Übermittlung des zugehörigen Passworts einen anderen Kanal zu verwenden. Dabei bietet es sich an, dies per Telefonanruf bei der vom MILI dort bestimmten Person zu erledigen. Dies würde eine geeignete Maßnahme nach Art. 32 Abs. 1 DSGVO darstellen, die neben Art, Umfang, Umständen und Zwecken der Verarbeitung auch die Faktoren des Stands der Technik und der Implementierungskosten berücksichtigt und ein dem Risiko angemessenes Schutzniveau bietet. Alternative Verfahren sind ebenfalls denkbar, beispielsweise wenn vor der E-Mail-Zulieferung die zu verwendenden, ausreichend komplex gestalteten individuellen Passwörter den Zuständigen in den Meldebehörden per Briefpost zugesandt werden oder die Möglichkeit des Hochladens der Daten in einen geschützten Bereich auf einem Server des MILI über eine verschlüsselte Verbindung geschaffen wird.

Es ist festzustellen, dass das Innenministerium einerseits bei der Gestaltung des Befragungsverfahrens sich frühzeitig mit dem ULD in Verbindung setzte und Empfehlungen einholte, aber andererseits bezüglich der Datensicherheit bei der Übersendung der zu verwendeten Meldedaten darauf leider verzichtete.

Was ist zu tun?

Die Grundidee der Zwei-Faktor-Sicherheit basiert darauf, dass die beiden Faktoren voneinander unabhängig sind. Ohne ausreichende Sicherheit dürfen personenbezogene Daten nicht übertragen werden – das müssen auch Meldebehörden und Ministerien berücksichtigen. Künftig sollte in vergleichbaren Fällen die Kritik der kommunalen Datenschutzbeauftragten ernst genommen und das Verfahren umgestaltet werden.

4.1.5 Unzulässiges Anfertigen und Speichern von Scans oder Kopien der Geburtsurkunde bei Beantragung von Ausweisdokumenten

Im Rahmen einer Beschwerde erhielt das ULD Kenntnis davon, dass im Bürgerbüro einer Stadtverwaltung bei der Beantragung von Ausweisdokumenten Geburtsurkunden eingescannt und gespeichert wurden. Der betroffenen Person wurde mitgeteilt, dass die Anfertigung einer Kopie ihrer Geburtsurkunde und deren Speicherung durch das Bürgerbüro eine Pflichtvoraussetzung für die Beantragung eines neuen Personalausweises sei. Informationen über die Rechtsgrundlage oder sonstige Umstände der Datenverarbeitung wurden der Person nicht erteilt. Im Rahmen der Anhörung durch das ULD erklärte die Stadtverwaltung, dass es sich bei dem Verfahren um ein „Serviceangebot" des Bürgerbüros handele. Die Bürgerinnen und Bürger hätten durch die Speicherung eines Scans ihrer Geburtsurkunde den Vorteil, dass sie diese bei der Beantragung weiterer Dokumente zukünftig nicht erneut vorlegen müssten.

Es stellt sich bereits die Frage, ob ein solches „Serviceangebot" überhaupt vom öffentlich-rechtlichen Auftrag eines Bürgerbüros bzw. Einwohnermeldeamtes umfasst sein kann. In jedem Fall setzt eine solche Verarbeitung personenbezogener Daten das Vorliegen einer Rechtsgrundlage voraus.

Dabei ist zu berücksichtigen, dass die Geburtsurkunde einer Person nicht nur die Schreibweise ihres Namens erkennen lässt, sondern in der Regel auch personenbezogene Daten ihrer Eltern beinhaltet. In vielen Fällen enthält die Urkunde auch Angaben über die Zugehörigkeit der Person und ihrer Eltern zu einer Religionsgemeinschaft. Dabei handelt es sich um besondere Kategorien personenbezogener Daten, deren Verarbeitung sich nur nach den strengen Vorgaben des Artikels 9 DSGVO zulässig ist.

Eine Rechtsgrundlage ist jedoch für die Anfertigung und Speicherung von Scans oder Kopien der Geburtsurkunde bei der Beantragung von Ausweisdokumenten nicht gegeben: Weder kann eine Einwilligungserklärung im Sinne von Art. 6 Abs. 1 Buchst. a DSGVO die Datenverarbeitung legitimieren, noch konnte diese auf § 11 LDSG-alt oder auf Art. 6 Abs. 1 Buchst. e DSGVO in Verbindung mit § 3 Abs. 1 LDSG-neu gestützt werden.

Die Verarbeitung besonderer Kategorien personenbezogener Daten erfordert außerdem das Vorliegen eines erheblichen öffentlichen Interesses, das bei einem bloßen „Serviceangebot" zu verneinen ist. Weitere gesetzliche Ausnahmetatbestände liegen nicht vor, auch ist keine spezialgesetzliche Rechtsgrundlage für die Verarbeitung der besonderen Kategorien personenbezogener Daten über Herkunft und Religionszugehörigkeit gegeben.

Insbesondere stellt § 3 Abs. 1 Bundesmeldegesetz (BMG) keine taugliche Rechtsgrundlage in diesem Sinne dar. Der vom Ministerium für Inneres, ländliche Räume und Integration vertretenen Ansicht, dass die Meldebehörden Scans und Kopien von Geburtsurkunden auf dieser Grundlage fertigen und speichern dürften (Runderlass des Ministeriums vom 27. Juni 2018 über das Verhältnis von Melderegister,

Passregister und Personalausweisregister, Speichern von Nachweisen), ist nicht zuzustimmen. Die Verpflichtung der Meldebehörden durch § 3 Abs. 1 BMG beschränkt sich zunächst auf die Speicherung der dort unter Nr. 1-19 genannten Grunddaten. Nur wenn zum Nachweis der Richtigkeit der Grunddaten weitere „Hinweise" **erforderlich** sind, können auch diese im Melderegister gespeichert werden. Nach diesem Erforderlichkeitsgrundsatz dürfen nur solche Daten verarbeitet werden, die zur Zweckerreichung absolut notwendig sind. Bloß irgendwie dienliche oder förderliche Angaben sind nicht erforderlich in diesem Sinne. Ihre Speicherung würde auch gegen den Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO, zuvor „Datensparsamkeit" gemäß § 4 LDSG-alt) verstoßen. Angaben sind erst dann notwendig, wenn zur Erreichung des beabsichtigten Ziels keine sinnvolle oder zumutbare Alternative zur Datenverarbeitung gegeben ist.

Nach Einsichtnahme in die Geburtsurkunde durch eine Mitarbeiterin oder einen Mitarbeiter des Bürgerbüros und lesendem Abgleich der korrekten Schreibweise des Namens ist die Anfertigung und Speicherung einer Kopie der Urkunde nicht mehr notwendig. Ebenso wenig wäre die Speicherung einer Kopie der Promotionsurkunde, des Personalausweises oder des Reisepasses erforderlich. Einwohnermeldeämter bzw. Bürgerbüros müssen von der Anfertigung und Speicherung von Kopien oder Scans von Geburtsurkunden absehen, da es dafür keine Rechtsgrundlage gibt.

Was ist zu tun?

Das Ministerium für Inneres, ländliche Räume und Integration sollte den Runderlass vom 27. Juni 2018 über das Verhältnis von Melderegister, Passregister und Personalausweisregister, Speichern von Nachweisen unter dem Gesichtspunkt der Datenminimierung überprüfen und korrigieren.

4.1.6 Veröffentlichung von Daten der Wahlbewerber bei der Kommunalwahl

Das ULD erreichten zahlreiche Beschwerden darüber, dass im Kontext der Kommunalwahl im Jahr 2018 eine Reihe von persönlichen Daten der Wahlbewerber im Internet veröffentlicht wurde.

Das ULD musste den Beschwerdeführern mitteilen, dass die Veröffentlichung der Daten nicht zu beanstanden war, da sie von der Gemeinde- und Kreiswahlordnung (GKWO) so vorgesehen ist. § 74 Abs. 2 GKWO bestimmt, welche Daten ein Wahlvorschlag enthalten muss, nämlich den Familiennamen, den Vornamen (bei mehreren Vornamen den oder die Rufnamen), den Beruf oder den Stand, das Geburtsdatum, die Staatsangehörigkeit und die Anschrift (Hauptwohnung) der Bewerberin oder des Bewerbers sowie beim Wahlvorschlag einer politischen Partei oder Wählergruppe den Namen der Partei oder Wählergruppe. § 77 GKWO verpflichtet die Gemeindewahlleiterin oder den Gemeindewahlleiter, die zugelassenen Wahlvorschläge bekannt zu geben. Nach § 77 Abs. 1 Satz 2 GKWO hat diese Bekanntmachung die in § 74 Abs. 2 GKWO bezeichneten Angaben zu enthalten. Lediglich das vollständige Geburtsdatum, das bei der Einreichung der Wahlvorschläge anzugeben ist, wird bei der Veröffentlichung auf das Geburtsjahr gekürzt. Nur falls ausnahmsweise für den Wahlbewerbenden eine Auskunftssperre im Melderegister eingetragen ist, entfällt die Angabe zur Anschrift; dann kann stattdessen eine sogenannte Erreichbarkeitsanschrift eingetragen werden.

Die Bekanntmachung der Wahlvorschläge richtet sich nach § 87 GKWO. Aus Abs. 1 Satz 3 der Vorschrift ergibt sich, dass die Veröffentlichung

auch im Internet erfolgen kann. Anders als bei der Veröffentlichung durch Aushang ist für die Veröffentlichung im Internet keine Höchstdauer vorgeschrieben. Da die Veröffentlichung der Daten der Wahlbewerbenden auf gesetzlichen Vorschriften beruhte, konnte das ULD diese nicht verhindern.

Allerdings hatte es auf politischer Ebene bereits im Jahr 2016 eine Initiative zur Einschränkung der zu veröffentlichenden Daten gegeben. Seinerzeit hatte die Fraktion der PIRATEN anlässlich einer Änderung der wahlrechtlichen Vorschriften einen Entschließungsantrag eingebracht, wonach der Landtag die Landesregierung auffordern solle, in der Wahlordnung statt der genauen Adresse der Wahlbewerberinnen und Wahlbewerber nur die Postleitzahl der Wohnanschrift und eine Erreichbarkeitsadresse zu verwenden (Drucksache 18/3588, auffindbar über die Mediathek des Landtages).

Diese Position wurde vom ULD in seiner damaligen Stellungnahme vom 29. Januar 2016 zu dem Gesetzentwurf (Umdruck 18/5561) unterstützt und von der Landesbeauftragten für Datenschutz in der Sitzung des Innen- und Rechtsausschusses vom 23. März 2016 bekräftigt (die Niederschrift der 126. Sitzung ist in der Mediathek des Landtages abrufbar). Gleichwohl ist die Mehrheit der Abgeordneten dieser Auffassung nicht gefolgt.

In der laufenden Legislaturperiode hat es im Landtag einen erneuten Versuch gegeben, die Veröffentlichungspflichten der GKWO einzuschränken. Der entsprechende Antrag der AfD-Fraktion (Drucksache 19/692) sowie der Alternativantrag aller anderen im Landtag vertretenen Fraktionen bzw. Parteien (Drucksache 19/715) wurden am 27. April 2018 im Landtag ausführlich diskutiert (Plenarprotokoll 19/30 ab Seite 2124). Dabei kam auch zur Sprache, dass in Berlin und Brandenburg die Veröffentlichung einer Erreichbarkeitsadresse anstelle der Wohnanschrift ausreiche. Schließlich wurde der Antrag der Mehrheitsfraktionen angenommen, wonach die Landesregierung im Innenausschuss über Übergriffe auf Kandidatinnen und Kandidaten sowie Sachbeschädigungen jeder Art zu Wahlen berichten sollte. Dieser Bericht wurde vom Innenminister in der Sitzung vom 30. Mai 2018 abgegeben. Der Ausschuss nahm den Bericht zur Kenntnis; weitere Beschlüsse wurden nicht gefasst.

Was ist zu tun?

Der Gesetzgeber sollte erneut erwägen, zum Schutze der Wahlbewerberinnen und Wahlbewerber die Veröffentlichung einer Erreichbarkeitsanschrift anstelle der Wohnadresse ausreichen zu lassen.

4.1.7 Melderegisterdaten für Seniorenbeiräte?

In vielen Kommunen in Schleswig-Holstein gibt es einen Seniorenbeirat. Dieser vertritt die Interessen der älteren Mitbürgerinnen und Mitbürger in der jeweiligen Kommune. Er kann gegenüber den Organen der Kommune Anregungen, Empfehlungen und Stellungnahmen abgeben. Kommunalrechtlich handelt es sich um einen „sonstigen Beirat" im Sinne der §§ 47d, 47e der Gemeindeordnung (GO). Eine kommunale Satzung regelt das Nähere, insbesondere das Wahlverfahren.

Von einigen Seniorenbeiräten ist der Wunsch geäußert worden, die Namen und Anschriften aller Einwohner der jeweiligen Kommune, die das 60. Lebensjahr vollendet haben, aus dem Melderegister der Kommune zu erhalten. Dazu hat das ULD festgestellt, dass sich eine Befugnis

zur Übermittlung der Daten nicht aus § 34 Abs. 1 Bundesmeldegesetz (BMG) ergibt. Nach dieser Vorschrift darf die Meldebehörde einer anderen öffentlichen Stelle aus dem Melderegister bestimmte Daten, u. a. Namen und Anschriften, übermitteln, soweit dies zur Erfüllung der in der Zuständigkeit des Empfängers liegenden öffentlichen Aufgaben erforderlich ist.

Es kann hier dahinstehen, ob es sich bei einem Seniorenbeirat um eine eigenständige öffentliche Stelle oder um einen Teil der Kommune als öffentliche Stelle handelt. In jedem Fall ist nicht ersichtlich, dass es für den Seniorenbeirat erforderlich ist, die Adressdaten aller über 59-jährigen Einwohner der Gemeinde zu erhalten, um seine gesetzlichen und satzungsmäßigen Aufgaben auszuführen. Nach einer typischen Formulierung in der Satzung über die Bildung eines Seniorenbeirats bestehen die Aufgaben des Beirats vor allem in der Vertretung der Interessen der Senioren und in ihrer Beratung. Aus welchem Grund dazu eine partielle Kopie des Melderegisters erforderlich ist, ist nicht ersichtlich.

Dabei ist weiter zu beachten, dass die einschlägigen Satzungen es den Verwaltungen der Kommunen regelhaft erlauben, Daten aus dem Melderegister zu nutzen, um die Wahl des Seniorenbeirats durchzuführen (dies gilt jedenfalls, wenn der Seniorenbeirat von den über 59-jährigen Einwohnern direkt gewählt wird). Im Rahmen der Durchführung der Wahl werden alle über 59-Jährigen über das Bestehen eines Seniorenbeirats und dessen Aufgaben informiert. Besteht dann seitens der Senioren Interesse an Beratung usw., können sie sich mit dem Beirat in Verbindung setzen.

Zu dem gleichen Ergebnis kommt man, wenn man das Ansinnen auf Mitteilung der Adressdaten aller über 59-jährigen Einwohner als Antrag auf eine sogenannte Gruppenauskunft über eine Vielzahl nicht namentlich bezeichneter Personen nach § 46 BMG ansieht. Voraussetzung für die Zulässigkeit einer Gruppenauskunft ist das Vorliegen eines öffentlichen Interesses. Gemeint ist damit ein Interesse der Allgemeinheit, das eine deutlich höhere Schwelle darstellt als ein berechtigtes oder rechtliches Interesse. Aus den oben genannten Gründen kann hier auch nicht vom Vorliegen eines öffentlichen Interesses ausgegangen werden.

Datenschutzrechtlich wäre es dagegen unproblematisch, wenn das Meldeamt nur bestimmte statistische Daten über die Zusammensetzung der Gruppe der Senioren übermittelt, solange daraus nicht Rückschlüsse auf einzelne Personen möglich sind.

Jubiläum

Jubiläum im Sinne des Gesetzes sind der 70. Geburtstag, jeder fünfte weitere Geburtstag und ab dem 100. Geburtstag jeder folgende Geburtstag. Ehejubiläen sind das 50. und jedes folgende Ehejubiläum.

Eine weitere häufiger gestellte Frage betrifft die Mitteilung von Alters- oder Ehejubiläen der Einwohner. Nach § 50 Abs. 2 BMG darf die Meldebehörde auf Anfrage von Mandatsträgern, Presse oder Rundfunk Auskunft über Familiennamen, Vornamen, Doktorgrad, Anschrift sowie Datum und Art des Jubiläums erteilen. Dies gilt nicht, wenn der Betroffene gegen diese Art der Auskunft Widerspruch eingelegt hat.

Im Hinblick auf den Seniorenbeirat stellt sich die Frage, ob dessen Mitglieder auch als Mandatsträger im Sinne der Vorschrift anzusehen sind. Allgemein ist Mandatsträger jeder, der in ein Amt gewählt wird und im Rahmen des Aufgabenbereiches aktiv ist, für den er gewählt wurde. Die §§ 47d, 47e GO in Verbindung mit der jeweiligen Satzung legen das Wahlverfahren für die Mitglieder des Seniorenbeirats und dessen Aufgaben fest. Für die Mitglieder des Seniorenbeirates gilt daher, dass sie zum einen in ein Amt gewählt werden und dass sie zum anderen in einem Aufgabenbereich aktiv werden, für den sie gewählt worden sind. Damit handelt es sich bei den Mitgliedern des Seniorenbeirates um Mandatsträger im Sinne von § 50 Abs. 2 Satz 1 BMG. Daher dürfen auch die Mitglieder des Seniorenbeirates Daten über Jubiläen der Einwohner von der Meldebehörde verlangen, und die Meldebehörde muss diese mitteilen, soweit keine Widersprüche der betroffenen Personen nach § 50 Abs. 5 BMG vorliegen.

Entsprechendes gilt auch für die Mitglieder von Ortsbeiräten nach den §§ 47b, 47c GO, die in den Gemeinden teilweise auch Dorfvorstand genannt werden.

Das ULD hat weitere Informationen zu Widerspruchsmöglichkeiten in Bezug auf die Weitergabe der eigenen Meldedaten zusammengestellt:

https://www.datenschutzzentrum.de/uploads/informationsmaterial/melderecht-2017.pdf

4.1.8 Erteilung von Gruppenauskünften nach § 46 Bundesmeldegesetz an Stadtwerke, Breitbandausbau im öffentlichen Interesse

Im Zusammenhang mit Werbeveranstaltungen und Informationsschreiben zur Förderung des Breitbandausbaus erreichten das ULD mehrere Anfragen zur Zulässigkeit der Übermittlung von Adressdaten zu diesen Zwecken. In einem Fall beantragten Mitarbeiter der Stadtwerke die Adressdaten von Anwohnern einer bestimmten Region bei einem Einwohnermeldeamt. Die Anfrage wurde als sogenannte Gruppenauskunft gemäß § 46 Bundesmeldegesetz (BMG) formuliert. Danach dürfen u. a. Anschriften und Geburtsdaten zur Bestimmung einer Gruppe von Personen genutzt werden, deren Daten (wie Name und Anschrift) dann von den Meldebehörden an andere Stellen mitgeteilt werden können. Erforderlich ist hierfür das Vorliegen eines öffentlichen Interesses.

Der Rechtsbegriff „öffentliches Interesse" ist unbestimmt und bedarf der Auslegung. Dabei sind im Rahmen einer Interessenabwägung die Rechte der betroffenen Personen mit denen der Allgemeinheit abzuwägen. Die Förderung des Breitbandausbaus gehört aktuell zu den Spitzenthemen der Europa-, Bundes- und Landespolitik. Im Zentrum steht dabei der gesellschaftliche Nutzen aus der Schaffung gleichwertiger Lebensbedingungen und wirtschaftlicher Wettbewerbsfähigkeit auch in ländlichen Regionen, wobei Ausbau und Finanzierung maßgeblich durch die in den Märkten agierenden Netzbetreiber (zu denen auch die Stadtwerke gehören können) erfolgen sollen. Insofern hält das ULD es für vertretbar, den Breitbandausbau dem allgemeinen Interesse zuzuschreiben.

Da im vorliegenden Fall die Übermittlung der Adressdaten für die Informationsschreiben verschlüsselt erfolgte sowie ausdrücklich an die im Schreiben der Behörde benannten Auflagen geknüpft war und die Löschung zum Zeitpunkt der Überprüfung bestätigt wurde, konnte die Interessenabwägung hier zugunsten der Allgemeinheit entschieden und das öffentliche Interesse für die Durchführung einer Gruppenauskunft im Sinne von § 46 BMG bejaht werden.

Was ist zu tun?

Meldebehörden sollten weiterhin kritisch prüfen, ob die Weitergabe insbesondere von großen Teilen der Meldedaten an andere öffentliche Stellen oder im Wege der Gruppenauskunft zulässig ist.

4.1.9 Einsatz elektronischer Wasserzähler mit Funkauslesung

Im Berichtszeitraum erhielt das ULD mehrere Anfragen und Eingaben, die den Einbau von elektronischen Wasserzählern mit Funkauslesung betrafen. Das ULD hatte Gelegenheit, sich bei einem Wasserverband einen gängigen Typen eines elektronischen Wasserzählers vorführen und erläutern zu lassen. Die vorgeführten Zähler messen den Wasserdurchfluss nicht mehr mechanisch, sondern per Ultraschall. Gemessen wird standardmäßig nicht nur die Menge des durchfließenden Wassers, sondern auch die Temperatur des Wassers und der Umgebung des Zählers (das kann bei Problemen mit der Wasserqualität von Bedeutung sein). Außerdem werden bestimmte betriebswidrige Zustände über Fehlercodes aufgezeichnet. Zu diesen gehören der kontinuierliche Abfluss größerer Mengen von Wasser (Hinweis auf ein Leck im System), Wasserfluss in der verkehrten Richtung (manche Anwender versuchen den Zähler zu überlisten, indem sie ihn falsch herum einbauen) und das gänzliche Fehlen von Wasser (Betrugsversuch, bei dem das Wasser am Zähler vorbeigeleitet wird). Diese Daten werden in einem Speicher in dem Zähler hinterlegt. Sie können mit einem speziellen Lesegerät ausgelesen werden, das dazu mit dem Zähler unmittelbar in Berührung gebracht oder dicht herangehalten werden muss. Zusätzlich verfügen die Zähler über ein Sendemodul. Über dieses wird etwa alle 16 Sekunden für die Dauer von 0,01 Sekunden ein Satz von Daten versendet, der die Zählernummer, den Zählerstand, die Fehlercodes der letzten vier Wochen, die Temperatur (Wasser und Umgebung) sowie den Zählerstand am letzten Tag des Vormonats enthält. Die ausgesendeten Informationen werden mit einem asymmetrischen Verfahren verschlüsselt, wobei jeder Zähler einen eigenen Schlüssel hat. Die Reichweite des Funksignals beträgt bis zu einem Kilometer, kann aber deutlich darunterliegen, wenn der Zähler z. B. hinter Betonmauern eingebaut ist. Dann wird gegebenenfalls eine Außenantenne montiert.

Laut Hersteller des Gerätes ermöglicht die Technik eine tägliche Ablesung des Wasserverbrauchs und etwaiger Fehler über eine fest installierte Antenne in der Nähe. Damit könnten Anwender dann beispielsweise darauf aufmerksam gemacht werden, dass bei ihnen ein dauerhaft hoher Verbrauch stattfindet, z. B. wenn die Bewässerung im Garten ein Leck hat. Der Wasserverband, der die Zähler nutzen wollte, plante allerdings, die Auslesung der Zähler lediglich einmal im Jahr vorzunehmen. Dazu soll ein mit einem Empfangsgerät und einem Laptop ausgestattetes Fahrzeug durch das Versorgungsgebiet fahren und die Meldungen automatisch entgegennehmen.

Insgesamt ist festzuhalten, dass diese Art von Wasserzähler zwar elektronisch misst, aber nicht wirklich „intelligent" genannt werden kann. Der Aussagewert des Wasserverbrauchs dürfte auch weit unter dem von elektronischen Stromzählern (Smart Meter) gespeicherten Daten liegen, aus denen sich personenbezogene Informationen über bestimmte Verhaltensweisen der Nutzer ergeben können. Allerdings kommt es auch bei den elektronischen Wasserzählern zur Aufzeichnung von Daten, deren Erforderlichkeit nicht ohne Weiteres erkennbar ist. So wird insbesondere die Umgebungstemperatur (d. h. in der Regel die Temperatur im Keller des Hauses) regelmäßig für die Abrechnung des Wasserverbrauchs keine Rolle spielen.

Der Wasserverband verbaut Wasserzähler pro Versorgungseinheit, d. h. in der Regel ein Zähler pro Haus. Datenschutzrechtlich folgt daraus, dass es sich bei den aufgezeichneten Daten jedenfalls bei Einfamilienhäusern um personenbezogene Daten der Hausbewohner handelt. Für den oben erwähnten „intelligenten" Stromzähler hat der Bundesgesetzgeber im Zusammenhang mit dem Erlass des Erneuerbare-Energien-Gesetzes das Messstellenbetriebsgesetz erlassen, das eine detaillierte Regelung zu Datenschutz und Datensicherheit für jene Zähler enthält. Anders sieht es jedoch im Hinblick auf die elektronischen Wasserzähler mit Funkauslesung aus. Hier fehlt es weitgehend an einer gesetzlichen Regelung. Die einzige einschlägige Vorschrift findet sich in § 18 Abs. 1 Satz 1 der Verordnung über Allgemeine Bedingungen für die Versorgung mit Wasser (AVBWasserV). Dort heißt es: „Das Wasserversorgungsunternehmen stellt die vom Kunden verbrauchte Wassermenge durch Messeinrichtungen fest, die den eich-

rechtlichen Vorschriften entsprechen müssen." Diese Vorschrift lässt sich als Befugnis zur Verarbeitung personenbezogener Daten verstehen, aber eben nur im Hinblick auf die verbrauchte Wassermenge. Für die weiteren Daten, insbesondere die Aufzeichnung der Fehlercodes und der Temperatur sowie für die Übertragung der Daten durch Funksignal, fehlt es an einer Rechtsgrundlage. Eine kommunale Satzung wäre im Hinblick auf den bei Grundrechtseingriffen relevanten Gesetzesvorbehalt („Wesentlichkeitstheorie") nicht ausreichend, da keine vom Parlament verabschiedete gesetzliche Vorschrift den Erlass einer solchen Satzung zulässt.

In Anlehnung an eine Empfehlung des Bayerischen Landesbeauftragten für den Datenschutz sieht es das ULD in dieser Situation für hinnehmbar an, wenn 1. für eine Übergangszeit der Einsatz des elektronischen Funkwasserzählers seine Grundlage in einer Satzung der Kommune bzw. des Verbandes findet und 2. die Betroffenen die Möglichkeit haben, ohne Begründung gegen den Einbau eines Funkwasserzählers Widerspruch einzulegen (Opt-Out-Lösung). Der Widerspruch kann sich dabei gegen die Verwendung des Funkmoduls und/oder gegen die Speicherung weiterer Daten als des bloßen Wasserverbrauchs richten. In diesem Fall sind die entsprechenden Funktionen abzuschalten. Das ULD hat sich davon überzeugt, dass dies jedenfalls für den in Augenschein genommenen Zählertyp möglich ist. Der Wasserversorger hat über die Möglichkeit des Widerspruchs zu unterrichten. Allerdings kann der Betroffene nicht verlangen, dass ein herkömmlicher mechanischer Wasserzähler anstatt des elektronischen verbaut wird. Da die oben genannte Vorschrift technikoffen formuliert ist, können die Wasserversorgungsunternehmen bestimmen, mit welcher Technik der Wasserverbrauch gemessen wird.

Darüber hinaus hält es das ULD in jedem Fall für unzulässig, die Temperaturdaten in den Satz der bei der jährlichen Ablesungsfahrt erhobenen Daten aufzunehmen. Zwar kann die Wasser- und Umgebungstemperatur bei bestimmten Ereignissen von Bedeutung sein, z. B. um bei höheren Temperaturen die dann ansteigende Keimbelastung des Wassers nachvollziehen zu können. Daher werden die Temperaturwerte für bestimmte Zeiträume im Speicher des Zählers abgelegt (wenn kein allgemeiner Widerspruch eingelegt wurde, siehe oben). Dort können die Werte nur mit Zutun des Wasserkunden abgerufen werden. Für die einmal im Jahr zu Abrechnungszwecken erhobenen Verbräuche spielen die Temperaturen allerdings keine Rolle, sodass eine Erhebung in diesem Zusammenhang ausscheidet.

Die vom ULD kontaktierten Wasserversorger haben zugesagt, sich an die oben dargelegten Maßgaben beim Einbau elektronischer Wasserzähler zu halten.

Was ist zu tun?

Die Wasserversorger dürfen elektronische Funkwasserzähler nur einsetzen, wenn dies auf Basis einer rechtlichen Grundlage geschieht. Solange eine nationale gesetzliche Regelung fehlt, kann es für eine Übergangszeit hingenommen werden, wenn dies in einer Satzung der Kommune bzw. des Wasserverbandes geregelt ist und außerdem die Betroffenen dem Einbau und Betrieb eines Funkwasserzählers widersprechen können. Notwendig ist stets eine ausreichende Transparenz über die Datenverarbeitung.

4.1.10 Hundekennzeichnung mit Namen und Adresse der Hundehalter

Im Berichtszeitraum kam es zu Irritationen bei Hundehaltern in einer großen Stadt im Süden des Landes. Hunde wurden im öffentlichen Raum von den Mitarbeitern des Ordnungsamtes nicht nur daraufhin kontrolliert, ob durch eine Steuermarke die ordnungsgemäße Anmeldung zur Hundesteuer nachgewiesen werden konnte. Es wurde auch verlangt, dass der Name und die vollständige Anschrift der Halter deutlich sichtbar an der „Anleinvorrichtung" anzubringen sei. Dies war offenbar bei keinem der kontrollierten Hunde der Fall. Für den Fall eines erneuten Verstoßes wurde die Verhängung eines Bußgeldes angedroht.

Einige irritierte Hundehalter und -halterinnen wandten sich an das ULD. Sie machten vor allem geltend, dass eine so weitgehende Pflicht zur öffentlichen Präsentation ihres Namens und ihrer Anschriften ihre Datenschutzrechte verletze. Insbesondere wenn jemand schon einmal Opfer von Stalking gewesen sei, könne es dadurch zu akuten Gefährdungen kommen.

Die Aktivitäten der Ordnungsbehörde gingen auf das neue Hundegesetz des Landes zurück, das am 1. Januar 2016 in Kraft getreten war. Es ersetzte das frühere Gefahrhundegesetz. Wurden nach jenem noch bestimmte Hunderassen zu Gefahrhunden erklärt, so kann nach dem neuen Gesetz jeder Hund – unabhängig von der Rasse – zu einem „gefährlichen Hund" werden, wenn er sich entsprechend verhält, z. B. einen Menschen beißt. Relativ unbemerkt von der Öffentlichkeit hat dieses Gesetz aber auch weitere Pflichten für die Hundehalter mit sich gebracht. So ist ein Hund, der älter als drei Monate ist, nach § 5 Hundegesetz durch ein elektronisches Kennzeichen (Transponder) mit einer Kennnummer zu kennzeichnen (sogenannter Tasso-Chip). Mittels eines Lesegeräts lässt sich eine Nummer von dem Transponder abfragen. Ist der Hund bei einem entsprechenden Anbieter registriert, kann z. B. bei einem zugelaufenen Hund der Halter festgestellt werden.

Weiterhin hat nach § 3 Abs. 5 des neuen Hundegesetzes derjenige, der einen Hund „außerhalb eines ausbruchsicheren Grundstücks führt oder laufen lässt, (…) diesem ein Halsband, eine Halskette oder eine vergleichbare Anleinvorrichtung mit einer Kennzeichnung anzulegen, aufgrund derer die Hundehalterin oder der Hundehalter ermittelt werden kann". Die Stadt hatte diese Vorschrift – nach Konsultation mit dem zuständigen Innenministerium – so ausgelegt, dass Name und Anschrift des Halters gut lesbar am Hund angebracht sein müssten. Dagegen würde z. B. die in das Halsband eingestickte Handynummer, auf die sich eine Halterin berief, nicht ausreichen.

Das ULD wandte sich an die Stadt und fragte nach, worauf die dortige Auslegung des Gesetzes gestützt werde. Der Wortlaut (Kennzeichnung, aufgrund derer die Hundehalterin oder der Hundehalter ermittelt werden kann) spricht jedenfalls nicht von öffentlicher, für jeden lesbarer Präsentation von Namen und Adresse. Auf Nachfrage räumte die Stadt dann ein, dass es ausreiche, wenn die Daten sich z. B. in einem verschraubten Adressanhänger an der Anleinvorrichtung befinden.

Angesichts dieser Unklarheiten stellt sich die Frage nach dem Sinn und Zweck der Vorschrift. Soll es darum gehen, einer von einem Hund gebissenen Person schnell Informationen über den schadensersatzpflichtigen Halter zur verschaffen? In diesem Fall würde nur der gut sichtbare Name mit Anschrift dem Geschädigten nutzen, was aber zu unzumutbaren Einschränkungen der Rechte der Halter führt. Die nach der jetzigen Auslegung eingeschränkte Pflicht, zwar den Namen und die Adresse am Hund zu befestigen, dies aber in nicht leicht ablesbarer Form, bringt jedenfalls keinen erkennbaren Nutzen. Es kann wohl kaum erwartet werden, dass eine gerade von einem Hund gebissene Person diesem an die Anleinvorrichtung fasst, um den verschraubten Adressanhänger zu öffnen. Sollte es nur um die Identifizierung des Halters für den Fall gehen, dass der Hund abhandenkommt, so kann die Zuordnung über den Transponder hergestellt werden, der auch verpflichtend ist.

Einen Nebeneffekt hatte das ordnungsgemäße „Chippen" eines Hundes nach § 5 Hundegesetz

für eine Hundehalterin in derselben Stadt. Sie wollte ihren Hund zur Hundesteuer anmelden. Dabei informierte sie die Stadt auch über die Transpondernummer des Hundes. Die Stadt vermutete, dass der Hund schon länger von der Betroffenen gehalten wurde. Um dies herauszufinden, wandte sich die Stadt an das Tasso-Register und fragte nach, ab wann der Hund mit der Transpondernummer bei dem Register gemeldet war. Das Tasso-Register gab der Stadt die gewünschte Auskunft. Dies führte zu einer Nacherhebung der Hundesteuer für sieben Jahre in einer vierstelligen Größenordnung. Die Nachprüfung durch das ULD ergab, dass die Stadt diese Information rechtmäßig vom Tasso-Register erheben durfte. Nach § 93 Abgabenordnung haben auch andere als die Steuerpflichtigen der Finanzbehörde die zur Feststellung eines für die Besteuerung erheblichen Sachverhalts erforderlichen Auskünfte zu erteilen. Die Vorschrift gilt auch bei der Erhebung von kommunalen Steuern nach dem Kommunalabgabengesetz.

Was ist zu tun?

Der Gesetzgeber sollte prüfen, ob die Pflicht nach § 3 Abs. 5 des Hundegesetzes erforderlich ist.

4.1.11 Freizeitfischerei und Datenschutz

Anfang des Jahres 2018 hatte das Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung (MELUND) den beteiligten Verbänden einen Gesetzentwurf zur Änderung des Landesfischereigesetzes zugeleitet.

Der Gesetzentwurf sah vor, zur besseren Kontrolle der Tagesfangbeschränkungen in der Freizeitfischerei ein neues Kontrollrecht in § 44 Abs. 1 Satz 1 des Landesfischereigesetzes einzuführen. Den Fischereiaufsichtspersonen sollte die Befugnis gewährt werden, den Fahrtverlauf von Wasserfahrzeugen zu kontrollieren. Dazu sollte die Schiffsführung auf Verlangen den Fahrtverlauf belegen und dabei auch notwendigen Einblick in elektronische Aufzeichnungen wie beispielsweise Seekartenplotter gewähren. Das ULD wies in seiner Stellungnahme gegenüber dem MELUND darauf hin, dass dieses Gesetzesvorhaben auf datenschutzrechtliche Bedenken stieß.

Ausweislich der Gesetzesbegründung zielte die Änderung vor allem darauf ab, den Fischereiaufsichtspersonen Zugang zu den „in der gewerblichen Schifffahrt inzwischen verwendeten und teilweise vorgeschriebenen elektronischen Navigations- und Aufzeichnungsgeräten" zu ermöglichen. Dies sei insbesondere für die Kontrolle auf Angelkuttern wichtig. Mithin zielte die neue Kontrollbefugnis in erster Linie auf gewerbliche Aktivitäten ab.

Der Gesetzeswortlaut selbst ließ diese Begrenzung jedoch nicht erkennen. Vielmehr erfasst der Begriff „Wasserfahrzeuge" jede Art von Booten, inklusive kleiner Sportboote, auf denen Privatpersonen der Freizeitfischerei nachgehen. Der Wortlaut der Vorschrift des Gesetzentwurfs hätte es den Fischereiaufsichtspersonen erlaubt, auch von Schiffsführern solcher kleinen Sportboote den Nachweis des Fahrtverlaufes zu verlangen. Erfahrungsgemäß führen solche Sportboote jedoch keine Seekartenplotter oder ähnliche Geräte mit. Dagegen ist es nicht ausgeschlossen und inzwischen sogar eher wahrscheinlich, dass diese Schiffsführer den Fahrtverlauf z. B. über entsprechende Anwendungen auf ihrem privaten Smartphone oder Tablet-Computer aufzeichnen. Die Vorschrift hätte es ihrem Wortlaut nach erlaubt, dass die Fischereiaufsichtsperson die Schiffsführer zur Vorlage ihres privaten Smartphones auffordert und dann versucht, in einer entsprechenden App den Fahrtverlauf nachzuvollziehen.

Bei den auf einem privaten Smartphone oder Tablet-Computer aufgezeichneten Daten über die Fahrtroute handelt es sich um personenbezogene Daten des betroffenen Besitzers des Gerätes. Das Gleiche gilt bei der Verwendung eines Kartenplotters auf einem Sportboot, das einer natürlichen Person gehört. Gerade bei Anwendungen auf mobilen Endgeräten muss davon ausgegangen werden, dass nicht nur die zu überprüfenden Fahrtverläufe gespeichert sind und bei einer Kontrolle erkennbar werden, sondern auch weitere darüber hinausgehende Daten, die der privaten Lebensführung der Betroffenen zuzurechnen sind.

Daher hätte die ursprünglich vorgeschlagene Formulierung zur Änderung des Landesfischereigesetzes einen unverhältnismäßigen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen mit sich gebracht. Das ULD hatte dem MELUND daher dringend empfohlen, bereits im Wortlaut deutlich zu machen, dass lediglich eine Kontrolle von gewerblichen Aktivitäten beabsichtigt war. Vorgeschlagen wurde z. B. eine Klarstellung, dass mit dem Begriff „Wasserfahrzeuge“ in der neu geschaffenen Vorschrift nicht Sportboote im Sinne von § 2 Nr. 3 der Sportbootführerscheinverordnung vom 3. Mai 2017 gemeint sind. Von dem Anwendungsbereich wären damit „nicht gewerbsmäßig, für Sport- und Erholungszwecke verwendete Fahrzeuge“ ausgeschlossen.

In der im April dem Landtag zugeleiteten Fassung des Gesetzentwurfs (Drucksache 19/677) verzichtete das MELUND gänzlich auf die ursprünglich angedachte neue Befugnis, den Fahrtverlauf von Wasserfahrzeugen zu kontrollieren. In dieser „entschärften“ Fassung traten die Änderungen schließlich am 30. November 2018 in Kraft.

Was ist zu tun?

Alle Ressorts sollten bei der Gesetzgebung frühzeitig die Landesbeauftragte für Datenschutz mit ihrer Dienststelle einbeziehen, wenn die Vorhaben Auswirkungen auf das Grundrecht auf Datenschutz haben können. So lässt sich schon zu einem frühen Zeitpunkt in der Regel eine effektive und datenschutzkonforme Lösung finden.

4.1.12 Mobile Endgeräte und Ratsinformationssysteme für Kommunalpolitiker

Auch in der Kommunalpolitik hält die Digitalisierung Einzug. Erhielten die kommunalen Mandatsträger in der Vergangenheit ihre Sitzungsunterlagen in Papierform, so werden heute in vielen Kommunen elektronische Lösungen verwendet. Diese reichen von Ratsinformationssystemen über die Ausstattung der Mandatsträger mit Tablet-Computern, die teilweise von der Kommune beschafft werden.

Zu den damit einhergehenden Anforderungen an den Datenschutz erreichten das ULD im Berichtszeitraum zahlreiche Fragen. Das ULD hatte bereits im Jahr 2015 eine Ausarbeitung über die Verwendung von Tablets durch Gemeindevertreter online gestellt. Die dortigen Aussagen behalten Gültigkeit, allerdings ist zu beachten, dass anstelle der Vorschriften des alten Landesdatenschutzgesetzes und der mittlerweile aufgehobenen Datenschutzverordnung des Landes die Vorgaben der Datenschutz-Grundverordnung getreten sind:

https://www.datenschutzzentrum.de/artikel/913-.html

Im März 2018 hat das ULD die obigen Ausführungen durch eine neue Veröffentlichung zu Ratsinformationssystemen und mobiler Datenverarbeitung durch kommunale Mandatsträge-

rinnen und Mandatsträger ergänzt, die sich bereits auf die Vorschriften der DSGVO bezieht:

https://www.datenschutzzentrum.de/uploads/it/2018-03-13-Ratsinformationssysteme.pdf

Was ist zu tun?

Beim Einsatz von Ratsinformationssystemen und der Verwendung von mobilen Datenverarbeitungsgeräten für kommunale Mandatsträger sollten die Hinweise des ULD beachtet werden.

4.1.13 Reichsbürgererlass

Das Innenministerium hat im Berichtszeitraum durch Erlass umfangreiche Meldungen von Reichsbürgern angeordnet. Der Erlass schreibt den Melde-, Pass- und Personalausweisbehörden der Kommunen vor, Vorfälle mit sogenannten Reichsbürgern aufzuzeichnen und an die örtliche Polizeidienststelle sowie an das Innenministerium weiterzugeben. Damit soll vor allem eine Entscheidungsgrundlage für die Zuverlässigkeitsüberprüfung bei waffenrechtlichen Entscheidungen geschaffen werden. Für solche Überprüfungen fragt regelmäßig die Waffenbehörde bei der Polizei nach Erkenntnissen. Durch den Erlass soll sichergestellt werden, dass die Polizei über die notwendigen Erkenntnisse verfügt.

So verständlich das Ziel vor dem Hintergrund der tödlichen Schüsse auf einen Polizeibeamten in Bayern im Jahr 2016 auch sein mag: Der Erlass wirft mehr Fragen auf, als er Antworten gibt. Dies beginnt schon mit der Einschätzung, ob eine Person als Reichsbürger anzusehen ist. Diese Entscheidung wird den Kommunen überlassen. Ausreichend klare Bewertungskriterien benennt der Erlass nicht. Noch weniger klar ist, welche Vorfälle zu melden sind. Der Erlass zählt zwar einige Beispiele auf, doch diese bleiben exemplarisch. Eine abstrakte Beschreibung der Ereignisse, die meldepflichtig sind, fehlt.

Der im Erlass beschriebene Informationsaustausch zwischen Melde- und Passbehörden, Waffenbehörden, Polizei und dem Innenministerium funktioniert nur, wenn er durch eine eigene Datenverarbeitung bei allen Stellen flankiert wird. Hierzu trifft der Erlass keine eigenen Regelungen, sondern setzt eine entsprechende Organisation der Datenverarbeitung voraus.

Dies führt zu Fragen, die bis heute nicht in allen Stellen vollständig geklärt sind – z. B.: Wie und wo werden die Informationen bei der übermittelnden Stelle erfasst und für die Meldung zusammengetragen? Dürfen oder müssen sie sogar bei der übermittelnden Stelle gespeichert werden? Wenn ja, wie lange? Dürfen diese Daten dann auch für eigene Informationszwecke der übermittelnden Stelle verwendet werden? Wie werden die Daten bei den Empfängern weiterverarbeitet? Wird dort eine eigene Relevanzprüfung vorgenommen? Wenn ja, werden die übermittelnde Stelle und die anderen Empfänger über das Ergebnis informiert? Wie lange und für welche Zwecke werden die Daten bei den Empfängern gespeichert? Wie wird die Transparenz für die betroffenen Personen sichergestellt? Wer informiert die betroffenen Personen worüber?

Das ULD erreichen hierzu immer wieder Fragen von Verantwortlichen. Durch unsere Beratung konnten einzelne Fragen für einzelne Verantwortliche gelöst werden. Für eine vollständige Klärung aller Fragen ist ein Gesamtkonzept erforderlich, das von den Verantwortlichen erstellt werden muss. Sinnvoll wäre hierfür ein Zusammenwirken aller beteiligten Bereiche unter Koordinierung des Innenministeriums.

Was ist zu tun?

Der Reichsbürgererlass wirft viele Fragen auf, ohne sie selbst zu regeln. Dies betrifft die Datenverarbeitung sowohl bei den übermittelnden Stellen als auch bei den Empfängern. Die betroffenen Verantwortlichen – Innenministerium, Kommunen, Polizei – müssen diese Fragen klären und für ihre Datenverarbeitung Festlegungen treffen.

4.2 Polizei und Verfassungsschutz

4.2.1 Gesetzliche Pflichtprüfungen

Die Verarbeitung von personenbezogenen Daten durch die Polizei und die Verfassungsschutzbehörde ist für die betroffenen Personen häufig nicht oder nicht vollständig transparent. Bei verdeckten Maßnahmen liegt dies in der Natur der Sache. Doch auch bei Strafverfahren oder anderen Vorgängen, die den betroffenen Personen bekannt sind, haben diese meist keine Kenntnis darüber, wie lange die Daten gespeichert werden und – vor allem – in welchen Informationssystemen fortan welche Informationen über sie gespeichert werden. Als Kompensation für diese Intransparenz kommt der Kontrolle durch die Datenschutzaufsichtsbehörde eine wichtige Rolle zu. Dies hat das Bundesverfassungsgericht in seinem Urteil zum Antiterrordateigesetz deutlich hervorgehoben. Aus diesem Grund wurden in den letzten Jahren in zahlreichen nationalen und EU-Gesetzen Prüfpflichten für die Datenschutzaufsichtsbehörden aufgenommen. So verpflichtet beispielsweise das nach der Entscheidung des Bundesverfassungsgerichts geänderte Antiterrordateigesetz die Datenschutzaufsichtsbehörde, die Datei mindestens alle zwei Jahre zu prüfen.

Die EU-Vorschriften über das Schengener Informationssystem (SIS II), das Visainformationssystem (VIS), Eurodac, das neu eingeführte Entry-Exit-System (EES) sowie das neue Reiseinformations- und -genehmigungssystem (ETIAS) sehen ebenfalls regelmäßige Pflichtprüfungen durch die Datenschutzaufsichtsbehörden der Mitgliedstaaten vor. Da die Daten in diesen Informationssystemen hauptsächlich von den Behörden der Länder stammen, sind insoweit die Aufsichtsbehörden der Länder verpflichtet, die Richtigkeit der Daten und die Zulässigkeit ihrer Speicherung zu prüfen.

Im Berichtszeitraum wurden das Bundeskriminalamtgesetz und die Polizeigesetze einiger Länder geändert. Dort wurde eine Pflicht der Datenschutzaufsichtsbehörde eingeführt, Speicherungen in polizeilichen Informationssystemen und Zugriffe auf solche Systeme sowie bestimmte verdeckte Ermittlungsmaßnahmen mindestens alle zwei Jahre zu prüfen.

Die vom ULD durchgeführten anlasslosen Kontrollen (Tz. 4.2.5 und Tz. 4.2.6) bestätigen die Notwendigkeit solcher Kontrollen. Gleichwohl sind sie zeitaufwendig und setzen eine angemessene Personalausstattung voraus, damit andere gesetzliche Pflichten, wie etwa Kontrollen aufgrund von individuellen Beschwerden betroffener Personen, ebenso erfüllt werden können. Zudem dürfen gesetzliche Prüfpflichten nicht dazu führen, dass es der Aufsichtsbehörde nicht mehr möglich ist, Kontrollen aus eigener Initiative durchzuführen. Das ULD hat in der Vergangenheit Kontrollen häufig als Reaktion auf bestimmte Ereignisse oder auf Bitten des Landtages durchgeführt (siehe z B. 36. TB, Tz. 4 2.3: Prüfung der Datei „Fußball SH“; 35. TB, Tz. 4.3.1: Prüfung von Funkzellenabfragen). Bei der Einführung von etwaigen weiteren Prüfpflichten und bei der Personalausstattung der Dienststelle sollte darauf geachtet werden, dass solche eigeninitiierten oder anlassbezogenen Kontrollen weiterhin möglich bleiben.

Was ist zu tun?

Gesetzliche Pflichten für anlasslose Kontrollen sind ein sinnvolles Instrument zur Wahrung der Rechte der betroffenen Personen. Dies setzt jedoch voraus, dass die Aufsichtsbehörde in der Lage ist, die Pflichten zu erfüllen, ohne dabei andere Pflichten zu vernachlässigen oder der Möglichkeit eigener Schwerpunktsetzung beraubt zu werden.

4.2.2 Umsetzung der EU-Richtlinie für den Datenschutz bei der Verfolgung und Verhütung von Straftaten im Landesrecht

In den Berichtszeitraum fiel nicht nur das Wirksamwerden der Datenschutz-Grundverordnung zum 25. Mai 2018, sondern auch der Ablauf der Umsetzungsfrist der EU-Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung zum 6. Mai 2018. Erfreulich ist, dass der Landesgesetzgeber einer unserer zentralen Forderungen nachgekommen ist und im Landesdatenschutzgesetz allgemeine Regelungen zur Umsetzung der Richtlinie geschaffen hat. Somit gelten für alle Stellen, die der Richtlinie unterfallen, einheitliche allgemeine Anforderungen.

Die Vorschriften des dritten Abschnitts des Landesdatenschutzgesetzes zur Umsetzung der Richtlinie gelten für alle Stellen, die Straftaten oder Ordnungswidrigkeiten verfolgen, soweit sie für diese Zwecke personenbezogene Daten verarbeiten. Auch die Verarbeitung durch die Polizei zum Zweck der Abwehr von Gefahren für die öffentliche Sicherheit unterliegt diesen Regelungen. Zudem gilt Abschnitt 3 des Landesdatenschutzgesetzes für den Straf- und Maßregelvollzug und für Maßnahmen nach dem Jugendgerichtsgesetz.

Leider stimmen die allgemeinen Regelungen für den Bereich der Richtlinie nicht immer vollständig mit den Anforderungen aus der Datenschutz-Grundverordnung überein. Anders als der Bundesgesetzgeber hat der Landesgesetzgeber keine übergreifenden Regelungen getroffen, die für beide Bereiche anwendbar sind.

Dies hat z. B. zur Folge, dass öffentliche Stellen, die sowohl Tätigkeiten nach der Datenschutz-Grundverordnung als auch nach der Richtlinie wahrnehmen, sowohl nach den Vorschriften der Datenschutz-Grundverordnung als auch nach dem Landesdatenschutzgesetz die Pflicht zur Benennung einer oder eines Datenschutzbeauftragten haben. In dem Fall erfolgt die Benennung auf Basis des Rechtsregimes, das vorrangig anwendbar ist (Tz. 4.1.2). Achtung: Beschäftigte im Bereich der Richtlinie müssen anders als in der allgemeinen Verwaltung ausdrücklich auf das Datengeheimnis verpflichtet werden.

Andere Unterschiede zwischen der Datenschutz-Grundverordnung und dem Abschnitt 3 des Landesdatenschutzgesetzes beruhen dagegen auf abweichenden Vorgaben der EU-Richtlinie. Dies gilt z. B. für die umfangreichen Pflichten zur Protokollierung von Datenverarbeitungen. Auch im Hinblick auf die Sicherstellung der Datenqualität und der Unterscheidung von verschiedenen Rollen von Personen, z. B. Beschuldigte, Zeugen, Geschädigte, gelten besondere Anforderungen.

Neu ist im Abschnitt 3 des Landesdatenschutzgesetzes, ähnlich wie in der Datenschutz-Grundverordnung, die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung vor der Einführung neuer Verarbeitungsverfahren, die zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führen können.

Neu ist außerdem die Pflicht zur Meldung von Verletzungen des Datenschutzes an das ULD.

Verletzungen der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust oder zur Offenlegung von personenbezogenen Daten geführt haben, müssen dem ULD unverzüglich, spätestens 72 Stunden nach Bekanntwerden, gemeldet werden. Eine Ausnahme gilt nur, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Führt sie zu einem hohen Risiko, sind zusätzlich auch die betroffenen Personen selbst zu informieren.

Mit der Einführung der allgemeinen Datenschutzregelungen im Landesdatenschutzgesetz ist die Umsetzung der Richtlinie noch nicht abgeschlossen. Es steht noch die Umsetzung in den Fachgesetzen aus. Im Landesrecht sind in erster Linie das Polizeirecht und das Justizvollzugsdatenschutzgesetz zu ändern.

Was ist zu tun?

Strafverfolgungsbehörden, Ordnungswidrigkeitenbehörden und Vollzugseinrichtungen müssen die allgemeinen Datenschutzregelungen des Abschnitts 3 des Landesdatenschutzgesetzes beachten. Für die Polizei gilt dies auch dann, wenn sie zur Gefahrenabwehr tätig wird. Der Landesgesetzgeber muss Regelungen zur Umsetzung der Richtlinie im Polizeirecht und in den Vollzugsgesetzen treffen.

4.2.3 Bodycams bei der Polizei – Begleitung des Pilotversuchs

Insbesondere um Polizeibeamte effektiver vor Gewalt zu schützen, erprobt die Landespolizei seit Juni 2018 den Einsatz von Körperkameras oder neudeutsch „Bodycams“. Dazu wurden zunächst 40 Geräte angeschafft, die ein Jahr lang von Polizisten aus Kiel, Lübeck sowie von der Bereitschaftspolizei getestet werden sollen.

Die Geräte können Bild- und Tonaufnahmen anfertigen. Es gibt zwei Betriebsmodi. Neben dem permanenten Aufzeichnen kann die Kamera auch vorab in eine Art Bereitschaftsmodus versetzt werden, in dem ein 30-sekündiges „Pre-Recording“ läuft. In diesem Zustand macht die Kamera Aufnahmen, die alle 30 Sekunden überschrieben werden. Wird sie währenddessen abgeschaltet, wird dieser 30-Sekunden-Speicher gelöscht. Wechselt man während des Pre-Recordings in den „Aufnahmemodus“, werden die letzten 30 Sekunden permanent gespeichert sowie alles, was darauf folgt.

Gestützt wird der Pilotversuch auf § 184 Abs. 3 Landesverwaltungsgesetz (LVwG). Als diese Vorschrift geschaffen wurde, hatte man Bodycams als Technologie noch nicht vor Augen. Es überrascht daher nicht, dass die mit dem Einsatz verbundenen schweren Eingriffe in das Persönlichkeitsrecht betroffener Personen nicht ausreichend geregelt werden (siehe Gutachten des Wissenschaftlichen Dienstes des Landtages Schleswig-Holstein vom 21. Dezember 2016, LT-Umdruck 18/7482, sowie die Stellungnahme des ULD vom 29. April 2016, LT-Umdruck 18/6051).

Aus Sicht des ULD muss es daher erklärtes Ziel sein, die Geeignetheit dieses Einsatzmittels im Rahmen des Pilotversuchs zu erforschen. Wenn man sich für einen Einsatz über den Pilotversuch hinaus entscheidet, ist eine spezifische Rechtsgrundlage erforderlich, die den Schutz der Beamtinnen und Beamten und die Bürgerrechte ausgewogen berücksichtigt und in Einklang bringt. Vor diesem Hintergrund hat sich das ULD entschlossen, die Aufnahmen, die im Rahmen des Pilotversuches angefertigt werden, gemeinsam mit der Polizei zu sichten.

§ 184 Abs. 3 LVwG

Zum Schutz einer Polizeivollzugsbeamtin oder eines Polizeivollzugsbeamten oder eines Dritten kann die Polizei bei polizeilichen Maßnahmen nach diesem Gesetz oder anderen Rechtsvorschriften erforderlichenfalls personenbezogene Daten offen durch Bildaufnahmen und Bild- oder Tonaufzeichnungen anfertigen. Die Aufnahmen und Aufzeichnungen sind spätestens drei Tage nach dem Anfertigen zu löschen. Dies gilt nicht, wenn diese zur Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung benötigt werden.

Bis November 2018 wurden etwa 150 Videos gesichtet. Dabei sind insbesondere folgende Aspekte aufgefallen:

Präventive Schutzwirkung

Die bloße Anwesenheit einer Videokamera kann Polizeibeamte nicht vor Gewalt schützen, sondern allenfalls diese Gewalt dokumentieren. Als Instrument der Abschreckung kann eine Bodycam nur dann Wirkung entfalten, wenn sie entsprechend wahrgenommen wird. Schriftliche Hinweise auf der Uniform sowie der kleine Monitor an der Kamera tragen zur Wahrnehmung dieses Einsatzmittels bei, reichen aber alleine nicht aus. Auf einigen Aufnahmen konnte man beispielsweise sehen, dass gefilmte Personen die Kamera erst relativ spät überhaupt bemerkt haben. Um überhaupt präventiv wirken zu können, ist daher das Verhalten der einsetzenden Beamten von besonderer Bedeutung.

Da es sich um eine offene Datenerhebung bei der betroffenen Person handelt, ist es erforderlich, laut und deutlich auf den Einsatz der Bodycam hinzuweisen. Nur so kann der abschreckende Effekt der Bodycam überhaupt Wirkung entfalten. Die gesichteten Aufnahmen zeichnen diesbezüglich ein uneinheitliches Bild. Es sind deutliche Unterschiede zwischen den Aufnahmen aus Lübeck und Kiel erkennbar. In einer der Städte wird fast ausnahmslos auf die Videoaufzeichnung hingewiesen. Selbst bei tumultartigen Szenen, in denen der Bodycam-Träger selber eingreifen muss, erfolgt in der Regel ein lauter Hinweis. Auf den Aufnahmen aus der anderen Stadt fehlt dieser Hinweis relativ häufig. Teilweise nehmen die betroffenen Personen die Bodycam erst sehr spät wahr.

Stark alkoholisierte Personen scheinen generell weniger auf die Bodycam zu reagieren.

Filmen in Wohnungen

Die Polizei wird immer häufiger bei Fällen häuslicher Gewalt gerufen. Nicht selten setzt sich diese Gewalt auch nach Eintreffen der Beamten in der Wohnung fort und richtet sich auch gegen die Beamten selbst. Die Forderung, Bodycam-Aufnahmen auch in Wohnungen zuzulassen, ist deshalb immer häufiger zu hören.

Wohnungen unterliegen einem besonderen Schutz nach Artikel 13 Grundgesetz (GG). Es handelt sich um persönliche Rückzugsorte, die die Privat- und Intimsphäre von Menschen berühren. Das Erstellen von Video- und Tonaufnahmen in diesem besonders geschützten Bereich unterliegt daher hohen verfassungsrechtlichen Schranken. Ob eine mit dem Grundgesetz vereinbare und gleichzeitig praktikable Nutzung von Bodycams in Wohnungen möglich ist, ist fraglich. Die meisten Länderpolizeien verzichten daher auf den Einsatz in Wohnungen. Auch in Schleswig-Holstein ist der Einsatz von Bodycams in Wohnungen unzulässig, da es keine Rechtsgrundlage dafür gibt. Gleichwohl gab es mehrere Aufnahmen, auf denen Einsätze in Wohnungen zu sehen waren. In einem Fall gab es nicht einmal eine gefährliche Situation, sondern lediglich sehr persönliche, freundliche Gespräche, da die Polizei offenbar auf Wunsch der Bewohner vor Ort war.

Unabhängig von dem fachlichen Bedarf und der Frage, ob eine praktikable, mit dem Grundgesetz vereinbare Rechtsgrundlage für den Einsatz von Bodycams in Wohnungen geschaffen werden kann oder nicht, müssen die Beamten noch besser im Umgang mit diesem neuen Einsatzmittel geschult und sensibilisiert werden. Da es sich um Eingriffsverwaltung handelt, muss die Polizei sicherstellen, dass der unzulässige Einsatz von Bodycams in Wohnungen unterbleibt.

Länge der Aufnahmen

Häufig bewegen sich die Aufnahmen im Bereich weniger Minuten. Sie zeigen potenziell gewaltbereite Personen oder Angriffe/Widerstandshandlungen. Einzelne Aufnahmen liegen aber auch im Bereich von 45 Minuten und mehr. Entscheidend für die Länge ist natürlich die Situation im Einzelfall. Bei andauernden Widerstandshandlungen – selbst von bereits gefesselten Personen – kann eine längere Aufzeichnung gerechtfertigt sein, da die gefährliche Situation für die Beamten noch anhält.

Bei einigen Videos war allerdings auffällig, dass diese teilweise noch lange weiterliefen, obwohl die Situation sich wieder entspannt hatte. Dies kann sicherlich damit erklärt werden, dass es häufig schlicht vergessen wird, die Kamera auszuschalten. Immerhin ist das Einsatzmittel relativ neu, und die Klärung gefährlicher Situationen erfordert ein hohes Maß an Konzentration. Dabei kann die laufende Kamera schnell in Vergessenheit geraten. Dies kann durch kontinuierliches Training und Schulungen wahrscheinlich verbessert werden. Es zeigt aber auch, dass der rechtskonforme Einsatz der Bodycam den Beamten zusätzliche Aufmerksamkeit abverlangt.

Verhältnismäßigkeit des Eingriffs

Bei einigen Aufnahmen war eine gefährliche Situation nicht (mehr) erkennbar. Die Bodycam wurde offenbar prophylaktisch eingeschaltet, bevor beispielsweise einige – sich friedlich verhaltende – Personen befragt wurden.

Der Einsatz einer Bodycam stellt einen schweren Eingriff in das Persönlichkeitsrecht der Betroffenen dar. Ein verhältnismäßiger Einsatz ist daher nur möglich, wenn er auf den Schutz anderer gewichtiger Rechtsgüter beschränkt wird. Dazu zählen vor allem Leib und Leben der Polizeibeamten.

In einzelnen Fällen wurde die Bodycam-Aufnahme offensichtlich gestartet, weil der Beamte beleidigt wurde. In diesen Fällen wurde explizit darauf hingewiesen, dass Beleidigungen eine Straftat sind und man diese nun auf Video aufgezeichnet habe. Dies ist bei eingeschaltetem Pre-Recording auch nachträglich möglich (30 Sekunden in die Vergangenheit).

Das Auslösen einer Bodycam-Aufnahme, um lediglich eine Beleidigung zu dokumentieren, ist allerdings unverhältnismäßig und daher unzulässig. Eine Beleidigung ist eine Straftat, die mit bis zu einem Jahr Gefängnis oder einer Geldstrafe geahndet werden kann. Im Gegensatz dazu ist bereits die Aufzeichnung des nichtöffentlich gesprochenen Wortes eine Straftat, die für den Normalbürger mit bis zu drei Jahren Gefängnis oder einer Geldstrafe ins Gewicht fällt. Zusätzlich werden bei der Bodycam noch Filmaufnahmen gemacht, die Betroffene oft in unangenehmen oder für sie im Nachhinein peinlichen Situationen zeigen. Unbeteiligte Dritte können als „Beifang" ebenfalls von den Aufnahmen betroffen sein. Darüber hinaus hat der Bürger kein Mitspracherecht. Es handelt sich um eine Zwangsmaßnahme, die er dulden muss.

Dies macht deutlich, dass ein Bodycam-Einsatz nur infrage kommt, wenn Tatsachen die Annahme rechtfertigen, dass eine Gefahr für Leib, Leben oder gleichgewichtige Rechtsgüter besteht. Der Wunsch, eine Beleidigung zu dokumentieren, kann – für sich genommen – den Einsatz der Bodycam nicht rechtfertigen. Außerdem konnten und können Beleidigungen nach wie vor auch ohne Tonaufzeichnung zur Anzeige gebracht werden.

Der Einsatz des Pre-Recordings erhöht ebenfalls die Eingriffsintensität. Denn im Gegensatz zu einer einfachen Videokamera, die – für den Betroffenen sichtbar – entweder ein- oder ausgeschaltet ist, erlaubt das Pre-Recording dem Beamten, die Entscheidung über das permanente Aufzeichnen eines Sachverhaltes in die Zukunft zu verlegen. Einige Landesgesetzgeber haben sich daher bewusst gegen das Pre-Recording entschieden.

Pre-Recording kann in bestimmten Situationen jedoch auch als milderes Mittel gegenüber der permanenten Aufzeichnung angesehen werden. Wie bereits ausgeführt, ist der Einsatz der Bodycam nur zum Schutz gewichtiger Rechtsgüter zulässig. Das Pre-Recording gibt dem Beamten mehr Zeit, die Situation richtig einzuschätzen. Wirkt jemand sehr aufgebracht, beruhigt sich nach Ansprache jedoch schnell, kann der Beamte sich dank des Pre-Recordings entscheiden, keine permanente Aufzeichnung auszulösen. Genauso kann eine bereits laufende

Aufnahme schneller beendet und in den Pre-Recording-Modus zurückgewechselt werden, wenn eine Situation beispielsweise unter Kontrolle zu sein scheint. Kommt es danach doch noch zu weiteren Widerstandshandlungen, kann dies dank des Pre-Recordings wiederum dokumentiert werden, indem die Aufnahme erneut ausgelöst wird. So könnte auch die Länge permanenter Aufnahmen auf das erforderliche Maß reduziert werden.

Entscheidend ist natürlich, dass die Beamten sich ihrer Verantwortung sowie des Spielraums, den das Pre-Recording ihnen bietet, bewusst sind und diesen Spielraum auch aktiv nutzen.

Rechtsschutz

Die Regelung in § 184 Abs. 3 LVwG, auf die der Bodycam-Pilotversuch gestützt wird, sieht vor, dass Aufnahmen spätestens drei Tage nach Anfertigung zu löschen sind, wenn sie nicht für die Verfolgung von Straftaten und Ordnungswidrigkeiten von erheblicher Bedeutung weiter benötigt werden.

Dies steht im Widerspruch zum Gebot des effektiven Rechtsschutzes aus Artikel 19 Abs. 4 GG. Betroffene Personen können in dieser kurzen Frist keinen effektiven Rechtsschutz erlangen. Auch ihre datenschutzrechtlichen Auskunftsrechte laufen dadurch ins Leere. Eine unabhängige datenschutzrechtliche Kontrolle durch die Datenschutzaufsichtsbehörde ist unter diesen Umständen ebenfalls nicht möglich.

Zusammenfassung

Die Sichtung der Bodycam-Aufnahmen hat bis jetzt gezeigt, dass die Bodycam ein Einsatzmittel ist, dass zwar technisch relativ simpel zu bedienen ist, jedoch dem einsetzenden Beamten einiges abverlangt. Die richtige Einschätzung der Gefahrenlage, der verhältnismäßige Einsatz, die Nutzung von Spielräumen durch das Pre-Recording, die Einhaltung des Verbotes, in Wohnungen zu filmen, und der laute und deutliche Hinweis auf den Einsatz der Bodycam sind nur einige Aspekte, die einen erheblichen Einfluss auf die tägliche Praxis der Beamten haben. Der rechtssichere und überprüfbare Einsatz von Bodycams ist und bleibt eine Herausforderung.

Was ist zu tun?

Sollen Bodycams über den Pilotversuch hinaus eingesetzt werden, ist der Gesetzgeber gefordert, einen klaren Rahmen für den Einsatz zu schaffen. Erfolgreich kann dieses Einsatzmittel nur sein, wenn es gelingt, den Schutz von Leib und Leben der Beamten zu verbessern, ohne dabei die Rechte der Bürgerinnen und Bürger unverhältnismäßig zu beschneiden. Aufseiten der Anwender bei der Polizei sind intensive Schulungen und regelmäßiges Einsatztraining erforderlich, um eine rechtssichere Verwendung dieses Einsatzmittels zu gewährleisten.

4.2.4 @rtus-Löschkonzept

Bereits seit der Produktivsetzung des Vorgangsbearbeitungssystems „@rtus" der Landespolizei im Jahr 2007 hat das ULD die undifferenzierte, lange Speicherdauer (oder „Aussonderungsprüffrist") kritisiert (29. TB, Tz. 4.2.9; 30. TB, Tz. 4.2.8; 33. TB, Tz. 4 2 2; 34. TB, Tz. 4.2.1).

Die im Gesetz verankerte Unterscheidung nach Art und Schwere der zugrunde liegenden Tat fand lange keine softwareseitige Entsprechung in @rtus. Bereits vor einigen Jahren haben wir über den Entwurf eines neuen Löschkonzeptes für @rtus berichtet (35. TB, Tz. 4.2.1). Nachdem

das Konzept weiter verfeinert und softwareseitig implementiert wurde, konnte Ende 2017 mit der Umsetzung begonnen werden.

Das neue Konzept unterscheidet u. a. zwischen Straftaten, Ordnungswidrigkeiten und dem Berichtswesen. In vielen Fällen sind außerdem die Verfahrensausgänge von entscheidender Bedeutung für die Löschfristen. Unter bestimmten Umständen können personenbezogene Daten aus Strafverfahren auch länger gespeichert werden, wenn diese Daten zur Aufklärung oder Verhütung künftiger Straftaten erforderlich sind.

Aufgrund der verschiedenen polizeifachlichen Anforderungen, der entsprechenden rechtlichen Vorgaben sowie den Abhängigkeiten zwischen den personenbezogenen Daten in @rtus mit anderen polizeilichen Verfahren wie Merlin oder INPOL/PIAV handelt es sich bei dem Löschkonzept um ein relativ komplexes Regelwerk. In manchen Bereichen unterstützt die Software den Sachbearbeiter dabei, vergleichbare Löschfristen für ähnlich gelagerte Fälle nach definierten Standards festzulegen. Besonders an den Schnittstellen zu anderen Fachverfahren sowie bei der Eingabe von Verfahrensausgängen ist oft noch „Handarbeit" vonnöten. Außerdem ermöglicht @rtus erstmalig auch dem Sachbearbeiter, individuell auf die Löschfristen Einfluss zu nehmen – sie also im Einzelfall zu verkürzen oder zu verlängern.

Dies ist grundsätzlich zu begrüßen, da die Erforderlichkeit personenbezogener Daten für die Polizeiarbeit vom Einzelfall abhängig ist und damit nicht pauschal von einer automatisierten Systementscheidung abhängig gemacht werden kann.

Besonders begrüßt wird der Umstand, dass sich die Landespolizei dazu entschlossen hat, dass neue Löschkonzept auch mit Wirkung für die Vergangenheit umzusetzen. Die Polizei schätzt, dass dadurch etwa 1,3 Millionen Vorgänge vorzeitig gelöscht wurden. Da diese Datensätze teilweise Abhängigkeiten zu anderen Fachverfahren wie Merlin oder INPOL/PIAV haben, hat diese Entscheidung zu einem nicht unerheblichen Arbeitsaufwand über mehrere Monate geführt.

Mit Abschluss der retrograden Einführung im Frühjahr 2018 wird nunmehr der gesetzlichen Vorgabe der Differenzierung Genüge getan. Die Rechte der betroffenen Bürgerinnen und Bürger erhalten dadurch das nötige Gewicht. Außerdem wurden die polizeilichen Systeme von Daten befreit, die für die Aufgabenerfüllung nicht mehr erforderlich sind.

Was ist zu tun?

Ein wichtiger Schritt wurde gemacht. Jetzt muss die Zukunft zeigen, ob das neue Löschkonzept den verschiedenen Anforderungen und Situationen gerecht wird. Insbesondere in den Bereichen, die individuelle Entscheidungen ermöglichen oder „Handarbeit" erfordern, muss sich zeigen, ob das Konzept praxistauglich ist und Entscheidungen nachvollziehbar dokumentiert werden.

4.2.5 Prüfung von Antiterrordatei und Rechtsextremismus-Datei

Die Antiterrordatei (ATD) im Bereich der Bekämpfung des internationalen Terrorismus sowie die Rechtsextremismus-Datei (RED) im Bereich der Bekämpfung des gewaltbezogenen Rechtsextremismus dienen beide der Informationsanbahnung und in Eilfällen auch der Gefahrenabwehr. Dies soll insbesondere die Zusammenarbeit zwischen den Nachrichtendiensten und den Polizeien in Bund und Ländern verbessern.

Im klassischen Verwaltungshandeln, etwa durch Verwaltungsakt, werden behördliche Maßnahmen an den Einzelnen adressiert und mit einer Begründung versehen, die gegebenenfalls gerichtlich überprüfbar ist. Im Gegensatz dazu findet die Datenverarbeitung nach dem Antiterrordateigesetz (ATDG) und dem Rechtsextremismus-Datei-Gesetz (RED-G) außerhalb jeder unmittelbaren Wahrnehmbarkeit statt. Sie erfolgt ohne Begründung gegenüber der betroffenen Person, ohne ihr Wissen und kann daher in der Regel auch nicht gerichtlich überprüft werden.

Wie das Bundesverfassungsgericht in seinem Urteil vom 24. April 2013 (1 BvR 1215/07) betont, ist als Kompensation für den schwach ausgestalteten Individualrechtsschutz die regelmäßige aufsichtsbehördliche Kontrolle von besonderer Bedeutung. Kontrollen müssen daher nach § 10 Abs. 2 ATDG und § 11 Abs. 2 RED-G alle zwei Jahre von den Datenschutzaufsichtsbehörden durchgeführt werden.

Das ULD hat deshalb die beiden Dateien bei der Landespolizei sowie bei der Verfassungsschutzbehörde einer Kontrolle unterzogen.

Beim Verfassungsschutz gibt es seit einigen Jahren für jede Speicherung einen Erfassungsbogen. Darauf wird u. a. die Rechtsgrundlage für die Speicherung vermerkt sowie das Vorliegen der Tatbestandsmerkmale kurz begründet. Dementsprechend musste für die Prüfung relativ selten der Aktenrückhalt zurate gezogen werden.

Bei der Landespolizei existiert solch ein Erfassungsbogen nicht. Dementsprechend war die Prüfung aufwendiger. Für jeden Fall musste der Aktenrückhalt herangezogen werden. Dabei wurden jedes Mal aus den geschilderten Sachverhalten die relevanten Tatsachen herausgesucht und mit den gesetzlichen Speichervoraussetzungen abgeglichen. Im Prinzip musste die rechtliche Bewertung, die der Sachbearbeiter im Rahmen der Einstellung der Daten in die Datei vorgenommen hatte, mangels Dokumentation wiederholt werden. Dies erschwerte die Prüfung und entspricht nicht den datenschutzrechtlichen Standards.

Öffentliche Stellen sind verpflichtet, die von ihnen vorgenommenen Bewertungen zu begründen, wenn sie Befugnisse in Anspruch nehmen. Transparenz entsteht durch eine nachvollziehbare Dokumentation dieser Begründung.

Der Umstand, dass personenbezogene Daten in der Regel ohne das Wissen der Betroffenen in die ATD/RED eingestellt werden (dürfen), befreit nicht von dieser Verpflichtung. Es stellt vielmehr besondere Anforderungen an die Dokumentation behördlichen Handelns. Das Bundesverfassungsgericht führt in seinem Urteil (Rn. 214) dazu Folgendes aus:

> „Weil eine Transparenz der Datenverarbeitung und die Ermöglichung individuellen Rechtsschutzes durch das Antiterrordateigesetz nur sehr eingeschränkt sichergestellt werden können, kommt der Gewährleistung einer effektiven aufsichtlichen Kontrolle umso größere Bedeutung zu. Der Verhältnismäßigkeitsgrundsatz stellt deshalb an eine wirksame Ausgestaltung dieser Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis gesteigerte Anforderungen."

Das Maß an Transparenz und Nachvollziehbarkeit behördlicher Entscheidungen, das normalerweise dem Betroffenen zusteht, muss demnach der aufsichtlichen Kontrolle zugänglich sein. Die Möglichkeit, aufgrund des Aktenrückhaltes eigene Bewertungen vorzunehmen, unter der Annahme, dass die zuständige Behörde wahrscheinlich zu demselben Ergebnis gekommen ist, genügt diesem Standard nicht.

Darüber hinaus waren bei der Polizei im Bereich der RED teilweise nicht alle speicherrelevanten Vorgänge aufgeführt. Eine dokumentierte Begründung, warum im konkreten Einzelfall die Speichervoraussetzungen vorliegen, würde auch in diesem Bereich zu einer Verbesserung der Qualität führen.

Offensichtlich rechtswidrige Speicherungen wurden bei keiner der beiden Behörden gefunden. In Einzelfällen müssen jedoch noch Fragen geklärt werden.

Was ist zu tun?

Behördliche Entscheidungen im Bereich der Eingriffsverwaltung sind für betroffene Personen besonders intensive Eingriffe in ihr Persönlichkeitsrecht. Dies trifft insbesondere auf Entscheidungen zu, die ohne Wissen der betroffenen Personen und ohne Möglichkeit der Intervention getroffen werden. In diesen Bereichen kommt der Dokumentation behördlicher Entscheidungen und gesetzlicher Tatbestände eine besondere Bedeutung zu, um eine effektive aufsichtliche Kontrolle zu gewährleisten.

4.2.6 Folgen aus der Prüfung der Falldatei Rauschgift

Im vergangenen Berichtszeitraum wurde bereits über die Prüfung der „Falldatei Rauschgift" (FDR) berichtet (36. TB Tz. 4.2.2). Bei der „Falldatei Rauschgift" (FDR) handelt es sich um eine Bund-/Länderdatei des polizeilichen Informationssystems INPOL. Sie diente insbesondere der Aufklärung und/oder Verhütung von Straftaten nach dem Betäubungsmittelgesetz, die von länderübergreifender, internationaler oder erheblicher Bedeutung waren.

Aufgrund der vielen – teilweise gravierenden – Mängel, die bei der damaligen Prüfung aufgefallen sind, wurden die Datensätze vom Bundeskriminalamt und den betroffenen Ländern bereinigt und danach in das INPOL-Fall-Nachfolgesystem PIAV (Polizeilicher Informations- und Analyseverbund) migriert. Für Schleswig-Holstein bedeutet das, dass nur etwa 25 Prozent der Fälle aus der FDR nach PIAV migriert worden sind. Mehr als 15.000 Fälle erfüllten nicht die Voraussetzungen für eine weitere Speicherung.

Interessant ist in diesem Zusammenhang, welche Auswirkung das auf die polizeiliche Kriminalstatistik Schleswig-Holstein (PKS) aus dem Jahr 2017 hatte. Die Zahl der „Erstkonsumenten harter Drogen" war laut dieser Statistik deutlich zurückgegangen. Dies wurde u. a. wie folgt kommentiert:

„Der Großteil der eigentlichen Erstkonsumenten wurde im Zusammenhang mit dem Besitz einer geringen Menge (§ 31a BtMG-Fälle) festgestellt. In diesen Fällen erfolgte jedoch **nach der Verschärfung der datenschutzrechtlichen Bestimmungen** keine Erfassung mehr als Erstkonsument harter Drogen …" [Hervorhebung durch die Redaktion].

Diese Formulierung überrascht, impliziert sie doch, dass sich datenschutzrechtliche Bestimmungen geändert haben bzw. sogar „verschärft" wurden. Außerdem wird der Datenschutz indirekt zur Ursache des Problems erklärt, dass eine – für politische und präventive Zwecke relevante und damit gesamtgesellschaftlich wichtige – statistische Größe nicht erhoben werden konnte.

In Wirklichkeit beschränkt das BKA-Gesetz in der Fassung von 1997 die Speicherung von personenbezogenen Daten in einer INPOL-Datei u. a. auf Straftaten von „erheblicher Bedeutung". Straftaten von erheblicher Bedeutung sind der mittleren Kriminalität zuzuordnen. Verstöße im Zusammenhang mit dem Besitz einer geringen Menge Betäubungsmittel erfüllen diese Voraussetzung nicht. Die Vorgehensweise des Bundes und der Länder, Erstkonsumenten harter Drogen pauschal in einer INPOL-Datei zu speichern, war damit von Beginn an schlicht rechtswidrig. Es wurde also nichts „verschärft". Diese, über Jahre gelebte, rechtswidrige Praxis ist einfach nur im Rahmen einer datenschutzrechtlichen Kontrolle aufgefallen.

Datenschutzrechtliche Bestimmungen verhindern auch nicht die Erfassung gesellschaftlich relevanter statistischer Größen. So wurde das LKA Schleswig-Holstein bereits 2016 mit dem

Abschlussbericht zur FDR-Prüfung darauf hingewiesen, dass geprüft werden sollte, „ob diese Daten zukünftig in anonymisierter Form als Kriminal-, Landes- oder Bundesstatistik geführt werden können". Eine INPOL-Datei ist dafür schlicht das falsche Instrument.

Was ist zu tun?

Der Zweck heiligt nicht die Mittel. Der Datenschutz verhindert nicht die Wahrnehmung notwendiger staatlicher Aufgaben. Er hilft vielmehr dabei, die richtigen Instrumente auszuwählen, um das Ziel zu erreichen und dabei die Bürgerinnen und Bürger vor unnötigen Eingriffen in ihr Persönlichkeitsrecht zu schützen. Das zeichnet einen Rechtsstaat aus. Datenschutz von Beginn an mitzudenken ist daher Teil der Lösung und nicht des Problems.

4.2.7 Rockeraffäre und die Polizei, Aktenvorlagebegehren und Parlamentarischer Untersuchungsausschuss

Die im Berichtszeitraum öffentlich diskutierten Vorwürfe gegen die Landespolizei im Zusammenhang mit den Ermittlungen im Bereich der Rockerkriminalität und Mobbinghandlungen durch Vorgesetzte haben auch das ULD beschäftigt. Sie haben u. a. dazu geführt, dass der Innenminister einen Sonderbeauftragten zur Aufarbeitung der erhobenen Vorwürfe eingesetzt hat. Der Schleswig-Holsteinische Landtag hat zunächst die Vorlage von Akten der Landesverwaltung und Justiz zu unterschiedlichen Themenkomplexen gefordert. Nach Sichtung der Akten hat der Landtag einen Parlamentarischen Untersuchungsausschuss eingesetzt.

Das ULD hat das Ministerium für Inneres, ländliche Räume und Integration in unterschiedlichen Verfahren und Fragestellungen beraten.

Zunächst ging es darum, die Voraussetzungen für die Vorlage von Akten an den Landtag zu klären. Unter den angeforderten Unterlagen befanden sich nach Einschätzung des Innenministeriums auch solche, die von Berufsgeheimnisträgern geführt werden und dem Schutz des Berufsgeheimnisses unterliegen. Diese durften demzufolge dem Landtag nur vorgelegt werden, soweit die betroffenen Personen die Berufsgeheimnisträger von ihrer Schweigepflicht entbunden haben. Bei der Gestaltung des Verfahrens und der Formulierung einer entsprechenden Schweigepflichtentbindungserklärung hat das ULD das Innenministerium beraten.

Das ULD ist daraufhin vom Innenministerium gebeten worden, das Verfahren der Aktenvorlage, das federführend im Innenministerium bearbeitet wurde, in datenschutzrechtlicher Hinsicht zu begleiten. Die Begleitung durch das ULD erstreckte sich hauptsächlich auf die besonders vertraulich zu behandelnden Unterlagen, die von den Berufsgeheimnisträgern für die Aktenvorlage zur Verfügung gestellt wurden. Nach den Verfahrensregeln, die das Innenministerium für diese Unterlagen festgelegt hatte, durften sie nur durch bestimmte Personen geöffnet werden. Die Öffnung sollte danach im Beisein von Beschäftigten des ULD stattfinden. Unmittelbar nach der Öffnung sollten die Unterlagen, ebenfalls im Beisein der Beschäftigten des ULD, paginiert und im Hinblick auf eine eventuell erforderliche Einstufung als Verschlusssache gesichtet werden. Anschließend sollten sie im Innenministerium verwahrt werden. Die Beschäftigten des ULD haben den Prozess der Öffnung und Sichtung im Hinblick darauf begleitet, dass

- keine unbefugten Personen in dieser Phase Kenntnis erlangen,

- die Akten in dieser Phase vollständig bleiben und
- das Innenministerium Vorkehrungen trifft, um die Vollständigkeit revisionssicher zu machen (Paginierung).

In gleicher Weise wurde mit der Zulieferung durch Betroffene verfahren, denen von der Landespolizei eine gleichartige Behandlung ihrer Unterlagen zugesichert worden war.

Dem Umgang mit anderen Unterlagen, vor allem mit solchen, die von anderen Stellen – wie der Justiz – an das Innenministerium übergeben worden sind, hat das ULD nicht beigewohnt. Ausschlaggebend waren hierfür zwei Erwägungen. Erstens hielt das ULD besondere Maßnahmen zur Sicherung der Vollständigkeit und Integrität jedenfalls für die von den Gerichten und Staatsanwaltschaften zugelieferten Akten nicht für erforderlich. Vielmehr ging das ULD davon aus, dass diese Akten über eine eigene Paginierung verfügen, sodass die Revisionssicherheit damit sichergestellt ist. Zweitens hielt das ULD für diese Vorgänge besondere Maßnahmen zur Gewährleistung des vertraulichen Umgangs mit persönlichkeitsrelevanten Informationen nicht für erforderlich, um das Vertrauen in die Behandlung der Akten durch das Innenministerium im Hinblick auf die in der Öffentlichkeit thematisierten Vorwürfe und Bedenken zu sichern.

Auch nach der Aktenvorlage an den Landtag gab es weitere Fragen zum Umgang mit personenbezogenen Daten. Hauptsächlich betrafen diese Fragen den Umgang mit dem vom Sonderbeauftragten erstellten Bericht. Dem Bericht liegen die Unterlagen aus dem Aktenvorlagebegehren zugrunde. Außerdem wurden Personen zu ihren Wahrnehmungen im Zusammenhang mit dem gesamten Themenkomplex befragt. Diese Angaben gingen ebenfalls in den Bericht ein. Angesichts der Menge an personenbezogenen Daten, die hier über unterschiedliche Personen erhoben und verarbeitet wurden, verwundert es nicht, dass das Interesse der betroffenen Personen an einer Transparenz über die Verarbeitung „ihrer" Daten groß ist. Hierbei stellen sich allerdings umfangreiche datenschutzrechtliche Fragen. Denn häufig betreffen die dem Bericht zugrunde liegenden und die im Bericht wiedergegebenen Daten nicht nur eine, sondern gleich mehrere Personen. Es ist daher nur eingeschränkt möglich, einer Person Informationen zur Verfügung zu stellen, ohne gleichzeitig die Persönlichkeitsrechte anderer zu beeinträchtigen.

Mittlerweile werden in der Landespolizei erste Konsequenzen aus der Aufarbeitung der Vorkommnisse umgesetzt. Auch dies führt teilweise zu einer Ausweitung der Verarbeitung personenbezogener Daten. In die Erstellung von Konzepten ist das ULD ebenfalls beratend eingebunden.

Was ist zu tun?

Bei den im Raum stehenden Vorwürfen geht es nicht nur um Ermittlungen im Rockermilieu und um Daten, die zum Schutz von Vertrauenspersonen und aus polizeitaktischen Gründen besonders vertraulich zu behandeln sind. Es sind vor allem höchstpersönliche Informationen über Angehörige der Landespolizei – Mitarbeitende wie Vorgesetzte – betroffen. Diese bedürfen eines mindestens ebenso hohen Schutzes, um die Persönlichkeitsrechte der betroffenen Personen zu wahren. Dies gilt für alle Stellen, die über diese Daten verfügen.

4.2.8 Einführung der elektronischen Akte beim Verfassungsschutz

Bereits seit einigen Jahren wird das Thema „elektronische Aktenhaltung (E-Akte)“ immer bedeutsamer. Seit der Einführung des § 52d Landesverwaltungsgesetz (LVwG) hat die E-Akte in immer mehr Amtsstuben Einzug gehalten oder befindet sich in der Einführung. Bereits der Wortlaut des § 52d LVwG macht deutlich, dass vor allem datenschutzrechtliche Aspekte bei der Konzeptionierung und Verwendung eines solchen Hilfsmittels eine bedeutende Rolle spielen.

Die E-Akte ist nicht nur ein Mittel, um Prozesse zu standardisieren und Arbeitsabläufe zu vereinfachen. Sie bietet außerdem ganz neue Möglichkeiten, personenbezogene Daten aus Akten zu recherchieren, zu verknüpfen und auszuwerten. Dabei ist nicht alles, was technisch möglich ist, auch erlaubt. So ist es beispielsweise zulässig und gewollt, dass Gruppierungen und auch Einzelpersonen gezielt durch den Verfassungsschutz beobachtet werden, wenn sie Anlass dafür gegeben haben. Solche Personen konnten schon vor der E-Akte in nachrichtendienstlichen Informationssystemen rechtmäßig gespeichert werden.

Wer als unbescholtene Bürgerin oder unbescholtener Bürger unwissentlich Kontakt mit einer Zielperson hatte oder in einem relevanten Zeitungsbericht Erwähnung findet, konnte auch bisher Teil einer allgemeinen, phänomenbezogenen Akte werden, ohne dies zu wissen. In der Welt der Papierakte gingen diese Personen jedoch irgendwann „unter“. Sie waren nicht ohne Weiteres recherchierbar oder analysierbar. Dies ändert sich nun durch die elektronische Aktenführung. Damit sind technische Auswertungen und Abfragen möglich, die bisher nur im Bereich der nachrichtendienstlichen Informationssysteme möglich waren. Die E-Akte vereinfacht dadurch nicht nur Verwaltungsprozesse. Sie schafft auch neue datenschutzrechtliche Herausforderungen, denen man begegnen muss.

Diese Herausforderungen hat auch die Verfassungsschutzbehörde gesehen und deshalb frühzeitig das ULD um Beratung gebeten. In mehreren Besprechungen wurde das geplante E-Aktensystem vorgestellt und Lösungen für datenschutzrechtliche Fragestellungen gesucht. Durch die Benennung eines behördlichen Datenschutzbeauftragten konnten datenschutzrechtliche Aspekte bereits in der Konzeptionierungsphase mit eingearbeitet werden. Entwürfe der wesentlichen Konzeptpapiere – z. B. der Dateianordnung, der Dienstvereinbarung der technischen Konzepte sowie der Dienstanweisung – waren bereits vorhanden und konnten im Rahmen der Beratung näher betrachtet und verbessert werden.

Im Rahmen der Beratung sind noch einige Mängel an der Protokollierung aufgefallen. Hier soll technisch nachgebessert werden. Außerdem wurde deutlich, dass die bestehende Rechtsgrundlage für das Führen von Akten (§ 13 LVerfSchG) an die Besonderheiten im Zusammenhang mit der elektronischen Aktenführung angepasst werden muss. Hier muss durch den Gesetzgeber transparent geregelt werden, was mit der elektronischen Akte geht und was nicht. Bis zur Anpassung des Gesetzes sollen im Rahmen einer Übergangslösung entsprechende Regelungen zunächst im Rahmen einer Selbstverpflichtung festgeschrieben werden. Die Einhaltung wird insbesondere von dem behördlichen Datenschutzbeauftragten kontrolliert.

Da hier ein Stück weit Neuland betreten wird, ist es allerdings schwierig, alle möglichen Auswirkungen vorherzusehen. Das ULD empfiehlt daher, die Wirksamkeit der ergriffenen Maßnahmen zum Schutz der Rechte der betroffenen Personen zu evaluieren. Insbesondere sollte dabei betrachtet werden, ob sie geeignet sind, einen effektiven Schutz zu gewährleisten, und ob alle technischen Möglichkeiten – die im Verhältnis zum Aufwand stehen – tatsächlich ausgeschöpft werden. Darüber hinaus sollten regelmäßige Kontrollen durch den behördlichen Datenschutzbeauftragten stattfinden.

Was ist zu tun?

Bei der Einführung neuer Datenverarbeitungsverfahren empfiehlt es sich, frühzeitig den behördlichen Datenschutzbeauftragten einzubeziehen. Wer Datenschutz bereits bei der Konzeptionierung mit berücksichtigt, handelt rechtssicher und spart sich an anderer Stelle viel Arbeit.

4.2.9 Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Bei Großveranstaltungen, für die ein erhöhtes Sicherheitsrisiko besteht, ist es mittlerweile gängige Praxis, dass Personen, die bei oder teilweise auch im Umfeld solcher Veranstaltungen tätig werden, im Hinblick auf ihre Zuverlässigkeit vorab überprüft werden. Dazu werden die Daten der Personen dem Veranstalter gemeldet. Dieser leitet sie an die Landespolizei weiter, die überprüft, ob Sicherheitsbedenken gegen den Einsatz der Personen bestehen. Sicherheitsbedenken werden als zusammengefasste Bewertung ohne Angabe der einzelnen Erkenntnisse an den Veranstalter zurückgemeldet. Dieser entscheidet dann, ob die Person zur Veranstaltung zugelassen wird oder nicht.

Auch wenn das Sicherheitsinteresse bei einigen Veranstaltungen nachvollziehbar ist, mussten wir solche Zuverlässigkeitsüberprüfungen in der Vergangenheit beanstanden bzw. im Berichtszeitraum für die Zuverlässigkeitsüberprüfung beim Wacken Open Air 2018 eine Verwarnung aussprechen. Denn es fehlt die hierfür erforderliche gesetzliche Grundlage. Hierauf haben wir seit der Einführung des Verfahrens zur Fußball-WM 2006 wiederholt hingewiesen (34. TB, Tz. 4.2.2; 31. TB, Tz. 4.2.3; 30. TB, Tz. 4.2.3; 29. TB, Tz. 4.2.5; 28. TB, Tz. 4.2.9). Auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat im April 2018 mit einer Entschließung das Erfordernis einer gesetzlichen Regelung erneut bekräftigt:

https://www.datenschutzkonferenz-online.de/media/en/20180426_en_zuverlaessigkeitspruefungen_veranstaltungen.pdf

Auf eine Einwilligung der betroffenen Personen kann die Durchführung der Zuverlässigkeitsüberprüfung nicht gestützt werden. Viele betroffene Personen wirken im Rahmen ihres Arbeitsverhältnisses an einer Veranstaltung mit, z. B. als Beschäftigter eines Caterers oder eines Sicherheitsunternehmens. Die für eine Einwilligung erforderliche Freiwilligkeit fehlt daher in den meisten Fällen.

Die gesetzliche Grundlage soll zum einen sicherstellen, dass das Verfahren der Zuverlässigkeitsüberprüfung nur bei besonders gefährdeten Veranstaltungen zum Einsatz kommt. Ebenso wichtig ist es zum anderen, durch gesetzliche Vorgaben bestimmte Anforderungen an das Verfahren festzulegen. Dazu gehören klare Kriterien für die Bewertung der Zuverlässigkeit von Personen ebenso wie ein transparentes Verfahren. Nur durch frühzeitige Information über die Ergebnisse der Zuverlässigkeitsprüfung werden die betroffenen Personen in die Lage versetzt, etwaige Gegendarstellungen vorzubringen. Dadurch können auch Fehler in den Datengrundlagen erkannt werden, was insgesamt der Qualität des Verfahrens zugutekommt.

Wir haben das Innenministerium auf das Erfordernis einer gesetzlichen Regelung hingewiesen und stehen mit diesem im Austausch über die Gestaltung einer solchen Vorschrift.

Was ist zu tun?

Sollen auch künftig Zuverlässigkeitsüberprüfungen vor bestimmten Veranstaltungen vorgenommen werden, muss hierfür eine tragfähige gesetzliche Grundlage geschaffen werden.

4.3 Justiz

4.3.1 Veröffentlichung von Gerichtsurteilen

Im Berichtszeitraum erreichte uns eine Beschwerde einer Bürgerin gegen die Veröffentlichung der Gerichtsentscheidung aus ihrem Verfahren. Die Bürgerin hatte Sorge, dass Leser der Entscheidung sie identifizieren und aus der Entscheidung weitere Informationen über sie erfahren könnten. Das Gericht entfernte daraufhin die Angaben zum Arbeitgeber und zu Vereinen, in denen die Bürgerin tätig war, aus der Entscheidung.

Die Beschwerde hat das Gericht zum Anlass genommen, Fragen des Datenschutzes bei der Veröffentlichung von Gerichtsentscheidungen grundsätzlich mit uns zu erörtern. Auf dieser Grundlage beabsichtigt das Gericht, seine internen Regelungen für die Veröffentlichung von Entscheidungen zu überarbeiten.

Die rechtlichen Grundlagen für die Veröffentlichung von Gerichtsentscheidungen und die erforderliche Wahrung der Persönlichkeitsrechte ergeben sich aus dem Verfassungsrecht. Sowohl die Publikation von veröffentlichungswürdigen Gerichtsentscheidungen als auch der Schutz der Persönlichkeitsrechte natürlicher Personen genießen Verfassungsrang. Beide Verfassungspositionen müssen jeweils im Einzelfall in einen gerechten Ausgleich gebracht werden. Nach der Rechtsprechung wird dies in der Regel in der Weise gelöst, dass die zu veröffentlichenden Entscheidungen hinsichtlich persönlicher Angaben und Umstände zu anonymisieren sind. Dabei ist der von der Rechtsprechung verwandte Begriff der „Anonymisierung“ nicht als Anonymisierung im Sinne des Datenschutzrechts zu verstehen. Die Datenschutz-Grundverordnung enthält zwar keine Legaldefinition für die Anonymisierung, geht jedoch davon aus, dass es anonyme (und auch anonymisierte) Informationen gibt. Für diese sollen nach Erwägungsgrund 26 die Grundsätze des Datenschutzes nicht gelten. Dementsprechend beschreibt Erwägungsgrund 26 anonyme Informationen als „Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann“. Für eine Vielzahl von Gerichtsverfahren wird eine Anonymisierung im Sinne der DSGVO nicht erreichbar sein. Es gibt häufig einen Kreis von Personen – etwa Zeugen oder Sachverständige aus dem Gerichtsverfahren, Saalöffentlichkeit, soweit eine mündliche Verhandlung stattgefunden hat, Personen mit Insiderwissen aus den am Verfahren beteiligten Organisationen wie Behörden oder Unternehmen –, für die der Sachverhalt und die Entscheidungsgründe Rückschlüsse auf die betroffenen Personen ermöglichen. Es handelt sich daher nicht um eine Anonymisierung, sondern um die Herstellung einer herausgabefähigen Fassung, die den Persönlichkeitsrechten der betroffenen Personen Rechnung trägt.

Die Rechtsprechung deutscher Gerichte gibt einige Hinweise darauf, wie eine herausgabefähige Fassung herzustellen ist. So reicht es nach einem Beschluss des VGH Baden-Württemberg im Regelfall aus, im Rubrum die Angaben über die Parteien und ihre Vertreter vollständig zu löschen und im Sachverhalt sowie in den Entscheidungsgründen die Namen aller Personen und Orte bis auf die Anfangsbuchstaben zu entfernen. Sofern dies in Einzelfällen nicht zu

einer ausreichenden Unkenntlichmachung der betroffenen Personen führt, ist unter Abwägung des Informationsinteresses der Öffentlichkeit und der Persönlichkeitsrechte der betroffenen Personen eine weitere Bearbeitung erforderlich. Für die Einzelfallbearbeitung können kaum allgemeingültige Kriterien aufgestellt werden. Hier wird stets eine Abwägung unter Berücksichtigung aller Umstände des Einzelfalls erforderlich sein. Wichtig ist daher, dass die Richterin oder der Richter aus dem zugrunde liegenden Verfahren in den Veröffentlichungsprozess eingebunden wird. Die Beurteilung, ob die Standardbearbeitung ausreicht, um Rückschlüsse auf die Personen ausreichend zu verhindern oder zu erschweren, und ob gegebenenfalls weitere Angaben entfernt werden müssen, ist komplex und erfordert Kenntnisse über den zugrunde liegenden Sachverhalt und die Parteien des Rechtsstreits. Hier ist sicherlich die entscheidende Richterin oder der entscheidende Richter am besten in der Lage, eine Einschätzung vorzunehmen.

In Ausnahmefällen kann die Abwägung auch zu dem Ergebnis führen, dass eine Veröffentlichung zum Schutz der Persönlichkeitsrechte ganz unterbleiben muss. Dies ist z. B. der Fall, wenn die Entscheidung einer Person zugeordnet werden kann, sensible personenbezogene Daten für das Verständnis der Entscheidung zwingend erforderlich sind und daher nicht entfernt werden können und das öffentliche Interesse an der Entscheidung die Persönlichkeitsrechte der betroffenen Personen nicht überwiegt.

Was ist zu tun?

Vor der Veröffentlichung von Gerichtsentscheidungen sind diese so zu bearbeiten, dass die betroffenen Personen unkenntlich gemacht werden.

4.3.2 Veröffentlichung von Daten aus den Insolvenzbekanntmachungen auf privaten Webseiten

Im Berichtszeitraum hat das ULD zahlreiche Beschwerden von betroffenen Personen erhalten, die bei einer Internetrecherche meist mit großem Schrecken festgestellt haben, dass Informationen über ihr häufig lange zurückliegendes Insolvenzverfahren frei zugänglich im Internet veröffentlicht waren. Die Webseiten mit den Insolvenzveröffentlichungen wurden regelmäßig vom außereuropäischen Ausland betrieben. Anbieterinformationen enthielten diese Webseiten nicht. Für die betroffenen Personen ist diese Veröffentlichung meist mehr als nur ärgerlich. Das Insolvenzverfahren lag in fast allen Fällen viele Jahre zurück. Die Personen hatten sich zwischenzeitlich eine neue Existenz aufgebaut; einige hatten einen neuen Arbeitgeber oder einen neuen Lebenspartner, der von der früheren Insolvenz keine Kenntnis hatte. Die plötzliche Veröffentlichung des alten Verfahrens hat viele Betroffene in eine verzweifelte Lage gebracht.

Als Datenschutzaufsichtsbehörde für schleswig-holsteinische Unternehmen und öffentliche Stellen haben wir keine Möglichkeit, gegen die Veröffentlichung selbst vorzugehen. Die Webseiten sind stets außerhalb der EU registriert, und Angaben über den Betreiber waren in keinem der Fälle vorhanden.

Für betroffene Personen besteht jedoch die Möglichkeit, zumindest die Löschung der Einträge aus Suchmaschinen zu entfernen. Hierzu kann sich jede betroffene Person direkt an Suchmaschinenbetreiber wenden und die Löschung von bestimmten Einträgen beantragen. Hierüber lassen sich zumindest die Treffer bei

Suchmaschinen entfernen, auch wenn die Webseite weiterhin online ist.

Wichtig ist jedoch vor allem ein ausreichender Schutz der Insolvenzdaten an der ursprünglichen Quelle ihrer ersten Veröffentlichung. Das Insolvenzgesetz sieht eine Veröffentlichung von Insolvenzdaten im Internet vor. Die Veröffentlichung erfolgt in dem von der nordrhein-westfälischen Justiz zentral betriebenen Justizportal. Auch wenn der Zeitraum der unbeschränkten Veröffentlichung sehr kurz ist, besteht in dieser Zeitspanne für Dritte die Möglichkeit, die Daten zu kopieren und für eigene Zwecke zu speichern. So können die im amtlichen Justizportal längst gelöschten Insolvenzdaten auch Jahre später noch im Internet an anderen Stellen wieder auftauchen.

4.3.3 Videodolmetschen

Im Justizvollzug müssen Gespräche mit Gefangenen oftmals kurzfristig geführt werden. Nicht nur bei akuten gesundheitlichen Beschwerden eines Gefangenen, sondern z. B. auch bei Neuzugängen in der Untersuchungshaft, um etwa besondere Rahmenbedingungen für die Unterbringung zu erfahren. Für solche Situationen hat das Justizministerium die Einführung eines Videodolmetschdienstes geplant und uns hierzu um Beratung gebeten. Ein solcher Dienst wird von einem Unternehmen angeboten, das hierfür mit einer Vielzahl von Dolmetschern zusammenarbeitet.

Bei der Inanspruchnahme dieses Dienstes handelt es sich um eine Datenverarbeitung im Auftrag. Dies hat zur Folge, dass die Justizvollzugsanstalt für die Datenverarbeitung auch beim Dienstleister verantwortlich ist. Es war daher durch die auftraggebende Justiz durch entsprechende Weisungen sicherzustellen, dass datenschutzrechtliche Vorgaben beim Auftragnehmer durch ausreichende technische und organisatorische Maßnahmen gewährleistet werden.

Risiken für die Rechte und Freiheiten der betroffenen Personen liegen zum einen in der Person der Dolmetscher selbst, d. h. in ihrer Fachkunde und Zuverlässigkeit. Zum anderen liegen sie in der Art und Weise der Erbringung der Übersetzungsleistung. Diese wird über Internetverbindungen, vermittelt durch den Dienstleister, erbracht. Die Dolmetscher arbeiten dabei entweder in den Räumen des Dienstleisters oder an einem privaten Arbeitsplatz. Hierdurch entstehen zum einen Risiken auf dem Übertragungsweg der Daten für einen Zugriff durch Unbefugte oder einen Zugriff durch den Dienstleister. Zum anderen entstehen, insbesondere wenn Dolmetscher an einem Heimarbeitsplatz arbeiten, Risiken für die Vertraulichkeit der Daten. Sie können durch Dolmetscher aufgezeichnet werden. Außerdem können sie anderen im Raum oder Nebenräumen anwesenden Personen bekannt gegeben werden. Hierdurch können Schäden für die Persönlichkeitsrechte der betroffenen Personen entstehen. Es können aber auch weiter gehende Schäden an anderen Rechten entstehen, wenn die Daten beispielsweise an Nachrichtendienste oder an Personen und Institutionen weitergegeben werden, von denen die betroffenen Personen verfolgt werden.

Wir haben dem Justizministerium daher empfohlen, insbesondere Folgendes zu beachten:

- Die Identität des Dolmetschers muss für den Auftraggeber prüfbar und sichergestellt sein.
- Der Dolmetscher muss über die erforderliche Fachkunde und Zuverlässigkeit verfügen. Diese muss für den Auftraggeber prüfbar sein. Es muss möglich sein, Dolmetscher abzulehnen, die diese Voraussetzungen nicht erfüllen.
- Es muss sichergestellt und prüfbar sein, dass der Dolmetscher die Übersetzung persönlich und nicht im Beisein Dritter erbringt.
- Die Datensicherheit muss beim Dolmetscher sichergestellt sein, z. B. muss gewährleistet sein, dass Daten nicht kopiert oder an Dritte weitergegeben werden.

Was ist zu tun?

Dienstleistungen des Videodolmetschens mit Dolmetschern, die von einer Zentrale vermittelt werden und ihre Leistungen über eine Videoverbindung erbringen, dürfen nur eingesetzt werden, wenn die Sicherheit der Daten vertraglich und durch technische und organisatorische Maßnahmen beim Anbieter und beim Dolmetscher gewährleistet ist.

4.3.4 Nachgehakt – mehr Transparenz bei Funkzellenabfragen

Im letzten Tätigkeitsbericht haben wir anlässlich der Prüfung von nicht individualisierten Funkzellenabfragen in Strafverfahren (35. TB, Tz. 4.3.1) ein Verfahren skizziert, das zu mehr Transparenz für die von dieser Maßnahme Betroffenen führt (36. TB, Tz. 4.3.7).

Es geht um Folgendes: Die Polizei kann auf Basis von § 100g Abs. 2 Satz 2 StPO nicht individualisierte Funkzellenabfragen durchführen. Dabei werden von Mobilfunkanbietern alle Verkehrsdatensätze abgefragt, die an einem Ort in einem von der Ermittlungsbehörde festgelegten Zeitraum erzeugt worden sind.

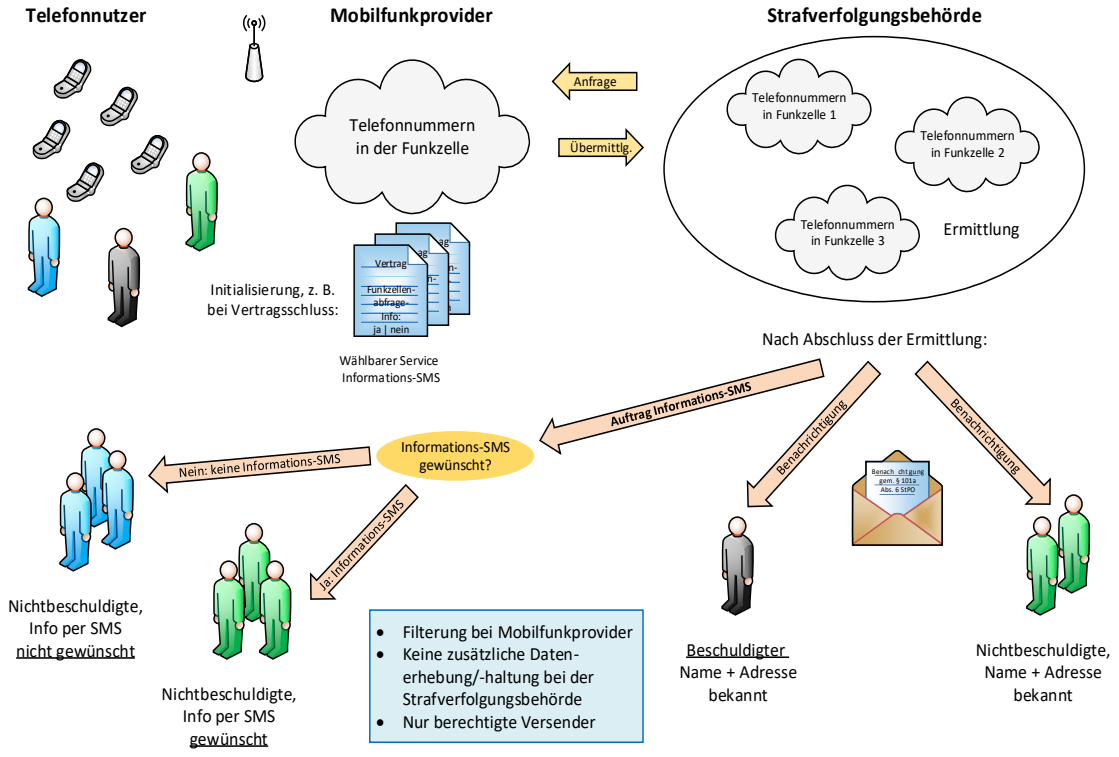


Abbildung: Kombination von Benachrichtigung und Informations-SMS

Solche Verkehrsdaten fallen bei Telefonaten, SMS oder Datenverbindungen zum Internet an. Typisch für Funkzellenabfragen ist, dass oft zahlreiche Personen erfasst und deren Verkehrsdaten anschließend für die Dauer des Ermittlungsverfahrens und in vielen Fällen auch darüber hinaus gespeichert werden. Werden diese Personen nicht namentlich identifiziert,

müssen sie über die Maßnahme nicht benachrichtigt werden. Das ist unbefriedigend, weil es sich um einen Grundrechtseingriff handelt. In der Diskussion hat sich herausgestellt, dass viele Personen gerne darüber informiert wären. Einen technischen Lösungsansatz für mehr Transparenz für die Betroffenen hat das ULD im Innen- und Rechtsausschuss des Schleswig-Holsteinischen Landtages und im 36. Tätigkeitsbericht vorgestellt und als freiwillige Maßnahme empfohlen.

Seitdem gibt es eine neue Entwicklung: Das Land Berlin hat ein eigenes Funkzellenabfragen-Transparenz-System (FTS) entwickelt, das allen Interessierten zur Verfügung steht. Es basiert auf einer Information per SMS für vorher registrierte Mobilfunknummern und ähnelt unserem Vorschlag. Dem Vernehmen nach können auf Anfrage andere Bundesländer bei der Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung in Berlin Unterstützung erhalten, um die FTS-Lösung ebenfalls – z. B. in eigenen Landesinstanzen – nutzen zu können. Damit könnte also auch Schleswig-Holstein mit wenig Aufwand die Transparenz für Betroffene von Funkzellenabfragen im eigenen Bundesland erhöhen.

Der Prüfbericht des ULD ist veröffentlicht unter:

http://www.landtag.ltsh.de/infothek/wahl18/umdrucke/5000/umdruck-18-5038.pdf

Der Bericht „Möglichkeiten für verbesserte Transparenz bei Funkzellenabfragen" ist veröffentlicht unter:

http://www.landtag.ltsh.de/infothek/wahl18/umdrucke/7500/umdruck-18-7553.pdf

Was ist zu tun?

Das Land sollte prüfen, ob Interessierten als transparenzfördernde Maßnahme die Möglichkeit gegeben werden soll, sich informieren zu lassen, wenn sie von Funkzellenabfragen in Schleswig-Holstein betroffen sind. Der Aufwand dafür ist nicht hoch, weil auf die Erfahrungen und Ausarbeitungen des Landes Berlin zurückgegriffen werden kann.

4.4 Ausländerverwaltung

4.4.1 Gesetzentwurf für den Vollzug der Abschiebungshaft

Die geplante Einrichtung einer Abschiebungshaftanstalt in Schleswig-Holstein muss durch Gesetz geregelt werden. Im Gesetzgebungsverfahren für das Abschiebungshaftvollzugsgesetz haben wir gegenüber dem federführenden Ministerium Stellung genommen.

Der Gesetzentwurf regelt den Vollzug der Abschiebungshaft. Dabei werden zwangsläufig personenbezogene Daten verarbeitet. Für den Justizvollzug gibt es seit 2016 mit dem Justizvollzugsdatenschutzgesetz einen einheitlichen Standard für die Datenverarbeitung. Wir haben dem Ministerium empfohlen, diesen Standard – soweit passend – auch für die Abschiebungshaft zu übernehmen. Insbesondere hinsichtlich der vorgesehenen Videoüberwachung bestand noch ein erheblicher Anpassungsbedarf, um das Datenschutzniveau des Justizvollzugsdatenschutzgesetzes zu erreichen. Das Justizvollzugsdatenschutzgesetz enthält differenzierte und umfängliche Regelungen zur Videoüberwachung in den unterschiedlichen Bereichen einer Anstalt und in deren unmittelbarer Umgebung. Die Voraussetzungen und Grenzen des Einsatzes sind für die einzelnen Bereiche spezifisch geregelt. Der

Gesetzentwurf für das Abschiebungshaftvollzugsgesetz ist aufgrund unserer Stellungnahme deutlich verbessert worden, bevor er in den Landtag eingebracht wurde. Insbesondere wurden folgende Verbesserungen vorgenommen:

- Die Videoüberwachung ist durchgängig nur noch als offene Maßnahme erlaubt.
- Die Voraussetzungen für die Überwachung sind präzisiert und insgesamt angehoben worden; es wird nach bestimmten Bereichen unterschieden.
- Die Speicherdauer wurde auf 48 Stunden reduziert.
- Wie auch nach dem Justizvollzugsdatenschutzgesetz muss die Einrichtung ein einheitliches Konzept für die Videoüberwachung erstellen. Bei der Planung ist zu berücksichtigen, dass den Untergebrachten überwachungsfreie Bereiche verbleiben.

4.4.2 Fotografie eines Ausweisdokuments

Ein EU-Bürger beschwerte sich bei uns darüber, dass bei einer Kontrolle im Rahmen eines Hausbesuchs sein Reisepass von einer Mitarbeiterin der Ausländerbehörde fotografiert wurde. Seiner Auffassung nach war dies rechtswidrig, denn er hatte seine Einwilligung dazu nicht erteilt.

Die Kontrolle diente der Identitätsprüfung sowie der Erfassung der Daten des Bürgers, um sie anschließend im Ausländerzentralregister einzugeben. Zur Verfahrensvereinfachung wurden die Passdaten durch eine Fotografie erhoben.

Das Abfotografieren des Reisepasses war unrechtmäßig. Die Ausländerbehörde ist zwar zur Identitätsfeststellung befugt, sodass sie grundsätzlich auch die Befugnis zum Anfertigen von Kopien bzw. Ablichtungen eines Reisepasses hat. Dies gilt jedoch nur, soweit die Daten für die Aufgabenerfüllung erforderlich sind. Für die Erfassung der Daten im Ausländerzentralregister waren nicht sämtliche Angaben auf dem Reisepass erforderlich. Bei der betroffenen Person handelte es sich um einen EU-Bürger. EU-Bürger werden bei dauerhaftem Aufenthalt zwar ebenfalls im Ausländerzentralregister gespeichert; im Vergleich zu Drittstaatenausländern aber mit einem verringerten Datensatz. Das Lichtbild wird bei EU-Bürgern nicht gespeichert, durch das Abfotografieren ist es aber ebenfalls gespeichert worden. Die Speicherung der Passdaten haben wir daher als einen Verstoß gegen datenschutzrechtliche Vorschriften beanstandet.

Ein weiteres Problem bestand darin, dass die Ausländerbehörde keine Dienstkamera genutzt hat, sondern das private Handy der Mitarbeiterin zum Einsatz kam. Der Einsatz von Kameras setzt voraus, dass die aufgenommenen personenbezogenen Daten durch hinreichende technische und organisatorische Maßnahmen geschützt sind. Dazu gehören insbesondere folgende Maßnahmen:

- Schutz gegen Auslesen der Daten durch Unbefugte, z. B. bei einem Verlust des Datenträgers,
- Schutz gegen Übertragung an Dritte, z. B. gegen den Zugriff durch Apps,
- Verfahrensregelungen für eine umgehende Bearbeitung und anschließende rückstandslose Löschung der Aufnahmen,
- Gewährleistung, dass die Daten ausschließlich auf dem Datenträger verbleiben und nicht an anderen Orten, z. B. in einer angeschlossenen Cloud, gespeichert werden.

Ein Einsatz privater Geräte von Beschäftigten, insbesondere Smartphones, ist nicht geeignet, diese Anforderungen zu erfüllen. Es ist vor allem dem Verantwortlichen nicht möglich, die Einhaltung dieser Anforderungen auf privaten Geräten sicherzustellen und seiner datenschutzrechtlichen Verantwortung nachzukommen. Daher kann ein Einsatz privater Geräte auch mit ausdrücklichem Einverständnis der betroffenen Person nicht in Betracht kommen.

Was ist zu tun?

Daten aus Ausweispapieren sollten nicht durch einfaches Fotografieren oder Kopieren erhoben werden, da hierdurch in der Regel auch nicht für die Aufgabenerfüllung erforderliche Informationen erhoben und für eine gewisse Dauer gespeichert werden. Der Einsatz privater Geräte ist nicht geeignet, die Pflichten des Verantwortlichen zur Gewährleistung der Datensicherheit zu erfüllen. Die öffentliche Verwaltung muss dafür sorgen, dass private Geräte nicht für die Verarbeitung personenbezogener Daten eingesetzt werden.

4.5 Soziales

4.5.1 Kindeswohlgefährdung – Meldepflicht oder nur Meldebefugnis?

Ziel des Bundeskinderschutzgesetzes (BKiSchG) ist es, das Wohl von Kindern und Jugendlichen zu schützen und ihre körperliche, geistige und seelische Entwicklung zu fördern. Das Kinderschutzgesetz Schleswig-Holstein fordert, dass die Jugendämter in lokalen Netzwerken mit den freien Trägern der Jugendhilfe zusammenarbeiten. Kinderärzte, Berufspsychologen, Hebammen und Entbindungspfleger, Familien- oder Jugendberater, Sozialarbeiter und Sozialpädagogen, Lehrer usw. sind einzubinden. Diese Zusammenarbeit erfordert einen Datenaustausch zwischen den Beteiligten. Was müssen Angehörige von Berufsgruppen, die einer besonderen Schweigepflicht unterliegen, beachten?

§ 4 BKiSchG definiert ein gestuftes Verfahren. Liegen in einem konkreten Einzelfall den zuvor genannten Personen gewichtige Anhaltspunkte für eine Kindeswohlgefährdung vor („Gefährdungseinschätzung"), so sollen diese zunächst mit den Kindern oder Jugendlichen und, soweit erforderlich und möglich, mit den Sorgeberechtigten die Situation erörtern. Es soll auf die Inanspruchnahme von Hilfen, z. B. des zuständigen Jugendamtes, hingewirkt werden. Bei der Einschätzung der Kindeswohlgefährdung besteht gegenüber dem Jugendamt der gesetzliche Anspruch, dass „insoweit erfahrene Fachkräfte" (z. B. eines Kinderschutzzentrums) beraten. Für diese Beratung sind die Daten der Betroffenen vor der Übermittlung zu pseudonymisieren.

§ 8a SGB VIII sieht für die Jugendämter die Verpflichtung vor, in Vereinbarungen mit den freien Trägern der Jugendhilfe, die Leistungen der Jugendhilfe erbringen, sicherzustellen, dass deren Fachkräfte eine Gefährdungseinschätzung vornehmen, hierbei eine „insoweit erfahrene Fachkraft" hinzu- sowie das Kind bzw. den Jugendlichen und die Erziehungsberechtigten einbeziehen.

Kann die Kindeswohlgefährdung nicht abgewendet werden und ist ein Tätigwerden des Jugendamtes erforderlich, sind die benannten Personen auch ohne Einwilligung der Betroffenen befugt, deren Daten an das zuständige Jugendamt zu übermitteln. § 4 Abs. 3 BKiSchG stellt eine Befugnisnorm dar, beinhaltet jedoch keine Meldepflicht.

Meldepflichten ergeben sich aus § 47 SGB VIII für die Träger einer erlaubnispflichtigen Einrichtung. Diese müssen – auch ohne Einwilligung der Betroffenen – Ereignisse oder Entwicklungen, die geeignet sind, das Wohl der Kinder und Jugendlichen zu beeinträchtigen, der zuständigen Behörde anzeigen. Der Gesetzgeber beabsichtigt diese Meldepflicht auf die Träger einer Einrichtung der offenen Jugendarbeit, die keiner Erlaubnis bedarf, auszuweiten (so der aktuelle Entwurf eines Gesetzes zur Stärkung von Kindern und Jugendlichen).

Was ist zu tun?

Datenschutz verhindert keinen Kinderschutz! Berufsgruppen, die einer besonderen Schweigepflicht unterliegen, haben gegenüber dem Jugendamt einen Beratungsanspruch und können nach bestem Wissen und Gewissen entscheiden, das Jugendamt über die Erkenntnisse zu unterrichten, auch wenn die Betroffenen hiermit nicht einverstanden sind.

4.5.2 Heim- bzw. Telearbeit mit Sozialdaten möglich?

Sozialdaten sind personenbezogene Daten von Antragstellern bzw. Empfängern von Sozialleistungen und unterliegen dem Sozialgeheimnis. Jugendämter, Jobcenter oder Wohngeldbehörden müssen besondere Anforderungen des Sozialdatenschutzrechts beachten, wenn Sozialdaten im Rahmen von Heim- bzw. Telearbeit verarbeitet werden sollen.

Der Wunsch nach flexiblen Arbeitsbedingungen für die Beschäftigten macht auch vor Sozialbehörden nicht halt. Der Schutz der besonders sensiblen Sozialdaten darf aber nicht darunter leiden, wenn die Beschäftigten zu Hause Sozialdaten verarbeiten. Wichtige Punkte sind zu klären (Transport, Lagerung, Vernichtung der Daten, Einrichtung von Zutrittskontrollen, Schutz gegen Einsichtnahme durch Dritte, Verlust- und Diebstahlrisiko …).

Das ULD empfiehlt insbesondere Folgendes:

- Soweit möglich auf die Verarbeitung von Sozialdaten während der Heimarbeit zu verzichten und stattdessen die Heimarbeit auf die Bearbeitung von Unterlagen mit nicht personenbezogenen Daten zu beschränken.
- Eine rein elektronische Datenverarbeitung ist der Bearbeitung von Papierunterlagen vorzuziehen.
- Die Datenverarbeitung sollte über ein VPN auf einem dienstlichen System erfolgen.
- Das genutzte System ist mit einer verschlüsselten Festplatte zu versehen.
- Notwendig ist ein dienstliches Management mit dienstlicher Konfiguration des Systems inklusive Virenschutz.
- Erforderlich ist zudem die Überwachung des Sicherheitsstatus (Sicherheitspatches).
- Wenn möglich sollte vor Ort auf eine Druckmöglichkeit verzichtet werden.
- Wenn möglich besteht keine Speichermöglichkeit auf dem Endgerät (sondern in Dateiablagen/Terminalservices).

Was ist zu tun?

Bevor Sozialdaten im Rahmen von Heim- bzw. Telearbeit von Mitarbeitern zu Hause verarbeitet werden, sollten Alternativen geprüft werden. Eine elektronische Datenverarbeitung ist einer konventionellen Datenverarbeitung mit Papierakten vorzuziehen. Es müssen umfangreiche technische und organisatorische Maßnahmen zum Schutz der Sozialdaten getroffen und regelmäßig überprüft werden.

4.5.3 Übermittlung personenbezogener Daten von Pflegekräften durch die Pflegeberufekammer zum Zweck der Wahlwerbung

Im Zusammenhang mit der ersten Wahl zur Kammerversammlung der Pflegeberufekammer Schleswig-Holstein erreichten das ULD mehrere Anfragen. Mitglieder der Pflegeberufekammer seien im Vorfeld der Wahl von Bewerbern zum Zwecke der Wahlwerbung angeschrieben worden. Auf Anfrage von Bewerberinnen und Bewerbern eines gültigen Wahlvorschlages übermittelte die Pflegeberufekammer Anschriften der wahlberechtigten Pflegekräfte des jeweiligen Einzugsgebietes zum Zwecke der Wahlwerbung.

Pflegeberufekammer Schleswig-Holstein

Am 15. Juli 2015 beschloss der Schleswig-Holsteinische Landtag das Gesetz zur Errichtung einer Kammer für die Heilberufe in der Pflege (PflBerErG) und das Gesetz über die Kammer und die Berufsgerichtsbarkeit für die Heilberufe in der Pflege (Pflegeberufekammergesetz – PfBKG). Nach eigenen Angaben vertritt die in Form einer Körperschaft des öffentlichen Rechts organisierte Pflegeberufekammer die Belange von derzeit etwa 20.000 registrierten Pflegefachkräften. Mitglieder sind Gesundheits- und Krankenpfleger, Gesundheits- und Kinderkrankenpfleger und Altenpfleger. Freiwillige Mitgliedschaften sind für Assistenzberufe der Pflege und für Auszubildende möglich.

Die für die Zulässigkeit der Übermittlung personenbezogener Daten erforderliche Rechtsgrundlage fand sich in § 9 Abs. 8 der Landesverordnung über die Wahl zur Kammerversammlung der Pflegeberufekammer Schleswig-Holstein sowie die von der Kammerversammlung durchzuführenden Wahlen (Wahlverordnung der Pflegeberufekammer – PBKWVO) vom 14. März 2017 (GS Schl.-H. II, Gl.Nr. 2122-9-1) in Verbindung mit § 11 Abs. 1 Nr. 2 LDSG-alt (nach neuem Recht Art. 6 Abs. 1 Buchst. e DSGVO, § 3 Abs. 1 LDSG).

Eine weitere Zulässigkeitsvoraussetzung ist gemäß § 9 Abs. 8 Satz 1 PBKWVO, dass kein Widerspruch erfolgt ist. Im Rahmen des am 15. Dezember 2017 veröffentlichten Wahlausschreibens wurde ein hinreichender Hinweis auf das Widerspruchsrecht gemäß § 9 Abs. 8 PBKWVO erteilt. Anhaltspunkte für die Missachtung von gegenüber dem Wahlleiter erklärten Widersprüchen wurden dem ULD nicht bekannt.

In § 9 Abs. 8 Satz 1 PBKWVO wird eine eindeutige Zweckbindung für die Verarbeitung personenbezogener Daten festgelegt. Darüber hinaus definiert § 9 Abs. 8 Satz 3 PBKWVO eine klare Speicherbegrenzung, wonach die Bewerber eines gültigen Wahlvorschlages die erhaltenen Daten spätestens einen Monat nach Durchführung der Wahl löschen müssen.

Vor diesem Hintergrund war die gegenständliche, von der Pflegeberufekammer Schleswig-Holstein durchgeführte Datenübermittlung von Anschriften der Wahlberechtigten an Bewerberinnen und Bewerber eines gültigen Wahlvorschlages zum Zwecke der Wahlwerbung datenschutzaufsichtsrechtlich nicht zu beanstanden.

Was ist zu tun?

Die Bewerberinnen und Bewerber eines gültigen Wahlvorschlags, die eine Datenübermittlung angefordert haben, durften die Daten nur zum Zwecke der Wahlwerbung und längstens bis einen Monat nach Durchführung der Wahl verarbeiten. Sie sind insoweit selbst Verantwortliche im Sinne von § 4 Nr. 7 DSGVO mit eigenen Rechten und Pflichten. Falls noch nicht geschehen, müssen die Empfänger der Adresslisten unverzüglich die datenschutzkonforme Löschung der empfangenen personenbezogenen Daten veranlassen und dokumentieren.

4.5.4 Einsicht der Eltern in Akte der Schulsozialarbeiterin

Im Falle eines über 14 Jahre alten Jugendlichen begehrten die Eltern Einsicht in die Akte der Schulsozialarbeiterin. Die Akte enthielt Informationen, die die Sozialarbeiterin von dem Jugendlichen im Vertrauen erhalten hatte und die im Zusammenhang mit einer möglichen Kindeswohlgefährdung standen. Der Jugendliche war mit der Einsichtnahme durch die Eltern nicht einverstanden. Die Schulsozialarbeiterin wandte sich an das ULD mit der Frage, ob sie den Eltern Einsicht zu gewähren habe.

Die Sozialarbeiterin war von der Kommune (als Schulträger) für die Aufgabe der Schulsozialarbeit eingesetzt worden; bei der Schulsozialarbeit handelt es sich gemäß § 13 SGB VIII um eine Aufgabe der Jugendhilfe. Damit war die Frage nach den Vorschriften über den Datenschutz bei der Jugendhilfe (§§ 61 ff. SGB VIII) zu beantworten.

Die Daten, um die es bei der möglichen Akteneinsicht ging, waren der Sozialarbeiterin im Rahmen der Schulsozialarbeit anvertraut worden und fielen damit unter § 65 SGB VIII. Danach dürfen Sozialdaten, die Mitarbeitern z. B. im Rahmen der Schulsozialarbeit zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind, nur unter sehr eingeschränkten Bedingungen von diesen Mitarbeitern weitergegeben werden. Anders als normalerweise im Datenschutz ist hier die Mitarbeiterin oder der Mitarbeiter persönlich Adressat der Norm, nicht wie sonst die verantwortliche öffentliche Stelle.

Die Einsicht in die Akte kann gewährt werden, wenn nach § 65 Abs. 1 Nr. 1 SGB VIII die Einwilligung dessen, der die Daten anvertraut hatte, vorliegt. Hier stellte sich die Frage, auf wessen Einwilligung es ankommt, auf die des Jugendlichen oder die der Eltern.

Das ULD geht davon aus, dass Jugendliche ab dem Alter von 14 Jahren in der Regel die nötige Einsichtsfähigkeit haben, um selbst über die Ausübung ihres Grundrechts auf informationelle Selbstbestimmung zu verfügen. Sie können damit z. B. selbst datenschutzrechtlich relevante Einwilligungen abgeben. Diese Altersgrenze erscheint sachgerecht, da mit dem Alter von 14 Jahren die Strafmündigkeit und die Religionsmündigkeit einsetzen. Letztlich kommt es auf die Einschätzung der Urteilsfähigkeit des Jugendlichen im Einzelfall an.

Diese Auffassung wird durch eine ältere Entscheidung des Bundesverfassungsgerichts (1 BvR 845/79 vom 09.02.1982) gestützt. Das BVerfG hatte darüber zu entscheiden, ob das seinerzeitige Bremische Schulverwaltungsgesetz mit der darin enthaltenen Schweigepflicht von Schülerberatern gegenüber Erziehungsberechtigten mit dem Elternrecht aus Art. 6 Abs. 2 Grundgesetz vereinbar war. Das Gericht führte dazu aus: „Das Elternrecht dient als pflichtgebundenes Recht dem Wohle des Kindes; es muss seinem Wesen und Zweck nach zurücktreten, wenn das Kind ein Alter erreicht hat, in dem es eine genügende Reife zur selbständigen Beurteilung der Lebensverhältnisse (…) erlangt

hat. (…) Dabei hat für die Ausübung höchstpersönlicher Rechte der Grundsatz zu gelten, daß der zwar noch Unmündige, aber schon Urteilsfähige die ihm um seiner Persönlichkeit willen zustehenden Rechte eigenständig ausüben können soll."

Im Falle eines Konfliktes zwischen diesem Recht des Kindes und dem Elternrecht aus Art. 6 Abs. 2 Grundgesetz kann ein Schweigerecht der Berater gegenüber den Erziehungsberechtigten bestehen. Dies sei allerdings „auf die Ausnahmefälle begrenzt, in denen konkrete Tatsachen vorliegen, welche bei Information der Erziehungsberechtigten die unmittelbare und gegenwärtige Gefahr einer körperlichen oder seelischen Schädigung des Kindes wahrscheinlich machen". Diese Aspekte mussten auch in die Entscheidung einfließen, ob es bei der Einwilligung nach § 65 Abs. 1 Nr. 1 SGB VIII auf die des Jugendlichen oder die der Eltern ankommt. Die im Fall vorliegenden Hinweise auf eine Kindeswohlgefährdung sprachen dafür, nur auf die Einwilligung des Jugendlichen abzustellen.

Zum gleichen Ergebnis kommt man im Hinblick auf eine zusätzlich eventuell bestehende berufliche Schweigepflicht nach § 203 StGB (z. B. für staatlich anerkannte Sozialpädagog(inn)en oder Sozialarbeiter(innen)).

In der Folge standen den Eltern auch andere Einsichts- und Auskunftsrechte nicht zu. Das Recht zur Akteneinsicht in einem Verwaltungsverfahren nach § 25 SGB X schied aus, weil kein Verwaltungsverfahren im Sinne des Gesetzes eröffnet worden war. Außerhalb eines Verwaltungsverfahrens ist der Anspruch auf Akteneinsicht nach pflichtgemäßem Ermessen zu entscheiden und schied hier im Hinblick auf § 25 Abs. 3 SGB X in Verbindung mit § 65 SGB VIII aus, da wegen der berechtigten Interessen der beratenen Person und auch der anderen in diesem Zusammenhang in den Aufzeichnungen erwähnten Personen die Vorgänge geheim gehalten werden mussten.

Auch ein datenschutzrechtlicher Auskunftsanspruch der Eltern nach Artikel 15 DSGVO, darauf gerichtet zu erfahren, welche Daten in der Akte über sie gespeichert sind, schied aus. Denn nach § 83 SGB X besteht das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 DSGVO nicht, soweit die betroffene Person nach § 82a Abs. 1, 4 und 5 SGB X nicht zu informieren ist. Nach § 82a Abs. 1 Nr. 2 SGB X entfällt die Informationspflicht, soweit die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Dies ist, wie oben dargestellt, im Hinblick auf die strenge Schweigeverpflichtung nach § 65 SGB VIII der Fall.

Eine Weitergabe der Akteninhalte an die Eltern darf also nur erfolgen, wenn die Einwilligung des Jugendlichen vorliegt. Dabei ist darauf zu achten, dass es sich tatsächlich um eine freiwillig abgegebene Einwilligung handelt, die den Anforderungen von Art. 7 Abs. 4 DSGVO genügt.

Dabei hätte die Einwilligung des Jugendlichen allerdings die Weitergabe an die Eltern nur erlaubt, eine entsprechende Pflicht bestand dagegen nicht. Dies ergibt sich aus § 64 Abs. 2 SGB VIII, wonach eine Übermittlung für die Erfüllung von Aufgaben nach § 69 SGB X (…) nur zulässig ist, soweit dadurch der Erfolg einer zu gewährenden Leistung nicht infrage gestellt wird. Dieser Rechtsgedanke lässt sich auf den vorliegenden Fall übertragen. Daher sollte auch bei Einwilligung durch den Jugendlichen keine Weitergabe der Informationen aus der Akte an die Eltern erfolgen, wenn dadurch die Leistung (also der Erfolg der bisher erbrachten Beratung) infrage gestellt würde.

Was ist zu tun?

Besteht eine Verschwiegenheitspflicht aus dem Jugendhilferecht oder aus beruflichen Schweigepflichten im Hinblick auf Informationen über Minderjährige, so kann es zu Konflikten darüber kommen, wer in die Durchbrechung der Schweigepflicht einwilligen darf: der Jugendliche oder der Sorgeberechtigte. Dies ist anhand der oben dargelegten Vorgaben zu prüfen.

4.5.5 Nutzung von Sozialdaten zu Zwecken der Organisationsuntersuchung

In einer Kreisverwaltung sollte eine Organisationsuntersuchung im Jugendamt und Sozialamt stattfinden. Dabei sollten durch einen externen Dienstleister auch Fallakten ausgewertet werden. Die beauftragte Firma sah dabei kein datenschutzrechtliches Problem: Ihre Mitarbeitenden unterlägen als Rechtsanwälte oder Wirtschaftsprüfer einer Schweigepflicht. Auch werde bei der Sichtung der Akten lediglich die Struktur des Vorganges untersucht und keinesfalls personenbezogene Daten erhoben.

Das ULD hat dazu festgestellt, dass es bei der Aktenauswertung zu Zwecken einer Organisationsuntersuchung durchaus zu einer Verarbeitung der in den Akten gespeicherten personenbezogenen Daten kommt. Nach der DSGVO gehört zur Verarbeitung jede Verwendung der Daten und damit auch die Auswertung der Daten im Hinblick auf die Struktur der Fallbearbeitung, auch wenn die Daten aus den Fallakten nicht auf andere Datenträger übertragen werden.

Die fraglichen Daten waren ursprünglich zur Erfüllung der Aufgaben des Jugend- und Sozialamtes erhoben worden und sollten nun für eine Organisationsuntersuchung genutzt werden. Diese Nutzung der Daten beinhaltet eine Zweckänderung im Vergleich zum Ausgangszweck.

Es war davon auszugehen, dass die fraglichen Daten zum großen Teil, wenn nicht in Gänze, unter das Sozialgeheimnis (§ 35 SGB I) fallen. Damit kommen die Datenschutzvorschriften der §§ 67 ff. SGB X ergänzend zur DSGVO zur Anwendung. Nach § 67c Abs. 3 SGB X ist eine Speicherung, Veränderung oder Nutzung von Sozialdaten zulässig, wenn dies für die Wahrnehmung von Aufsichts-, Kontroll- und Disziplinarbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für den Verantwortlichen erforderlich ist. Damit stellt das Sozialdatenschutzrecht eine spezielle Rechtsgrundlage zur Verfügung, die die Nutzung von Sozialdaten für Zwecke der Organisationsuntersuchung erlaubt.

Dies gilt auch für Daten im Bereich der Jugendhilfe. Zwar finden sich hier bestimmte spezielle Vorschriften zum Sozialdatenschutz in den §§ 61 ff. SGB VIII. Diese Vorschriften schließen jedoch die Anwendung von § 67c SGB X nicht aus.

Etwas anderes gilt lediglich bei Sozialdaten, die Mitarbeitenden eines Trägers der öffentlichen Jugendhilfe zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind (§ 65 SGB VIII). Hier besteht ein verstärkter Vertrauensschutz: Die von dieser Vorschrift erfassten Informationen dürfen nicht in die Organisationsuntersuchung einbezogen werden, falls es nicht gelingt, die Daten aus diesen Akten zu anonymisieren oder die Einwilligung der Betroffenen einzuholen. Beides darf nur durch die zur Geheimhaltung verpflichteten Mitarbeiter selbst geschehen.

In Übereinstimmung mit der einschlägigen datenschutzrechtlichen Literatur geht das ULD davon aus, dass die Organisationsuntersuchung auch von externen Unternehmen durchgeführt werden darf. Als Teil der notwendigen technisch-organisatorischen Maßnahmen sollten

dabei Verschwiegenheitsverpflichtungen der bei der Untersuchung eingesetzten Mitarbeiter des externen Unternehmens unterzeichnet werden. Weiterhin sollte sich das Unternehmen zur Einhaltung geeigneter Maßnahmen verpflichten, wie z. B. der unverzüglichen Löschung oder Rückgabe von Daten nach Abschluss der Untersuchung.

Was ist zu tun?

Grundsätzlich ist es in den meisten Fällen zulässig, in Verfahrensakten enthaltene Daten für Zwecke der Organisationsuntersuchung auch durch Externe zu nutzen. Dabei sind geeignete technisch-organisatorische Maßnahmen festzulegen.

4.6 Schutz des Patientengeheimnisses

4.6.1 Die neue DSGVO – so können Heilberufler die Vorgaben umsetzen

Das ULD hat unter

https://uldsh.de/dsgvo-aerzte

einen ausführlichen Informationsbeitrag veröffentlicht. Folgende zentrale Punkte müssen bekannt sein und beachtet werden:

Wer ist Verantwortlicher?

Die Betreiberin oder der Betreiber der Praxis, Apotheke usw. ist die oder der Verantwortliche im Sinne der Rechtsvorschriften. Ihr bzw. ihm obliegt die „Rechenschaftspflicht".

Was sind die Rechtsgrundlagen für die Verarbeitung von Patientendaten?

Werden personenbezogene Daten (Patientendaten) zum Zwecke der Gesundheitsversorgung verarbeitet, ist regelhaft der (Behandlungs-)Vertrag die Rechtsgrundlage (siehe Art. 9 Abs. 2 Buchst. h DSGVO und § 22 Abs. 1 Nr. 1 Buchst. b BDSG). Zusätzliche Dienste, wie z. B. ein Recall-Service, erfordern eine gesonderte Einwilligung des Betroffenen.

Muss ein Datenschutzbeauftragter benannt werden?

Ein Datenschutzbeauftragter ist in jedem Fall zu benennen, wenn in der Regel mindestens zehn Personen ständig, d. h. nicht nur gelegentlich, mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Hierzu gehören auch die Heilberufler selbst, Verwaltungskräfte und Teilzeitbeschäftigte.

Wie erfülle ich die Informationspflichten?

Werden zum ersten Mal, z. B. von einer Patientin oder einem Patienten, Daten in einer Arztpraxis erhoben, so hat diese oder dieser Anspruch darauf, dass ihr oder ihm von dem Verantwortlichen die in Artikel 13 DSGVO benannten Informationen mitgeteilt werden. Der Verantwortliche muss die Erfüllung seiner Informationspflicht nachweisen können. Wir empfehlen, neuen Patientinnen oder Patienten einen Flyer bzw. Handzettel (Datenschutz-Steckbrief) auszuhändigen. Muss die Patientin oder der Patient bei ihrer oder seiner ersten Vorsprache einen Anamnesebogen ausfüllen, kann in diesem ein entsprechender Hinweis aufgenommen werden. Es ist nicht zwingend erforderlich, dass die Patientin oder der Patient die Aushändigung mit ihrer oder seiner Unterschrift bestätigt, wenn z. B. das Praxissystem vorsieht, dass die Mitarbeiterin oder der Mitarbeiter die Aushändigung zwingend vermerkt.

Muss ein Verzeichnis der Verarbeitungstätigkeiten erstellt werden?

Ja! Das Verzeichnis der Verarbeitungstätigkeiten umfasst sowohl konventionelle als auch automatisierte Verarbeitungstätigkeiten und stellt einen wichtigen Bestandteil der Dokumentationspflicht des Verantwortlichen dar. Das ULD hat unter

https://www.datenschutzzentrum.de/dsgvo

Vorlagen veröffentlicht.

Muss eine Datenschutz-Folgenabschätzung durchgeführt werden?

Eine Datenschutz-Folgenabschätzung ist u. a. erforderlich, wenn Gesundheitsdaten in großem Maßstab verarbeitet werden. Dies dürfte insbesondere dann der Fall sein, wenn mindestens zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, also immer dann, wenn auch ein Datenschutzbeauftragter zu benennen ist.

Weitere Pflichten:

- Festlegung von Aufbewahrungsfristen für personenbezogene Daten und die fristgerechte Löschung von personenbezogenen Daten,
- technische und organisatorische Maßnahmen treffen, damit Unbefugte keinen Zugang zu den Daten haben,
- Abschluss von Verträgen mit Dienstleistern, wenn diese Daten im Auftrag für die Praxis verarbeiten (z. B. mit IT oder Aktenvernichtungsunternehmen usw.),
- Beachtung der Datenschutzrechte der Patienten,
- Meldung von Datenschutzverletzungen bzw. Datenpannen.

Wir empfehlen unseren aktuellen für Arzt- und Zahnarztpraxen entwickelten „Selbst-Check":

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

4.6.2 Patientendaten nach zehn Jahren löschen?

Das weiß doch jeder: Ärzte müssen Patientenunterlagen zehn Jahre lang aufbewahren. Stimmt das wirklich, und wenn ja, bedeutet dies, dass die Patientendaten nach Ablauf der zehn Jahre zwingend gelöscht werden müssen?

Ein Arzt hat nicht nur das Recht, sondern auch die Pflicht, die Behandlung eines Patienten zu dokumentieren. Entsprechende Vorgaben finden sich nicht nur im Art. 9 Abs. 2 Buchst. h DSGVO bzw. § 22 Abs. 1 Nr. 1 Buchst. b BDSG, sondern auch im § 630f Abs. 1 BGB und § 10 der Berufsordnung der Ärztekammer Schleswig-Holstein.

Art. 17 Abs. 1 Buchst. a DSGVO definiert auch für Patienten das „Recht auf Vergessenwerden". Personenbezogene Daten sind unverzüglich zu löschen, sofern diese für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind. Dennoch darf die Patientendokumentation nicht sofort nach Behandlungsende vernichtet werden.

Die Patientendokumentation muss aufbewahrt werden, wenn dies zur Erfüllung einer rechtlichen Pflicht erforderlich ist (Art. 17 Abs. 3 Buchst. b DSGVO) oder einer Löschung satzungsgemäße oder vertragliche Aufbewahrungsfristen entgegenstehen (§ 35 Abs. 3 BDSG).

Aus § 630f Abs. 3 BGB bzw. § 10 Abs. 3 der Berufsordnung der Ärztekammer Schleswig-Holstein ergibt sich die Pflicht zur Aufbewahrung der Patientendokumentation für einen Zeitraum von mindestens zehn Jahren nach Abschluss der Behandlung.

Ein Verstoß gegen diese Dokumentations- und Aufbewahrungspflicht kann nach § 630f BGB zu einer Beweislastumkehr führen. Hat der Behandelnde eine medizinisch gebotene wesentliche Maßnahme und ihr Ergebnis entgegen § 630f Abs. 1 oder Abs. 2 BGB nicht in der Patientenakte aufgezeichnet oder hat er die Patientenakte entgegen § 630f Abs. 3 BGB nicht aufbewahrt, so wird vermutet, dass er diese Maßnahme

nicht getroffen hat (§ 630h Abs. 3 BGB). Eine unterlassene oder lückenhafte Dokumentation einer aus medizinischer Sicht zu dokumentierenden Maßnahme führt jedoch zunächst nur zu der Vermutung, dass die Maßnahme unterblieben ist. Der Bundesgerichtshof ging in der Vergangenheit davon aus, dass dennoch im Grundsatz die Beweislast bei dem Patienten liegt. Er oder sie muss den Schaden, eine Fehlbehandlung und die Kausalität der Fehlbehandlung für den Schaden beweisen. Zu einer Beweislastumkehr (d. h., der Arzt muss nachweisen, dass kein Fehler vorlag) kann es nur kommen, wenn eine gänzlich unterlassene oder unvollständige Dokumentation einen groben Behandlungsfehler oder das Unterlassen einer Diagnostik mit behandlungspflichtigem Ergebnis indiziert.

Ist die Zehnjahresfrist erfüllt, sollte geprüft werden, ob die Unterlagen vernichtet werden können. Allerdings gibt es für bestimmte Patientenunterlagen längere Fristen. So sieht z. B. die Strahlenschutzverordnung Aufbewahrungsfristen von 30 Jahren vor.

§ 199 Abs. 2 BGB sieht vor, dass Schadensersatzansprüche, die auf der Verletzung des Lebens, des Körpers oder der Gesundheit beruhen, ohne Rücksicht auf ihre Entstehung und die Unkenntnis oder grob fahrlässige Kenntnis in 30 Jahren von der Begehung der Handlung, der Pflichtverletzung oder dem sonstigen, dem Schaden auslösenden Ereignis an verjähren. Nach unserer Kenntnis werden daher insbesondere im stationären Bereich Patientenunterlagen in der Regel 30 Jahre lang aufbewahrt. Zwar stellt diese lange Aufbewahrung von Patientenunterlagen im Hinblick auf § 199 Abs. 2 BGB nicht zwangsläufig einen Datenschutzverstoß dar. Es gilt jedoch zu beachten, dass nach Ablauf der in § 630f Abs. 3 BGB definierten Zehnjahresfrist die zuvor dargestellte Beweislastumkehr nicht mehr greift. Wenn also nach Ablauf der Zehnjahresfrist keine Unterlagen mehr vorhanden sind, muss der Patient den Beweis für den Schaden, die Fehlbehandlung und Kausalität erbringen. Solange noch Unterlagen vorhanden sind, hat der Patient nach § 630g BGB das Recht auf Einsicht und Kopien und kann diese auch vor Gericht verwerten. Sind keine Unterlagen mehr vorhanden, so läuft dieser Anspruch naturgemäß ins Leere.

Vor diesem Hintergrund hat das ULD in der Vergangenheit die Aufbewahrungsfrist von zehn Jahren regelhaft für geboten, aber auch für hinreichend erachtet.

4.6.3 Neu – Auftragsverarbeitung ohne Einwilligung der Patienten möglich!

IT-Systemadministration, Aktenvernichtung – manche Aufgaben können externe Dienstleister kompetent übernehmen. Damit jedoch ein externer Dienstleister mit der Verarbeitung personenbezogener Daten (Auftragsverarbeitung) beauftragt werden darf, bedarf es zunächst eines schriftlichen Vertrages zwischen Auftraggeber und Auftragnehmer. Artikel 28 DSGVO gibt dezidiert vor, welche Inhalte dieser Vertrag haben muss.

Ärzte, Apotheker und andere Berufsgruppen, die einer besonderen berufsrechtlichen Schweigepflicht unterliegen, benötigten bislang zudem die schriftliche Einwilligung (Schweigepflichtentbindungserklärung) der Patienten, um deren Gesundheitsdaten durch Dienstleister verarbeiten zu lassen. Dies ist seit November 2017 durch eine Änderung im § 203 Abs. 3 Satz 2 Strafgesetzbuch (StGB) nicht mehr erforderlich.

Heilberufler usw. dürfen seitdem ihren Dienstleistern bzw. den dort tätigen Personen („mitwirkenden Personen“) Patientendaten offenbaren, soweit dies für die Erbringung der Dienstleistung erforderlich ist. Allerdings muss der Auftraggeber Sorge dafür tragen, dass sein Dienstleister und die dort tätigen Personen zur Geheimhaltung verpflichtet werden.

4.6.4 Übermittlung von Patientendaten von Kurkliniken an die Gemeinde?

In einem Erholungsort in Schleswig-Holstein hatte die Kommune unter Hinweis auf die Kurabgabesatzung von ortsansässigen Kliniken verlangt, den Namen der dort untergebrachten Patienten und die Dauer des Aufenthalts zu übermitteln. Auf dieser Grundlage wollte die Kommune dann einen Kurabgabebescheid erstellen. Die Kliniken sollten sodann die Kurabgabe bei den Patienten erheben und an die Kommune abführen. Die Kliniken hielten dieses Vorgehen für unvereinbar mit der ärztlichen Schweigepflicht und wandten sich an das ULD.

Auf Nachfrage des ULD verwies die Kommune auf § 10 Abs. 4 Kommunalabgabengesetz (KAG) als Rechtsgrundlage für ihr Vorgehen. Danach dürfen Kommunen diejenigen, die Personen beherbergen, dazu verpflichten, die beherbergten Personen zu melden und die Kurabgabe einzuziehen und abzuführen. Dies gelte auch für Kliniken. Die vom ULD vorgeschlagene anonymisierte Datenübermittlung könne der vorgesehenen Meldepflicht nicht gerecht werden, da nur unter Angabe der geforderten Daten die Angaben nachgeprüft und ein Kurabgabebescheid erlassen werden könne.

Nach Auffassung des ULD war schon zweifelhaft, ob die Kliniken überhaupt unter die Meldepflicht des KAG bzw. der kommunalen Satzung fallen. Die Meldepflicht trifft diejenigen, die Personen beherbergen oder ihnen Wohnraum zu Erholungszwecken überlassen. Bereits bauplanungsrechtlich unterscheidet sich das „Beherbergen" von der „Unterbringung". Kliniken oder Krankenhäuser werden nicht als Betriebe des Beherbergungsgewerbes aufgefasst. Selbst Erholungsheime gehören nur dann zu den Beherbergungsbetrieben, wenn diese der Unterbringung im Urlaub und nicht der Heilbehandlung dienen.

Noch deutlicher wird die Unterscheidung mit Blick auf Abschnitt 4 des Bundesmeldegesetzes (BMG). Das BMG unterscheidet zwischen der besonderen Meldepflicht in Beherbergungsstätten und der besonderen Meldepflicht in Krankenhäusern, Heimen und ähnlichen Einrichtungen. Beherbergungsstätten sind in § 29 Abs. 1 BMG definiert als „Einrichtungen, die der gewerbs- oder geschäftsmäßigen Aufnahme von Personen dienen". Aus der Systematik ergibt sich, dass damit Krankenhäuser gerade nicht erfasst sind. Nur für die Meldepflicht in Beherbergungsstätten („Hotelmeldepflicht") erlaubt das BMG, dass durch Landesrecht bestimmt werden kann, dass für die Erhebung von Fremdenverkehrs- und Kurbeiträgen weitere Daten auf dem Meldeschein erhoben werden dürfen (§ 30 Abs. 3 BMG). Eine vergleichbare Regelung findet sich zur Meldepflicht in Krankenhäusern gerade nicht. Eine Auslegung des KAG und der kommunalen Satzung, wonach auch Krankenhäuser der Meldepflicht zum Zwecke der Erhebung der Kurabgabe nachzukommen haben, verstößt daher gegen höherrangiges Bundesrecht.

In jedem Fall erwächst das Verbot für die Kommunen, Patientendaten bei der Klinik zu erheben, aus § 203 Abs. 1 Strafgesetzbuch („ärztliche Schweigepflicht") in Verbindung mit §§ 102 Abs. 1 Nr. 3, 104 Abs. 1 der Abgabenordnung (die Vorschriften der Abgabenordnung gelten ergänzend zum KAG). Danach kann ein Berufsgeheimnisträger die Vorlage von Unterlagen über das, was ihm in dieser Eigenschaft anvertraut worden oder bekannt geworden ist, im Steuerverfahren verweigern. Offenbart er gleichwohl solche Unterlagen, macht er sich strafbar. Der Bundesfinanzhof hat dazu festgehalten, dass ein Berufsgeheimnisträger alle mandantenbezogenen Informationen zurückhalten darf, auch wenn es in dem Verfahren um seine eigenen steuerlichen Belange geht. Der Kommune steht im Verfahren zur Erhebung der Kurabgaben also keine Befugnis zur Erhebung von Daten zu, die unter die ärztliche Schweigepflicht fallen.

Zu den durch die ärztliche Schweigepflicht geschützten Informationen gehören nicht erst detaillierte Angaben zu Diagnose und Behandlung. Bereits die Information über das bloße Bestehen des Patientenverhältnisses ist von der Schweigepflicht umfasst. Damit scheidet schon die Übermittlung der Namen der Patienten aus.

Was ist zu tun?

Die ärztliche Schweigepflicht bietet einen starken Schutz. Sie kann von den Gemeinden in der Regel auch im Zusammenhang mit der Erhebung von Kurabgaben nicht durchbrochen werden.

4.7 Wissenschaft und Bildung

4.7.1 Neue Rolle des ULD – primär Aufsichtsbehörde statt Direktberatung aller öffentlichen Schulen

Mit der neuen Datenschutz-Grundverordnung änderten sich auch die Aufgaben des ULD. Nahm vorher die Beratung von öffentlichen Schulen und Bildungszentren einen großen Raum ein, so ließ sich das nach dem 25. Mai 2018 nicht mehr im ausreichenden Maße aufrechterhalten. Insbesondere führte die DSGVO dazu, dass in Schleswig-Holstein alle öffentlichen Stellen eigene Datenschutzbeauftragte haben mussten, die zuvörderst die Beratung der Stellen in Datenschutzfragen übernehmen sollen. Für sämtliche öffentlichen Schulen wurde ein Datenschutzbeauftragter bestellt, der durch ein Kompetenzteam im Bildungsministerium unterstützt wird.

Somit ist nunmehr der „Datenschutzbeauftragte Schulen und IQSH" für die Beratung der Schulen zuständig. Er ist über die E-Mail-Adresse: DatenschutzbeauftragterSchule@bimi.landsh.de (Telefon: 0431 988-2452) erreichbar. Das ULD bleibt natürlich für die Aufsicht über die Schulen zuständig.

Dabei findet eine regelmäßige Abstimmung zwischen dem Datenschutzbeauftragten für die Schulen und uns statt. Auch wird er die beliebte FAQ zu aktuellen Datenschutzfragen rund um den Schulbereich vom ULD übernehmen und weiter pflegen.

Was ist zu tun?

Es ist weiterhin eine enge Zusammenarbeit zwischen ULD und dem Datenschutzbeauftragten für die Schulen aufrechtzuerhalten.

4.7.2 Einheitliche Schulverwaltungssoftware (SWESH) und Schulportal SH

Das Ministerium für Bildung, Wissenschaft und Kultur (MBWK) plant, eine einheitliche Schulverwaltungssoftware (SWESH) an allen öffentlichen Schulen in Schleswig-Holstein einzuführen. Schulverwaltungsprozesse sollen damit landeseinheitlich und schulübergreifend gestaltet werden. Es soll so einfacher werden, Schülerstammdaten bei einem Schulwechsel weiterzugeben, Zeugnisformulare würden standardisiert, eine zentrale Plattform für die Noteneingabe würde bereitgestellt, und die Stunden- und Vertretungsplansoftware würde vereinheitlicht.

Des Weiteren soll mit dem sogenannten Schulportal SH eine webbasierte und datenschutzkonforme digitale Bildungsplattform aufgebaut werden. Langfristig sollen Lehrkräfte sowie Schülerinnen und Schüler im Portal arbeiten und miteinander kommunizieren können. Für die elektronische Kommunikation mit Lehrkräften soll außerdem eine dienstliche E-Mail-Adresse bereitgestellt werden. Es besteht für die Lehrkräfte dann keine Veranlassung mehr, private E-Mail-Adressen zu benutzen, die oftmals den datenschutzrechtlichen Anforderungen nicht genügen.

Über eine zentrale Benutzerverwaltung soll sichergestellt werden, dass nur ein berechtigter Nutzerkreis Zugriff auf das Portal erhält. Das hierfür erforderliche Identitätsmanagement soll vom Land selbst zentral betrieben werden, um die Hoheit über die sensiblen Benutzerdaten zu sichern.

Ferner soll das Schulportal mit bestehenden Diensten des Landes (z. B. SchulCommSy als virtuelles Lehrerzimmer oder der Bildungsmediathek) sowie weiteren externen Angeboten (z. B. von Schulverlagen) verknüpft werden.

Das Schulportal soll nach Vorstellung des MBWK als sogenannte Bildungscloud drei wesentliche Funktionen erfüllen:

- den Zugang zu digitalen Bildungsmedien (z. B. digitale Schulbücher, Bildungsmediatheken, freie Bildungsmaterialien als Open Education Ressources (OER)),
- die Bereitstellung von digitalen Werkzeugen (u. a. E-Mail für Lehrkräfte, Online-Office für das geräteunabhängige Arbeiten, Messenger-Dienste) und
- die Möglichkeit zur Digitalisierung von Unterricht (Lernmanagementsysteme).

Das ULD wird zusammen mit dem zentralen Datenschutzbeauftragten des MBWK für die öffentlichen Schulen und dessen Team an der Ausgestaltung und Umsetzung dieser Angebote beratend mitwirken.

4.8 Steuerverwaltung

4.8.1 Änderung der datenschutzrechtlichen Aufsicht über Finanzbehörden

Die Änderung der Abgabenordnung (AO) durch Artikel 6 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) hat zu einer Neuregelung der datenschutzrechtlichen Aufsicht über die Finanzbehörden geführt. Gemäß § 32h Abs. 1 AO obliegt die diesbezügliche aufsichtsrechtliche Zuständigkeit nunmehr dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), sofern die Verarbeitung personenbezogener Daten im Anwendungsbereich der Abgabenordnung erfolgt.

Neben den Steuern oder Steuervergütungen, die durch Bundesrecht oder Recht der Europäischen Union geregelt sind (und sofern diese durch Bundesfinanzbehörden oder durch Landesfinanzbehörden verarbeitet werden), gilt die Zuständigkeit des BfDI auch für die Datenverarbeitung zur Erhebung von Realsteuern (Grundsteuer, Gewerbesteuer), soweit ihre Verwaltung den Gemeinden übertragen worden ist (§ 1 Abs. 2 Nr. 1 AO).

Bei der Landesbeauftragten für Datenschutz Schleswig-Holstein verbleibt jedoch die aufsichtsrechtliche Zuständigkeit über die Finanzbehörden des Landes, sofern diese personenbezogene Daten verarbeiten

- zur Erhebung landesrechtlicher oder kommunaler Steuergesetze (z. B. Hundesteuersatzung, Kurabgabesatzung, Zweitwohnungssteuersatzung usw.) oder
- über die eigenen Beschäftigten der Steuerverwaltung in anderen als den Bundesbehörden (Personaldatenschutz).

Datenschutzprüfungen bei den Finanzbehörden in Schleswig-Holstein können von BfDI und ULD in ihren jeweiligen Zuständigkeitsbereichen getrennt oder zusammen vorgenommen werden.

Was ist zu tun?

Beschwerden über die Verarbeitung personenbezogener Daten durch Finanzbehörden im Anwendungsbereich der Abgabenordnung (z. B. im Zusammenhang mit der Abgabe der Einkommensteuererklärung) müssen an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gerichtet werden.

4.8.2 Überarbeitungsbedarf kommunaler Abgabensatzungen

Ein Überarbeitungsbedarf kommunaler Satzungen besteht bereits vor dem Hintergrund, dass seit dem 25. Mai 2018 infolge der direkten Geltung der DSGVO und der Neufassung des LDSG eine Vielzahl der in den datenschutzrechtlichen Klauseln zitierten Normen des LDSG-alt nicht mehr zur korrekten Fundstelle führen wird.

Darüber hinaus fällt bei der Prüfung datenschutzrechtlicher Regelungen in kommunalen Abgabensatzungen immer wieder auf, dass die Klauseln zur Verarbeitung personenbezogener Daten oft zu unbestimmt formuliert sind. Nicht selten werden Klauseln aus teils veralteten Mustersatzungen übernommen, ohne dass diese auf die konkrete, in der Gemeinde geplante Datenverarbeitung angepasst werden. Teilweise ist dann der Zweck der Verarbeitung nicht klar genug bestimmt. Auch ist oft der Umfang der Verarbeitungstätigkeit zu allgemein beschrieben und damit zu weit gefasst. Viele Satzungen enthalten lediglich eine Vielzahl von Erhebungsbefugnissen, jedoch keine klaren Löschfristen. Die Grundsätze des Art. 5 Abs. 1 DSGVO werden auf diese Weise nicht gewahrt.

Sollen für die Erhebung kommunaler Abgaben besondere Kategorien personenbezogener Daten verarbeitet werden, sind außerdem die Vorgaben des Artikels 9 DSGVO und des § 12 LDSG zu beachten. Danach ist die Verarbeitung dieser Daten grundsätzlich untersagt, sofern sie nicht auf Grundlage des Rechts eines Mitgliedstaates („das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht“) aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist.

Im Bereich des kommunalen Abgabenrechts ist daher zu prüfen, ob besondere Kategorien personenbezogener Daten verarbeitet werden sollen. Dies wäre z. B. der Fall, wenn zur Berechnung einer Kurabgabe Angaben über den Grad einer Behinderung (Gesundheitsdaten) vom Steuerschuldner erfragt würden. In diesen Fällen muss die Satzung eine entsprechende, hinreichend bestimmte Rechtsgrundlage enthalten.

Ist keine hinreichende Rechtsgrundlage enthalten oder werden weitere Grundsätze des Art. 5 Abs. 1 DSGVO nicht eingehalten, liegt ein Verstoß gegen die DSGVO vor, der die Aufsichtsbehörden zu Maßnahmen nach Artikel 58 DSGVO befugt.

Was ist zu tun?

Verantwortliche müssen prüfen, ob bei der Erhebung kommunaler Abgaben besondere Kategorien personenbezogener Daten verarbeitet werden und ob die in ihren Satzungen enthaltenen Regelungen hinreichend bestimmt sind. Zudem ist zu prüfen, ob Verweise auf das LDSG-alt nunmehr auf die entsprechende Regelung der DSGVO oder des LDSG-neu umzuschreiben sind. Bei der Evaluation der Satzungen ist die oder der behördliche Datenschutzbeauftragte einzubeziehen.

4.8.3 Anforderung von Auszügen der Steuererklärung bei der Zweitwohnungssteuer

Im Rahmen zweier Beschwerden wurde das ULD darauf aufmerksam gemacht, dass bei der Erhebung der Zweitwohnungssteuer von Steuerpflichtigen verlangt wurde, die Anlage V zur Einkommensteuererklärung als Nachweis für die Dauervermietung zu erbringen. Auf diese Weise sollte nachgewiesen werden, dass die Zweitwohnung nicht zur persönlichen Lebensführung vorgehalten wurde, sondern als (steuerbefreite) Kapitalanlage dem Eigentümer im Erhebungszeitraum nicht zur freien Verfügung stand.

Aufgrund des steuerrechtlichen Amtsermittlungsgrundsatzes sind Finanzbehörden zunächst gehalten, alle für die Besteuerung notwendigen – einschließlich der für die Steuerpflichtigen positiven – Umstände von Amts wegen zu ermitteln. Hierbei können sie im Rahmen der Kooperationsmaxime auch die Steuerpflichtigen zur Mitwirkung verpflichten.

Die Erhebung und weitere Verarbeitung personenbezogener Daten stellt jedoch zugleich einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Steuerpflichtigen dar. Aus diesem Grund muss sich die Amtsermittlungspflicht in den Grenzen der Verhältnismäßigkeit bewegen. Die Ermittlungen müssen nach pflichtgemäßem Ermessen – auch hinsichtlich der Beweismittel – geführt werden. Jede Datenerhebung ist daraufhin zu überprüfen, ob sie verhältnismäßig, d. h. geeignet, erforderlich und angemessen ist.

Nach Ansicht des ULD bestehen bereits Zweifel daran, ob die Anforderung der Anlage V der Einkommensteuererklärung überhaupt geeignet ist, den Nachweis darüber zu führen, dass bzw. in welche Höhe Mieteinnahmen durch die Steuerpflichtigen erzielt wurden. Denn es ist alleine aus der Anlage heraus noch nicht ersichtlich, dass sie überhaupt beim Finanzamt in dieser Form eingereicht wurde. Ohne die Gegenprüfung durch das zuständige Finanzamt kann die Richtigkeit des Dokuments nicht festgestellt werden. Der Anlage zur Steuererklärung kommt daher im Zweifel kein größerer Beweiswert zu als jeder anderen Erklärung der Steuerpflichtigen auch.

Des Weiteren bestehen erhebliche Zweifel daran, ob die Anforderung der Anlage V zur Einkommensteuererklärung erforderlich ist, um ihren angestrebten Zweck – den Nachweis einer Dauervermietung der Zweitwohnung – zu erreichen. Die Erforderlichkeit in diesem Sinne ist dann nicht gegeben, wenn die begehrte Information lediglich dienlich oder förderlich, nicht aber unbedingt notwendig zur Zweckerreichung ist. In der Regel wird der Nachweis einer Dauervermietung auch durch mildere Mittel erbracht werden können, beispielsweise durch die Vorlage von (gegebenenfalls teilgeschwärzten) Auszügen aus einem Dauermietvertrag. Die Anlage V zur Einkommensteuererklärung enthält dagegen eine Vielzahl weiterer personenbezogener Daten (z. B. die Angabe von Werbungskosten), die für den Nachweis der Dauervermietung allenfalls Indizien darstellen.

Erhebt ein Verantwortlicher eine Vielzahl von personenbezogenen Daten, die nicht erforderlich für die Erreichung des in der einschlägigen Rechtsgrundlage beschriebenen Zweckes sind,

so verstößt dies gegen den Grundsatz der Rechtmäßigkeit der Datenverarbeitung gemäß Art. 5 Abs. 1 Buchst. a DSGVO und gegen den Grundsatz zur Datensparsamkeit gemäß Art. 5 Abs. 1 Buchst. c DSGVO.

Was ist zu tun?

Bei der Erhebung örtlicher Aufwandssteuern müssen die Gemeinden prüfen, ob die personenbezogenen Daten, die sie im Rahmen von Steuererklärungen, Formularen und Fragebögen von den Steuerpflichtigen einfordern, verhältnismäßig zur anvisierten Aufgabenerfüllung sind. Die verwendeten Formulare müssen so gestaltet sein, dass freiwillige Angaben als solche erkennbar sind. Weiterhin muss dort, wo eine Teilschwärzung möglich ist oder verschiedene Unterlagen als Nachweis erbracht werden können, auf die Auswahlmöglichkeiten hingewiesen werden. Zudem sind die Informationspflichten des Artikels 13 DSGVO durch die Gemeinden umzusetzen.

4.8.4 Einsatz von Software und Dienstleistung bei der Verwaltung von Kurabgaben

Das ULD erhielt im Rahmen einer Beschwerde Kenntnis davon, dass eine Gemeinde die örtliche Kurabgabe von den Gästen durch die Gastgeber bzw. Beherbergungsbetriebe mittels Meldescheinen und Online-Meldescheinen berechnen und einziehen ließ. Die Prüfung und Verwaltung der Kurabgaben erfolgte durch eine von der Gemeinde beliehene Tourismusagentur, welche die Formulare zur Verfügung stellte.

Beliehenes Unternehmen

Einem beliehenen Unternehmen hat eine öffentliche Stelle Aufgaben der öffentlichen Verwaltung übertragen.

Die Tourismusagentur beauftragte hierzu einen Dienstleister, der die Software für den Online-Meldeschein bereitstellte. Die Gastgeber bzw. Beherbergungsbetriebe konnten so über eine Webseite die Daten ihrer Gäste und die Abrechnung an die Agentur übermitteln. Die analogen Meldescheine ließ die Tourismusagentur durch einen weiteren Dienstleister händisch über einen eigenen Zugang zur Software einpflegen.

Die Überprüfung der Tourismusagentur durch das ULD ergab, dass keine hinreichenden Verträge über diese Auftragsdatenverarbeitungen im Sinne von § 17 LDSG-alt (entspricht nun der Auftragsverarbeitung gemäß Artikel 28 DSGVO) geschlossen wurden.

Dass ein Vertrag mit dem Softwareanbieter kurzerhand rückdatiert wurde, hat das ULD gemäß § 42 Abs. 2 LDSG-alt beanstandet. Für die händische Übertragung der analogen Meldescheine in die Software lag zwar ein Auftragsdatenverarbeitungsvertrag mit dem Dienstleister vor. Dieser entsprach jedoch nicht den Anforderungen des § 17 LDSG-alt, was gemäß § 42 Abs. 1 LDSG-alt bemängelt wurde.

Was ist zu tun?

Verantwortliche müssen überprüfen, ob sie Dienstleister oder Software von Drittanbietern zur Verwaltung ihrer örtlichen Kurabgaben einsetzen und ob in diesen Fällen die Vorgaben des Artikels 28 DSGVO korrekt umgesetzt werden. Altverträge sind zu überprüfen und gegebenenfalls an die neue Rechtslage anzupassen. Sofern noch nicht geschehen, sind auch die Informationspflichten der Artikel 12 ff. DSGVO umzusetzen. Das bedeutet: Analoge Meldescheine und Online-Formulare sind so zu gestalten, dass die betroffenen Personen nachvollziehen können, was mit ihren personenbezogenen Daten passiert.

05

KERNPUNKTE

Datenschutz für Mieterinnen und Mieter

Datenschutz im Verein

Beschäftigtendatenschutz

Meldepflichtige Datenpannen

5 Datenschutz in der Wirtschaft

5.1 Entschließung der DSK zur (Nicht-)Anwendbarkeit des TMG neben der DSGVO

Mitgliedstaatliche datenschutzrechtliche Regelungen werden aufgrund des Anwendungsvorrangs der DSGVO grundsätzlich durch diese verdrängt, wenn es keine spezifischen Regelungen gibt, die ein Fortbestehen bereits existierender Regelungen anordnen oder Öffnungsklauseln Spielräume zur mitgliedstaatlichen Ausgestaltung offenlassen bzw. vorgeben. Die DSGVO enthält eine Kollisionsregel zum Verhältnis der DSGVO zur E-Privacy-Richtlinie. Danach werden natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union durch die DSGVO keine zusätzlichen Pflichten auferlegt, soweit sie besonderen, in der E-Privacy-Richtlinie festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

Richtlinien bedürfen im Unterschied zu Verordnungen der Umsetzung durch die Mitgliedstaaten. Grundsätzlich entfaltet erst das in Umsetzung der Richtlinie geschaffene mitgliedstaatliche Recht Rechtswirkung gegenüber Einzelnen. Eine Richtlinie selbst kann keine Verpflichtungen für Einzelne begründen. Die Kollisionsregel in der DSGVO umfasst daher die in Umsetzung der E-Privacy-Richtlinie erlassenen mitgliedstaatlichen Vorschriften. Dies betrifft vor allem die Regelungen des TKG, die als Umsetzung der E-Privacy-Richtlinie 2002/58/EG anzusehen sind. Durch die Richtlinie 2009/136/EG wurde der Anwendungsbereich der E-Privacy-Richtlinie ausgeweitet. Danach werden nicht lediglich Anbieter von öffentlichen Telekommunikationsdiensten, sondern auch Anbieter von „Diensten der Informationsgesellschaft“ angesprochen. Diese entsprechen den Diensten, die in Deutschland als Telemediendienste bezeichnet und durch das Telemediengesetz (TMG) reguliert werden. Spezielle datenschutzrechtliche Vorgaben finden sich im 4. Abschnitt des TMG. Diese können jedoch nur dann neben der DSGVO zur Anwendung kommen, wenn es sich dabei um Umsetzungen der E-Privacy-Richtlinie handelt und sie somit der Kollisionsregel der DSGVO unterfallen.

Das TMG ist nach wie vor in all seinen Bestandteilen in Kraft. Eine Anpassung der datenschutzrechtlichen Vorschriften des TMG an die DSGVO wurde nicht vorgenommen. Es stellte sich daher die Frage nach der Anwendbarkeit der datenschutzrechtlichen Vorschriften seit der Geltungserlangung der DSGVO.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vertritt hierzu – nach Vorlage eines Beschlussentwurfs der Unterarbeitsgruppe E-Privacy des Arbeitskreises Medien der DSK – folgende Position:

Im Verhältnis zum nationalen Recht kommt seit dem 25.05.2018 die DSGVO für sämtliche automatisierte Verarbeitungen personenbezogener Daten vorrangig zur Anwendung. Die Vorschrift des Artikels 95 DSGVO findet keine Anwendung auf die Regelungen im 4. Abschnitt des TMG. Denn diese Vorschriften stellen vorrangig eine Umsetzung der durch die DSGVO aufgehobenen Datenschutzrichtlinie dar und unterfallen, da sie auch nicht auf der Grundlage von Öffnungsklauseln in der DSGVO beibehalten werden dürfen, demgemäß dem Anwendungsvorrang der DSGVO. Hiervon betroffen sind damit auch etwaige unvollständige Umsetzungen der E-Privacy-Richtlinie in diesem Abschnitt, welche jedenfalls isoliert nicht mehr bestehen bleiben können.

Da auch eine unmittelbare Anwendung der E-Privacy-Richtlinie in diesen Fällen nicht in Betracht kommt, kann sich die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Diensteanbieter von Telemedien folglich nur aus Art. 6 Abs. 1 DSGVO ergeben. Darüber hinaus sind die allgemeinen Grundsätze zur Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1 DSGVO sowie die besonderen

Vorgaben z. B. aus Art. 25 Abs. 2 DSGVO (Datenschutz „by Default“) einzuhalten.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder veröffentlichte diese Positionsbestimmung am 26.04.2018. Gleichzeitig wurde beschlossen, eine Konsultation von betroffenen Wirtschaftsverbänden und Unternehmen durchzuführen.

Nachdem diese stattgefunden hat, wird nun zur Erläuterung und Konkretisierung der Positionsbestimmung eine Ergänzung formuliert.

Die Stellungnahme ist unter dem folgenden Link abrufbar:

https://www.datenschutzkonferenz-online.de/media/ah/201804_ah_positionsbestimmung_tmg.pdf

5.2 Neufassung des „Code of Conduct“ der Versicherungswirtschaft

Im Jahre 2012 war die Versicherungswirtschaft in Deutschland die erste Branche, die zur Förderung der Beachtung datenschutzrechtlicher Regelungen förmlich anerkannte Verhaltensregeln erlassen hat (34. TB, Tz. 5.1.3). Verhaltensregeln haben den Zweck, abstrakte Bestimmungen der Datenschutzgesetze mit Blick auf Abläufe in der Versicherungsbranche zu konkretisieren und zu ergänzen. Die förmliche Anerkennung der Verhaltensregeln erfolgte damals durch den Berliner Beauftragten für den Datenschutz und die Informationsfreiheit.

Auf Grundlage einer in den Verhaltensregeln enthaltenen Klausel sollte bei jeder den Regelungsinhalt betreffenden Rechtsänderung und spätestens fünf Jahre nach Abschluss der Überprüfung der Verhaltensregeln durch die zuständige Datenschutzaufsichtsbehörde eine Evaluierung stattfinden. Infolge des Stichtags für die Geltung der Datenschutz-Grundverordnung, dem 25.05 2018, und dem Ablauf der Evaluierungsfrist im Jahre 2017 bestanden gleich zwei Gründe, eine Überarbeitung der Verhaltensregeln vorzunehmen.

Die Versicherungswirtschaft unterbreitete den Datenschutzaufsichtsbehörden frühzeitig Entwürfe zur Änderung der bestehenden Verhaltensregeln. Näheres zur beabsichtigten neuen Ausgestaltung der Verhaltensregeln wurde durch das ULD in der Funktion als Vorsitz des Arbeitskreises der unabhängigen Datenschutzbehörden des Bundes und der Länder für die Versicherungsbranche mit den deutschen Datenschutzaufsichtsbehörden und der Versicherungswirtschaft in mehreren Sitzungsterminen erörtert. Die für die förmliche Anerkennung der Verhaltensregeln zuständige Berliner Beauftragte für den Datenschutz und die Informationsfreiheit kam mit Abschluss der Erörterungen zu dem Ergebnis, dass die Vorgaben der Datenschutz-Grundverordnung für die Versicherungswirtschaft branchenspezifisch konkretisiert wurden. Diese Einschätzung wird auch vom ULD geteilt.

„Code of Conduct“ der Versicherungswirtschaft

Das Regelungswerk ist unter folgendem Link abrufbar:

www.gdv.de/resource/blob/23938/4aa2847df2940874559e51958a0bb350/download-code-of-conduct-data.pdf

Die förmliche Anerkennung der neuen Verhaltensregeln durch die Berliner Beauftragte für den Datenschutz und die Informationsfreiheit wurde bisher noch nicht vorgenommen, da restliche Fragen zur Einsetzung einer zusätzlichen Kontrollstelle nach den Vorgaben der Datenschutz-Grundverordnung noch geklärt werden müssen. Demnach kann die Überwachung der Einhaltung der Verhaltensregeln unbeschadet der Aufgaben und Befugnisse der Aufsichtsbehörden von einer Stelle durchgeführt werden, die über das geeignete Fachwissen hinsichtlich des Gegenstandes der Verhaltensregeln verfügt und die von der zuständigen Aufsichtsbehörde zu diesem Zweck akkreditiert

wurde. Verhaltensregeln sehen wiederum Verfahren vor, welche es jener Kontrollstelle ermöglichen, die obligatorische Überwachung der Einhaltung der Verhaltensregeln vorzunehmen. Bis zur Klärung der damit im Zusammenhang stehenden Fragen verwendet die Versicherungswirtschaft die Verhaltensregeln als interne Bestimmungen.

Angepasst wurden etwa Regelungen zur Einwilligung und zum Umgang mit besonderen Datenkategorien wie Gesundheitsdaten, zu den Informationspflichten gegenüber betroffenen Personen, zur gemeinsamen Verantwortung von zwei oder mehreren Unternehmen, zu den Rechten betroffener Personen wie z. B. Auskunft, Berichtigung, Einschränkung der Verarbeitung und Datenübertragbarkeit, zur Datenschutz-Folgenabschätzung, zur Benennung von Datenschutzbeauftragten und zur Meldung von Datenschutzverstößen.

5.3 Neufassung der Orientierungshilfe „Selbstauskünfte für Mietinteressenten“

Infolge der Geltung der Datenschutz-Grundverordnung und der Berücksichtigung neuerer Rechtsprechung wurde eine Überarbeitung der Orientierungshilfe „Selbstauskünfte für Mietinteressenten“ erforderlich. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder haben die entsprechende Neufassung gemeinsam erörtert und beschlossen.

Vor der Vermietung von Wohnraum werden von den Mietinteressenten verschiedene personenbezogene Angaben erhoben, wobei nur solche Daten verarbeitet werden dürfen, für die der Vermieter berechtigte Interessen vorweisen kann oder sich eine Erforderlichkeit der Datenerhebung für die Durchführung des Mietvertrags ableiten lässt. Es kann zwischen drei Zeitpunkten differenziert werden, nämlich dem Besichtigungstermin, der vorvertraglichen Phase, in welcher der Mietinteressent dem künftigen Vermieter mitteilt, eine bestimmte Wohnung anmieten zu wollen, und dem Stadium, in welchem die Entscheidung über den auszuwählenden Mietinteressenten fallen soll. Im Rahmen dieser drei Zeitpunkte kann die Erhebung bestimmter Angaben zulässig sein (35. TB, Tz. 5.4).

Wesentliche Ergänzungen wurden in der Orientierungshilfe insbesondere im Rahmen des Stadiums vorgenommen, in welchem der Vermieter sich für einen Mietinteressenten entscheidet. Fragen zu Kontaktinformationen aktueller oder früherer Vermieter der Mietinteressenten sind zunächst mangels einer Erforderlichkeit zur Durchführung des Mietverhältnisses unzulässig. Erfragt werden dürfen aber Angaben zur Erfüllung mietvertraglicher Pflichten, sofern diese Aufschluss über die Zahlungsfähigkeit der Mietinteressenten geben. Solche Angaben können sich etwa auf die Zahlung der vereinbarten Miete und der Nebenkosten beziehen. Auch Fragen nach Pflichtverletzungen aus dem bisherigen Mietverhältnis über Wohnraum können zulässig sein, allerdings unter der Bedingung, dass die Pflichtverletzung eine Kündigung rechtfertigt und solche Pflichtverletzungen für die Zukunft zu erwarten sind. Die Kündigung muss u. a. rechtskräftig oder in tatsächlicher Hinsicht unbestritten sein.

Bezüglich der Anforderung einer Selbstauskunft der Mietinteressenten ist zu berücksichtigen, dass diese nach der Rechtsprechung nicht verpflichtet sind, eine Mietschuldenfreiheitsbescheinigung zu erstellen. Daher kann eine solche Bescheinigung vom Mietinteressenten bei der beabsichtigten Neuanmietung von Wohnraum nicht verlangt werden. Zulässig wäre es hingegen, vom Mietinteressenten wahlweise entweder von Vorvermietern geschuldete Quittungen über empfangene Zahlungen oder geschwärzte Kontoauszüge und Mietverträge als Beleg zu geleisteten Mietzahlungen an Vorvermieter sowie zur Höhe des Mietzinses und damit zum Nachweis einer bestehenden Bonität zu erbitten.

Bereits in der Erstfassung der Orientierungshilfe wurde erläutert, dass die Einholung von Einwilligungen der Mietinteressenten zur Erhebung von Angaben nicht das richtige Mittel für den Vermieter darstellt. Die Freiwilligkeit von Einwilligungserklärungen als zentrales Wirksamkeitskriterium hat mit Geltung der Datenschutz-

Grundverordnung nochmals besonderes Gewicht erhalten. Demnach läge im Bereich der Anmietung von Wohnraum keine freiwillige und damit unwirksame Einwilligungserklärung vor, wenn der Abschluss des Mietvertrags von der Einwilligung in die Erhebung nicht erforderlicher Angaben abhängig gemacht wird.

Orientierungshilfe „Selbstauskünfte für Mietinteressenten":

www.datenschutzkonferenz-online.de/media/oh/20180207_oh_mietauskuenfte.pdf

Was ist zu tun?

Vermieter von Wohnraum dürfen von Mietinteressenten nur erforderliche Angaben erheben. Personenbezogene Daten, für die berechtigte Vermieterinteressen bestehen, dürfen nur erhoben werden, wenn die Gesamtabwägung mit schutzwürdigen Mietinteressenten dies rechtfertigt. Im Falle der Verwendung von Vermieterfragebögen sind die Maßgaben der Orientierungshilfe einzuhalten.

5.4 Interessante Einzelfälle

5.4.1 Juristische Personen als Datenschutzbeauftragte?

Vorbehaltlich einer künftigen Klärung der Frage durch die Rechtsprechung wird vorliegend die Auffassung vertreten, dass nur natürliche Personen als Datenschutzbeauftragte benannt werden können. Etwa die Benennung einer GmbH selbst als Datenschutzbeauftragte ist demnach nicht statthaft. Diese GmbH könnte aber die Dienste ihrer Mitarbeiter als Datenschutzbeauftragte anbieten, die dann von anderen Unternehmen entsprechend benannt werden.

Die Datenschutzaufsichtsbehörden auf europäischer Ebene gehen in Auslegung der Datenschutz-Grundverordnung davon aus, dass u. a. Unternehmen mit einer anderen Stelle (natürliche oder juristische Person) einen Dienstleistungsvertrag schließen können. Dieser Vertrag hat aber nicht die Benennung dieser anderen Stelle selbst als Datenschutzbeauftragte zum Gegenstand. Stattdessen soll der Vertrag vorsehen, welche natürlichen Personen allein oder als „Team" die Funktion eines Datenschutzbeauftragten übernehmen sollen. Der zugrunde liegende Dienstleistungsvertrag soll nicht ohne Weiteres von einem Verantwortlichen oder Auftragsverarbeiter gekündigt werden können. Den natürlichen Personen, die auf Basis des Vertrags als Datenschutzbeauftragte eingesetzt werden, komme eine Art arbeitsrechtlicher Kündigungsschutz zu, indem diese vor ungerechtfertigten Entlassungen durch deren Arbeitgeber geschützt seien.

Daher wird durch die Aufsichtsbehörden auf europäischer Ebene nicht die Aussage getroffen, dass juristische Personen selbst als Datenschutzbeauftragte in Betracht kommen. Vielmehr wird die Konstellation erörtert, wonach etwa eine juristische Person einen Dienstleistungsvertrag mit einem Verantwortlichen oder Auftragsverarbeiter schließt. Diese juristische Person beschäftigt wiederum natürliche Personen, welche letztlich die Funktion eines Datenschutzbeauftragten für den Verantwortlichen oder Auftragsverarbeiter wahrnehmen sollen.

Leitlinien in Bezug auf Datenschutzbeauftragte

Hinweise der europäischen Datenschutzaufsichtsbehörden zur Benennung von Datenschutzbeauftragten (WP 243) können unter folgendem Link aufgerufen werden:

www.datenschutzkonferenz-online.de/media/wp/20170405_wp243_rev01.pdf

Datenschutzbeauftragte werden auf der Grundlage ihrer beruflichen Qualifikation und insbesondere des Fachwissens benannt, welches diese auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis erworben haben. Ferner kann die oder der Datenschutzbeauftragte Beschäftigte oder Beschäftigter des Verantwortlichen oder Auftragsverarbeiters sein oder die Aufgaben auf Grundlage eines Dienstleistungsvertrags erfüllen. Die besseren Argumente sprechen dabei für die ausschließliche Benennung natürlicher Personen. Vor allem das Abstellen auf die berufliche Qualifikation legt den Schluss nahe, dass die erforderliche Befähigung im Rahmen einer Berufsausbildung bzw. eines Studiums erworben wurde, was nur durch natürliche Personen erfolgen kann.

Zwar können die Vorgaben des deutschen Datenschutzrechts im Bundesdatenschutzgesetz nicht zur Auslegung der Datenschutz-Grundverordnung herangezogen werden. Unabhängig davon kann auch aus diesen Vorgaben abgeleitet werden, dass nur Menschen als Datenschutzbeauftragte benannt werden sollen. So beziehen sich jene Vorgaben etwa auf die Anwendung arbeitsrechtlicher Kündigungsregeln und auf die Zubilligung eines Zeugnisverweigerungsrechts, was nur bei der Benennung natürlicher Personen als Datenschutzbeauftragte von Bedeutung sein kann (36. TB, Tz. 5.3).

Die Kontaktdaten der Datenschutzbeauftragten sind nach den Vorgaben der DSGVO an die zuständige Datenschutzaufsichtsbehörde zu melden. Ein Meldeformular wird unter folgendem Link bereitgestellt:

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

5.4.2 Benennung von Datenschutzbeauftragten – mindestens zehn beschäftigte Personen

Ergänzend zu den Vorgaben der Datenschutz-Grundverordnung müssen nichtöffentliche Stellen wie Unternehmen insbesondere dann einen Datenschutzbeauftragten benennen, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Im Vergleich zur Rechtslage vor der Geltung der Datenschutz-Grundverordnung sind insoweit keine Änderungen eingetreten.

Für die Vorgängervorschrift im alten Bundesdatenschutzgesetz hatte der Gesetzgeber die Intention, eine „Beschäftigung" von Personen nicht nur für Arbeitnehmer, sondern etwa auch für Auszubildende und freie Mitarbeiter anzunehmen. Gerade freie Mitarbeiter waren daher bei der Beurteilung der Frage, ob „mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden", mitzuzählen. Diese Intention hat sich mit der Geltung der Neuregelung seit dem 25.05.2018 nicht geändert, zumal der Gesetzgeber auch vom Wortlaut her gesehen die Altregelung übernommen hat.

Personen, welche Zugriff auf Kundendatenbanken nehmen, etwa vertragliche Unterlagen einsehen können, Personaldaten verwalten oder in automatisierter Form personenbezogene Daten verarbeiten, welche z. B. über die Lebensumstände von Einzelpersonen Auskunft geben, müssen bei der Frage der Verpflichtung zur Benennung eines Datenschutzbeauftragten mitgezählt werden (10-Personen-Regel nach § 38 Abs. 1 BDSG). Mitarbeiterinnen und Mitarbeiter an Kassen, die lediglich eine EC- oder Kundenkarte einlesen, jedoch nicht auf eine Kundendatenbank mit Daten zugreifen oder gegebenenfalls nur manuell die Kontodaten auf der Karte in Augenschein nehmen, jedoch nicht in automatisierter Form zur Kenntnis nehmen

können, insbesondere nicht nach Abschluss des Bezahlvorgangs, sind nicht mitzuzählen.

Fragen zur Anwendung der 10-Personen-Regel wurden an das ULD häufig auch im Zusammenhang mit der Beauftragung von Monteuren in Handwerksbetrieben herangetragen. Erhalten die Monteure lediglich die Kontaktdaten der Kunden sowie Angaben zur Ausführung eines Auftrags, der vor Ort erledigt werden soll, so sind diese Personen nicht mitzuzählen. Diese Einschätzung beruht auf der Annahme, dass in diesen Fällen nur sehr wenige personenbezogene Daten flüchtig zur Kenntnis genommen werden, dies oft nicht in automatisierter Form erfolgt und entsprechende Angaben nicht im dauerhaften Zugriff der Monteure verbleiben. Anders wäre der Sachverhalt wiederum zu beurteilen, wenn die Monteure einen Zugriff auf eine Kundendatenbank erhalten und etwa dauerhaft Auftragshistorien abrufen können. Im letzteren Fall wären die Monteure im Rahmen der Prüfung der 10-Personen-Regel mitzuzählen.

Häufig wurde im Berichtszeitraum auch von Sportvereinen nachgefragt, ob bei der Prüfung, ob tatsächlich mindestens zehn Personen beschäftigt werden, die automatisiert mit personenbezogenen Daten arbeiten, Personen hinzugezählt werden müssen, die z. B. auf Datenbanken mit Angaben zu Mitgliedern und Sportlerinnen und Sportlern bestimmungsgemäß Zugriff nehmen. Verarbeiten Trainer Spielerdaten wie etwa Trainings- und Wettkampfergebnisse, Kontaktdaten der Spieler, Angaben zum Gesundheitszustand, zum Muskelaufbau und zur Ernährung, so sind auch diese hinzuzuzählen. Sportvereine müssen dabei den Überblick darüber haben, welche Mitglieder welche personenbezogenen Daten der Sportlerinnen und Sportler verarbeiten und zu Datenzugriffen autorisiert sind, um die Verpflichtung zur Benennung eines Datenschutzbeauftragten prüfen zu können.

Im Rahmen der Praxis-Reihe „Datenschutzbestimmungen praktisch umsetzen" ist u. a. auch eine Broschüre zur Benennung von Datenschutzbeauftragten erschienen, die über folgenden Link aufgerufen werden kann:

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

5.4.3 Erforderlichkeit der Benennung von Datenschutzbeauftragten in Kindertagesstätten

Bei Kindertagesstätten (Kitas) handelt es sich unabhängig von der Trägerschaft um eigenständige Verantwortliche im Sinne der DSGVO. Für die rechtmäßige und ordnungsgemäße personenbezogene Datenverarbeitung ist die jeweilige Leitung der Kindertagesstätte zuständig.

Welche datenschutzrechtlichen Vorschriften für die personenbezogene Datenverarbeitung anzuwenden sind, richtet sich nach der jeweiligen Trägerschaft. Für alle Kitas gilt zunächst die DSGVO. Ergänzend dazu finden für Kitas in kommunaler Trägerschaft primär die Vorschriften des Landesdatenschutzgesetzes (LDSG), für Kitas in privater Trägerschaft (Träger der freien Jugendhilfe, Elternvereine usw.) das Bundesdatenschutzgesetz (BDSG) und für Kitas in kirchlicher Trägerschaft die jeweiligen Datenschutzgesetze der Kirchen Anwendung.

Bei Kitas in kommunaler Trägerschaft ist die Benennung eines Datenschutzbeauftragten schon nach Art. 37 Abs. 1 Buchst. a DSGVO erforderlich. Danach haben alle Behörden und öffentlichen Stellen einen Datenschutzbeauftragten zu benennen. Eine kommunale Kita ist zwar in der Regel organisatorisch verselbstständigt. Rechtlich ist sie aber ein Teil der Kommune und damit Teil einer öffentlichen Stelle. Nach Art. 37 Abs. 3 DSGVO kann für mehrere öffentliche Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden. Daher kann z. B. der Datenschutzbeauftragte der Kommune auch Datenschutzbeauftragter der kommunalen Kita sein. Wenn für die Kita kein gesonderter Datenschutzbeauftragter benannt wurde, geht das ULD davon aus, dass der kommunale DSB auch für die kommunalen Kitas zuständig ist.

Bei Einrichtungen in privater Trägerschaft geht das ULD davon aus, dass ein Fall von Art. 37 Abs. 1 Buchst. b DSGVO gegeben ist. Nach dieser Vorschrift ist ein Datenschutzbeauftragter zu benennen, wenn die Kerntätigkeit des Verantwortlichen in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.

Zur Kerntätigkeit eines Verantwortlichen gehören alle Vorgänge, die einen festen Bestandteil seiner Haupttätigkeit darstellen. In Schleswig-Holstein ist das systematische Beobachten und Dokumentieren der kindlichen Entwicklung Bestandteil der Arbeit der Erzieherinnen und Erzieher. Bereits im Jahr 2006 hat die Landesregierung dazu die Broschüre „Systematisches Beobachten und Dokumentieren" herausgegeben. Im Vorwort heißt es dort: „Im Mittelpunkt des gesetzlichen Auftrages der Kindertageseinrichtungen (…) steht das aktive und lernbereite Kind, dessen Bildungsweg in der Kindertageseinrichtung durch eine individualisierte und differenzierte Erziehungsarbeit unterstützt, angeregt und gefordert werden soll. Beobachtung und eine darauf aufbauende Bildungsdokumentation nehmen deswegen einen zentralen Stellenwert ein. Sie sind notwendig, um Kinder und ihre Lernprozesse zu verstehen. Beobachtungen müssen kontinuierlich stattfinden und schriftlich festgehalten werden, um sie als Grundlage von Gesprächen mit dem Team, den Eltern und der Grundschule nutzen zu können."

Daraus ergibt sich, dass die Dokumentation zur Kerntätigkeit der Erzieher und Erzieherinnen gehört. Dabei ist es unerheblich, ob diese Dokumentation in elektronischer oder konventioneller Form geführt wird.

Eine weitere Voraussetzung für die Benennungspflicht nach der oben genannten Vorschrift war weiterhin, dass die Beobachtungs- und Entwicklungsdokumentation als „umfangreiche regelmäßige und systematische Beobachtung" im Sinne von Art. 37 Abs. 1 Buchst. b DSGVO zu qualifizieren ist. Mit der Dokumentation in den Kindertagesstätten sollen die Entwicklungsfortschritte, Verhaltensänderungen und das Sozialverhalten der Kinder festgehalten werden. Die Informationen werden den Eltern, aber auch (nach schriftlicher Einwilligung der Eltern) den Schulen zur Verfügung gestellt. Die Dokumentation zeigt den Verlauf der Entwicklungsschritte der Kinder und ist somit geeignet, die geistige, sprachliche und motorische Entwicklung, die Vorlieben, Interessen und das Verhalten der Kinder zu analysieren. Damit handelt es sich nach Auffassung des ULD bei der Dokumentation um eine entsprechende Beobachtung, die eine Benennungspflicht nach Art. 37 Abs. 1 Buchst. b DSGVO auslöst.

Unabhängig davon kann sich die Pflicht zur Benennung eines Datenschutzbeauftragten auch aus § 38 Abs. 1 BDSG ergeben. Dies ist der Fall, wenn in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Bei der Personenzahl sind sämtliche Erzieher und Erzieherinnen zu berücksichtigen, die die Entwicklung der Kinder dokumentieren. Geschieht dies automatisiert, so liegt nach unserer Einschätzung auch nach § 38 Abs. 1 BDSG die Pflicht zur Benennung eines Datenschutzbeauftragten vor.

Die Benennung eines gemeinsamen Datenschutzbeauftragten wäre auch für private Kitaträger zulässig. Denkbar wäre auch die gemeinsame Benennung von Datenschutzbeauftragten durch kommunale und private Träger. Dabei muss in jedem Fall sichergestellt werden, dass den gemeinsam benannten Datenschutzbeauftragten ausreichend Zeit zur Verfügung steht, um ihrer Aufgabe im Hinblick auf alle beteiligten Kitas nachkommen zu können.

Was ist zu tun?

Für Kindertagesstätten ist regelmäßig ein Datenschutzbeauftragter zu benennen.

5.4.4 Steuerberater als Auftragsverarbeiter?

Im Kurzpapier Nr. 13 der Datenschutzkonferenz wird ausgeführt, dass die Einbeziehung eines Steuerberaters bezüglich der Verarbeitung personenbezogener Daten in der Regel keine Auftragsverarbeitung darstellt. DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren werden hingegen als Anwendungsbeispiel für eine Auftragsverarbeitung aufgeführt.

Stellungnahme der Datenschutzkonferenz

Das erwähnte Kurzpapier Nr. 13 zur Einbindung von Auftragsverarbeitern kann unter folgendem Link aufgerufen werden:

www.datenschutzzentrum.de/artikel/1205-.html

Steuerberater und Steuerbevollmächtigte üben ihren Beruf nach den Vorgaben des Steuerberatergesetzes insbesondere unabhängig und eigenverantwortlich aus, sodass eine für die Auftragsverarbeitung nach Artikel 28 DSGVO erforderliche weisungsgebundene Tätigkeit regelmäßig nicht in Betracht kommt. Werden im Zusammenhang mit der Lohnbuchhaltung auch die Lohnkonten eingerichtet und lohnsteuerrechtliche Abschlussarbeiten zum Jahresende erbracht, sind auch besondere steuerrechtliche Kenntnisse erforderlich, die eine Beratung durch den Steuerberater notwendig machen können.

Näheres zur Differenzierung zwischen den verschiedenen Tätigkeiten im Zusammenhang mit der Lohnbuchhaltung hat das Bundesverfassungsgericht bereits in der Vergangenheit entschieden. Für die laufende Lohnbuchhaltung wurden dabei hingegen keine besonderen steuerrechtlichen Kenntnisse gefordert, da nach Auffassung des Gerichts es in diesem Bereich um die Erledigung von Routinearbeiten geht, die mehr ein korrektes Rechnen und den sachgemäßen Umgang z. B. mit Lohnsteuertabellen umfassen. Für die laufende Lohnbuchhaltung besteht damit bekanntlich auch kein Buchführungsprivileg für steuerberatende Berufe. Hilfeleistungen in der laufenden Lohnbuchhaltung sind demnach nicht den steuerberatenden Berufen vorbehalten.

Würde ein Steuerberater nun im Einzelfall ausschließlich Aufgaben der laufenden Lohnbuchhaltung wahrnehmen (kein Einrichten von Lohnkonten, keine Abschlussarbeiten bzw. keine beratende Tätigkeit), so bleiben die allgemeinen Berufspflichten nach dem Steuerberatungsgesetz natürlich bestehen. Andererseits besteht bei der Ausführung des Auftrags auch kein nennenswerter eigener Entscheidungsspielraum. Es kommt im Wesentlichen darauf an, dass routinemäßig eine korrekte Berechnung erfolgt, etwa anhand von Bruttolohn und Lohnzahlungszeitraum, Kürzung um Freibeträge, Berücksichtigung von Familienstand, Kinderzahl und Steuerklasse usw. In diesem Kontext spricht einiges dafür, eine Auftragsverarbeitung anzunehmen. Die Annahme einer weisungsgebundenen Tätigkeit liegt auch nicht fern, da der Mandant die Lohndaten seiner Mitarbeiter dem Steuerberater dann für die laufende Lohnbuchhaltung zugänglich macht, um (lediglich) ein korrektes Berechnungsergebnis zu erhalten. Entsprechende Tätigkeiten sind vergleichbar mit der Wahrnehmung der laufenden Lohnbuchhaltung durch Personen außerhalb der steuerberatenden Berufe (kaufmännische Berufe nach den gesetzlichen Vorschriften zur Berufsausbildung).

In der Praxis dürfte sich aber die Frage stellen, ob ein Steuerberater tatsächlich nur bzw. ausschließlich mit Aufgaben der laufenden Lohnbuchhaltung beauftragt wird. Regelmäßig wird hier durch den Steuerberater zusätzlich eine Beratung durchgeführt, die mit der Einrichtung der Lohnkonten und den erwähnten Abschlussarbeiten im Zusammenhang steht. In all diesen Fällen wird keine Auftragsverarbeitung angenommen werden können. Steuerberatern steht im Übrigen nach § 11 des Steuerberatungsgesetzes eine besondere Rechtsgrundlage zur Erhebung und Verwendung personenbezogener Daten zu.

5.4.5 Einholung von Selbstauskünften von Mietinteressenten

Wie bereits unter Tz. 5.3 (Neufassung der Orientierungshilfe „Selbstauskünfte von Mietinteressenten") erläutert, erheben Vermieter bereits vor der Vermietung von Wohnraum persönliche Angaben von Mietinteressenten, um auf deren Basis eine Entscheidung über den Vertragsabschluss treffen zu können. Im Sommer 2017 ging beim ULD eine anonyme Beschwerde über einen sogenannten Bewerberbogen ein, der von einem Wohnungsunternehmen an potenzielle Mietinteressenten ausgehändigt wurde.

Im Rahmen einer Selbstauskunft sollte der Mietinteressent bereits vor der Besichtigung einer Wohnung Auskunft über seine Nationalität, über die Kontaktdaten zu seinem bisherigen Vermieter und seinem Arbeitgeber, seine Beschäftigungsdauer, seinen Pkw und gegebenenfalls sein Krad inklusive Kennzeichen und KFZ-Marke und zu seiner Vermögenssituation inklusive Haus- und Grundbesitz erteilen. Darüber hinaus wurde um Angabe seiner vollständigen Bankdaten, um Angabe zu bestehenden Schulden sowie bei Auszubildenden um Angabe der Arbeitgeber der Eltern und Höhe der Einkommen der Eltern gebeten.

Es wurde daraufhin ein Verfahren eingeleitet, in dessen Rahmen zunächst das aufsichtsbehördliche Auskunftsverlangen durch die Verhängung eines Zwangsgeldes gegen das Wohnungsunternehmen durchgesetzt werden musste. Im weiteren Verlauf des Verfahrens wurde klargestellt, dass die Verwendung von Einwilligungserklärungen gegenüber Mietinteressenten in Formularen zur Selbstauskunft nicht das richtige Mittel zur Datenerhebung ist. Für eine wirksame Einwilligung ist eine freie Entscheidung der betroffenen Person erforderlich. Wird der Abschluss eines Mietvertrags von der Erhebung bestimmter Angaben bei Mietinteressenten abhängig gemacht, entsteht eine Zwangslage, in welcher keine freiwillige und damit wirksame Einwilligungserklärung zustande kommen kann.

Vermieter haben jedoch die Möglichkeit, ein „berechtigtes Interesse" an der Beantwortung einzelner Fragen geltend zu machen, um eine Basis für eine Entscheidung über einen möglichen Mietvertragsabschluss schaffen zu können. In diesem Zusammenhang dürfen jedoch nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags „erforderlich" sind. Auf Basis einer Interessenabwägung muss dabei das Recht der Mietinteressenten auf informationelle Selbstbestimmung Beachtung finden.

Bezüglich der Zulässigkeit einer Datenerhebung bei Mietinteressenten ist zwischen dem Besichtigungstermin, der vorvertraglichen Phase, in welcher die Mietinteressenten dem künftigen Vermieter mitteilen, eine konkrete Wohnung anmieten zu wollen, und der Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten zu unterscheiden. In der ersten Phase des Besichtigungstermins dürfen lediglich Angaben zur Identifikation und Angaben aus dem Wohnberechtigungsschein erhoben werden.

In dem vorliegenden Fall konnte das verantwortliche Wohnungsunternehmen davon überzeugt werden, dass der bisher genutzte Bewerberbogen entsprechend überarbeitet werden muss und zukünftig nur solche Daten erhoben werden, die zur Durchführung der jeweiligen Phase erforderlich sind.

5.4.6 Klingelbretter – Verarbeitung von Namensschildern durch die Wohnungswirtschaft

Auch das ULD war mit Fragen zur Verarbeitung von Vor- und Nachnamen auf Klingelschildern befasst. Die Thematik hatte durch eine Untersagung der Verarbeitung in Österreich auch in den Medien und bei betroffenen Personen für Aufregung gesorgt. Die Wiener Wohnungsbaugesellschaft hatte sich nach Zustellung einer behördlichen Anordnung dazu entschlossen, die Namensschilder an Klingelbrettern abzumontieren und durch Nummern zu ersetzten. Gleiches

wurde für Unternehmen der Wohnungswirtschaft in Deutschland befürchtet.

Die Verwendung von Namensschildern für Klingelanlagen in Mehrfamilienhäusern durch die Wohnungswirtschaft unterfällt den Regelungen der DSGVO, wenn es sich dabei um eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten handelt oder eine nicht automatisierte Verarbeitung vorliegt, wobei die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Nun handelt es sich bei den Namen von betroffenen Personen um personenbezogene Daten.

Im Fokus der datenschutzrechtlichen Betrachtung stand in diesem Fall vielmehr die Frage, ob das Unterhalten der Klingelbretter einen datenschutzrechtlichen Verarbeitungsvorgang darstellt. Eine automatisierte Verarbeitung liegt in den Fällen vor, in denen die Verwaltung der Klingelschilder elektronisch erfolgt. Dies ist derzeit noch in den allerwenigsten Situationen der Fall. Meist wird ein Namensschild aus Papier oder einem anderen Material erstellt und auf das Klingelbrett oder hinter einem dafür vorgesehenen Sichtfenster angebracht. Erfolgt die Verarbeitung nicht automatisiert aus einem Mieterverzeichnis heraus, handelt es sich in der Regel um ein Ordnungssystem, in dem die Namen der betroffenen Personen einer bestimmten Wohnung zugeordnet werden. Es handelt sich dann um eine strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, und damit um eine Datei im datenschutzrechtlichen Sinne.

Ist ein sachlicher Anwendungsbereich der DSGVO gegeben, so darf eine Verarbeitung durch die Wohnungswirtschaft u. a. nur dann erfolgen, wenn die betroffenen Personen in die Datenverarbeitung eingewilligt haben oder eine der anderen Rechtsgrundlagen der DSGVO erfüllt ist.

Ist die Beschriftung Teil des Mietvertrages und verpflichtet sich der Vermieter zur Unterhaltung des Klingelschildes oder wird er von den Eigentümern damit beauftragt, so kann die Verarbeitung auf der Grundlage des Mietvertrages erforderlich sein. Üblicherweise finden sich solche Regelungen aber nicht im Mietvertrag. Vielmehr bleibt es den Mietern überlassen, den Inhalt des Klingelschildes zu bestimmen. Ist dies der Fall, so kann die Beschriftung auf der Grundlage einer Einwilligung erfolgen. Für diesen Fall sind die in der DSGVO vorhandenen Vorgaben zur Einwilligung aus Artikel 7 DSGVO zu beachten. Weiterhin sind die Informationspflichten aus Artikel 13 DSGVO zu erfüllen.

Eine Erforderlichkeit der Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten wird bei Klingelschildern in der Regel nicht vorliegen. Denn das Interesse und die Wahrnehmung des informationellen Selbstbestimmungsrechts der betroffenen Person an der Bestimmung des Inhaltes des Klingelschildes werden gegenüber dem Interesse der Wohnungswirtschaft an einem einheitlichen Erscheinungsbild und der Sicherstellung der Erreichbarkeit von Einzelpersonen überwiegen.

In einem dem ULD vorliegenden Fall lag die Situation aber etwas anders, weil die betroffene Person vom Eigentümer der Wohnanlage die korrekte Beschriftung verlangte. Ist der Anwendungsbereich der DSGVO gegeben, besteht für den Vermieter auch die Pflicht, die personenbezogenen Daten auf den Klingelschildern sachlich richtig und erforderlichenfalls auf dem neuesten Stand zu führen. Hierzu sind gemäß Art. 5 Abs. 1 Buchst. d DSGVO alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit"). Für die Vermieter bedeutet dies, dass die Beschriftung der Klingelschilder bei Auszug von Mietern zu entfernen und durch die Benennung der neuen Mieter zu ersetzen ist.

Näheres zur Verwendung von Vor- und Nachnamen auf Klingelschildern können Sie dem nachfolgenden Link entnehmen:

www.datenschutzzentrum.de/artikel/1256-Klingelschild-kein-Datenschutzverstoss-von-der-Muecke-zum-Elefanten.html

5.4.7 Missachtung von Rechten betroffener Personen durch werbende Unternehmen

Viele Menschen fühlen sich erheblich gestört, wenn sie von Unternehmen per Brief, E-Mail oder am Telefon beworben werden, obwohl sie dem Unternehmen zuvor keine ausdrückliche Einwilligung hierzu erteilt haben. Um zunächst Kenntnis über die dort gespeicherten Daten zu erhalten und eine zukünftige Werbung zu unterbinden, werden die Unternehmen regelmäßig mit Auskunfts- und Löschungsbegehren sowie Widerrufen konfrontiert, die grundsätzlich unverzüglich zu bearbeiten sind. Das ULD erhielt im Berichtszeitraum eine Vielzahl von Eingaben, in denen die Missachtung der Betroffenenrechte durch werbende Unternehmen beklagt wurde. In zahlreichen Fällen wurden die Anträge und Widerrufe nur sehr verzögert oder zum Teil auch gar nicht bearbeitet.

Mit Geltung der DSGVO sind alle detaillierten Regelungen des bisherigen Bundesdatenschutzgesetzes zur Verarbeitung von personenbezogenen Daten zum Zwecke der Werbung entfallen. Neben der Erhebung einer Einwilligung kann die Verarbeitung von personenbezogenen Daten zum Zwecke der Werbung in bestimmten Fällen nunmehr auch auf Grundlage eines berechtigten Interesses erfolgen. Hierfür muss die Verarbeitung der entsprechenden Daten jedoch erforderlich sein, und es dürfen die schutzwürdigen Interessen der betroffenen Person nicht überwiegen. Die Datenschutz-Grundverordnung verlangt in diesem Zusammenhang eine Interessenabwägung, in der u. a. zu berücksichtigen ist, ob die betroffene Person vernünftigerweise erwarten kann, beworben zu werden. Hierbei ist beispielsweise zwischen Bestandskunden und Dritten zu unterscheiden, wobei jedoch im Rahmen der Datenerhebung immer auch eine entsprechende vorherige Information der Betroffenen über die vorgesehene Verarbeitung der Daten für Werbezwecke zu erfolgen hat und selbstverständlich auch die Rechte betroffener Personen zu beachten sind. Bei der Erhebung einer Einwilligung muss die betroffene Person über den Zweck der Verarbeitung und ihr bestehendes Widerrufsrecht in einer verständlichen Form und klaren, einfachen Sprache informiert werden.

Neben den datenschutzrechtlichen Vorschriften der Datenschutz-Grundverordnung haben die werbenden Unternehmen auch die Schutzvorschriften des Gesetzes gegen den unlauteren Wettbewerb zu berücksichtigen, welches insbesondere zwischen den verschiedenen Kontaktwegen unterscheidet und eine Telefonwerbung weiterhin nur mit einer ausdrücklichen Einwilligung erlaubt.

Näheres ergibt sich aus der im Rahmen der 96. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. November 2018 beschlossenen Orientierungshilfe über die Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung:

www.datenschutzkonferenz-online.de/media/oh/20181107_oh_werbung.pdf

Die vom ULD eingeleiteten Aufsichtsverfahren haben in der Regel dazu geführt, dass die Unternehmen umgehend die entsprechenden Auskünfte erteilt, Daten gelöscht und Werbewidersprüche beachtet haben. In Einzelfällen wurden die verantwortlichen Mitarbeiterinnen und Mitarbeiter nachgeschult und interne Bearbeitungsprozesse angepasst. Die Vielzahl der Einzelfälle hat jedoch ebenfalls gezeigt, dass in einzelnen Unternehmen der Durchführung von Werbemaßnahmen erheblich mehr Beachtung geschenkt wird als der Einhaltung der datenschutzrechtlichen Vorschriften.

5.4.8 Offline-Tracking/Ortung von Mobiltelefonen in Fußgängerzone

Durch Beschwerden erlangte das ULD Kenntnis davon, dass in zwei Städten in Schleswig-Holstein Messungen von Besucherströmen innerhalb bestimmter öffentlicher Bereiche der Städte mittels sogenanntem Offline-Tracking durchgeführt werden.

Bei diesen Verfahren wird sich des Umstands bedient, dass mobile Endgeräte meist voreingestellt in regelmäßigen Abständen sogenannte „Probe Requests" aussenden, die technisch dazu geeignet und bestimmt sind, über die WLAN-Schnittstelle des Endgeräts eine Verbindung zu einem Netzzugangspunkt (wie z. B. WLAN-Hotspots) zu erleichtern. Dabei werden Datenpakete ausgesendet, die u. a. die „Media Access Control (MAC)"-Adresse des Netzadapters des jeweiligen mobilen Endgeräts enthalten. Da sich die zur Messung der Besucherströme eingesetzten Geräte gegenüber den Endgeräten wie WLAN-Hotspots/Netzzugangspunkte verhalten, ohne tatsächlich einen Netzzugang bereitzustellen, können die von den Endgeräten ausgesendeten Datenpakete durch die eingesetzten Geräte erhoben und dann zwecks Analyse der Kundenströme weiterverarbeitet werden.

In beiden Fällen wurde ein aufsichtsbehördliches Verfahren eingeleitet und den Verantwortlichen (die – einmal als Verein, einmal als GmbH organisiert – jeweils zu Zwecken des Stadtmarketings tätig sind) im Rahmen der Anhörung die Rechtsauffassung des ULD mitgeteilt, wonach für das Erheben von MAC-Adressen im öffentlichen Raum zur Messung von Besucherströmen keine Rechtsgrundlage ersichtlich ist.

Dabei wird maßgeblich von folgenden Erwägungen ausgegangen: MAC-Adressen stellen personenbezogene Daten dar. Für die Erhebung von MAC-Adressen bedarf es daher einer Rechtsgrundlage. Eine Erhebung und weiter gehende Verarbeitung auf Grundlage einer Interessenabwägung ist nicht möglich, da eine Interessenabwägung im vorliegenden Fall zu einem Überwiegen der Interessen der betroffenen Personen führt.

Dies gilt vor allem aufgrund des Umstands, dass die Daten bei einem Verweilen bzw. Betreten öffentlicher Räume erhoben werden und dies ohne Kenntnis der betroffenen Personen stattfindet. Aufgrund der technischen Voreinstellungen mobiler Endgeräte haben betroffene Personen praktisch keine hinreichende Möglichkeit, die Aussendung und – damit einhergehend – die Verarbeitung ihrer personenbezogenen Daten zu unterbinden.

Stichprobenartige Tests haben ergeben, dass ein Unterbinden der Aussendung von „Probe Requests" je nach eingesetztem Betriebssystem nicht ohne Weiteres bzw. nur schwer möglich ist. Bei einigen Betriebssystemen bzw. bestimmten Versionen hiervon konnte eine Aussendung erst unterbunden werden, als der sogenannte Flugmodus aktiviert wurde, d. h. global alle aktiven Funkverbindungen des Endgeräts deaktiviert wurden.

Es ist nicht davon auszugehen, dass es sich um allgemein zugängliche personenbezogene Daten handelt. Eine allgemeine Zugänglichkeit setzt nämlich voraus, dass Daten dazu geeignet und bestimmt sind, von der Allgemeinheit abgerufen werden zu können. Die Bestimmung über die Zugänglichkeit trifft derjenige, in dessen Hoheit die Daten zu verorten sind. Sofern es sich um MAC-Adressen und damit um personenbezogene Daten handelt, sind als Verfügungsberechtigte die betroffenen Personen anzusehen, denen die MAC-Adressen als personenbezogene Daten zuzurechnen sind.

Es mangelt an einer aktiven Entscheidung der betroffenen Personen, die MAC-Adressen öffentlich zugänglich zu machen. Darüber hinaus sind die „Probe Requests" auch nicht dazu bestimmt, das Betreten bestimmter öffentlicher Räume zu dokumentieren, sondern einzig und allein dazu, eine Verbindung zu Netzzugangspunkten zu erleichtern.

Offline-Tracking in der E-Privacy-Verordnung?

In Entwürfen der E-Privacy-Verordnung wird auch Offline-Tracking behandelt. Sollte sich der Gesetzgeber dazu entschließen, dort Vorgaben zu machen, führt dies zu einer Änderung der bis dahin geltenden Rechtslage.

Da die Geräte im öffentlichen Raum eingesetzt worden sind, kommt auch keine vertragliche oder vorvertragliche Beziehung der betroffenen Personen zur erhebenden verantwortlichen Stelle in Betracht. Auch Einwilligungserklärungen wurden von den betroffenen Personen

nicht abgefordert, sodass keine Rechtsgrundlage ersichtlich ist, auf der eine Erhebung rechtskonform möglich ist.

Beide Verantwortlichen haben den Betrieb der Gerätschaften noch im laufenden aufsichtsbehördlichen Verfahren eingestellt. Die Verfahren wurden dann eingestellt.

5.4.9 Wirksamkeit von Einwilligungen bezüglich unverschlüsselter E-Mail-Kommunikation?

Durch eine Beschwerde gelangte dem ULD zur Kenntnis, dass ein Verantwortlicher Einwilligungserklärungen zur Versendung unverschlüsselter E-Mails einholt. Der Verantwortliche ist in einem Bereich tätig, in dem personenbezogene Daten mit einem erhöhten Schutzbedarf verarbeitet werden.

Die Nutzung von E-Mail-Kommunikation zur Verarbeitung personenbezogener Daten ist nur unter den Voraussetzungen, die die DSGVO aufstellt, zulässig. Das bedeutet, dass Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umzusetzen haben, um sicherzustellen und den Nachweis dafür erbringen zu können, dass eine Verarbeitung DSGVO-konform erfolgt. Dabei haben Verantwortliche u. a. den Stand der Technik zu berücksichtigen.

Der Verpflichtung, den Stand der Technik zu berücksichtigen und angemessene Schutzmaßnahmen einzurichten, kann sich ein Verantwortlicher nicht dadurch entziehen, dass er betroffenen Personen eine Erklärung dahin gehend abverlangt, dass diese eine Verarbeitung ohne angemessene Maßnahmen gutheißen.

Über die von der DSGVO explizit benannten besonderen Kategorien personenbezogener Daten hinaus gibt es Kategorien von personenbezogenen Daten, deren Verarbeitung aufgrund des ihnen anhaftenden Risikos für die Rechte und Freiheiten der betroffenen Personen einen erhöhten Schutzbedarf aufweisen. Dazu gehören z. B. Daten aus dem Bereich der Bankgeschäfte, sodass eine Übertragung von personenbezogenen Daten mit Bezug zu Bankgeschäften nach Auffassung des ULD nicht über einen unverschlüsselten Kommunikationskanal erfolgen darf, ohne Rücksicht darauf, ob die betroffene Person hierzu eventuell eine als Einwilligung bezeichnete Erklärung abgegeben hat. Eine solche Einwilligungserklärung ist unwirksam.

Nachdem der Verantwortliche im Rahmen eines aufsichtsbehördlichen Verfahrens auf diese Rechtsauffassung hingewiesen wurde, hat dieser erklärt, von den eingeholten Erklärungen keinen Gebrauch zu machen und keine weitere Erklärung dieser Art einzuholen.

Was ist zu tun?

Gerade Kreditinstitute sind gehalten, bei der Kontaktaufnahme mit Kunden nicht Formulare bzw. Vertragsklauseln zu verwenden, die den Kundinnnen und Kunden die Erklärung abverlangen, hinsichtlich der Beratung zu oder der Abwicklung von Bankgeschäften auf eine verschlüsselte und damit sichere Kommunikation zu verzichten. Die Einhaltung der Regeln zur Datensicherheit ist nicht verhandelbar.

5.4.10 Löschung aller Daten einer Kategorie in Datenbank mangels Erforderlichkeit

Aufgrund einer Beschwerde wurde das ULD darauf aufmerksam, dass ein Kreditinstitut bei der Erhebung personenbezogener Daten in einer laufenden Geschäftsbeziehung eine Datenkategorie abgefragt hat, ohne zu überprüfen, ob diese Kategorie für die Geschäftsbeziehung erforderlich ist oder nicht.

Im konkreten Fall führte das Kreditinstitut für einen einzelnen Kunden ein Konto. Hinsichtlich der Kontoführung konnten vonseiten des Kunden keine besonderen Wünsche festgestellt werden. Insbesondere bat der Kunde nicht um die Gewährung eines Darlehens. Die Konditionen für die Kontoführung sollten nicht verändert werden.

Gleichwohl bat das Kreditinstitut den Kunden um Übermittlung seines Familienstandes. Im Rahmen der Prüfung des Sachverhalts stellte das ULD fest, dass der Kunde kein Gemeinschaftskonto mit seiner Ehefrau führt, infolgedessen auch nicht die Stellung gemeinsamer Freistellungsaufträge von Bedeutung war, der Kunde keine minderjährige Person ist und auch kein Kreditrahmen ausgeschöpft oder erweitert werden sollte.

Nach den Vorgaben der DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Der Verordnungsgeber hat hierbei den Datenminimierungsgrundsatz normiert. Damit im Zusammenhang steht, dass nur die zur Zweckerfüllung erforderlichen personenbezogenen Daten erhoben werden dürfen. Bezüglich der Angabe des Familienstandes konnte nicht festgestellt werden, dass deren Verarbeitung für die weitere Kontoführung erforderlich ist.

Im Verlauf der Ermittlungen hat sich gezeigt, dass diese Erhebungspraxis nicht auf einen Einzelfall beschränkt war, sondern entsprechende Prozesse global implementiert waren. Das Kreditinstitut hat nach Mitteilung der Rechtsauffassung des ULD ihre Prozesse angepasst und verzichtet nun auf die Abfrage, Erhebung und Speicherung der Angabe in den Fällen, in denen die Erforderlichkeit dieser Angabe nicht festgestellt wurde.

Was ist zu tun?

Kreditinstitute müssen stets prüfen, ob die Erhebung personenbezogener Daten von Kunden und auch von Interessenten erforderlich ist, um etwa eine gesetzliche Vorgabe zu erfüllen oder um eine laufende Kundenbeziehung weiter zu betreuen, indem z. B. ein Kontoführungsvertrag erfüllt wird.

5.4.11 Umgang mit Bewerbungsdaten

Immer wieder erreichen das ULD Eingaben zum Thema „Aufbewahrung von eingeschickten oder ausgedruckten Bewerbungsdaten“. Im Bereich der Beschäftigtendaten hat der Bundesgesetzgeber mit § 26 Abs. 1 BDSG-neu eine dem § 32 Abs. 1 BDSG-alt vergleichbaren Erlaubnistatbestand geschaffen. Insoweit kann bei der Beurteilung der Fälle für die Entscheidung der Begründung von Beschäftigungsverhältnissen auf die vertrauten Anwendungsfälle zurückgegriffen werden. Die Bewerbung fällt daher als Teil der Begründung eines Beschäftigungsverhältnisses in den Anwendungsbereich der oben genannten Normen.

Beschäftigtendatenschutz für Bewerbende

Für Bewerberinnen und Bewerber gelten die datenschutzrechtlichen Bestimmungen des Beschäftigtendatenschutzes. Arbeitgeber sind gehalten, die Zulässigkeit der Aufbewahrung von Bewerbungsunterlagen zu prüfen.

Bewerbungsunterlagen, wie z. B. Bewerbungsmappen, enthalten die personenbezogenen Daten der sich bewerbenden Person. Bewerber für ein Beschäftigungsverhältnis gelten nach den gesetzlichen Vorgaben als Beschäftigte. Bei Bewerberdaten handelt es sich um personenbezogene Daten von Beschäftigten, die nur für Zwecke des Beschäftigungsverhältnisses verarbeitet werden dürfen, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Für die Aufbewahrung der Unterlagen gelten die allgemeinen Anforderungen der Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO. Der Arbeitgeber oder die Vermittlungsagentur hat daher angemessene technische und organisatorische Maßnahmen zu treffen, die die Bewerbungsunterlagen angemessen schützen. In einem Büro offen herumliegende Unterlagen sind dann nicht hinreichend geschützt, wenn nicht nur das zugriffsberechtigte Personal, sondern auch andere Beschäftigte oder gar Dritte darauf Zugriff nehmen können.

Generell darf der potenzielle Arbeitgeber die Unterlagen eines abgelehnten Bewerbers fünf Monate lang aufbewahren (§ 61 Abs. 1 Arbeitsgerichtsgesetz in Verbindung mit § 21 Abs. 4 Allgemeines Gleichbehandlungsgesetz). Die Erforderlichkeit der Speicherung nach Abschluss eines Bewerbungsverfahrens endet daher in der Regel spätestens nach fünf Monaten. Bewerber können die Rückgabe ihrer Unterlagen und Löschung elektronischer Daten gemäß Art. 17 Abs. 1 DSGVO verlangen, wenn die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Nach Beendigung der Bewerbung wird dies in der Regel der Fall sein.

Bewerber haben aber unabhängig davon die Möglichkeit, dem potenziellen Arbeitgeber eine Einwilligung zur weiteren Aufbewahrung der Bewerbungsunterlagen zu erteilen, indem etwa eine Berücksichtigung der Bewerbung für ein zukünftiges Bewerbungsverfahren gewünscht wird. Soweit Bewerber dem Unternehmen eine Einwilligung zur Verarbeitung gemäß Art. 6 Abs. 1 Buchst. a DSGVO erteilt haben, können sie diese gemäß Art. 17 Abs. 1 Buchst. a DSGVO auch widerrufen oder, soweit das Unternehmen ein berechtigtes Interesse (Art. 6 Abs. 1 Buchst. f DSGVO) an der Speicherung geltend macht, dem widersprechen.

5.4.12 Erhebung von Lichtbildern im Rahmen der Zeiterfassung

Im Rahmen der umfassenden Digitalisierung der Arbeitswelt stellt sich vermehrt die Frage, ob die vom Arbeitgeber immer zahlreicheren Datenerhebungen tatsächlich für die Zwecke des Beschäftigungsverhältnisses erforderlich sind.

Ende 2017 ging beim ULD eine Beschwerde ein, in der von einer Arbeitnehmerin beklagt wurde, dass ihr Arbeitgeber im Rahmen der Zeiterfassung zu Beginn und am Ende des Arbeitstages jeweils ein Lichtbild seiner Beschäftigten erhebt und diese weder über den Zweck der Verarbeitung noch über die Speicherdauer und die Nutzung der Lichtbilder informiert habe.

Arbeitgeber dürfen lediglich die für die betrieblichen Zwecke erforderlichen Daten über ihre Beschäftigten verarbeiten. Da die geleistete Arbeitszeit Grundlage für die Bemessung des Entgeltanspruches ist, haben Arbeitgeber grund-

sätzlich die Befugnis, die Arbeitszeit der Arbeitnehmer zu erfassen. Dies erfolgt in der Regel mit Stech- oder Magnetkarten.

Im Rahmen der Abwägung einer Erforderlichkeit einer weiter gehenden Erhebung eines Lichtbildes im Rahmen der Zeiterfassung sind das Recht auf informationelle Selbstbestimmung des Beschäftigten und der Grundsatz der Datenminimierung zu beachten.

Grundsatz der Datenminimierung

Der Umfang der erhobenen personenbezogenen Daten muss dem Zweck angemessen sowie auf das für den Zweck der Verarbeitung notwendige Maß beschränkt sein.

Das Unternehmen teilte im Rahmen der Anhörung mit, dass das Verfahren zur generellen Vermeidung von Missbräuchen an der Zeiterfassung eingeführt wurde. Einer solchen Begründung kann aber lediglich in Einzelfällen für befristete Zeiträume gefolgt werden, wenn es bereits einen Missbrauch gegeben hat oder es zumindest konkrete Verdachtsfälle für einen Missbrauch gibt und alle gegebenenfalls bestehenden milderen Mittel bereits ausgeschöpft wurden.

Der Arbeitgeber hat bei der Verarbeitung von personenbezogenen Daten seine Informations- und Transparenzpflichten auch gegenüber seinen Beschäftigten zu beachten und diese insbesondere über den jeweiligen Zweck, die Speicherdauer und die bestehenden Rechte betroffener Personen zu informieren.

Das betroffene Unternehmen hat in dem vorliegenden Fall die Erhebung der Lichtbilder im Rahmen der Zeiterfassung bereits im Anhörungsverfahren umgehend abgeschaltet und mitgeteilt, auch zukünftig von einer Erhebung von Lichtbildern abzusehen.

Was ist zu tun?

Der Arbeitgeber hat zu prüfen, ob die Verarbeitung der entsprechenden Daten für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Die bestehenden Informations- und Transparenzpflichten sind gegenüber den betroffenen Beschäftigten einzuhalten. Auch der Abschluss von Kollektivvereinbarungen kann ein adäquates Mittel zur Schaffung einer Grundlage für eine rechtmäßige Verarbeitung darstellen.

5.4.13 GPS-Überwachung von Außendienstmitarbeitern

Ein weiterer Fall, der sich im Rahmen der Digitalisierung der Arbeitswelt und der Auswirkung auf die Beschäftigten ereignete, bezog sich auf den Einsatz von GPS-Ortungssystemen in Montagefahrzeugen.

Ein Beschwerdeführer beklagte, dass das eingesetzte System neben den Standortübertragungen u. a. auch zahlreiche weitere Fahrzeugdaten, wie beispielsweise den Stand der Zündung, an den Arbeitgeber übermittelte und eine Vielzahl von Kollegen auf diese Daten zugreifen konnten.

Auch beim Betrieb von GPS-Ortungssystemen ist wiederum der Grundsatz der Datensparsamkeit zu beachten. Es dürfen auch hier lediglich die für die betrieblichen Zwecke erforderlichen Daten erhoben werden. Eine Erhebung von überflüssigen Daten, die beispielsweise bei einer erlaubten Privatnutzung von Fahrzeugen anfallen können, ist unzulässig.

Der Arbeitgeber teilte im Anhörungsverfahren mit, dass er die Daten für die Disposition und zur Erstellung von Serviceberichten für seine Kunden benötigen würde, konnte in diesem

Zusammenhang aber nicht erläutern, warum hierfür eine permanente GPS-Ortung, die genaue Route und die Erhebung der Fahrgeschwindigkeit sowie des Zündungsstandes erforderlich sei. In den erwähnten Serviceberichten wurden lediglich die Fahr-, Arbeits- und Pausenzeiten sowie eine Gesamtkilometerangabe aufgeführt, die von den betroffenen Mitarbeitern auch problemlos ohne ein GPS-Ortungssystem erhoben werden können.

Achtung: Datenschutz-Folgenabschätzung

Für eine rechtmäßige Fahrzeugdatenverarbeitung und Geolokalisierung von Beschäftigten kann eine Datenschutz-Folgenabschätzung erforderlich sein.

Beim Einsatz entsprechender Systeme ist darauf zu achten, dass Beschäftigte keinem permanenten Kontrolldruck ausgesetzt sein dürfen und daher GPS-Ortungssysteme, mit denen das Arbeitsverhalten von Beschäftigten permanent kontrolliert wird, datenschutzrechtlich unzulässig sind. Ein entsprechender Einsatz eines solchen Systems kann auch nicht auf eine Einwilligungserklärung des Beschäftigten gestützt werden, da nicht von der für eine wirksame Einwilligung erforderlichen Freiwilligkeit ausgegangen werden kann.

Im Rahmen der bestehenden Informations- und Transparenzpflichten hat der Arbeitgeber im Falle des Einsatzes eines entsprechenden Systems seine Beschäftigten u. a. über den Erhebungszweck und -umfang sowie über die bestehenden Betroffenenrechte und die Speicherdauer in transparenter Weise zu informieren und in diesem Zusammenhang auch mitzuteilen, aufgrund welcher Anlässe durch wen ein Zugriff auf die erhobenen Daten erfolgt. Auch der Abschluss einer Betriebsvereinbarung kann in diesem Zusammenhang hilfreich und geboten sein.

Nachdem um Vorlage des entsprechenden Verarbeitungsverzeichnisses und um Mitteilung gebeten wurde, inwieweit der betriebliche Datenschutzbeauftragte überhaupt an der Einführung des Verfahrens beteiligt wurde, stellte das Unternehmen den Betrieb des GPS-Ortungssystems ein und kündigte an, nunmehr eine datenschutzkonforme Lösung erarbeiten zu wollen.

5.4.14 Versendung von Gehaltsnachweisen per E-Mail

Immer wieder wenden sich betroffene Personen an das ULD und fragen nach der Rechtmäßigkeit der Versendung von Gehaltsnachweisen per E-Mail durch die Arbeitgeber.

Bei Gehaltsnachweisen handelt es sich um personenbezogene Daten von Beschäftigten, deren Verarbeitung für den Nachweis der Gehaltsberechnung und Auszahlung dienen und damit zur Durchführung des Beschäftigungsverhältnisses erforderlich sind. Zunehmend werden solche Gehaltsnachweise nicht mehr analog oder per Brief an die Beschäftigten verteilt oder versendet, sondern elektronisch zugestellt. Erfolgt die Versendung im firmeneigenen Netz und haben nur die Berechtigten, z. B. über persönliche dienstliche E-Mail-Adressen, darauf Zugriff, bestehen in der Regel gegen die elektronische Versendung keine datenschutzrechtlichen Bedenken. Erfolgt die Versendung wie in den vorgelegten Fällen jedoch an die privaten E-Mail-Accounts bei Fremdprovidern außerhalb des Verantwortungsbereichs des Arbeitgebers, sind besondere Schutzmaßnahmen zu treffen.

Der für die Verarbeitung verantwortliche Arbeitgeber hat gemäß § 32 DSGVO sicherzustellen, dass die Sicherheit der Verarbeitung und insbesondere die Vertraulichkeit der Informationen gewährleistet sind. Als Maßnahme kommt dafür eine hinreichende Verschlüsselung bei der Versendung in Betracht. Keinesfalls kann aber der Arbeitgeber von dem Beschäftigten die Zurverfügungstellung einer E-Mail-Adresse zu Zwecken der Zusendung einer Gehaltsabrechnung verlangen.

Die Zusendung an einen privaten E-Mail-Account ist nicht erforderlich, da regelmäßig eine analoge Zustellung möglich ist. Wünscht der Arbeitgeber eine elektronische Zustellung, obliegt es ihm, eine hinreichend sichere Zustellmöglichkeit zu schaffen.

5.4.15 Führung einer Negativliste über „vereinsschädigende Personen“

Das ULD erreichte eine Beschwerde über eine von einem Verein geführte „Negativliste“. In dieser Liste führte der Verein Personen auf, die sich in der Vergangenheit vereinsschädigend verhalten hätten, um zu erreichen, dass diese Personen auch zukünftig nicht wieder im Verein aktiv werden können. Das Führen einer solchen Liste wurde in der dortigen Mitgliederversammlung beschlossen.

Im eingeleiteten Verfahren konnte der Verein keine Angaben darüber machen, auf welche Rechtsgrundlage das Verfahren gestützt werde und welche konkreten Sachverhalte dazu führen, dass eine Person als vereinsschädigend eingestuft und in die Liste aufgenommen wird, oder ob es auch Möglichkeiten gäbe, aus dieser Liste wieder entfernt zu werden.

Personenbezogene Daten dürfen auch von Vereinen nur verarbeitet werden, wenn es hierfür eine Rechtsgrundlage gibt. Vereinsbeschlüsse oder -satzungen dürfen dabei nicht im Widerspruch zu geltenden datenschutzrechtlichen Vorschriften stehen.

Im Falle einer entsprechenden Verarbeitung hat der Verein auch zu dokumentieren, welchen konkreten Zweck eine solche Liste hat, welche Daten wofür erforderlich sind, in welchen konkreten Fällen Personen in die Liste aufgenommen werden, wie lange diese Daten dort gespeichert und wann diese gelöscht werden. Darüber hinaus sind betroffene Personen u. a. auch über die Gründe für eine solche Speicherung und ihre bestehenden Datenschutzrechte transparent zu informieren.

Für die vorgenannten Erfordernisse ist es dabei unerheblich, ob die verantwortliche Stelle im Vereinsregister eingetragen ist oder ob es sich um einen nicht rechtsfähigen Verein handelt.

Im Rahmen der Praxis-Reihe „Datenschutzbestimmungen praktisch umsetzen“ ist u. a. auch eine Broschüre zum Datenschutz im Verein erschienen:

http://uldsh.de/vereine

Nachdem während des laufenden Verfahrens der Verein einen neuen Vorstand gewählt hat, teilte dieser anschließend umgehend mit, dass sich für den neuen Vorstand keine Grundlage zum Führen einer solchen Liste ergäbe, die „Negativliste“ gelöscht wurde und auch zukünftig vom Führen einer „Negativliste“ abgesehen werde.

Was ist zu tun?

Personenbezogene Daten dürfen auch von Vereinen nur verarbeitet werden, wenn es hierfür eine Rechtsgrundlage gibt. Vereinssatzungen dürfen dabei nicht im Widerspruch zu geltenden datenschutzrechtlichen Vorschriften stehen. Die bestehenden Informations- und Transparenzpflichten sind gegenüber den Mitgliedern und gegebenenfalls anderen betroffenen Personen zu beachten.

5.4.16 Veröffentlichung von Schriftverkehr im Vereinsschaukasten

Zahlreiche Bürgerinnen und Bürger engagieren sich in unterschiedlichen Formen ehrenamtlich in Vereinen. Da kann es auch immer mal wieder zum Streit kommen. So erhielt das ULD im vergangenen Jahr eine Beschwerde darüber, dass ein Vereinsvorsitzender ein Schreiben eines Vereinsmitgliedes an die anwaltliche Vertretung des Vereinsvorstandes in öffentlich zugänglichen Schaukästen ausgehängt habe. In dem betreffenden Schreiben waren u. a. auch verschiedene personenbezogene Daten des Vereinsmitgliedes enthalten.

Auch eine solche Offenlegung von personenbezogenen Daten stellt eine Verarbeitung dar und bedarf daher wiederum einer Rechtsgrundlage.

Sollte in diesem Zusammenhang angeführt werden, dass die Verarbeitung zur Wahrung der berechtigten Interessen des Vereins erforderlich war, ist zunächst diese „Erforderlichkeit" zu begründen. Sollten tatsächlich gewichtige Gründe angeführt werden können, ist zu prüfen, ob es anstelle der Veröffentlichung alternative Maßnahmen gibt, die nicht oder weniger tief in das Recht der betroffenen Person eingreifen und es dem Verein dennoch erlauben, seine Interessen wirksam durchzusetzen.

In dem vorliegenden Fall kann eine unter Umständen erforderliche Information von weiteren Vorstandsmitgliedern beispielsweise auch postalisch erfolgen, sodass zumindest eine Kenntnisnahme von Nichtvereinsmitgliedern ausgeschlossen werden kann.

Für einen Aushang des Schriftverkehrs inklusive der in dem Schreiben enthaltenen personenbezogenen Daten in einem öffentlich zugänglichen Schaukasten bestand vor diesem Hintergrund keine Erforderlichkeit, sodass dies unzulässig war.

Sollte im Rahmen der Prüfung des berechtigten Interesses festgestellt werden, dass der verfolgte Zweck einzig mit dem Mittel einer Veröffentlichung wirksam erreicht werden kann, wäre darüber hinaus als letzter Schritt abzuwägen, ob schutzwürdige Interessen der betroffenen Personen die berechtigten Interessen des Verantwortlichen überwiegen oder nicht.

Da nach einem erfolgten Hinweis auf den Verstoß der Vereinsvorsitzende das Schreiben aus dem Schaukasten entfernt hat, konnte von der Einleitung eines formellen Verfahrens gegen den Verein abgesehen werden.

Was ist zu tun?

Eine Veröffentlichung von personenbezogenen Daten ist regelmäßig nur nach vorheriger Einwilligung der betroffenen Person zulässig. Dabei ist zu beachten, dass diese in informierter Weise und freiwillig zu erfolgen hat. Das bedeutet u. a. auch, dass eine Vereinsmitgliedschaft nicht von der Abgabe einer Einwilligung abhängig gemacht werden darf.

5.4.17 Branchenprüfung von Sportverbänden zum Umgang mit Sportlerdaten

In der Vergangenheit erhielt das ULD wiederholt Eingaben zum Umgang mit Sportlerdaten in Sportvereinen und -verbänden. Dies wurde nunmehr als Anlass genommen, bei zehn sehr unterschiedlichen Sportverbänden eine Branchenprüfung durchzuführen.

Um eine Vergleichbarkeit der verschiedenen Sportverbände zu ermöglichen, wurden diese trotz der sehr unterschiedlichen Strukturen zunächst mit zwölf identischen Fragen konfrontiert. Hierbei wurden insbesondere nach den Datenkategorien, den jeweiligen Zwecken und deren Speicherdauer sowie eventueller Übermittlungen an Dritte wie beispielsweise Bundesverbänden gefragt. Darüber hinaus wurden Satzungsbestandteile und Einwilligungserklärungen auf deren Rechtmäßigkeit geprüft und um Erläuterung der technischen Infrastruktur inklusive Berechtigungs- und Löschkonzept sowie um Übersendung etwaiger Auftragsdatenverarbeitungsverträge gebeten. Abschließend war darzustellen, wie die Sportverbände die Wahrung der Rechte betroffener Personen sicherstellen und ob gegebenenfalls eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter benannt wurde.

Insgesamt wurden die Fragen sehr kooperativ beantwortet und Hinweise meist zügig umgesetzt. In einem Einzelfall konnte eine Beantwortung der vorgenannten Fragestellungen jedoch leider erst unter Androhung eines Zwangsgeldes durchgesetzt werden.

Während der laufenden Prüfungsverfahren benannten zahlreiche Sportverbände erstmalig Datenschutzbeauftragte, die anschließend an der Erstellung von Verfahrensverzeichnissen, Satzungsänderungen, der Anpassung von Datenverarbeitungsverträgen, Formularen und den jeweiligen Webauftritten mitwirkten.

Bei zwei Sportverbänden mussten jedoch bereits diese Benennungen nachgebessert werden: Beispielsweise lag in einem Fall ein Interessenkonflikt vor, da der Verbandsvorsitzende selbst als Datenschutzbeauftragter benannt wurde.

Ein Schwerpunkt der Prüfungen bestand insbesondere im Umgang mit Sportlerfotos und deren Veröffentlichungen. In diesem Zusammenhang mussten zahlreiche Fotos insbesondere von den Webauftritten und zum Teil auch ganze Bilddatenbanken gelöscht werden, da die Betroffenen weder entsprechende Einwilligungen erteilt hatten noch über die Erhebung des jeweiligen Fotos und deren Verwendungszwecke informiert wurden.

Da zahlreiche Landesverbände Turnierplaner, Punktspielergebnisdienste oder auch Spielerpassverwaltungen von Drittanbietern nutzen, sind in diesen Fällen entsprechende Auftragsdatenverarbeitungsverträge erforderlich. In einem Fall wurde ein solcher Vertrag leider erst auf mehrfache Nachfragen hin abgeschlossen und nachgereicht.

Da im Bereich der Spielerpässe neben den Landesverbänden häufig auch die Bundesverbände und die Sportvereine vor Ort beteiligt sind, stellten sich in diesem Zusammenhang zahlreiche Fragen zur Abgrenzung der Verantwortlichkeiten sowie zur rechtmäßigen Übermittlung der Daten und den Informationspflichten zur Sicherstellung einer für die betroffenen Personen transparenten Verfahrensweise.

In einzelnen Fällen ergaben sich datenschutzrechtlich bedenkliche Verfahrensweisen aus den Satzungen der übergeordneten Verbände. Auf Initiative eines Landesverbandes wurde eine Bundesspielordnung angepasst, in zwei anderen Fällen bemühten sich die Landesverbände auf Bundesebene leider vergeblich um eine Begrenzung der bisher dort enthaltenen dauerhaften Speicherung der Sportlerdaten, sodass die für die Bundesverbände zuständigen Aufsichtsbehörden entsprechend vom ULD unterrichtet wurden.

Die jeweiligen Landesverbände verhielten sich diesbezüglich deutlich kooperativer und passten ihre Satzungen nach entsprechenden Hinweisen an. So enthielten einzelne Satzungen bisher zum Teil zu weitreichende Grundlagen zu Datenhebungen zum Erhalt von Spielberechtigungen oder auch Passagen, dass mit Teilnahme am Spielbetrieb der Nutzung der Sportlerdaten für kommerzielle und für Werbezwecke automatisch zugestimmt wurde.

5.5 Videoüberwachung

Das Thema Videoüberwachung bleibt vielfältig und facettenreich. Sowohl die Anzahl an Beschwerden als auch die Anzahl von Beratungsanfragen, die das ULD erreichen, steigt stetig. Unternehmen und Privatpersonen entscheiden sich meist aus Sicherheitsgründen für eine Videoüberwachung. Dass diese Entscheidung weitreichende Konsequenzen nach sich zieht, ist vielen dabei oftmals nicht bewusst. Durch die Datenschutz-Grundverordnung, die seit dem 25. Mai 2018 verbindlich gilt, wird auch im Zusammenhang mit Videoüberwachung das Thema Datenschutz verstärkt in der Öffentlichkeit wahrgenommen und hinterfragt. Neben der klassischen Videoüberwachung gewinnen u. a. mit Kameras bestückte Drohnen und sogenannte Dashcams an Beliebtheit. Bei solchen mobilen Geräten bedeutet es in der Regel für die Betreiber einen noch größeren Aufwand, die Vorgaben aus der Datenschutz-Grundverordnung zu erfüllen.

5.5.1 Videoüberwachung nach der DSGVO

Besonders spürbar ist die Datenschutz-Grundverordnung für die Betreiber von Videoüberwachungsanlagen durch die gestiegenen Anforderungen hinsichtlich der Informations- und Transparenzpflichten. Während nach dem alten Bundesdatenschutzgesetz der „Umstand der Beobachtung und die verantwortliche Stelle […] durch geeignete Maßnahmen erkennbar zu machen“ waren, schreibt die Datenschutz-Grundverordnung in mehreren Artikeln konkret vor, wie und worüber die betroffenen Personen informiert werden müssen. Auch bei einer Videoüberwachungsanlage handelt es sich um Datenverarbeitung, die für die betroffenen Personen nachvollziehbar sein muss. Daher müssen sie zum Zeitpunkt der Datenerhebung u. a. über den Umstand der Beobachtung, die Identität der verantwortlichen Stelle, die Kontaktdaten des Datenschutzbeauftragten, die Zwecke und die Rechtsgrundlage der Verarbeitung sowie die Speicherdauer informiert werden (keine abschließende Aufzählung). Häufig erhält das ULD Hinweise von Bürgerinnen und Bürgern, dass jemand eine Videoüberwachungsanlage betreibt, ohne auf diese hinzuweisen.

Die Aufsichtsbehörden des Bundes und der Länder sind sich darüber einig, dass aufgrund der Menge an Informationen ein abgestuftes Verfahren der Informationserteilung sinnvoll ist. Daher wurde speziell für Videoüberwachung ein Muster für eine Hinweisbeschilderung erarbeitet, die nach Auffassung der deutschen Datenschutzaufsichtsbehörden die Vorgaben der Datenschutz-Grundverordnung erfüllt. Das Muster ist in der Broschüre zum Thema Videoüberwachung enthalten, die unter folgendem Link abrufbar ist:

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

Dabei handelt es sich zwar nicht um ein verbindlich vorgeschriebenes oder genormtes Muster. Wenn jemand von der vorgeschlagenen Gliederung oder Gestaltung abweicht, beispielsweise weil andere Farben oder erweiternde Symbole genutzt werden oder derjenige z. B. die Betroffenenrechte stärker hervorheben möchte, kann das auch zulässig sein. Allerdings müssen die verpflichtenden Angaben zwingend enthalten sein, weshalb es durchaus empfehlenswert ist, das vorgeschlagene Muster zu nutzen oder als Orientierung heranzuziehen. Angaben wegzulassen oder pauschale allgemeine Aussagen zu treffen, entspricht nicht der Zielsetzung der Datenschutz-Grundverordnung, nämlich die Datenverarbeitung für betroffene Personen verständlicher zu gestalten und ihre Rechte zu stärken.

Auch auf EU-Ebene wird eine mehrstufige Informationserteilung befürwortet. Die Einzelheiten dazu, welche Informationen zu welchem Zeitpunkt bzw. in welcher Abstufung zu erteilen sind, befinden sich zurzeit noch in der Abstim-

mung zwischen den Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten. Die deutschen Vertreter in den europäischen Gremien setzen sich in diesem Prozess aktiv für einheitliche Standards nach deutschem Vorbild ein. Verantwortliche in Deutschland sind auf der sicheren Seite, wenn die von den Aufsichtsbehörden vorgeschlagenen Hinweisschilder genutzt werden. Da sich die rechtliche Anwendung der Datenschutz-Grundverordnung noch in einem frühen Stadium befindet, stehen die gegenwärtigen Interpretationen und Handlungsvorschläge aber immer unter dem Vorbehalt eines möglicherweise notwendigen Anpassungsbedarfs. Es lohnt sich daher, die aktuellen Entwicklungen in diesem Bereich im Blick zu behalten.

Hinweisbeschilderung

Eine korrekte Hinweisbeschilderung führt nicht allein dazu, dass der Betrieb der Videoüberwachung rechtmäßig ist. Die Zulässigkeit der Videoüberwachung ist vielmehr, wie auch nach dem alten Recht, anhand der Datenschutz-Grundverordnung sowie des Bundes- oder Landesdatenschutzgesetzes zu prüfen. Wenn der Verantwortliche aufgrund dieser Prüfung zu dem Ergebnis kommt, dass eine Videoüberwachung betrieben werden darf, sind die Transparenzpflichten der Datenschutz-Grundverordnung durch eine entsprechende Hinweisbeschilderung zu erfüllen.

Um zu bewerten, ob eine Videoüberwachung rechtmäßig betrieben wird, kommt es immer auf den Einzelfall an. Für die Überwachung müssen gute Gründe vorliegen. Nach der alten Rechtslage durften Betreiber von Videoüberwachungsanlagen lediglich ihre eigenen Interessen mit dieser Maßnahme verfolgen. Neu ist, dass nunmehr auch Interessen Dritter als Gründe für die Installation einer Videoüberwachung angeführt werden können und von der Aufsichtsbehörde bei einer Prüfung zu berücksichtigen sind. Dabei muss es sich aber um einen näher bestimmten Kreis Dritter handeln, die spezifische Interessen an der Videoüberwachung vorbringen können. Unzulässig wäre es, beispielsweise neben dem eigenen Grundstück auch einen großen Teil der Nachbarschaft mit der Begründung zu überwachen, dass die Videoüberwachung so auch die Nachbarn vor Einbrüchen schützen könnte und damit auch in deren Interesse betrieben werde.

Nach wie vor muss vor der Installation einer Videoüberwachungsanlage eine Interessenabwägung durchgeführt werden. Hierbei gelten nicht mehr – wie zuvor – ausschließlich streng objektive Maßstäbe. Es müssen nun auch die sogenannten „vernünftigen Erwartungen" der betroffenen Personen berücksichtigt werden. In Schalterhallen einer Bank ist beispielsweise eher mit einer Videoüberwachung zu rechnen als in öffentlichen Parks, im Treppenhaus von Mehrfamilienhäusern oder gar in sanitären Einrichtungen.

Was ist zu tun?

Besonders die Informations- und Transparenzpflichten sind deutlich umfangreicher geworden. Die Betreiber von Videoüberwachungsanlagen müssen daher ihre bisherigen Informationskonzepte kontrollieren und, sofern noch nicht geschehen, an die DSGVO anpassen. Das ist wichtig, damit betroffene Personen ihre Rechte gegenüber den Verantwortlichen auch wirksam wahrnehmen können. Besonders in Bezug auf die Hinweisbeschilderung für Videoüberwachungsanlagen sollten die Betreiber genau prüfen, an welcher Stelle sinnvollerweise welche Angaben gemacht werden können.

5.5.2 Fotos nach der DSGVO

Seit Mai des Jahres 2018 erreicht das ULD eine Vielzahl von mehr oder weniger umfangreichen Beratungsanfragen von Berufs- und Hobbyfotografen. Diese Personengruppe wird durch die Datenschutz-Grundverordnung im Hinblick auf deren Auswirkung auf das tägliche Geschäft der Fotografie stark verunsichert. Insbesondere befürchten viele Fotografen, dass sie entweder für das Erstellen und Veröffentlichen eines jeden Fotos eine separate Einwilligung der abgebildeten Personen benötigen oder zumindest jede abgebildete Person umfassend über die Ausgestaltung der Datenverarbeitung informieren müssen, selbst wenn diese nur zufällig und am Rande auf der Aufnahme erscheint. Für Beunruhigung sorgt auch die Vielzahl der Rechtsgebiete, die beim Thema Fotografie nebeneinander betrachtet werden müssen: Die Datenschutz-Grundverordnung, das Kunsturhebergesetz, zivilrechtliche Vorschriften und auch strafrechtliche Vorschriften spielen eine Rolle. Je nachdem wer die Bildaufnahme für welchen Verwendungszweck erstellt, gelten unterschiedliche Vorschriften. So ist für einen Teil der fotografierenden Personen die Datenschutz-Grundverordnung nicht anwendbar; andere, scheinbar vergleichbare Personengruppen müssen sich – aus ihnen oftmals nicht nachvollziehbaren Gründen – an die Vorschriften der Datenschutz-Grundverordnung halten.

Die Haushaltsausnahme

Das Anfertigen und Speichern von Fotos durch natürliche Personen unterliegt – jedenfalls soweit die Fotos im persönlichen Bereich verbleiben – von vornherein nicht den Beschränkungen der Datenschutz-Grundverordnung, da es sich hierbei um eine sogenannte persönliche oder familiäre Tätigkeit handelt. Das führt aber nicht dazu, dass der private Bereich zu einem rechtsfreien Raum wird. Vielmehr können in diesem Bereich die allgemeinen zivil- und strafrechtlichen Vorschriften einschlägig sein. Erstellt also ein Elternteil auf dem Kindergeburtstag seines Sohnes Aufnahmen von ihm und den Gästen, würden die Vorschriften der Datenschutz-Grundverordnung zwar nicht anwendbar sein. Die Landesbeauftragte für Datenschutz hätte in diesem Fall keine Untersuchungs- und Abhilfebefugnisse. Die Eltern der anderen anwesenden Kinder könnten sich jedoch notfalls auf dem Zivilrechtsweg gegen das Erstellen der Aufnahmen wehren.

Datenschutz-Grundverordnung oder Kunsturhebergesetz?

Wenn aber der private Bereich verlassen wird, etwa weil die Fotos im Internet einem unbeschränkten Personenkreis zugänglich gemacht werden, müssen auch natürliche Personen für „private" Fotos die Datenschutz-Grundverordnung von Beginn an beachten. Das hat zur Folge, dass bereits das Erstellen eines Fotos auf eine gesetzliche Grundlage gestützt werden können muss.

Der Anwendungsbereich der Datenschutz-Grundverordnung ist außerdem grundsätzlich immer eröffnet, wenn Fotos für berufliche, gewerbliche, oder sonstige nicht ausschließlich persönliche Zwecke erstellt und verarbeitet werden. Wenn das der Fall ist, muss bereits das Erstellen eines Fotos anhand der Datenschutz-Grundverordnung beurteilt werden, da das Kunsturhebergesetz nur die Veröffentlichung von Bildnissen regelt. Das bedeutet, dass sich in diesem Fall die Beurteilung der Rechtmäßigkeit des Anfertigens von Aufnahmen nach Art. 6 Abs. 1 DSGVO richtet.

Art. 6 Abs. 1 Buchst. f DSGVO

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

[…]

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

Bei einer Veröffentlichung stellt sich zudem die Frage, ob das Kunsturhebergesetz anwendbar ist oder ob die Rechtmäßigkeit einer Veröffentlichung nach den Vorschriften der Datenschutz-Grundverordnung zu bewerten ist.

Besonderheit Presse

Im journalistischen Bereich ergibt sich eine Besonderheit durch das sogenannte Medienprivileg. In Artikel 85 DSGVO ist verankert, dass Mitgliedstaaten Abweichungen von der Datenschutz-Grundverordnung für die Verarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken erlassen können.

Hiervon hat Schleswig-Holstein Gebrauch gemacht. Nach § 10 Landespressegesetz Schleswig-Holstein gilt die Datenschutz-Grundverordnung für die Verarbeitung von personenbezogenen Daten für journalistische oder literarische Zwecke weitgehend nicht. Daraus ergibt sich, dass für den journalistischen Bereich das Kunsturhebergesetz weiterhin anwendbar ist.

Nicht journalistischer Bereich

Für Fotos, die außerhalb journalistischer oder literarischer Zwecke veröffentlicht werden, gilt die Datenschutz-Grundverordnung uneingeschränkt. Ob daneben für die Veröffentlichung auch das Kunsturhebergesetz anwendbar ist, war im vergangenen Jahr ein großes juristisches Streitthema. Für die Zulässigkeit von Veröffentlichungen bedeutet dies im Ergebnis keinen Unterschied. Nach Art. 6 Abs. 1 Buchst. f DSGVO ist ebenso wie nach § 23 Kunsturhebergesetz eine Abwägung der verschiedenen Interessen vorzunehmen. Die Regelbeispiele des Kunsturhebergesetzes können auch bei der Interessenabwägung nach der Datenschutz-Grundverordnung herangezogen werden.

Mittlerweile gibt es eine erste Gerichtsentscheidung, die ebenfalls die Frage der unmittelbaren Anwendbarkeit des Kunsturhebergesetzes offenlässt, weil die Anwendbarkeit der DSGVO zu keinem anderen Ergebnis führt (Landgericht Frankfurt am Main, Urteil vom 13.09.2018, 2-03 O 283/18).

§ 23 Kunsturhebergesetz

(1) Ohne die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:

1. Bildnisse aus dem Bereiche der Zeitgeschichte;

2. Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;

3. Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;

4. Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.

(2) Die Befugnis erstreckt sich jedoch nicht auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten oder, falls dieser verstorben ist, seiner Angehörigen verletzt wird.

Transparenzpflichten

Die Datenschutz-Grundverordnung enthält neben den Regelungen zur Zulässigkeit der Datenverarbeitung eine ganze Reihe weiterer Vorgaben. Hierzu gehören u. a. die Transparenzpflichten nach Artikel 13 und Artikel 14 DSGVO. Diese Pflichten sind für viele Tätigkeiten von Fotografinnen und Fotografen in der Praxis nicht immer einfach zu erfüllen. Das gilt vor allem wenn Fotografien von größeren Menschenmengen erstellt werden. Hier haben einzelne Fotografinnen und Fotografen häufig keine Möglichkeit, die betroffenen Personen über die Datenverarbeitung zu informieren. In solchen Fällen sind Ausnahmen von den Informationspflichten nach Maßgabe des Art. 14 Abs. 5 DSGVO möglich. Danach gilt die Pflicht zur Information nicht, wenn die Daten ohne Mitwirkung der betroffenen Person erhoben

werden und die Erteilung der Information sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde. An diese Voraussetzungen sind jedoch aufgrund des Ausnahmecharakters der Vorschrift hohe Anforderungen zu stellen.

Ergebnis und Ausblick

Im Ergebnis ist festzustellen, dass gegenwärtig eine Unsicherheit darüber besteht, welche Vorschriften in welchen Fällen für Fotografinnen und Fotografen und ähnliche Gruppen anzuwenden sind, die nicht unter das Pressegesetz oder den Rundfunkstaatsvertrag fallen. Zu rechtlichen Einschränkungen der Fotografie führt die Gemengelage der Rechtsvorschriften zwar nicht, wohl aber zu einer Belastung der Personen, die sich als Anwender mit den Vorschriften auseinandersetzen müssen.

Der Gesetzgeber hat den Spielraum, den Artikel 85 DSGVO für nationale Regelungen bietet, um die Freiheit der Meinungsäußerung und die Informationsfreiheit zu gewährleisten, noch nicht vollständig ausgeschöpft. Spezifische Regelungen zur Fotografie in diesen Bereichen könnten einen Mehrwert darstellen und die Rechtssicherheit erhöhen, wenn sie den gesamten Lebenszyklus einer Fotografie abbilden würden. Dafür müssten sie auch andere Arten der Datenverarbeitung als die im Kunsturhebergesetz geregelte Veröffentlichung einbeziehen und sich nicht auf die Frage der Zulässigkeit der Datenverarbeitung beschränken. Da das Kunsturhebergesetz lediglich die Verbreitung von Bildnissen regelt, gilt für alle anderen Verarbeitungsschritte derzeit die Datenschutz-Grundverordnung unmittelbar, so wie vor dem 25. Mai 2018 hierfür das Bundes- oder Landesdatenschutzgesetz galt. Ein neues Gesetz könnte durch Einbeziehung aller Phasen der Datenverarbeitung, von der Erstellung über die Veröffentlichung bis hin zur Löschung, eine umfassende Regelung für die Zulässigkeit der Verarbeitung von Personenfotos schaffen. Auch die Frage der Transparenz könnte in einem solchen Gesetz bereichsspezifisch geregelt werden.

Was ist zu tun?

Wünschenswert zur Klarstellung des Themenkomplexes wäre ein Gesetz, das den gesamten Lebenszyklus eines Fotos umfassend regelt. Dieses Gesetz sollte Regelungen zum Erheben über das Aufbewahren bis hin zum Veröffentlichen und schlussendlich Löschen von Fotografien beinhalten. Da insbesondere der Beruf des Fotografen sich nicht an Ländergrenzen orientiert, ist es sinnvoll, eine bundesländerübergreifende Regelung zu schaffen. Hier wäre somit der Bundesgesetzgeber gefragt.

5.5.3 Videoüberwachung im Studentenwohnheim

Das ULD hat sich aufgrund einer Beschwerde mit einer Videoüberwachung in einem Studentenwohnheim beschäftigt. Überwacht wurden die Gemeinschaftsküchen, Flure vor den Privatzimmern der Bewohner sowie das Treppenhaus des Gebäudes. Als Begründung führte der Verantwortliche an, dass die Studierenden die Angewohnheit hätten, zu später Stunde ausschweifende Partys insbesondere in den Gemeinschaftsküchen zu veranstalten. Dabei seien mehrfach u. a. diverse Einrichtungsgegenstände zerstört worden; zudem wurden Fahrstühle beschädigt und Mitbewohner durch verschiedene Handlungen gefährdet und belästigt.

Obwohl die Beschädigungen durch die Studierenden gravierend waren und es nachvollziehbar ist, dass man solchen Ausschweifungen

Einhalt gebieten möchte, hält das ULD die Videoüberwachung in den oben genannten Bereichen für höchst bedenklich. Es muss berücksichtigt werden, dass Studierende in einem Wohnheim zumindest für die Zeit eines Semesters tatsächlich leben, Zeit verbringen und Freunde treffen. In diesem sehr privaten Umfeld von dem eigenen Vermieter überwacht zu werden, kann keine Option sein. Die Unverletzlichkeit der Wohnung ist durch das Grundgesetz besonders geschützt. Zwar ist ein Studentenwohnheim eine andere Art von Wohnung, aber es stellt für die Studierenden zumindest für einen gewissen Zeitraum den zentralen Lebensmittelpunkt dar. Die Überwachung in einem solchen Bereich bedeutet einen erheblichen Eingriff in die Grundrechte und Grundfreiheiten der dort lebenden Studierenden sowie deren Besuch. Dieser kann nicht durch die eingangs näher dargestellten Beschädigungen aufgewogen werden. Auch kann die Eingriffsintensität für die betroffenen Personen durch Maßnahmen wie eine zeitliche Einschränkung oder ein strenges Zugriffs- und Berechtigungskonzept nicht so abgemildert werden, dass die Videoüberwachung akzeptiert werden könnte.

Da der Betreiber der Videoüberwachung diese zwischenzeitlich abgeschaltet hat, wurde dieser vor der erneuten Inbetriebnahme gewarnt. Außerdem wird die Einleitung eines Bußgeldverfahrens geprüft.

5.5.4 Nachbarschaftsüberwachung

Ein Großteil von Beschwerden zum Thema Videoüberwachung erhält das ULD von Personen, die sich von einem ihrer Nachbarn überwacht fühlen. Wenn am eigenen Haus schon einmal ein Einbruch verübt worden ist, ist die Schwelle, sich für eine Videoüberwachung zu entscheiden, meistens niedrig. Zu beobachten ist, dass viele Personen eine Videoüberwachungsanlage installieren, ohne den datenschutzrechtlichen Rahmen zu beachten und ohne ihre Nachbarn zu informieren. Häufig fehlt einzelnen Privatpersonen schlicht das Wissen, was genau bei der Installation einer Videoüberwachungsanlage aus datenschutzrechtlicher Sicht beachtet werden muss. Oftmals wird die Videoüberwachung eines Nachbarn im Rahmen eines ohnehin bereits eskalierenden Nachbarschaftsstreits auch als zusätzliche Belastung wahrgenommen, unabhängig davon, ob die Kameras aus datenschutzrechtlicher Sicht korrekt eingestellt sind. Solche Streitigkeiten, die ihre Wurzeln in ganz anderen Bereichen fernab von datenschutzrechtlichen Themen haben, führen auch häufig dazu, dass eine Seite sich bewusst für die Installation der Videoüberwachungsanlage entscheidet, entweder um das Fehlverhalten der anderen Seite zu dokumentieren oder als Trotzreaktion, da sich die andere Seite „ja auch nicht an Recht und Gesetz hält".

Videoüberwachung am eigenen Haus oder auf dem eigenen Grundstück kann durchaus in zulässiger Weise betrieben werden. Sofern mit der Videoüberwachung ausschließlich das eigene Grundstück überwacht wird, das sich erkennbar vom öffentlich zugänglichen Verkehrsraum abhebt, findet die Videoüberwachung im Rahmen der sogenannten Haushaltsausnahme statt.

Haushaltsausnahme

Wird eine Videoüberwachung von einer natürlichen Person ausschließlich zum Zweck sogenannter „ausschließlich persönlicher und familiärer Interessen" betrieben, ist die Datenschutz-Grundverordnung nicht anwendbar. Das ist regelmäßig dann der Fall, wenn die Videoüberwachung auf das eigene private Grundstück beschränkt wird und Nachbargrundstücke sowie öffentliche Verkehrsräume nicht mit überwacht werden. Wenn jedoch Aufnahmen veröffentlicht werden oder Angestellte im eigenen Haus oder auf dem eigenen Grundstück beschäftigt werden, dürfte die Videoüberwachung nicht mehr als ausschließlich persönliche oder familiäre Tätigkeit angesehen werden können.

Das hat zur Folge, dass die Datenschutz-Grundverordnung nicht anwendbar ist. Das wiederum hat zur Folge, dass die Videoüberwachung nicht der Kontrolle durch das ULD unterliegt. Somit hat in diesen Fällen die Landesbeauftragte für Datenschutz keine Befugnisse, beispielsweise Untersagungen auszusprechen oder ein Bußgeld zu verhängen. Wenn befürchtet wird, dass ein Nachbar neben seinem eigenen Grundstück auch umliegende und direkt angrenzende Nachbargrundstücke überwacht, kann man sich hiergegen auf dem Zivilrechtsweg wehren.

Nähere Hinweise hierzu sind unter folgendem Link veröffentlicht:

https://www.datenschutzzentrum.de/artikel/1051-.html

Was ist zu tun?

Die Videoüberwachung des eigenen Grundstücks darf auch nur dieses erfassen. Öffentliche Bereiche, wie z. B. Wege und Straßen, oder gemeinschaftlich genutzte Flächen, wie z. B. Auffahrten oder Treppenhäuser, müssen frei von Überwachungsmaßnahmen bleiben. Es ist sehr empfehlenswert, die direkten Nachbarn von der Videoüberwachung und den Gründen, die zu der Installation geführt haben, in Kenntnis zu setzen und sich offen gegenüber Fragen zu verhalten. Erfahrungsgemäß führt erhöhte Transparenz zu mehr Akzeptanz. Von einer provokanten Videoüberwachung aus dem Gefühl heraus, selbst durch Nachbarn ungerecht behandelt zu werden, sollte abgesehen werden.

5.5.5 Einsatz einer Dashcam

Unter einer Dashcam ist eine Kamera zu verstehen, die in oder an einem Fahrzeug angebracht ist und während der Fahrt das Geschehen aufzeichnet, das sich frontal vor dem Fahrzeug abspielt. Einerseits kann eine Dashcam Verkehrsunfälle dokumentieren und auf diese Weise gegebenenfalls zur Verkehrssicherheit oder zur Aufklärung von Verkehrsunfällen beitragen. Andererseits kann durch Dashcams auch eine Atmosphäre der Überwachung erzeugt werden, insbesondere wenn eine große Anzahl an Fahrzeugen mit einer solchen Kamera ausgestattet ist. Eine solche Überwachung würde ganz überwiegend anlasslos stattfinden, da ein Unfall eher die Ausnahme als die Regel darstellt. Auch kann nicht damit argumentiert werden, dass die Teilnahme am Straßenverkehr prinzipiell gefährlich sei, da dies die Schlussfolgerung zuließe, auch andere Verkehrsteilnehmer wie Fußgänger und Radfahrer könnten oder müssten sich mit Dashcams ausstatten. Dies würde im Ergebnis zu einer nahezu lückenlosen Überwachung des gesamten Verkehrsgeschehens führen. Der einzelne Verkehrsteilnehmer würde sich auf Kosten des allgemeinen Persönlichkeitsrechts anderer vor einem allgemeinen Lebensrisiko und nur möglicherweise eintretenden Schäden schützen wollen.

Die Aufgabe der Datenschutzaufsichtsbehörden besteht nun darin, durch Aufklärung über den datenschutzkonformen Einsatz von Dashcams und Sanktionierung nicht datenschutzkonformer Einsätze die Persönlichkeitsrechte der betroffenen Verkehrsteilnehmer zu schützen. Dabei muss besonders das Urteil des Bundesgerichtshofs (BGH) vom Mai 2018 berücksichtigt werden. Der BGH hält die permanente und anlasslose Aufzeichnung des Verkehrsgeschehens für nicht vereinbar mit den datenschutzrechtlichen Vorschriften. Die Verwertung der Aufnahmen als Beweismittel in einem Unfallhaftpflichtprozess sei dennoch zulässig.

Datenschutzrechtliche Zulässigkeit versus Beweisverwertung

Nur weil Dashcam-Aufnahmen in einem Gerichtsverfahren als Beweis zugelassen werden, bedeutet das nicht, dass der Betrieb dieser Dashcam auch aus datenschutzrechtlicher Sicht zulässig war. Wenn die Datenschutzaufsichtsbehörden von dem rechtswidrigen Betrieb einer Dashcam Kenntnis erlangen, können dem Betreiber oder der Betreiberin hohe Bußgelder oder ein Verbot durch die Aufsichtsbehörde drohen.

BGH, Urteil vom 15. Mai 2018 – VI ZR 233/17

Wenn mit Dashcams das allgemeine Verkehrsgeschehen gefilmt werden soll und der Zweck darin liegt, einen möglichen Unfallhergang zu dokumentieren, ist der Anwendungsbereich der Datenschutz-Grundverordnung eröffnet und die Rechtmäßigkeit einer solchen Kamera nach den darin enthaltenen Vorschriften zu prüfen. Der Einsatz einer Dashcam kann nur zulässig sein, soweit dies zur Wahrung berechtigter Interessen von Verantwortlichen oder Dritten erforderlich ist und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Dashcams, mit denen die gesamte Autofahrt vom Start bis zum Ende gefilmt und gespeichert wird, verarbeiten permanent ohne Anlass personenbezogene Daten. Das heißt, dass eine Vielzahl unbeteiligter Personen aufgezeichnet wird, ohne dass hierfür ein Grund besteht. Auch kann eine Person, die beispielsweise gerade eine Straße kreuzt, nicht oder nur schwierig wahrnehmen, dass ihr Verhalten in diesem Moment gefilmt wird. Die Interessen des Einzelnen, sich grundsätzlich frei und unbeobachtet im öffentlichen Verkehrsraum bewegen zu können, ist schwerer zu gewichten als das Interesse eines Autofahrers daran, einen Unfall aufzuklären, der sich nur möglicherweise ereignen könnte. Für den theoretisch möglichen Fall eines Verkehrsunfalls permanent Aufnahmen anzufertigen, um diese gegebenenfalls als Beweismittel in einem Gerichtsverfahren zu verwenden, kann den erheblichen Eingriff in das Grundrecht der betroffenen Personen auf den Schutz personenbezogener Daten nicht rechtfertigen.

Eine Ausnahme von diesem Ergebnis kann – so auch der Bundesgerichtshof – überhaupt nur in Betracht kommen, wenn eine Kamera bestimmte Datenschutzmechanismen aufweist. Dabei handelt es sich insbesondere um technische Maßnahmen, um den Eingriff in die Grundrechte der betroffenen Personen so gering wie möglich zu halten, wie z. B. die Verwendung einer Kamera, die nur kurzzeitig anlassbezogen aufzeichnet, etwa wenn eine Kollision stattfindet oder der Fahrer stark abbremst oder eine ruckartige Lenkradbewegung durchführt. Ein solcher Mechanismus ist auch eine automatisierte, dem Eingriff des Verwenders entzogene Löschung. Welche Maßnahmen konkret ergriffen werden müssen, hängt vom Einzelfall ab.

Schon jetzt muss das Risiko berücksichtigt werden, dass sich die Bevölkerung zu einer Gesellschaft weiterentwickelt, in der nicht nur alle Fahrzeuge mit eingebauten Kameras ausgestattet sind, sondern alle Bundesbürger mit Kameras ausgestattet herumlaufen, um gegebenenfalls Situationen aufzunehmen, die eine Straftat aufdecken oder für zivilrechtliche Haftungsfragen relevant sein könnten. Das Recht unbeteiligter Personen, selbst bestimmen zu können, wann man sich wo mit wem aufhält, ohne dass unbeteiligte Personen dies anlasslos dokumentieren, würde durch so eine gesellschaftliche Entwicklung erheblich beeinträchtigt werden.

Was ist zu tun?

Autofahrer sollten von einem leichtfertigen Umgang mit dem Betrieb einer Dashcam absehen. Außerdem ist im Hinblick auf Dashcams vor allem die gesellschaftliche Entwicklung in ihrer Gesamtheit zu betrachten. Welche Entwicklungen dienen wirklich der Sicherheit, und welche erhöhen lediglich das Sicherheitsgefühl und sind tatsächlich eher freiheitsberaubend? Sollte zukünftig jeder mit einer Art Dashcam ausgestattet sein – würde das dann die Sicherheit erhöhen oder die Freiheit eines Individuums einschränken? Der Gesetzgeber könnte mit einer klaren gesetzlichen Regelung entscheiden, ob und in welcher Ausgestaltung der Betrieb von Dashcams zulässig ist. Dies würde einerseits die Rechtssicherheit erhöhen und außerdem auf eine einheitliche (Sanktions-)Praxis der Aufsichtsbehörden hinwirken.

5.5.6 Videoüberwachung im Fitnessstudio

Bereits im letzten Tätigkeitsbericht wurde über den Verfahrensstand bei einer Videoüberwachung in einer Fitnessstudiokette berichtet (36. TB, Tz. 5.6.3). Im Jahr 2017 wurde dem Fitnessstudio der Betrieb der Videoüberwachung untersagt. Neben Trainingsflächen wurden Aufenthaltsbereiche und auch Umkleidebereiche gefilmt. Dies ist eine schwerwiegende Beeinträchtigung der Rechte und Freiheiten derjenigen, die in den betreffenden Studios trainieren und ihre Freizeit verbringen. Besonders die Videoüberwachung der Umkleidebereiche, in denen sich die Kunden des Fitnessstudios leicht oder gar nicht bekleidet aufhalten, greift erheblich in deren Privatsphäre ein. Gegen die Anordnung der Landesbeauftragten für Datenschutz hat der Betreiber zunächst Widerspruch eingelegt und dann, als dem Widerspruch nicht abgeholfen wurde, Klage vor dem Verwaltungsgericht in Schleswig erhoben. Die Entscheidung des Gerichts bleibt abzuwarten.

Nach wie vor erreichen das ULD Beschwerden oder Nachfragen von Mitgliedern der Fitnessstudiokette zu der Videoüberwachung in den Studios. Die Personen berichten, dass sie sich durch die Kameras beim Trainieren unangenehm beobachtet fühlen und nicht wissen, was genau mit den Aufnahmen geschieht.

5.5.7 Videoüberwachung von Beschäftigten

Immer wieder erreichen das ULD Eingaben von Beschäftigten, die von ihrem Arbeitgeber an ihrem Arbeitsplatz mit Kameras gefilmt werden. So wurden diese in Werkstätten, Großraumbüros, im Einzelhandel, Lagerräumen oder sogar in Sozialräumen aufgenommen. Einzelne Mitarbeiterinnen und Mitarbeiter berichteten hierbei von der Nutzung der Kameras für Verhaltens- und Leistungskontrollen durch ihre Vorgesetzten.

Eine solche Videoüberwachung stellt nach Auffassung des Bundesarbeitsgerichtes den denkbar intensivsten Eingriff in das informationelle Selbstbestimmungsrecht eines Beschäftigten dar. Diese kann dem Arbeitgeber ermöglichen, seine Beschäftigten in ihrer ganzen wahrnehmbaren Persönlichkeit zu beobachten (Monitoring) und/oder reproduzierbar festzuhalten (Aufzeichnung). Arbeitgeber dürfen lediglich die für die betrieblichen Zwecke erforderlichen

Daten über ihre Beschäftigten erheben. Dabei ist zu berücksichtigen, dass Arbeitnehmer grundsätzlich keinem permanenten Kontrolldruck durch ihren Arbeitgeber ausgesetzt sein dürfen.

Auch wenn verschiedene Unternehmen in den Verfahren für die von ihnen eingesetzte Videoüberwachung Gründe anführen, die vordergründig gar nichts mit den Beschäftigten zu tun haben (beispielsweise Verhinderung von Ladendiebstählen), müssen weiterhin auch die Interessen der Beschäftigten gewahrt bleiben. Im Rahmen der Abwägung der Erforderlichkeit einer solchen Videoüberwachung gegenüber dem Recht auf informationelle Selbstbestimmung des Beschäftigten ist u. a. auch entscheidend, inwieweit dem Beschäftigten noch Rückzugsmöglichkeiten verbleiben.

Verschiedene Arbeitgeber teilten darüber hinaus mit, dass ihre Beschäftigten mit der Videoüberwachung einverstanden seien und sich bei ihrem Vorgesetzten bisher auch noch nicht beschwert hätten, sodass diese auf die Grenzen der Wirksamkeit einer im Rahmen des Beschäftigtenverhältnisses erhobenen Einwilligung hingewiesen werden mussten.

Einwilligung

Im Beschäftigungsverhältnis kommt eine freiwillige und damit wirksame Einwilligung aufgrund des bestehenden Über-/Unterordnungsverhältnisses in der Regel nicht in Betracht.

Da sich in zahlreichen Beschwerden insbesondere darüber beklagt wurde, dass die Arbeitgeber lediglich die Kameras installiert hätten und sich ansonsten in Schweigen hüllen, mussten diese auch bei rechtmäßig betriebenen Systemen ihre Verfahren in den Bereichen der gesetzlich vorgeschriebenen Informations-, Transparenz- und Dokumentationspflichten nachbessern.

Hierbei sind die Beschäftigten u. a. über den Erhebungszweck und -umfang, Zugriffsanlässe und -berechtigungen, Protokollierung, Speicherdauer sowie über ihre bestehenden Rechte betroffener Personen zu informieren. Zur Wahrung der Rechte der Beschäftigten und eines transparenten Verfahrens kann auch der Abschluss von Kollektivvereinbarungen oder die Abgabe von Verpflichtungserklärungen der Arbeitgeber hilfreich sein. Diese sollten jedoch immer auch einen Ausschluss der Nutzung der Systeme für Verhaltens- und Leistungskontrollen beinhalten.

Im Rahmen der durchgeführten Verfahren wurden zahlreiche Kameras abgeschaltet, neu ausgerichtet oder Erfassungsbereiche geschwärzt, Dokumentationen und Beschilderungen nachgebessert und die Nutzung der Systeme für Verhaltens- und Leistungskontrollen zum Teil auch durch Aufnahme entsprechender Passagen in die Arbeitsverträge ausgeschlossen.

Abschließend ist darauf hinzuweisen, dass die Entscheidung über die Verwertungsmöglichkeit von Bildmaterial für arbeitsgerichtliche Verfahren den Gerichten obliegt. Diese sind grundsätzlich gehalten, von den Parteien angebotene Beweismittel zu berücksichtigen, sodass nicht jeder Verstoß gegen datenschutzrechtliche Bestimmungen zwangsläufig auch ein Beweisverwertungsverbot zur Folge hat.

5.6 Datenpannen in der Wirtschaft

Mit der Datenschutz-Grundverordnung wurde eine neue Meldepflicht für Datenschutzverletzungen eingeführt.

Eine Verletzung des Schutzes personenbezogener Daten ist in Art. 4 Nr. 12 DSGVO als eine Verletzung der Sicherheit definiert, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenbarung von Daten oder zum unbefugten Zugang zu solchen Daten führt. Anders als nach altem Recht umfasst die Definition alle Arten von personenbezogenen Daten. Solche Verletzungen sind nach Artikel 33 DSGVO der Datenschutzaufsichtsbehörde un-

verzüglich und möglichst binnen 72 Stunden zu melden. In der Meldung hat der Verantwortliche auch Ausführungen dazu zu machen, welche Maßnahmen zur Behebung der Verletzung und gegebenenfalls zur Abmilderung ihrer Folgen ergriffen wurden. Die Meldepflicht entfällt nur dann, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Formulare für die Meldung an das ULD sind abrufbar unter:

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

In gravierenden Fällen reicht die Meldung an die Datenschutzaufsichtsbehörde nicht aus. Es sind dann nach Artikel 34 DSGVO auch die betroffenen Personen zu informieren. Dies ist der Fall, wenn die Verletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

Durch die Meldepflicht soll frühzeitig Transparenz über eingetretene Datenschutzverletzungen hergestellt werden. Dadurch soll es allen Beteiligten ermöglicht werden, ein größeres Ausmaß des Schadens zu vermeiden, wie etwa einen Identitätsdiebstahl oder -betrug, finanzielle Verluste oder Rufschädigung. Die Datenschutzaufsichtsbehörde kann nach Eingang einer Meldung prüfen, ob sie gegenüber dem Verantwortlichen Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen anordnet. Eine Anordnung unterbleibt vor allem dann, wenn die vom Verantwortlichen ergriffenen Maßnahmen zur Behebung des Schadens als ausreichend anzusehen sind.

Beim ULD sind seit Ende Mai 2018 zahlreiche Meldungen eingegangen. Einige davon werden nachfolgend dargestellt:

- Eine Jugendhilfeeinrichtung verschickt einen unverschlüsselten USB-Stick mit Bildern von Kindern und Jugendlichen an das Jugendamt. Der USB-Stick geht beim Postversand verloren und ist bis heute nicht wieder aufgetaucht. Zukünftig sollen die Daten nur noch verschlüsselt übermittelt werden.
- Mitarbeiter eines Krankenhauses schauen sich die Patientenakte eines Kollegen an, obwohl sie nicht an der Behandlung beteiligt sind. Zukünftig sollen ein Berechtigungskonzept, die Protokollierung von lesenden Zugriffen, eine Dienstanweisung und Kontrollen sicherstellen, dass Mitarbeiter nur auf Patientendaten zugreifen, die sie auch etwas angehen.
- Eine Auszubildende in einer Zahnarztpraxis erkennt in einem neuen Patienten einen Bekannten und schickt schnell mal Kopien der Patientendaten an eine gemeinsame Freundin. Der Auszubildenden wurde fristlos gekündigt.
- Eine Hebamme macht Hausbesuche bei den von ihr betreuten Schwangeren. Ihr Auto wird aufgebrochen und der Hebammenkoffer mit den Patientenakten gestohlen. Zukünftig sollen Patientenunterlagen nicht mehr unbeaufsichtigt im Auto liegen gelassen werden.
- In einer Arztpraxis wird eingebrochen. Gestohlen wird u. a. auch die Datensicherung. Gott sei Dank waren die Daten verschlüsselt. Alles richtig gemacht!
- Eine Sozialarbeiterin verliert ihr dienstliches Smartphone mit unverschlüsselten Kontaktdaten, SMS-Nachrichten usw. Zukünftig sollen auch diese Daten durch eine Verschlüsselung gesichert werden.
- Der Klassiker: Arztbriefe, Arztrechnungen usw. werden per Post oder per Fax einem falschen Empfänger übersandt. Häufigste Ursache ist eine Namensverwechslung. Oder es werden zwei Briefe für unterschiedliche Empfänger in einem Brief versandt. Mitarbeiter müssen geschult und sensibilisiert werden.
- Eine Patientin stiehlt in einem Krankenhaus Patientenunterlagen (Entlassungsbriefe), und keiner weiß, wie sie an diese Unterlagen gelangen konnte. Aufwendig wurden alle Arbeitsabläufe der betroffenen Station überprüft. Räume, in denen Patientenunterlagen aufbewahrt werden, wurden zusätzlich gesichert.

- Ein Patient wartet in einem Behandlungsraum der Notfallambulanz eines Krankenhauses zwei Stunden lang auf den Arzt. Er ist allein. In dem Raum befindet sich ein Computer, und dieser ist nicht gesperrt. Der Patient hat damit Zugang zu den Daten sämtlicher Patienten des Krankenhauses. Zukünftig werden alle unbeaufsichtigten Computer automatisch gesperrt.

Was ist zu tun?

Kommt es zu einer Verletzung des Schutzes personenbezogener Daten, muss der Verantwortliche prüfen, welche Schäden für die betroffenen Personen drohen, und die erforderlichen Maßnahmen ergreifen, um den schon eingetretenen Schaden zu begrenzen und weitere Schäden zu verhindern. Dazu gehört auch die Prüfung, ob der Vorfall an die Datenschutzaufsichtsbehörde zu melden ist und die betroffenen Personen zu informieren sind.

5.6.1 Versendung von Urinbeuteln und Abgabe bei der Nachbarin

Im Herbst 2017 erreichte das ULD ein Hinweis auf die Verwendung von Paketaufdrucken mit Hinweisen zum Paketinhalt. Demnach wurde mitgeteilt, dass im Rahmen der Versendung einer Bestellung von Urinbeuteln der vom Unternehmen genutzte Versandkarton beidseitig mit zwei großen Etiketten versehen wurde, auf denen detailliert, übersichtlich und mehrsprachig der Inhalt der Sendung angegeben wurde.

Da Empfänger häufig nicht persönlich anwesend sind, um eigenhändig die Warensendung in Empfang zu nehmen, ist es bei den Paketzustellern weit verbreitet, dass sie bei Abwesenheit die Sendung gegebenenfalls bei den Nachbarn hinterlassen.

In dem vorliegenden Fall führte dies dazu, dass die bisher ahnungslose Nachbarin von der Inkontinenz des Betroffenen erfuhr, da dieser zum Zeitpunkt der Lieferung nicht vor Ort war und der Paketzusteller die Sendung der Nachbarin übergab.

Gründe für eine Erforderlichkeit der Angabe des Inhaltes auf der äußeren Verpackung konnten vom Unternehmen in dem daraufhin eingeleiteten Verfahren nicht vorgetragen werden. Da durch die Angabe des Inhaltes gegebenenfalls auch der Gesundheitszustand des Empfängers hergeleitet werden kann, handelte es sich um besonders sensible Informationen, die entsprechend besonders schützenswert sind. Des Weiteren kann eine Warenversendung in der Regel auch ohne Angabe des Inhaltes auf der äußeren Verpackung erfolgen.

Nach Mitteilung des Unternehmens habe eine Lagerkraft trotz eingehender Schulung versehentlich einen mit dem entsprechenden Etikett versehenen leeren Karton aus der Anlieferung für den Versand wiederverwendet, obwohl diese zu entsorgen oder nur für unkritische Zwecke zu verwenden seien.

Der Vorfall wurde vom Unternehmen als Anlass genommen, die Verfahrensweisen im Versand anzupassen und nunmehr zusätzliche Umkartons als neutrale Verpackungen einzusetzen. Darüber hinaus wurden auch die mit dem Versand betrauten Mitarbeiterinnen und Mitarbeiter nochmals entsprechend geschult.

5.6.2 Entsorgung von Kundenunterlagen in der Papiertonne eines Mehrfamilienhauses

Nach Entfall des ursprünglichen Erhebungszweckes und Ablauf etwaiger Aufbewahrungsfristen sind neben der elektronischen Löschung auch die betreffenden schriftlichen Dokumente und Unterlagen regelmäßig zu vernichten. In diesem Zusammenhang erhielt das ULD Kenntnis von sensiblen Kundenunterlagen, die in einer gemeinsam genutzten Papiertonne eines Mehrfamilienhauses entsorgt wurden.

Das betreffende Unternehmen hatte als einer der Nutzer des Mehrfamilienhauses die Unterlagen ungeschreddert in der dortigen Papiertonne entsorgt, sodass die übrigen Bewohnerinnen und Bewohner auf personenbezogene Kundendaten wie beispielsweise Name, Vorname, Telefonnummer, Wohnadresse, Geburtsdatum und Beruf zugreifen konnten.

Ein betriebsinternes Löschkonzept sollte neben konkreten Angaben über die Speicherdauer (bzw. Kriterien für die Festlegung der Dauer) auch Regelungen zur datenschutzkonformen Dokumentenentsorgung enthalten.

Darüber hinaus sind in diesem auch Verfahren zur Entsorgung externer Speichermedien wie CD-ROMs, DVDs, USB-Sticks und externen Festplatten festzulegen.

Löschen / Vernichten

Sowohl das „Löschen" als auch das „Vernichten" bilden einen eigenen Verarbeitungsvorgang im Sinne des Art. 4 Nr. 2 DSGVO.

Nachdem das Unternehmen darauf hingewiesen wurde, dass es verpflichtet ist, auch für die Entsorgung geeignete technisch-organisatorische Maßnahmen zu treffen, um eine Offenlegung zu verhindern, teilte dieses mit, für die Entsorgung nunmehr einen eigenen abschließbaren Papiercontainer sowie einen Schredder zu nutzen und die Mitarbeiterinnen und Mitarbeiter entsprechend informiert und sensibilisiert zu haben.

Was ist zu tun?

Ein Löschkonzept sollte die Art und Menge der zu entsorgenden Datenträger, die dabei zu berücksichtigenden Schutzstufen, die Auswahl geeigneter Vernichtungsverfahren, Vernichtungszyklen sowie Festlegungen zur Kontrolle der Maßnahmen, der Verantwortlichkeiten und eventueller Haftungen beinhalten.

5.6.3 Verwendung offener E-Mail-Verteiler

Seit Geltung der DSGVO erhält das ULD immer wieder Kenntnis von Fällen, in denen Verantwortliche E-Mail-Nachrichten an eine Vielzahl von Empfängern in einer Art und Weise aussenden, dass sämtliche angesprochene E-Mail-Adressen für alle anderen Empfänger der E-Mail sichtbar waren (sogenannter offener E-Mail-Verteiler). Dies geschieht in einigen Fällen offenbar in Unkenntnis der Funktionen des E-Mail-Clients.

Die Verarbeitung personenbezogener Daten ist gemäß Art. 6 Abs. 1 DSGVO nur zulässig, wenn dafür eine gesetzliche Grundlage oder die Einwilligung der betroffenen Personen vorliegt. Verantwortliche haben dafür Sorge zu tragen,

dass personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung (Art. 5 Abs. 1 Buchst. f DSGVO). Dazu sind u. a. geeignete technische und organisatorische Maßnahmen wahrzunehmen, um sicherzustellen, dass eine Verarbeitung personenbezogener Daten gemäß der DSGVO erfolgt.

Bei einer Vielzahl der verwendeten E-Mail-Adressen handelt es sich um solche, die im Format Vorname.Nachname oder ähnlich gestaltet sind. Für die Übermittlung der E-Mail-Adressen an die jeweils anderen Empfänger ist in den hier bearbeiteten Fällen keine Rechtsgrundlage gegeben.

Es mangelt offensichtlich an einer hinreichenden Sensibilisierung der Beschäftigten im Umgang mit personenbezogenen Daten und somit an hinreichenden organisatorischen Maßnahmen, die sicherstellen, dass Beschäftigte, die Umgang mit personenbezogenen Daten haben, bei der Erledigung von alltäglichen Vorgängen hinreichende Kenntnis von den Funktionalitäten der eingesetzten Datenverarbeitungsanlagen haben. Dabei ist zu berücksichtigen, dass es sich bei den Verantwortlichen teilweise um Berufsgeheimnisträger oder solche Verantwortlichen handelt, die in besonderem Maße dafür Sorge zu tragen haben, dass die von ihnen verarbeiteten personenbezogenen Daten rechtmäßig verarbeitet werden, da sie z. B. als Kreditinstitute personenbezogene Daten mit Bezug zu Bankgeschäften verarbeiten oder als politische Parteien personenbezogene Daten besonderer Kategorien verarbeiten.

Der Umstand, dass E-Mail-Adressen betroffener Personen auf solchen (offenen) E-Mail-Verteilern sichtbar für alle Empfänger sind, stellt ein Risiko für die persönlichen Rechte und Freiheiten der betroffenen natürlichen Personen dar. In mehreren Fällen wurde unter Abwägung insbesondere der Art, Schwere und Dauer des Verstoßes, dem Grad der Fahrlässigkeit, der Art und Weise, wie der Verstoß bekannt geworden ist, und unter Berücksichtigung der ergriffenen Maßnahmen zur Minderung des eventuell entstandenen Schadens von den zur Verfügung stehenden Abhilfemaßnahmen aus Art. 58 Abs. 2 DSGVO das Mittel der Verwarnung gewählt.

Was ist zu tun?

Verantwortliche müssen dafür Sorge tragen, dass personenbezogene E-Mail-Adressen nicht unbefugt Dritten zur Kenntnis gegeben werden. Hierfür kann die BCC-Funktion in E-Mail-Programmen genutzt werden. Unternehmen sind gehalten, ihre Beschäftigten zu unterweisen, bei der Kommunikation mittels E-Mail entsprechend sorgsam umzugehen und die Adressen nicht unbefugt zu offenbaren. Zur Wahrung der Rechenschaftspflichten kann es für Verantwortliche ratsam sein, schriftliche Arbeitsanweisungen zum Umgang mit E-Mail an die Beschäftigten weiterzureichen.

06

KERNPUNKTE

Dokumentation und Informationspflicht

Standard-Datenschutzmodell

Datenschutz-Folgenabschätzung

6 Systemdatenschutz

6.1 Fokus Schleswig-Holstein

6.1.1 Sicherheit und Datenschutz in der Infrastruktur

Technischer Datenschutz und Informationssicherheit sind wichtige Bestandteile der IT-Infrastruktur. Die IT-Infrastruktur der Landesverwaltung wird federführend durch das Zentrale IT-Management (ZIT) organisiert. Die vor vielen Jahren begonnene Zentralisierung wird fortgesetzt, indem Infrastrukturen (etwa Vernetzungen, WLANs, PC-Arbeitsplätze, Server) vereinheitlicht werden und operative Tätigkeiten auf Dienstleister, in erster Linie auf Dataport, übertragen werden.

Im Hinblick auf ein professionelles Management und sicheren Rechenzentrumsbetrieb ist dies positiv zu bewerten, da der Betrieb von Infrastrukturen zunehmend komplexer wird. Ebenso steigen Anforderungen an die Verfügbarkeit: Bei einem Ausfall von Netzen, Telefonen oder E-Akten-Systemen wären zahlreiche Behörden zumindest vorübergehend handlungsunfähig. Solche Anforderungen lassen sich in zentralen Infrastrukturen leichter mit einer hohen Qualität umsetzen als in dezentralen Systemen. Andererseits sind bei einem Ausfall oder einem Datenschutzvorfall eines Zentralsystems gleich eine Vielzahl von Behörden betroffen.

Dennoch überwiegen die Vorteile zentraler Lösungen – in einem maritimen Vergleich einem großen Frachter entsprechend, der auf hoher See Vorteile gegenüber einer Flotte kleiner Boote hat. Bei der Absicherung durch technische Datenschutz- und Datensicherheitsmaßnahmen kann man ebenfalls ein maritimes Bild verwenden: Da ein Schaden bei einem großen Schiff ungleich schwerer wiegt, ist es gerechtfertigt und dem Risiko angemessen, auch innerhalb der Infrastruktur Sicherheitsmaßnahmen zu ergreifen, z. B. durch den Einbau von Schotten.

Datenschutzrechtlich kommt noch eine Besonderheit hinzu: Auch wenn eine Infrastruktur als ein Ganzes wahrgenommen und zentral im Hinblick auf technische Aspekte verantwortet wird, bleiben die teilnehmenden Behörden zumindest für inhaltliche Aspekte der Datenverarbeitung verantwortlich. Dass die Trennung dieser Verantwortung und die Erhaltung notwendiger Autonomie der Behörden nicht ganz einfach sind, zeigen die Beiträge unter Tz. 6.3.3 und Tz. 6.3.4.

Organisatorisch schlägt sich dies für die Informationssicherheit in der Zusammenarbeit der Informationssicherheitsbeauftragten auf Landesebene nieder (ISMS = Integriertes Sicherheitsmanagementsystem, 36. TB, Tz. 6.1). Die Aufgabe, die Arbeit von Informationssicherheitsbeauftragten zu organisieren, sie zentral zu steuern und trotzdem individuellen Besonderheiten Rechnung zu tragen, ist nicht einfach. Dass es gut funktionieren kann, zeigt sich im Ressort der Justiz. Da Bedeutung und Aufgaben der Informationssicherheit zunehmen und auch eine Vereinheitlichung (z. B. in Form von Leitlinien oder operativen Richtlinien) geboten ist, ist ein schlagkräftiges ISMS im ZIT unter Beteiligung der Ressorts wichtig. Im Berichtszeitraum war dies nicht durch entsprechende Ressourcen unterfüttert.

Zu Fragen der Infrastruktur gehören auch die Umsetzungen neuer Initiativen wie die Open-Source-Strategie des Landes und neue Projekte der Digitalisierung. Die Verwendung von Open-Source-Software wird durch das ZIT geprüft und unterstützt. Für zahlreiche Server-Systeme stehen funktionale Open-Source-Produkte zur Verfügung. Auch im Bereich der Arbeitsplätze und der Software zur Bürokommunikation (z. B. Webbrowsing, E-Mail, Textverarbeitung) bemüht man sich um die Bereitstellung von Alternativen zur vorhandenen Software. Auch wenn eine Umstellung nicht immer einfach ist und in einigen Fällen auch erst in weiterer Zukunft möglich erscheint (z. B. auf der Ebene von Betriebssystemen für Büroarbeitsplätze), sollten

diese Anstrengungen fortgesetzt werden – nicht zuletzt um bei Problemen wie der Übertragung von Telemetriedaten bei Microsoft-Produkten Alternativlösungen nutzen zu können.

Muss Software einer neuen Produktkategorie beschafft werden (also keine Ersatzbeschaffung für ein laufendes Verfahren, das sich an der bisherigen Lösung orientiert), sind die Chancen besser, Open-Source-Software beschaffen zu können. In bekanntermaßen sensiblen Bereichen wie etwa zentralen Strukturen für Kommunikationsdienste (z. B. Messenger, Telefon, Ausgangsserver für E-Mail) dürfte es ohne Open-Source-Einsatz schwer sein, sich von der Sicherheit und der datenschutzgerechten Implementierung zu überzeugen. Zumindest in den zentralen Systemen sollte hier das Land seiner Vorbildrolle gerecht werden.

Dies gilt auch bei den zahlreichen Digitalisierungsprojekten im Lande, die datenschutzrechtliche Fragen und den technischen Datenschutz frühzeitig mitbedenken müssen, etwa bei der Digitalisierung im Bereich der Schule: Nicht alle Produkte und Anwendungen, die im privaten Umfeld durch ihre Funktionalität bestechen, sind im behördlichen oder schulischen Einsatz geeignet – hier erfolgt schließlich die Verwendung nicht aufgrund einer persönlichen Entscheidung, sondern aufgrund von staatlichen Vorgaben. Diese müssen sich an anderen Maßstäben messen lassen.

Was ist zu tun?

Die zentrale Betrachtung des Themas Informationssicherheit ist zu stärken. Bei der Weiterentwicklung der IT-Infrastruktur und bei Digitalisierungsprojekten sind Datenschutzaspekte frühzeitig zu betrachten. Open-Source-Produkte sollten eine vorrangige Rolle spielen.

6.1.2 Neufassung der Datenschutzverordnung?

Die Datenschutzverordnung für Schleswig-Holstein (DSVO-SH) trat am 31. Dezember 2018 außer Kraft. Der § 7 Abs. 2 des zuvor im Mai in Kraft gesetzten Landesdatenschutzgesetzes Schleswig-Holstein (LDSG) sieht vor, dass die Landesregierung eine Verordnung erlässt, um darin Anforderungen an ein Sicherheitskonzept sowie an Freigaben von Verarbeitungstätigkeiten und weitere Einzelheiten einer ordnungsgemäßen Datenverarbeitung bei öffentlichen Stellen zu regeln. Dies hat die Landesregierung bislang nicht gemacht.

Das ULD legte im November 2018 einen Entwurf für eine neue Verordnung vor, der auf der bisherigen DSVO-SH aufsetzte und die neuen Regelungen der DSGVO und des LDSG mit Bezug zu technisch-organisatorischen Maßnahmen einarbeitete. Der Entwurf des ULD enthält Regelungen zu den Themen Prüffähigkeit, Tests und Freigabe, Auftragsverarbeitung, gemeinsam Verantwortliche sowie Datenschutzmanagement.

Der Entwurf zu § 3 sieht die Sicherstellung der Prüffähigkeit einer Verarbeitungstätigkeit vor. Der Entwurf betrachtet drei Phasen: Phase 1 dient der Planung einer Verarbeitung in Bezug auf Datenbestände, IT-Systeme und Prozesse. Phase 2 betrifft Prüfungen des laufenden Betriebs auf der Grundlage der Dokumentationen und der Kontrollen der Datenschutz- und Datensicherheitsmaßnahmen. Die dritte Phase behandelt Prüfungen des Betriebs in der Vergangenheit anhand von Protokolldaten.

Der Entwurf zu § 4 sieht die Anforderung für „Test und Freigabe“ vor, da sich diese Regelung in der bisher gültigen DSVO-SH bewährt hat. Durch die Bearbeitung von formalen Anforderungen an die Gestaltung des Übergangs von der Projektphase in die Produktivphase einer

Verarbeitungstätigkeit wird der Verantwortliche angehalten, die Wirksamkeit der implementierten technisch-organisatorischen Datenschutzmaßnahmen vor Aufnahme des Echtbetriebs zu überprüfen.

Der Entwurf zu § 5 umfasst eine Regelung zur Auftragsverarbeitung. Dieser stellt insbesondere auf die Verpflichtung zur Kontrolle des Auftragnehmers durch den Verantwortlichen ab und legt nahe, Vereinbarungen darüber zu treffen, bei welchen Störungen, Problemen und Änderungen aufseiten des Verarbeiters der Verantwortliche beteiligt werden möchte.

Der Entwurf zu § 6 enthält eine Regelung zur Dokumentation bei gemeinsamer Verantwortung für die Verarbeitung in Fällen, in denen dies nicht ohnehin durch eine Rechtsvorschrift gemäß § 7 Abs. 4 LDSG festgelegt ist.

Der Entwurf zu § 7 enthält einen neuen Regelungsgegenstand, nämlich Anforderungen an ein Datenschutzmanagement. Diese Anforderungen konkretisieren Bestimmungen sowohl aus der DSGVO (Art. 24 Abs. 1 und Art. 32 Abs. 1 Buchst. d DSGVO) als auch aus dem neuen LDSG (§ 12 Abs. 3 Nr. 7 LDSG-neu). Das Datenschutzmanagement soll die Wirksamkeit der Schutzmaßnahmen und deren Prüfbarkeit sicherstellen sowie auf Veränderungen der Umstände (z. B. Änderungen von Rechtslagen, technischer Gestaltung oder Bedrohungen) reagieren. In der Dokumentation zum Datenschutzmanagement müssen Aussagen über die Bereitstellung von Ressourcen, zur Einbindung der oder des behördlichen Datenschutzbeauftragten und über deren oder dessen Einbindung in geplante Verfahren und Datenschutz-Folgenabschätzungen getroffen werden. Ferner sind die Prüfmethodik für die laufenden Verarbeitungstätigkeiten, insbesondere zur Wirksamkeit der technisch-organisatorischen Schutzmaßnahmen darzustellen sowie die Prozesse zu beschreiben, mit denen auf (negative) Prüfergebnisse reagiert wird und die Eingaben von betroffenen Personen bearbeitet werden.

Das Innenministerium des Landes hat gegenwärtig kein Interesse daran gezeigt, eine Datenschutzverordnung für Schleswig-Holstein zu erlassen. Die explizite Regelung „Die Landesregierung regelt durch Verordnung [...]“ wurde bisher nicht als Mussregelung verstanden. Dem ULD wurde stattdessen nahegelegt, die Inhalte seines Entwurfs einer DSVO-SH als Umsetzungshinweise herauszugeben. Das ULD wird daher den Entwurf für eine DSVO-SH veröffentlichen und Hilfestellung zu dessen Umsetzung geben.

Was ist zu tun?

Das Innenministerium sollte prüfen, ob die Landesregierung nicht doch die in § 7 Abs. 2 LDSG angekündigte Verordnung erlassen will. Parallel wird das ULD Umsetzungshinweise auf Basis des erarbeiteten Entwurfs einer Datenschutzverordnung veröffentlichen. Im Rahmen der Evaluation des LDSG ist zu überprüfen, ob es eines höheren Verbindlichkeitsgrades in Form einer Verordnung bedarf.

6.1.3 Überarbeitete Vorlagen zur Dokumentation von Verarbeitungstätigkeiten

Am 25. Mai 2018 hat die DSGVO Geltung erlangt. Nach Art. 5 Abs. 2 DSGVO müssen Verantwortliche nachweisen können, dass die Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden (Rechenschaftspflicht). Diese Grundsätze sind nach Art. 5 Abs. 1 DSGVO:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz,

- Zweckbindung,
- Datenminimierung,
- Richtigkeit,
- Speicherbegrenzung,
- Integrität und Vertraulichkeit.

Die Umsetzung der Rechenschaftspflicht kann mit einer angemessenen Dokumentation nachwiesen werden. Bis zum 31. Dezember 2018 gab es in Schleswig-Holstein die Datenschutzverordnung (DSVO), die für Behörden regelte, welche Dokumentationsbestandteile in einer datenschutzkonformen Dokumentation enthalten sein müssen (Tz. 6.1.2). Zur Umsetzung der DSVO hatte das ULD Dokumentationsvorlagen entwickelt, um eine Hilfestellung bei der Dokumentation von automatisierten Verfahren zu geben.

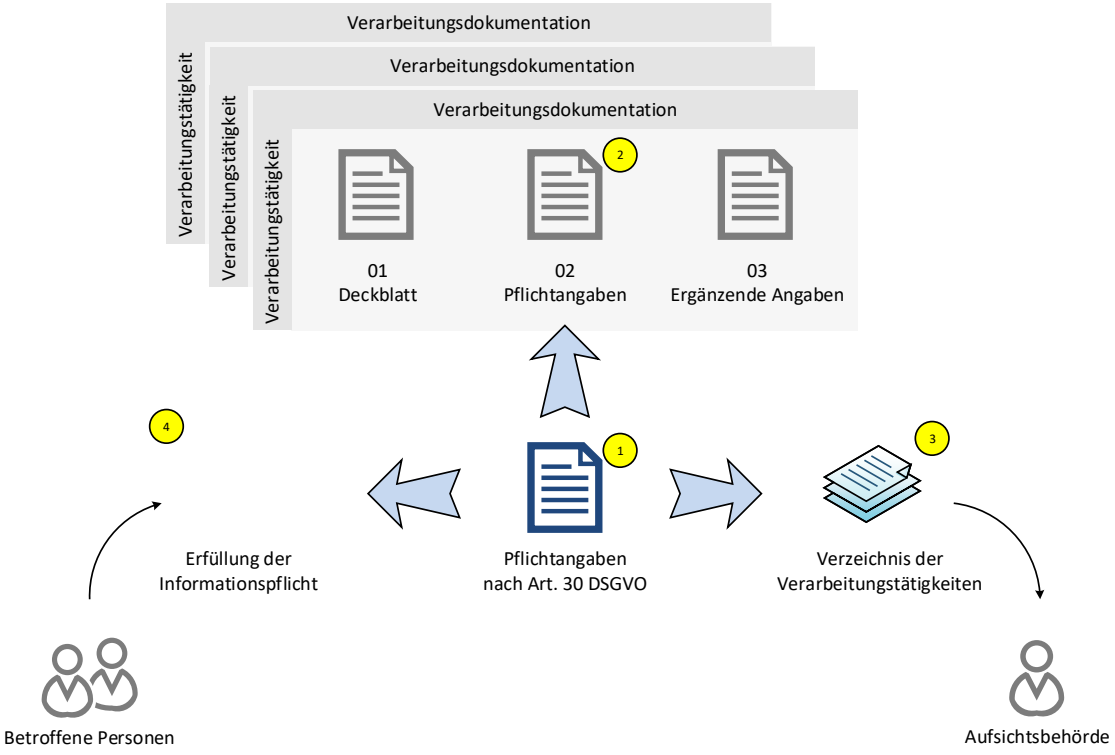


Abbildung: Pflichtangaben nach Artikel 30 DSGVO als zentraler Baustein

Um auch weiterhin einen roten Faden für die Strukturierung der Dokumentation anzubieten, hat das ULD die Dokumentationsvorlagen überarbeitet und stellt sie auf der Webseite zur Verfügung unter:

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

Diese Vorlagen sind auch außerhalb des Behördenumfeldes nutzbar, etwa für Firmen und Vereine.

Das Konzept der Dokumentationssystematik hat sich im Vergleich zur alten Rechtsgrundlage leicht verändert. Der modulare Aufbau sowie die Einbeziehung der Fachbereiche, des Managements und der Technik sind gleich geblieben. Die Verwendung der Pflichtangaben nach Artikel 30 DSGVO als ein zentraler Baustein innerhalb der Dokumentationsstruktur ist neu (siehe Abbildung).

Somit wird in diesem Konzept ein Einzeleintrag für das Verzeichnis der Verarbeitungstätigkeiten als ein zentrales Dokument (1) betrachtet, dass dreifach eingesetzt wird:

- als Bestandteil (3) im Verzeichnis der Verarbeitungstätigkeiten (originäre Verwendung, Artikel 30 DSGVO),
- als Bestandteil (2) der Dokumentation von Verarbeitungstätigkeiten (Verarbeitungsdokumentation, Erfüllung der Rechenschaftspflicht nach Artikel 5 DSGVO) und
- als Basisinformation zur Erfüllung der Informationspflicht (4) nach Artikel 13 und Artikel 14 DSGVO.

Bisher sind Vorlagen sowie Ausfüllhinweise und Konzepte zu folgenden Themen verfügbar:

- Vorlagen und Ausfüllhinweise zur Dokumentation von Verarbeitungstätigkeiten,
- Vorlage und Ausfüllhinweise für ein Verzeichnis der Verarbeitungstätigkeiten,
- Vorlage und Ausfüllhinweise (inklusive Konzept) zur Erfüllung der Informationspflicht,
- Vorlage zur Dokumentation der Technikgestaltung.

Weitere Vorlagen, Ausfüllhinweise und Handreichungen sind in Arbeit.

6.1.4 Der Datenschutz-Steckbrief zur Umsetzung der Informationspflicht

Es ist nicht einfach, betroffene Personen über die Verarbeitung ihrer personenbezogenen Daten in den verschiedenen Verarbeitungstätigkeiten so zu informieren, dass sie

- in einer präzisen und verständlichen Form vorliegen,
- in einer einfachen Sprache geschrieben sind und
- möglichst mit visuellen Elementen so aufbereitet werden, dass die Informationen leicht wahrzunehmen sind und sie anhand der Grafiken gut den Informations- und Mitteilungspflichten der Artikel 13 bis 22 DSGVO zugeordnet werden können.

Weiterhin ist die Gruppe der betroffenen Personen nicht homogen. Sie setzt sich aus Menschen unterschiedlichster Persönlichkeiten und Lebensumstände zusammen. Dabei kann es sich beispielsweise um Personen handeln,

- die Datenschutz für sich zwar wichtig empfinden, aber nicht die Zeit haben bzw. sich nicht die Zeit nehmen, die Datenschutzerklärungen sorgfältig zu lesen,
- die in Bezug auf das Thema Datenschutz hochinteressiert und -gebildet sind und ihre Rechte ganz genau und detailliert nachlesen,
- die den Datenschutz als unwichtig empfinden und der Meinung sind, nichts zu verbergen zu haben,
- für die Deutsch nicht die Muttersprache ist sowie
- Menschen, für die formale Texte schwierig zu verstehen sind (etwa für Kinder).

Alle diese Menschen können betroffene Personen sein und sollen anhand der Informationen, die die verantwortliche Stelle für sie herausgibt, verstehen können, welche Daten von ihnen wie verarbeitet werden.

Aus den Rückmeldungen von betroffenen Personen sind die üblichen langen und kompliziert zu lesenden Datenschutzerklärungen verantwortlicher Stellen seit der Einführung der DSGVO im Mai 2018 nicht der richtige Weg, um der Informationspflicht nachzukommen und alle betroffenen Personen angemessen zu informieren. Betroffene Personen neigen dazu – wenn sie diese Art von Datenschutzerklärungen überhaupt lesen –, diese zu überfliegen und aufgrund ihrer Länge und Komplexität einfach „wegzuklicken" – und das ist nicht das, was mit den neuen Rechten auf Information erreicht werden soll. Wie also vorgehen?

Der Datenschutz-Steckbrief geht in Verbindung mit einem dreistufigen Konzept einen anderen Weg und soll im besten Fall alle betroffenen Personen verständlich informieren: kurz und

prägnant, in einer einfachen Form und Sprache sowie durch grafische Elemente unterstützt. Er ist auf der obersten Ebene innerhalb einer Methodik angesiedelt, mit der die Informationspflicht in öffentlichen und privaten Organisationen umgesetzt und die gesamte Gruppe der betroffenen Personen angesprochen werden kann.

Die nachfolgende Abbildung visualisiert die Umsetzung der Informationspflicht:

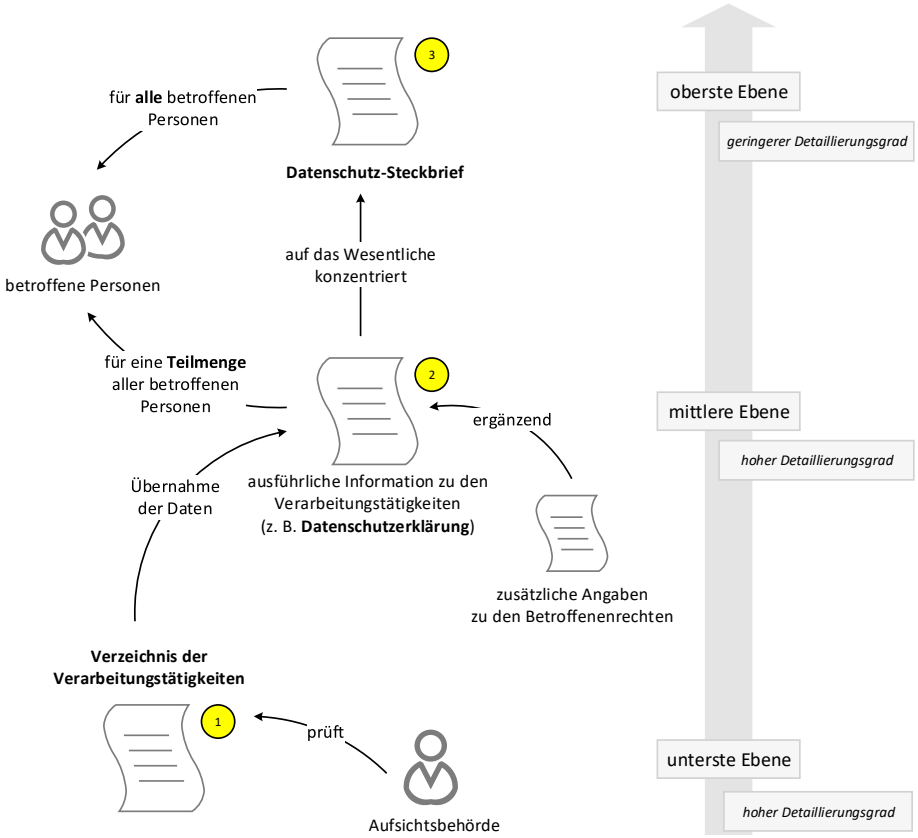


Abbildung: Dreistufenkonzept

Auf der untersten Ebene (Punkt 1 in der Abbildung) werden zunächst die Verarbeitungstätigkeiten in einer Organisation erfasst und zum Verzeichnis der Verarbeitungstätigkeiten zusammengeführt. Dieses Dokument stellt die Basis für die Umsetzung der Informationspflichten dar, da in diesem die meisten Informationen davon enthalten sind, die den betroffenen Personen zur Verfügung gestellt werden müssen.

Weiterhin ist dieses Verzeichnis sowohl ein Pflichtnachweis nach Artikel 30 DSGVO als auch ein Baustein bei der Verarbeitungsdokumentation (Tz. 6.1.3). Auf dieser Ebene wird mit einem hohen Detaillierungsgrad gearbeitet. Um das Verzeichnis der Verarbeitungstätigkeiten zu erstellen, kann die ULD-Vorlage verwendet werden:

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

Auf der mittleren Ebene (Punkt 2 in der Abbildung) werden den betroffenen Personen ausführliche Informationen in einem hohen Detaillierungsgrad zur Verfügung gestellt. Die Basis dieser Information sind die Angaben aus dem Verzeichnis der Verarbeitungstätigkeiten, die um zusätzliche Angaben entsprechend den Artikeln 13 bis 22 DSGVO ergänzt werden. Diese ausführlichen Informationen können den betroffenen Personen beispielsweise in Form einer Datenschutzerklärung auf der Organisations-

webseite zur Verfügung gestellt werden, oder das Verzeichnis der Verarbeitungstätigkeiten wird so geschrieben, dass es – ergänzt um die oben genannten zusätzlichen Angaben – veröffentlicht werden kann. Diese Ebene spricht die betroffenen Personen an, die sich umfassend und ausführlich über ihre Rechte informieren möchten.

Auf der obersten Ebene (Punkt 3 in der Abbildung) wird allen betroffenen Personen mit dem Datenschutz-Steckbrief eine leicht verständliche und kompakte Übersicht aller Informationen gegeben, die ihnen gemäß der DSGVO zur Verfügung gestellt werden müssen. Die Informationen können der mittleren Ebene entnommen werden. Die Herausforderung liegt in der (Um-)Formulierung der Inhalte. So sollten die Informationen kurz und prägnant beschrieben werden, sich auf das Wesentliche konzentrieren und in einer klaren und einfachen Sprache verfasst werden.

Die Vorlage des Datenschutz-Steckbriefs gibt weiterhin grafische Elemente vor, die frei verwendet werden können. Diese Ebene spricht mit dem Datenschutz-Steckbrief alle betroffenen Personen an, die sich mithilfe der einheitlichen und wiedererkennbaren Icons (Piktogrammen) sowie der einfachen und verständlichen Sprache schnell und strukturiert über die Verwendung ihrer Daten informieren möchten.

Die Vorlage des Datenschutz-Steckbriefes kann auf der ULD-Webseite heruntergeladen werden:

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

Die nachfolgende Abbildung zeigt die Bedeutung eines einzelnen Eintrags für das Verzeichnis der Verarbeitungstätigkeiten als zentrales Dokument und als Informationsbasis zur Umsetzung der Informationspflicht. Sie gibt aber auch einen Überblick über die zwei weiteren Einsatzbereiche des Einzeleintrags sowohl als Dokumentationsbestandteil zur Umsetzung der Rechenschaftspflicht als auch als Bestandteil im Verzeichnis der Verarbeitungstätigkeiten (Tz. 6.1.3).

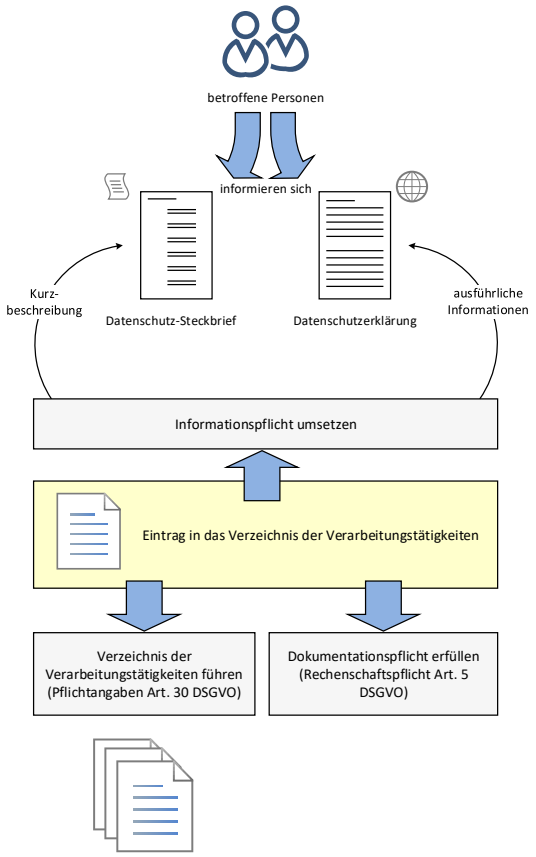


Abbildung: Elemente zur Umsetzung der Informations- und Rechenschaftspflicht

Was ist zu tun?

Mit dem Datenschutz-Steckbrief kann eine verantwortliche Stelle der Pflicht der Einfachheit und Verständlichkeit (Art. 12 Abs. 1 DSGVO) nachkommen. Durch eine zweistufige Informationsstrategie können die betroffenen Personen zielgruppengerecht informiert werden.

6.1.5 Datenschutz durch Gestaltung – auch bei Datenschutzerklärungen und Formularen

Zu den Informationspflichten gehört die Information über das Beschwerderecht bei einer Aufsichtsbehörde (Art. 13 Abs. 2 Buchst. d DSGVO, Art. 14 Abs. 2 Buchst. e DSGVO). Viele Stellen lösen dies so, dass sie in ihrer Datenschutzerklärung oder in Formularen gleich die vollständigen Erreichbarkeitsdaten des ULD prominent veröffentlichen. Die Kontaktdaten des Verantwortlichen sind dagegen oft viel schwerer zu finden. So erhält das ULD auch Post, die an die Verantwortlichen gerichtet ist, z. B. unterschriebene Einwilligungserklärungen oder Anhörungsbögen. Das soll natürlich nicht so sein! Es ist auch manchmal nicht auf den ersten Blick zu erkennen, ob es sich nicht doch um eine Beschwerde handelt, bei der das ULD auf problematische Formulierungen in Datenschutzerklärungen oder Formularen hingewiesen wird. In einem Fall kamen größere Mengen von Irrläufern beim ULD an. Nachdem wir Kontakt mit den Zuständigen aufgenommen hatten, wurde uns zugesichert, dass die Formulare künftig umgestaltet würden. Dennoch dauerte es noch Wochen, bis diese Fehlzuleitungen abebbten.

Was ist zu tun?

Die Anforderung „Datenschutz durch Gestaltung“ betrifft auch Datenschutzerklärungen und Formulare: Alle Verantwortlichen sollten schon aus eigenem Interesse auf eine geeignete Gestaltung achten, damit Fehladressierungen und Irrläufer vermieden werden.

6.2 Zusammenarbeit der Datenschutzbeauftragten im Bereich Systemdatenschutz

6.2.1 AK Technik und wichtige Arbeitsergebnisse

Die Datenschutzbehörden des Bundes und der Länder organisieren ihre Zusammenarbeit in regelmäßig, meist halbjährlich tagenden Arbeitskreisen. Für den Systemdatenschutz ist der Arbeitskreis Technik besonders relevant (35. TB, Tz. 6.2.1). Für die vertiefte Behandlung von Themen werden Arbeitsgruppen gebildet, so z. B. im Bereich des Standard-Datenschutzmodells (Tz. 6.2.2).

Im Berichtszeitraum waren wesentliche Fragestellungen die Funktionsweise, Einsatzgebiete und Grenzen von Verfahren der künstlichen Intelligenz, Anforderungen an die Verschlüsselung von E-Mails (Transportverschlüsselung, Ende-zu-Ende-Verschlüsselung), der Einsatz von Windows 10 in Behörden, die Bereitstellung von Cloud-Diensten sowie Maßnahmen zur Sicherheit von Online-Konten. Daneben war der Arbeitskreis Technik an der Erstellung von Dokumenten anderer Arbeitskreise beteiligt, u. a. der Orientierungshilfe „Aufbewahrung“, die sich der sicheren Aufbewahrung von Papierdokumenten einschließlich der Beachtung der Aufbewahrungsfristen widmet.

Exemplarisch sei die Befassung mit der Verschlüsselung von E-Mails hervorgehoben, um die Schwierigkeiten einer solchen Befassung darzustellen:

In der Vergangenheit wurden Dokumente zu einzelnen technischen Aspekten mit dem Fokus „Was ist technisch möglich?“ und „Was ist technisch sinnvoll?“ erstellt. Heutzutage versucht man, daneben die Frage „Was ist rechtlich erforderlich?“ zu beantworten. Bei der Antwort auf diese Frage tritt neben das technisch Mach-

bare auch die Frage der Erforderlichkeit im Hinblick auf die Sensibilität der Daten, möglicher Risiken für die Rechte und Freiheiten Betroffener, der Implementierungskosten und nicht zuletzt der Praktikabilität, insbesondere im E-Mail-Verkehr mit Bürgerinnen und Bürgern: Einige verfügen über etablierte Ende-zu-Ende-Verschlüsselungsverfahren wie S/MIME oder OpenPGP und erwarten (zu Recht), dass sie mit Behörden und Firmen auf diese Weise kommunizieren können. In der großen Breite haben sich aber solche Verfahren trotz jahrzehntelanger Verfügbarkeit (noch) nicht durchgesetzt, mit der Folge, dass die meisten der Bürgerinnen und Bürger für die Verwaltung und Firmen nicht per Ende-zu-Ende-verschlüsselter E-Mail erreichbar sind. Daher stellt sich die Frage, ob in diesen Fällen auch schwächere Sicherheitsverfahren wie eine Transportverschlüsselung zum Einsatz kommen dürfen – ebenso wie in der Papierwelt nur besonders wichtige Dokumente per Kurier und in verschlossenen Koffern verschickt werden und die Masse der Briefe nur durch das Papier des Briefumschlags und das Postgeheimnis geschützt ist.

Fraglich ist auch, unter welchen Umständen Bürgerinnen und Bürger in eine schwächer abgesicherte Kommunikation „einwilligen" können (siehe auch Tz. 4.1.3), bis wohin also die Verantwortung einer absendenden Behörde oder Firma reicht. Hinzu kommt, dass im Bereich der E-Mail üblicherweise sowohl Absender als auch Empfänger Dienstleister in Anspruch nehmen, die zumindest aufseiten der Bürgerinnen und Bürger nicht alle dem Telekommunikationsgesetz unterworfen sind (da sie diese Daten nicht in Deutschland verarbeiten) und teilweise laut ihren AGBs auch den E-Mail-Verkehr inhaltlich für eigene Zwecke auswerten. Oder plakativ gefragt: Dürfen Behörden E-Mail-Nachrichten an Bürgerinnen und Bürger senden, wenn deren E-Mail-Dienst von Providern angeboten wird, die erklärtermaßen Zugriff auf den Inhalt für eigene Zwecke nehmen? Steht dies zur Disposition der Empfängerinnen und Empfänger?

Transportverschlüsselung

Ähnlich wie Webserver und Webbrowser über das Protokoll „https" verschlüsselt kommunizieren können, können auch E-Mail-Server untereinander einen verschlüsselten Kanal aufbauen. Auf den E-Mail-Servern selbst liegen die Daten unverschlüsselt.

Dies lässt sich in der Briefpost mit dem Transport einer Postkarte in einem verschlossenen Transportbehälter zwischen Postverteilzentren und Empfänger vergleichen.

Eine reine Transportverschlüsselung kann vor inhaltlicher Auswertung durch den E-Mail-Diensteanbieter nicht schützen. Aber auch eine Ende-zu-Ende-Verschlüsselung betrifft nur den Inhalt von E-Mails, nicht aber Absender, Empfänger, Uhrzeit und Betreff. Eine Kommunikationsanalyse („Wer, wann, mit wem?") ist so möglich. Technisch ist der Einsatz einer Transportverschlüsselung einfach. Schwieriger ist die Frage zu beantworten, gegen welche Art von Angreifern sie Sicherheit bietet. Gegen „lauschende" Angreifer ist die Sicherheit groß. Gegen Anbieter, die manipulativ in den Netzverkehr eingreifen, sind zusätzliche Maßnahmen zu treffen, um sie von der Manipulation der verwendeten kryptografischen Schlüssel und Zertifikate abzuhalten. Dass solche Eingriffe erfolgen, ist keinesfalls ein Fantasiegebilde – auf anderen Ebenen (Webbrowser) wird ein solcher Eingriff mitunter „aus Sicherheitsgründen" gefordert (Tz. 10.1).

Allein dieser kurze Abriss zeigt, dass die Fragestellung „E-Mail-Verschlüsselung" sehr komplex ist und genau analysiert werden muss, bevor allgemeingültige rechtsverbindliche Hinweise gegeben werden können, die auch dem Anspruch an Praxistauglichkeit genügen.

6.2.2 Neues zum Standard-Datenschutzmodell (SDM)

Das Standard-Datenschutzmodell (SDM) ist ein unter den deutschen Datenschutzbehörden abgestimmtes Verfahren zur Auswahl und Implementierung von technisch-organisatorischen Datenschutzmaßnahmen. Im Berichtszeitraum wurden zwei wesentliche Aspekte des SDM vorangebracht:

Das SDM wurde vollständig und ausschließlich auf die Anforderungen der DSGVO umgestellt. Einer der wesentlichen Inhalte dieser Umstellung betraf dabei die Ermittlung des Risikos für die Rechte und Freiheiten Betroffener bzw. des Schutzbedarfs, für die in Artikel 24 und Artikel 25 der DSGVO eine Regelung enthalten ist. In der aktuellen Version bietet das SDM deshalb keine eigene Methode zur Risikoermittlung an. Vielmehr muss das Risiko seitens des Verantwortlichen bereits bestimmt sein, bevor mit dem SDM die Schutzmaßnahmen festgelegt werden können. Im April 2018 hat die Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) das SDM in der Version V1.1 dann erneut für eine weitere Evaluationsphase – ohne Gegenstimme, aber mit vier Enthaltungen – als Prüfungs- und Beratungsmodell akzeptiert.

Im September 2018 haben sich einige Datenschutzaufsichtsbehörden entschieden, nach dem Vorbild der IT-Grundschutzkataloge Datenschutzbausteine mit Schutzmaßnahmenkatalogen zu veröffentlichen. Zu diesen Aufsichtsbehörden zählen die Landesbeauftragten für den Datenschutz in Hessen, Mecklenburg-Vorpommern, Sachsen und das ULD sowie die Evangelische Kirche Deutschlands. Seit 2016 wurde vergeblich versucht, einen Katalog mit Bausteinen deutschlandweit abzustimmen. Die an der Veröffentlichung beteiligten Behörden waren bzw. sind der Ansicht, dass zur Evaluation des SDM auch die der Bausteine gehören muss, die deshalb der Praxis bekannt sein und angewendet werden sollten.

Die im September veröffentlichten Bausteine des SDM werden zentral auf dem Webserver der Kollegen von Mecklenburg-Vorpommern zum Download vorgehalten:

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

Als Entwürfe wurden bislang die Bausteine Aufbewahrung, Planung und Spezifikation, Dokumentation, Protokollierung, Trennung, Löschen und Vernichten sowie Datenschutzmanagement veröffentlicht.

Was ist zu tun?

Für 2019 ist die Publikation weiterer Bausteine vorgesehen. Gegenwärtig wird zudem an einer weiteren Verbesserung des Modells gearbeitet. Nutzer der Bausteine können Feedback und Anregungen an das ULD melden, damit aus den Entwürfen praxisgerechte Bausteine werden.

6.2.3 Wann ist eine Datenschutz-Folgenabschätzung erforderlich?

Das Instrument der Datenschutz-Folgenabschätzung wird in Artikel 35 der DSGVO sowie in § 43 LDSG geregelt. Artikel 35 DSGVO verlangt von Verantwortlichen zu prüfen, ob für seine Verarbeitungstätigkeiten Datenschutz-Folgenabschätzungen (DSFA) durchzuführen sind, weil voraussichtlich ein hohes Risiko für die Rechte und Freiheiten Betroffener besteht. Bei einem hohen Risiko müssen die Anforderungen der gesamten DSGVO bzw. des LDSG in besonders wirksamer Weise erfüllt werden. Insbesondere müssen Datenschutzmaßnahmen

ausgewählt und implementiert werden, um das (hohe) Risiko auf ein vertretbares Maß zu senken.

Ob eine DSFA erforderlich ist, ist im Rahmen einer Schwellwertanalyse zu prüfen. Wesentliche Indikatoren, dass eine DSFA erforderlich ist, sind abstrakt in Absatz 1 und beispielhaft in Absatz 3 des Artikels 35 DSGVO genannt. Interpretationshilfen dazu bieten die Erwägungsgründe 91 ff. der DSGVO. Als weitere Konkretisierung verpflichtet Absatz 4 die Datenschutzaufsichtsbehörden, in einer Liste verbindlich solche Verfahren zu nennen, für die in jedem Fall eine DSFA durchzuführen ist, die sogenannte „Muss-Liste". Parallel dazu berechtigt Absatz 5 die Datenschutzaufsichtsbehörden, eine Liste für Ausnahmefälle zu erstellen, in denen erklärtermaßen eine DSFA nicht erforderlich ist, eine sogenannte „Braucht-nicht-Liste". Von dieser Möglichkeit haben die bundesdeutschen Aufsichtsbehörden bewusst keinen Gebrauch gemacht.

Im Rahmen der Schwellwertanalyse bietet es sich daher an, zunächst anhand von Absatz 3 und danach anhand der Liste gemäß Absatz 4 zu prüfen, ob für die geplante Verarbeitungstätigkeit eine DSFA vorgeschrieben ist. Gibt es hier einen Treffer, braucht man sich über das „Ob" einer DSFA keine Gedanken mehr zu machen und kann gleich zur Durchführung schreiten.

Die Datenschutzaufsichtsbehörden standen daher vor der Aufgabe, Listen gemäß Art. 35 Abs. 4 DSGVO zu erstellen. Ziel war, eine bundesweit abgestimmte Liste zu erstellen, die in jedem Fall den nichtöffentlichen Bereich abdeckt. Als Vorbild stand dazu das Arbeitspapier WP 248 (rev. 01 vom 13. Oktober 2017) der Artikel-29-Datenschutzgruppe Pate. Zur Erinnerung: Die Artikel-29-Datenschutzgruppe war die Vorgängerorganisation des Europäischen Datenschutzausschusses, in der bis zum Mai 2018 die europäischen Datenschutzaufsichtsbehörden ihre Tätigkeiten koordinierten. Dieses Arbeitspapier führt neun Kriterien auf. Sobald mindestens zwei Kriterien erfüllt sind (in Ausnahmefällen reicht ein Kriterium), ist eine DSFA erforderlich. Mithilfe dieses Arbeitspapiers erstellte eine Arbeitsgruppe der Aufsichtsbehörden eine erste Fassung der Muss-Liste, die in einem europäischen Abstimmungsprozess noch leicht verändert wurde: Erstmals wurden im Rahmen der Vereinheitlichung der Umsetzung der DSGVO die Listen aller Aufsichtsbehörden durch den Europäischen Datenschutzausschuss gesichtet und im Falle von Abweichungen gegen die Regeln der DSGVO auf eine Anpassung gedrängt – zumindest in den Fällen, in denen eine grenzüberschreitende Datenverarbeitung erfolgt. Diese Anpassung der deutschen Liste wurde im Oktober 2018 umgesetzt; die aktuelle Liste ist neben einem Erläuterungstext unter

https://www.datenschutzzentrum.de/uploads/dsgvo/2018_10_17_DSK_DSFA-Liste-1_1.pdf

verfügbar. Eine Ergänzung dieser Liste um Verfahren der öffentlichen Datenverarbeitung, die auf Schleswig-Holstein begrenzt ist, kann das ULD eigenständig vornehmen; sie braucht nicht auf europäischer Ebene abgestimmt zu werden. Eine Abstimmung ist aber unter denjenigen Bundesländern, die Träger von Dataport sind und für die Dataport wesentliche Verfahren implementiert, sinnvoll und erfolgt derzeit.

Was ist zu tun?

Im Rahmen einer Schwellwertanalyse ist zu prüfen, ob für Verarbeitungstätigkeiten eine DSFA durchzuführen ist. Hilfestellungen für die Entscheidung bieten Art. 35 Abs. 3 DSGVO sowie die „Muss-Liste" des ULD. Ist eine DSFA nicht erforderlich, sind die Gründe zu dokumentieren: Auf die Frage „Warum wurde keine DSFA durchgeführt?" sollten Verantwortliche eine Antwort haben.

6.3 Ausgewählte Ergebnisse aus Beratungen und Prüfungen

6.3.1 Unterstützung bei der Durchführung von Datenschutz-Folgenabschätzungen

Es gibt in Schleswig-Holstein mehrere parallele Initiativen zur standardisiert-methodischen Unterstützung öffentlicher Stellen bei der Erarbeitung von Datenschutz-Folgenabschätzungen gemäß Artikel 35 DSGVO. Das ULD unterstützt die Initiativen des Zentralen IT-Management des Landes Schleswig-Holstein (ZIT) und des Arbeitskreises der behördlichen Datenschutzbeauftragten und empfiehlt daher Verantwortlichen, die eine Datenschutz-Folgenabschätzung (DSFA) durchführen müssen und erste Orientierungen suchen, Kontakt zu diesen Initiativen aufzunehmen.

Das ZIT hat für die Ebene der Ministerien drei Formulare zur Durchführung einer Datenschutz-Folgenabschätzung entwickelt: Ein Formular für die Durchführung einer Schwellwertanalyse zur Bestimmung der Höhe des Risikos für die Rechte und Freiheiten Betroffener, ein zweites Formular für die Durchführung der eigentlichen Datenschutz-Folgenabschätzung mit dem Ziel, die Verarbeitungstätigkeit rechtskonform einzurichten und die dafür zu ergreifenden Schutzmaßnahmen zu erkennen und festzulegen. Das dritte Formular unterstützt dann die Kontrolle und Dokumentation der Implementation der Schutzmaßnahmen. Die Stärke dieser Methode ist die Schwellwertanalyse.

Datenschutzbeauftragte aus dem kommunalen Bereich unterstützen die Schwellwertbestimmung und die Durchführung der DSFA in Form einer Tabellenkalkulation. Dass diese Lösung funktioniert, zeigte sich bereits an konkreten Projekten zur Durchführung sowohl der Schwellwertanalyse als auch der Bestimmung der zu treffenden rechtlichen Regelungen und technisch-organisatorischen Schutzmaßnahmen. Gegenwärtig fließen die Erfahrungen in die Weiterentwicklung dieses Tools hinein. Die Stärke dieser Methode besteht darin, dass Verantwortlichen durch „Was-wäre-wenn?"-Szenarien grafisch vor Augen geführt werden kann, was es für die Rechtskonformität bedeutet, wenn z. B. eine 80-Prozent-Lösung in 20 Prozent der Zeit oder eine lange schon geplante, aber bislang nicht umgesetzte Maßnahme aktuell endlich umgesetzt würde.

Es ist geplant, die Erfahrungen mit diesen beiden Methoden in die Plattform HiScout einfließen zu lassen. Mit der Dokumentations- und Managementplattform HiScout beabsichtigt das Land, ab 2019 die Maßnahmen der Informationssicherheit auf Basis der IT-Grundschutzkataloge sowie des operativen Datenschutzes auf der Grundlage des Standard-Datenschutzmodells (SDM) zu modellieren und zu überwachen. Die Integration der Schwellwertanalyse und der Datenschutz-Folgenabschätzung auf der Basis des SDM in die Plattform ist derzeit noch nicht abgeschlossen.

Was ist zu tun?

Die Schwellwertanalyse und die Datenschutz-Folgenabschätzung auf der Basis des SDM sollten in die Plattform HiScout vollständig integriert werden, um ein reibungsloses Arbeiten zu ermöglichen.

6.3.2 Digitale Personalakte

Die Digitalisierung der Personalakten des Landes (36. TB, Tz. 4.1.1) ist mittlerweile abgeschlossen. Das ULD wurde zusammen mit den gewerkschaftlichen Spitzenorganisationen fortlaufend informiert.

Die Papierakten wurden in mehreren Schüben von den personalaktenführenden Stellen abgeholt und in ein zentrales Scanzentrum gebracht. Dort wurden sie eingescannt, liegen aber in Papierform bis zum Abschluss der Qualitätskontrolle weiterhin als Papier vor. Neben der Begleitung einer datenschutzrechtlichen Kontrolle des Dienstleisters durch das ZIT am Standort des Scanzentrums hat das ULD auch die Abholung und Verpackung von Akten in Kiel im Rahmen eines Informationsbesuches begleitet. Dabei waren keine Auffälligkeiten zu verzeichnen.

Was ist zu tun?

Das ULD sollte weiterhin eingebunden werden, da sich auch zukünftig zahlreiche datenschutzrechtliche Fragen im Zusammenspiel mit der elektronischen Aktenführung und der Ausgestaltung von Akteneinsichten durch andere personalverwaltende Stellen und von Betroffenen stellen.

6.3.3 Gemeinsame Prüfung des Zentralen Meldedatenbestandes (ZMB)

Adressdaten und andere Meldedaten der Einwohnerinnen und Einwohner Schleswig-Holsteins werden in Registern der örtlichen Meldeämter gespeichert. Seit 2015 besteht nach einer Änderung des Bundesmeldegesetzes (BMG) die Verpflichtung, diese Daten u. a. für Online-Abfragen von (Verwaltungs-)Behörden und Strafverfolgungs- und Sicherheitsbehörden rund um die Uhr bereitzustellen. In Schleswig-Holstein geschieht dies bereits seit Jahren beim Dienstleister Dataport mithilfe einer Spiegeldatenbank („Zentraler Meldedatenbestand", ZMB), die tägliche Kopien der örtlichen Meldedaten erhält und zum Abruf bereitstellt. Abrufe erfolgen über das Schleswig-Holstein-Portal (Verwaltungsportal) und umfassen neben den beiden Abrufmöglichkeiten für (Verwaltungs-) Behörden und für Strafverfolgungs- und Sicherheitsbehörden auch die Möglichkeit einer einfachen Melderegisterauskunft. Bei dieser können Firmen und natürliche Personen kostenpflichtig Adressdaten abfragen.

Nicht jeder darf alle Daten der Melderegister abrufen. Die Abrufberechtigungen, der Umfang der abrufbaren Daten und auch die zur Suche notwendigen Eingabedaten sind durch das Bundesmeldegesetz sowie durch Landesrecht (Landesmeldegesetz, Landesmeldeverordnung) festgelegt. Auch Details zur Ausgestaltung und zum Betrieb der Spiegeldatenbank und zum Zusammenspiel mit den örtlichen Meldebehörden sind im Wege einer Verordnung festgelegt (Landesverordnung über die zentrale Stelle der Vermittlungsstelle und Spiegeldatenbank des Landes Schleswig-Holstein).

Die Spiegeldatenbank bei Dataport wird im Verbund mit den Bundesländern Hamburg und Sachsen-Anhalt betrieben. Dieser sogenannte Mehrländer-Meldedatenspiegel (MMS) bot Anlass zu einer gemeinsamen Prüfung der Datenschutzbehörden Hamburgs, Sachsen-Anhalts und Schleswig-Holsteins. Ziel der Prüfung war herauszufinden, ob die technische und organisatorische Ausgestaltung des MMS einen getrennten Betrieb dreier landesindividueller Länderspiegel darstellt oder ob nicht vielmehr die Implementierung dergestalt ist, dass faktisch ein gemeinsames Verfahren dreier Betei-

ligter betrieben wird. Ein gemeinsames Verfahren stand nach Hamburgischem (Landes-)Datenschutzrecht bis zum Mai 2018 unter einem Gesetzesvorbehalt. Seit dem Inkrafttreten der DSGVO würde man für ein solches Verfahren eine gemeinsame Verantwortlichkeit im Sinne des Artikels 26 DSGVO feststellen. Dies hätte zur Folge, dass die beteiligten Verantwortlichen einzelne Aspekte ihrer Verantwortlichkeiten, ihrer Funktionen und ihre Beziehungen gegenüber betroffenen Personen in einer Vereinbarung festlegen müssten; alternativ kann dies durch Rechtsvorschrift erfolgen.

Im Rahmen der Prüfung wurde festgestellt, dass von keinem der beteiligten Länder eine gemeinsame Verarbeitung gewollt ist und auch die Datenbestände und Funktionsweisen landesindividuell getrennt sind. Noch in Klärung befindet sich die Frage, inwieweit die technische Zusammenarbeit der Länder und die gemeinsame Beauftragung *einer* technischen Implementierung (MMS mit getrennten Datenbeständen), auf die die Verantwortlichkeiten nur gemeinsam Einfluss haben, regelnder Dokumente bedarf.

Offen ist derzeit ebenfalls, inwieweit die Protokollierungen der Abrufe durch Strafverfolgungs- und Sicherheitsbehörden, die aufgrund gesetzlicher Regelungen (§ 40 Abs. 3 Bundesmeldegesetz BMG) gerade nicht den einzelnen Meldebehörden zur Kenntnis gelangen sollen und daher durch diese Behörden selbst vorzunehmen sind, zentral durch das Verfahren MMS im Auftrag dieser Behörden erfolgen können und sollen.

Derzeit kann festgehalten werden, dass länderübergreifende Prüfungen einen größeren Zeitbedarf als landesindividuelle Prüfungen haben, da sich sowohl Prüfbehörden als auch die jeweils geprüften Stellen einschließlich des Auftragnehmers Dataport untereinander abstimmen müssen. Auf der „Habenseite" stehen eine Arbeitsteilung der Prüfbehörden sowie die Gewinnung detaillierter Erkenntnisse.

6.3.4 Community Cloud Mail Service

Unter dem Namen Community Cloud Mail Service (CCMS) betreiben die Bundesländer Bremen und Hamburg zusammen mit Dataport eine gemeinsame Plattform für die Verarbeitung von E-Mails (E-Mail-Server). Das Zentrale IT-Management des Landes (ZIT) pilotiert derzeit ebenfalls die Nutzung dieses Systems und plant den Umstieg zahlreicher Behörden, u. a. auch zur Ablösung von Altsystemen.

Wie auch das Verfahren Mehrländer-Meldedatenspiegel (MMS, Tz. 6.3.3) wird auch das Verfahren CCMS trägerländerübergreifend betrieben. Von einer gemeinsamen Entwicklung und einem gemeinsamen Betrieb verspricht man sich geringere Kosten durch Synergieeffekte. Dies ist prinzipiell nachvollziehbar, doch muss auch bei einem trägerländerübergreifenden Betrieb eine Mandantentrennung erfolgen. Dies betrifft zum einen die Trennung in Bezug auf die beteiligten Bundesländer, zum anderen in Bezug auf einzelne verantwortliche Stellen.

Zum weiteren Verständnis muss man wissen, dass CCMS neben Versand und Empfang von E-Mail-Nachrichten auch Funktionalitäten wie Kalender, Terminplanung und Adressbuch beinhaltet – Funktionen einer modernen Groupware. Bei der Nutzung dieser Funktionen greifen Benutzerinnen und Benutzer aber nicht nur auf eigene Daten bzw. E-Mail-Nachrichten zu, sondern auch auf Daten Dritter (z. B. Kalender und Adressbucheinträge), die ihnen vom System zur Verfügung gestellt werden.

Diese Funktionen sind zweifellos praktisch, sind aber im Hinblick auf Datenschutz und Sicherheit nicht unproblematisch, wenn der Umfang der angezeigten Daten nicht gesteuert wird: Ein Zugriff auf Adressen sowie Kalendereinträge ist innerhalb der eigenen Behörde praktisch und häufig auch dienstlich erforderlich. Auch behördenübergreifend ist ein Zugriff im Einzelfall bei der Zusammenarbeit von Beschäftigten sinnvoll und angemessen.

Schwierig wird es, wenn solche Zugriffe nicht mehr im Rahmen der Erforderlichkeit erfolgen und Zugriffe bundesländerübergreifend auf Tausende von Einträgen möglich sind, denn spätestens hier kommen Fragen des Beschäftigtendatenschutzes zum Tragen: Anders als im Bereich der Telefonauskunft, bei der ein Eintrag in Telefonbücher und Auskunftsplattformen durch Anschlussinhaber beeinflusst werden kann, legt hier der Arbeitgeber Art und Umfang des „Eintrags" fest. Das Gleiche gilt für den Detaillierungsgrad, mit dem Kalendereinträge standardmäßig für Dritte sichtbar sind.

Auch dieses Verfahren bot daher Anlass zu einer länderübergreifenden Zusammenarbeit der Datenschutzaufsichtsbehörden der Dataport-Trägerländer, um die Konfiguration zu hinterfragen. Im Rahmen zahlreicher Diskussionen und eines Austausches von Dokumenten von Konzepten wurde festgestellt, dass die derzeitige Konfiguration geeignet ist, die Daten der einzelnen Bundesländer getrennt zu verarbeiten. Regelungsbedürftig bleibt aber die Art und Weise der Zusammenarbeit der Auftraggeber, denn bestimmte Konfigurationsparameter für CCMS lassen sich nur „global", aber nicht länderindividuell festlegen.

Problematisch bleibt aus Sicht des ULD, dass zwar die Standardeinstellungen akzeptabel sind, aber durch Beschäftigte in einem Umfang geändert werden können, den Behördenleitungen als Verantwortliche im Sinne des Datenschutzrechtes nicht beeinflussen oder nachvollziehen können. So ist es beispielsweise für Nutzende möglich, im Rahmen einer „Selbstadministration" anderen Personen innerhalb des Ländermandanten Zugriffe auf Kalenderdetails und Postfachinhalte zu geben. Solche Funktionen, die für die innerbehördliche Arbeit sinnvoll sind (u. a. bei Funktionspostfächern), sollten aus Sicht einer Behördenleitung aber kontrollierbar und auf das eigene Haus technisch beschränkbar sein. Derzeit besteht das „Haus" aber aus allen an CCMS teilnehmenden Behörden des Landes, sodass nur organisatorische Maßnahmen möglich sind.

Was ist zu tun?

Bei der Einführung von CCMS ist auf die technische Durchsetzung der Trennung zwischen den Ländermandanten einerseits und den teilnehmenden Behörden als (datenschutzrechtlich) Verantwortlichen andererseits zu achten.

07

KERNPUNKTE

Gemeinsame Verantwortlichkeit

Betrieb von Facebook-Fanpages

Ermutigung der Hersteller zum Datenschutz

7 Neue Medien

7.1 Entscheidungen des EuGH zur gemeinsamen Verantwortlichkeit

Der EuGH hat am 5. Juni 2018 im Verfahren zur datenschutzrechtlichen Verantwortlichkeit von Betreibern von Facebook-Fanpages zwischenzeitlich eine wegweisende Entscheidung gefällt (36. TB, Tz. 7.1). Demnach sind der Betreiber des entsprechenden Facebook-Webauftritts und das Unternehmen Facebook gemeinsame Verantwortliche aus Datenschutzsicht:

www.datenschutzzentrum.de/artikel/1241-.html

Auch der EuGH sieht zwischen den Facebook-Seitenbetreibern und Facebook ein enges Kooperationsverhältnis, welches die Annahme gemeinsamer datenschutzrechtlicher Verpflichtungen rechtfertigt. Demnach ermöglichen die Seitenbetreiber dem Unternehmen Facebook die Setzung von Cookies auf den Rechnern von Seitenbesuchern, was der Verfolgung von Werbezwecken dient. Die Seitenbetreiber erhalten von Facebook hingegen die Option, durch Auswahl demografischer Daten der Seitenbesucher an einer zielgruppenspezifischen Datenauswertung für eigene Zwecke mitzuwirken, um z. B. das eigene Informationsangebot anzupassen oder selbst Werbezwecke zu verfolgen. Dabei wird nicht vorausgesetzt, dass der Seitenbetreiber zu den personenbezogenen Daten der Seitenbesucher Zugang hat.

Die Kriterien zur Beurteilung einer gemeinsamen Verantwortlichkeit aus Datenschutzsicht hat der EuGH jüngst auch in einer weiteren Entscheidung untermauert. Demnach ist eine Religionsgemeinschaft gemeinsam mit ihren als Verkündiger tätigen Mitgliedern als Verantwortliche für Verarbeitungen personenbezogener Daten anzusehen, wenn die Mitglieder im Rahmen der Verkündigungstätigkeit von Tür zu Tür personenbezogene Daten von angesprochenen Personen erheben und die Gemeinschaft die Verkündigung durch die Einteilung von Bezirken mit organisiert, ohne dass diese den Mitgliedern nachweisliche Anweisungen zur Verarbeitung bestimmter personenbezogener Daten erteilt hat.

Für die Annahme einer gemeinsamen Verantwortlichkeit war es in diesem Fall nicht erforderlich, dass die Religionsgemeinschaft Zugang zu den personenbezogenen Daten hat.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat ausgehend von der Entscheidung des EuGH zur Verantwortlichkeit beim Betrieb von Facebook-Fanpages den akuten Handlungsbedarf der Beteiligten aufgezeigt:

www.datenschutzzentrum.de/artikel/1244-.html

Vor dem Hintergrund der nun geltenden Regelungen der Datenschutz-Grundverordnung zählen hierzu folgende Punkte:

- Wer eine Fanpage besucht, muss transparent und in verständlicher Form darüber informiert werden, welche Daten zu welchen Zwecken durch Facebook und die Fanpage-Betreiber verarbeitet werden. Dies gilt sowohl für Personen, die bei Facebook registriert sind, als auch für nicht registrierte Besucherinnen und Besucher des Netzwerks.
- Betreiber von Fanpages sollten sich selbst versichern, dass Facebook ihnen die Informationen zur Verfügung stellt, die zur Erfüllung der genannten Informationspflichten benötigt werden.
- Soweit Facebook-Besucherinnen und -Besucher einer Fanpage durch Erhebung personenbezogener Daten getrackt werden, sei es durch den Einsatz von Cookies oder vergleichbarer Techniken oder durch die Speicherung der IP-Adresse, ist grundsätzlich eine Einwilligung der Nutzenden erforderlich, die die Anforderung der Datenschutz-Grundverordnung erfüllt.
- Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage-Betreibern ist in einer Vereinbarung festzulegen, wer von ihnen welche Verpflich-

tung der Datenschutz-Grundverordnung erfüllt. Diese Vereinbarung muss in wesentlichen Punkten den Betroffenen zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen können.

Was ist zu tun?

Die Betreiber von Facebook-Fanpages und Facebook müssen die Anforderungen der Datenschutz-Grundverordnung zur gemeinsamen Verantwortlichkeit erfüllen.

7.2 Facebook und Facebook-Seitenbetreiber – Mit Vereinbarung zur gemeinsamen Verantwortlichkeit alles gelöst?

Mit Urteil vom 5. Juni 2018 hat der Gerichtshof der Europäischen Union (EuGH), Aktenzeichen C-210/16, entschieden, dass eine gemeinsame Verantwortlichkeit von Facebook-Fanpage-Betreibern und Facebook besteht. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hatte zunächst in einer Entschließung vom 6. Juni 2018 deutlich gemacht, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen, insbesondere für die Betreiber einer Fanpage, ergeben (Tz. 7.1).

Bei einer gemeinsamen Verantwortlichkeit fordert die Datenschutz-Grundverordnung u. a. eine Vereinbarung zwischen den Beteiligten, die klarstellt, wie die Pflichten aus der DSGVO erfüllt werden.

Nachdem seit dem Urteil des EuGH drei Monate vergangen waren, ohne dass Facebook eine angekündigte Vereinbarung nach Artikel 26 DSGVO zur Verfügung gestellt hatte, machte die DSK am 5. September 2018 deutlich, dass der Betrieb einer Fanpage, wie sie derzeit von Facebook angeboten wird, ohne eine Vereinbarung nach Artikel 26 DSGVO rechtswidrig ist.

Am 11. September 2018 veröffentlichte Facebook eine sogenannte „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ sowie „Informationen zu Seiten-Insights“.

Im Zusammenhang mit einer Vereinbarung nach Artikel 26 DSGVO ist zunächst Folgendes zu beachten:

Datenschutzrechtliche Verantwortlichkeit richtet sich nach tatsächlichen Gegebenheiten und kann nicht durch Vereinbarungen abbedungen, zugeordnet oder zwischen Akteuren nach Belieben verschoben werden. Insofern hat eine Vereinbarung nach Artikel 26 DSGVO für sich genommen keinen konstitutiven Charakter. Sie stellt vielmehr eine Folgeverpflichtung dar, wenn zwei oder mehr Verantwortliche (Art. 4 Nr. 7 DSGVO) gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen (Art. 26 Abs. 1 Satz 1 DSGVO). Gemeinsam Verantwortliche sind dann verpflichtet, in einer Vereinbarung in transparenter Form festzulegen, wer von ihnen welche Verpflichtung der DSGVO erfüllt. Eine solche Vereinbarung muss gemäß Art. 26 Abs. 2 Satz 1 DSGVO die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend, d. h. insbesondere wahrheitsgetreu, widerspiegeln.

Sinn und Zweck einer Vereinbarung nach Art. 26 Abs. 2 DSGVO ist es, dass die jeweiligen Funktionen in den entsprechenden Verarbeitungsvorgängen bzw. die Beiträge zur Verarbeitung der verschiedenen Beteiligten transparent dargestellt werden. Damit sie diesen Vorgaben

genügt, müssen in einer Vereinbarung nach Artikel 26 DSGVO „klare Informationen mit Erläuterungen zu den verschiedenen Phasen und Akteuren der Verarbeitung“ (Artikel-29-Datenschutzgruppe, WP 169 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, S. 28) gegeben werden.

Insbesondere bedeutet dies, dass die Erfüllung der Datenschutzverpflichtungen eindeutig zugewiesen wird bzw. Ansprechpartner für mögliche Verletzungen dieser Bestimmungen klar bezeichnet werden, um präventiv „eine Beeinträchtigung des Schutzes personenbezogener Daten oder die Entstehung von ‚negativen Kompetenzkonflikten‘ bzw. von Schlupflöchern zu vermeiden, die dazu führen, dass bestimmte Verpflichtungen oder Rechte […] von keiner der Parteien erfüllt bzw. gewährleistet werden“ (Artikel-29-Datenschutzgruppe, WP 169, S. 27 f.).

Ob der jeweils Verantwortliche die Vorgaben der DSGVO einhält, unterliegt seiner Verantwortung. Dies gilt auch, wenn er die Verarbeitungstätigkeiten nicht selbst durchführt, sondern durch einen anderen gemeinsam mit ihm Verantwortlichen durchführen lässt. Der Verantwortliche kann sich nicht ins Blaue hinein darauf verlassen, dass eine Verarbeitung (durch einen anderen gemeinsam mit ihm Verantwortlichen) schon DSGVO-konform durchgeführt werde. Um davon ausgehen zu dürfen, müsste der eine Verantwortliche hinreichende Einblicke in die Verarbeitungstätigkeiten und die technischen und organisatorischen Maßnahmen des anderen Verantwortlichen haben. Zwar kann auch eine Vereinbarung nach Artikel 26 DSGVO dazu beitragen, dass von einem DSGVO-konformen Betrieb ausgegangen werden kann. Dies gilt jedoch nur, wenn eine solche Vereinbarung die notwendigen Informationen enthält.

Eine Vereinbarung zwischen gemeinsam Verantwortlichen steht im Zusammenhang mit der Rechenschaftspflicht der Verantwortlichen aus Art. 5 Abs. 2 DSGVO sowie den Anforderungen aus den Artikeln 24 und 25, wonach Verantwortliche die Einhaltung der DSGVO gewährleisten und nachweisen können müssen.

Ohne ausreichende Kenntnis über die Verarbeitungstätigkeiten, die der eigenen Verantwortung unterliegen, ist ein Verantwortlicher nicht in der Lage zu beurteilen, ob die Verarbeitungstätigkeiten rechtskonform sind oder nicht. Diesbezügliche Zweifel gehen dabei zulasten des Verantwortlichen, der es in der Hand hat, solche Verarbeitungen zu unterbinden.

Aus dem EuGH-Urteil:

„Der Umstand, dass ein Betreiber einer Fanpage eine von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, kann diesen nämlich nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien.“ (EuGH, C-210/16, Rn. 40)

Auch stellt eine gemeinsame Verantwortlichkeit keine Privilegierung hinsichtlich des Erfordernisses einer Rechtsgrundlage dar (siehe auch DSK, Kurzpapier Nr. 16: Gemeinsam für die Verarbeitung Verantwortliche, Artikel 26 DSGVO, abrufbar unter: *https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf*).

Verantwortliche benötigen stets eine eigene Rechtsgrundlage für die Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 DSGVO und – soweit besondere Kategorien personenbezogener Daten verarbeitet werden – nach Art. 9 Abs. 2 DSGVO. Dies gilt auch in den Fällen, in denen sie die Verarbeitungstätigkeiten nicht unmittelbar selbst durchführen, sondern durch andere gemeinsam mit ihnen Verantwortliche durchführen lassen. In diesem Zusammenhang hat der EuGH klargestellt (EuGH, C-210/16, Rn. 36) und bestätigt (EuGH, C-25/17, Rn. 75), dass ein fehlender tatsächlicher Zugriff auf personenbezogene Daten einer Verantwortlichkeit für die Verarbeitung dieser Daten nicht entgegensteht.

Aus der „Seiten-Insights-Ergänzung“ geht hervor, dass die Betroffenenrechte durch Facebook Ireland als einheitliche Anlaufstelle – bzw. vermittelt über die Fanpage-Betreiber – zentral erfüllt werden sollen. Dieser Ansatz steht im Einklang mit Art. 26 Abs. 1 Satz 3 DSGVO (und auch mit den Empfehlungen aus WP 169, S. 27 f.) Daraus lässt sich ableiten, dass bestimmte Prozesse im Umgang mit den Betroffe-

nenrechten seitens Facebook geschaffen wurden.

Allerdings spricht das Addendum auch von einer Übernahme der Verantwortung durch Facebook. Das geht so nicht: Unter Hinweis auf Art. 26 Abs. 3 DSGVO ist klarzustellen, dass gemeinsam Verantwortliche zwar vereinbaren können, wer bestimmte Handlungen zur Erfüllung von Betroffenenrechten primär übernimmt, es jedoch bei der Verantwortlichkeit aller (gemeinsam) Verantwortlichen für die Rechte der Betroffenen aus den Artikeln 12 ff. DSGVO bleibt.

Das Addendum sowie die „Informationen zu Seiten-Insights" enthalten keine weiter gehenden Informationen über die bereits von Facebook veröffentlichten Informationen, anhand derer die Fanpage-Betreiber verlässlich beurteilen könnten, ob die von Facebook durchgeführten Datenverarbeitungstätigkeiten DSGVO-konform sind und insbesondere die Verpflichtungen nach den Artikeln 24, 25 und 32 DSGVO erfüllen.

Wo die „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen" von einer Zustimmung dazu spricht, dass Facebook Ireland in der EU die Hauptniederlassung für die Verarbeitung von „Insights-Daten" für sämtliche Verantwortliche ist (Punkt 4), ist zu betonen, dass sich die Zuständigkeit der jeweiligen Aufsichtsbehörden für die Fanpage-Betreiber nach der DSGVO und den tatsächlichen Gegebenheiten richtet und daher nicht zur Disposition steht. Gemäß den Artikeln 55 ff. DSGVO bleibt eine Zuständigkeit der Aufsichtsbehörden für Fanpage-Betreiber in ihrem Hoheitsgebiet (unabhängig von den durch die DSGVO vorgesehenen Kooperations- und Konsistenzmechanismen) bestehen.

Was ist zu tun?

Facebook muss nachbessern. Wer eine Facebook-Fanpage betreiben will, muss Datenschutzkonformität bei Facebook als gemeinsam Verantwortlichen einfordern.

7.3 Möglichkeit zur Ermutigung von Herstellern zu Datenschutz – Beispiel Freifunk

Der Wirtschaftsausschuss des Schleswig-Holsteinischen Landtages beschäftigte sich mit Anträgen zur Anerkennung der Gemeinnützigkeit von Freifunk-Initiativen (Landtagsdrucksachen 19/757 und 19/778). In diesem Zusammenhang wurde auch die Landesbeauftragte für Datenschutz um Stellungnahme gebeten.

Zwar besteht keine Zuständigkeit des ULD in Fragen der Gemeinnützigkeit. Dennoch betrachten wir eine Anerkennung einer Gemeinnützigkeit als positiv, soweit dies eine DSGVO-konforme Gestaltung von Anwendungen, Diensten oder Produkten fördern kann. Dies kommt aus unserer Sicht auch bei Freifunk infrage, denn zu den wesentlichen Zielen der Freifunk-Initiativen gehören datenschutzfördernde Prinzipien wie beispielsweise Datensparsamkeit, Dezentralität und Überwachungsfreiheit.

Freifunk-Initiativen stellen Infrastrukturen und teilweise auch Router und Router-Firmware zur Verfügung und könnten damit unter den Begriff „Hersteller von Produkten, Diensten und Anwendungen" fallen.

Dieser Begriff wird in der DSGVO im Erwägungsgrund 78 aufgegriffen, der sich auf Art. 25 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) bezieht und in dem von einer „Ermutigung der Hersteller" die Rede ist.

Erwägungsgrund 78 DSGVO

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

Hintergrund dieser Aussage ist, dass die DSGVO keine Verpflichtungen direkt für Hersteller enthält, jedoch den Verantwortlichen und Auftragsverarbeitern ein DSGVO-konformer Betrieb häufig nur dann mit wenig Aufwand möglich ist, wenn die Produkte, Dienste und Anwendungen Datenschutzanforderungen berücksichtigen (Tz. 1.1).

Die DSGVO beschreibt nicht, wie eine Ermutigung der Hersteller ausgestaltet werden kann. Aber Impulse wie eine Förderung über die Anerkennung einer Gemeinnützigkeit sind aus unserer Sicht geeignet, die Ermutigung im Sinne des Erwägungsgrundes 78 der DSGVO zu leisten, wenn damit Datenschutzanforderungen bei der Entwicklung und Gestaltung der informationstechnischen Systeme und der Angebote von Anfang an berücksichtigt und geeignet implementiert werden.

Was ist zu tun?

Die Politik sollte überlegen, auf welche Weise Hersteller zu Datenschutz „by Design“ und „by Default“ ermutigt werden können. Die Anerkennung einer Gemeinnützigkeit für Initiativen kann dazu beitragen.

08

KERNPUNKTE

Selbstdatenschutz

Datenschutz im Erwerbsleben

Big Data

Internet of Things

8 Modellprojekte und Studien

Neben den gesetzlich zugewiesenen Aufgaben der Datenschutzaufsicht beteiligt sich das ULD als Behörde der Landesbeauftragten für Datenschutz an drittmittelfinanzierten Projekten und Studien mit besonderem Bezug zu Datenschutzthemen. Zum einen werden in den Projekten datenschutz- oder transparenzfördernde Technologien entwickelt. Die DSGVO normiert nunmehr ausdrücklich den Einsatz von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in Artikel 25 DSGVO als Anforderung an Verantwortliche. Die Auswahl der einzusetzenden Lösungen ist mit Rücksicht auf den Stand der Technik vorzunehmen, der sich auch über geförderte Forschungsprojekte weiterentwickelt. Zum anderen erfolgt eine Beteiligung an Projekten in Bereichen mit besonderem Risiko für betroffene Personen wie etwa Big Data. Diese Bereiche profitieren besonders durch eine frühzeitige Einbeziehung datenschutzrechtlicher Erwägungen im Entwicklungsprozess. Im Berichtszeitraum beteiligte sich das ULD an Projekten zu aktuellen Themen in den Bereichen Privatheit und selbstbestimmtes Leben (Tz. 8.1), Identitätenmanagement (Tz. 8.2), Datenschutz im Erwerbsleben (Tz. 8.3), Cybersicherheit und Datenschutz (Tz. 8.4), Big Data (Tz. 8.5) sowie zum Internet der Dinge (Tz. 8.6).

8.1 Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt

Weiter geht's beim Forum Privatheit: Das Projekt, das im Dezember 2013 gestartet und Anfang 2017 in die zweite Phase gewechselt ist, wurde Mitte 2018 vom Bundesministerium für Bildung und Forschung evaluiert und kann seine interdisziplinäre Arbeit zur Gewährleistung und Weiterentwicklung informationeller Selbstbestimmung und des Privaten in der digitalen Welt bis März 2021 fortsetzen.

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.

Mittlerweile hat das Leuchtturmprojekt einen guten Grad an Bekanntheit in Deutschland und sogar ein wenig darüber hinaus erreicht. Was ansonsten selten passiert, klappt im Forum Privatheit ausgezeichnet: Auf den Jahrestagungen zu verschiedenen Fokusthemen (2017: Fortentwicklung des Datenschutzes, 2018: Zukunft der Datenökonomie) kommen jeweils ganz unterschiedliche Communities zusammen, die sonst wenig Berührungspunkte haben. Bei dem Forum Privatheit handelt es sich nicht um einen fest installierten „Think Tank", sondern der Charme liegt in der dynamischen Vernetzung je nach Thema und Interessenschwerpunkten.

Im Fokus der Tätigkeit des ULD-Teams standen die Beschäftigung mit den neuen Instrumenten der DSGVO wie Datenschutz-Folgenabschätzung oder Datenschutz durch Gestaltung aus der Wissenschafts- und Praxisperspektive, Technikentwicklungen wie Cross-Device Tracking mit Ultraschall (Tz. 10.3), Konstrukte auf Ebene der Rechtsprechung des Bundesverfassungsgerichts (wie die Überwachungsgesamtrechnung) oder des Europäischen Gerichtshofs und die Operationalisierung der (grund-)rechtlichen Vorgaben.

https://forum-privatheit.de

Was ist zu tun?

Das Forum Privatheit bietet vielfältige Perspektiven auf aktuelle Datenschutzthemen, mit denen es sich zu beschäftigen lohnt. Fördergeber sollten weiter Interdisziplinarität unterstützen, um gut durchdachte, praxistaugliche und nachhaltige Lösungen zu erreichen.

8.2 Identitätenmanagement

Identitätenmanagement für einen besseren Selbstdatenschutz begleitet das ULD als Thema bereits seit vielen Jahren in den Forschungsprojekten. In der Online-Welt sind dabei u. a. die Wahrung der Anonymität, z. B. im Verhältnis zu Webseitenbetreibern und anderen Diensteanbietern, und die zuverlässige Verschlüsselung von Nachrichten bedeutsam. Mit Anonymisierung und Datenschutz online bzw. in mobilen Umgebungen befassten sich die Projekte AN.ON-Next (Tz. 8.2.1) und AppPETs (Tz. 8.2.2). Im Projekt VVV wurden Lösungen für einen effizienten und sicheren Schlüsselaustausch zwecks Gewähr einer Ende-zu-Ende-Verschlüsselung im E-Mail-Verkehr entwickelt (Tz. 8.2.3).

8.2.1 Projekt AN.ON-Next – praktikable und rechtssichere Anonymität im Internet

Die Freiheit und Möglichkeit, sich online anonym zu äußern und auszutauschen, ist ein zentrales Recht in einer freiheitlichen Demokratie. Hierfür stehen vielfältige Mittel zur Verfügung, am bekanntesten ist wohl das Tor-Netzwerk. Zwar wurden durch schrittweise Anleitungen und vorgefertigte Installationspakete die Einstiegshürden erheblich reduziert, dennoch ist eine größere Verbreitung ausgeblieben. Hier gilt es, die Hürden weiter zu senken. Ziel ist eine weitgehende Unbeobachtbarkeit des Surfverhaltens von Nutzerinnen und Nutzern gegenüber Webseitenbetreibern und Diensteanbietern sowie anderen lokalen Angreifern. Die Dienstqualität darf dabei nicht spürbar eingeschränkt werden, sodass auch Echtzeitkommunikation, wie dies in Videokonferenzen nötig ist, genutzt werden kann.

Der Lösungsansatz des Projekts „Anonymität Online der nächsten Generation" (AN.ON-Next) sieht dabei vor, die Anonymisierung so weit wie möglich in die Internetinfrastruktur zu verlegen. So können z. B. Zugangsprovider ihre Kundinnen und Kunden durch einen einschaltbaren Anonymisierungsdienst gegenüber einer Profilbildung von Webseitenbetreibern schützen. Zugleich ist kein weiteres Zutun der Nutzerinnen und Nutzer erforderlich. Neben der providerbasierten Anonymisierung wurden Datenschutzaspekte der kommenden 5G-Mobilfunkstandards betrachtet.

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

8.2.2 Projekt AppPETs – Datenschutz eingebaut in Smartphone-Anwendungen

Im Projekt „Datenschutzfreundliche Smartphone-Anwendungen ohne Kompromisse" (AppPETs) wird an der Entwicklung einer freien Bibliothek sowie von Diensten geforscht, die zur Entwicklung von datenschutzfreundlichen Smartphone-Apps verwendet werden können. Die Bereitstellung einer Sammlung von für Datenschutz und Datensicherheit relevanten Stan-

dardfunktionen ermöglicht Entwicklern die einfache und sichere Implementierung von Lösungen. Dies reduziert das Risiko fehlerhafter oder weniger datenschutzfreundlicher Umsetzungen; ein Rückgriff auf Bibliotheken mit für den Datenschutz kritische Funktionalität könnte unterbleiben.

Im Projekt wird ein Prozess zur Überprüfung der datenschutzrechtlichen Standards bei der Implementierung der Bibliotheken sowie ein Prüfkonzept zur Durchführung dieser Überprüfung entwickelt. Am Ende dieses Verfahrens soll ein Zertifikat stehen, anhand dessen Nutzerinnen und Nutzer nachvollziehen können, ob die AppPETs-Bibliothek bzw. -Services entsprechend den Vorgaben in der Smartphone-Anwendung implementiert wurden und ob diese Vorgaben im weiteren Lebenszyklus der Anwendung weiterhin eingehalten werden.

Daneben sollen Smartphone-Entwickler mittels eines auf Grundlage der Implementierungsvorgaben abgeleiteten Entwicklerleitfadens zu datenschutzfördernder Anwendungsentwicklung angehalten werden und die Grundsätze des Datenschutzes bereits zum Zeitpunkt der Entwicklung berücksichtigen.

Beim Datenschutz durch Technikgestaltung darf nicht allein auf die Implementierungskosten geachtet werden. Vielmehr sind diese im Kontext der Verarbeitungszwecke, dem Stand der Technik und dem Risiko für die Betroffenen zu sehen.

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

Was ist zu tun?

Im technischen Datenschutz müssen die Anforderungen an Datenschutz „by Design" und „by Default" fortgeschrieben und konkrete Mindeststandards (Stand der Technik) definiert werden, damit für die betroffenen Personen ein verbindlicher Schutzstandard und für die Verantwortlichen Rechtssicherheit entsteht.

8.2.3 Projekt VVV – Verschlüsselung einfacher machen

Im März 2018 wurde das vom BMBF geförderte Projekt „Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln" (VVV) erfolgreich abgeschlossen (36. TB, Tz. 8.2.4). Ziel des Projekts war es, die Verteilung öffentlicher OpenPGP-Schlüssel bzw. S/MIME-Zertifikate zu vereinfachen.

Diese Schlüssel sind Grundlage Ende-zu-Ende-verschlüsselter E-Mail-Kommunikation. Mit den vom VVV-Projekt entwickelten Plug-ins stehen nun Konzepte zur Verfügung, die das Versenden Ende-zu-Ende-verschlüsselter E-Mail-Nachrichten mittels gängiger E-Mail-Anwendungen weiter vereinfachen. Für das E-Mail-Programm Thunderbird wurde ein entsprechendes Plug-in im Projekt entwickelt.

Plug-in

Ein Plug-in ist ein Zusatzmodul für eine bestehende Anwendung, wie beispielsweise ein E-Mail-Programm. Damit lassen sich zusätzliche Funktionen mit wenig Aufwand in bestehende Anwendungen integrieren.

Im Gegensatz zu den bisher bestehenden Verteilungskonzepten ist bei der VVV-Lösung neben Sender und Empfänger keine unbekannte dritte Stelle zur Schlüsselverwaltung mehr erforderlich. Bisher wurde diese Aufgabe im PGP-Umfeld von Schlüsselservern wahrgenommen und die Authentizität durch Signaturen anderer Teilnehmer gewährleistet. Die Verwal-

tung der Schlüssel wird dem E-Mail-Serviceanbieter übertragen und liegt damit bei der Instanz, der Nutzerinnen und Nutzer ihre bislang unverschlüsselten E-Mail-Nachrichten ohnehin anvertrauten. Dieses System bietet mehrere Vorteile:

- Kontrolle der Nutzerinnen und Nutzer über den öffentlichen Schlüssel bzw. das S/MIME-Zertifikat von der Erstellung bis zur endgültigen Löschung,
- Sicherstellung der Aktualität und Authentizität auf Dauer,
- leichtes Auffinden sowie automatischer Abruf der Schlüssel der Kommunikationspartner.

Damit sind die Grundvoraussetzungen für den Einsatz asymmetrischer Verschlüsselung auch im öffentlichen Bereich geschaffen. Eine moderne Verwaltung kann ohne das Medium E-Mail als Kommunikationskanal nicht funktionieren. E-Mail-Nachrichten sind unabhängig von Sprechzeiten und bieten Bürgerinnen und Bürgern die Möglichkeit, Anliegen und Fragen jederzeit an die zuständigen Stellen zu richten. Häufig kann dieser Zugang jedoch nicht oder nur eingeschränkt genutzt werden, weil die Vertraulichkeit der Kommunikation auf diesem Wege nicht gewährleistet ist. Daher sollte E-Mail nicht für die Übermittlung sensibler Informationen verwendet werden. Die in VVV ausgearbeiteten Umsetzungsvorschläge können in diesem Kontext auch einen Beitrag zur datenschutzgerechten Digitalisierung der öffentlichen Verwaltung leisten.

https://datenschutzzentrum.de/projekte/vvv/

Was ist zu tun?

Jeder Verantwortliche sollte prüfen, wie sich Ende-zu-Ende-verschlüsselte E-Mail-Kommunikation in die bestehende technische Infrastruktur integrieren lässt. Die erforderlichen Schlüssel sind in geeigneter Form zur Verfügung zu stellen.

8.3 Datenschutz und Erwerbstätigkeit

Besondere Zwangslagen für Betroffene bestehen bei Datenverarbeitungen im Rahmen ihrer Erwerbstätigkeit. Einwilligungen sind hier besonders schwierig, weil die Freiwilligkeit mit Blick auf das Abhängigkeitsverhältnis zum Arbeitgeber oft nicht gewährleistet ist. Daher müssen Systeme und Prozesse zur Verarbeitung von Beschäftigtendaten von vornherein so datensparsam wie möglich gestaltet werden. In zwei Projekten hat sich das ULD mit ausgewählten Gruppen Betroffener näher befasst: Im Projekt EMPRI-DEVOPS (Tz. 8.3.1) betrachten wir gemeinsam mit Projektpartnern technische Lösungen für den Bereich der Softwareentwicklung, in dem besonders enge Protokollierungen der einzelnen Arbeitsschritte üblich sind. Im abgeschlossenen Projekt PARADISE wurde die Fragestellung, wie ein besserer Schutz der Aufenthaltsdaten von Athleten bei Dopingkontrollen ermöglicht werden kann, bearbeitet und dazu auch das neue Anti-Doping-Gesetz betrachtet (Tz. 8.3.2).

8.3.1 Projekt EMPRI-DEVOPS – Datenschutz in digitalen Arbeitswelten

Die Digitalisierung verspricht im Bereich digitaler Arbeitswelten zahlreiche Vorteile. So können Teams bereits heute standortübergreifend mittels entsprechender Softwaretools vernetzt zusammenarbeiten, konferieren und dabei flexibel auf veränderte Anforderungen in der Zusammenarbeit reagieren. Insbesondere im Bereich der Softwareprogrammierung und allgemein im

Bereich mobiler Arbeitswelten ist der Einsatz entsprechender Tools essenziell.

Technikunterstützte Arbeitsweisen versprechen erhöhte Flexibilität und neue Optimierungsmöglichkeiten. Damit wächst auch der Druck zur (Selbst-)Vermessung im „Quantified Workplace". Das steigende Interesse an möglichst vielen Daten über die Beschäftigten verdeutlicht der Preisträger 2018 des deutschen Big Brother Awards in der Kategorie Arbeitswelt. Das Unternehmen bietet eine App an, die sensible Gesundheitsdaten, etwa den Stand der Stressbelastung oder das Schlafverhalten der Beschäftigten, sammelt und Arbeitgebern über ein zentrales Dashboard zur Verfügung stellt.

Bei der Softwarenutzung entstehen darüber hinaus zahlreiche Metadaten und Protokolle, die Aufschluss über persönliche Aspekte der Beschäftigten geben und an denen unterschiedliche Begehrlichkeiten entstehen können. Verstärkte Überwachungsmöglichkeiten und damit einhergehende erhöhte Risiken für die Persönlichkeitsrechte der Beschäftigten bestehen insbesondere, wenn bei der Zusammenarbeit Tools eingesetzt werden, die Leistungskontrollen und eine Überwachung durch Unternehmen oder Kolleginnen und Kollegen über das erforderliche Maß hinaus ermöglichen. In der Praxis wird die Sensibilität dieser Datenspuren in Form von Metadaten bislang nur wenig beachtet.

Das ULD beschäftigt sich daher seit November 2018 im Projekt „Employee Privacy in Software Development and Operations" (EMPRI-DEVOPS) mit der datenschutzfreundlichen Gestaltung von Tools, die typischerweise im Kontext der agilen Softwareprogrammierung und der Systemadministration zum Einsatz kommen. Neben der datenschutzrechtlichen Begleitung der Projektpartner bei der datenschutzfreundlichen Technikgestaltung „by Design" betrachtet das ULD die besonderen datenschutzrechtlichen Rahmenbedingungen, die im Beschäftigungsverhältnis zu berücksichtigen sind. Neben der DSGVO können dabei Bestimmungen des BDSG sowie spezielle arbeitsrechtliche Regelungen im Individual- und Kollektivarbeitsrecht relevant werden.

Die DSGVO überlässt es den Mitgliedstaaten, spezifische Regelungen zum Beschäftigtendatenschutz zu erlassen, wovon der deutsche Gesetzgeber mit § 26 BDSG in eingeschränktem Umfang Gebrauch gemacht hat. Die Norm beschränkt zulässige Datenverarbeitungen auf für die Zwecke des Beschäftigungsverhältnisses erforderliche Verarbeitungssituationen und stellt erhöhte Anforderungen an die Einwilligung im Beschäftigungskontext. Darüber hinaus gibt es insbesondere im Bereich der Mitarbeiterüberwachung eine umfangreiche und nicht immer einheitliche Rechtsprechung, die Rechtsunsicherheiten für Beschäftigte und Arbeitgeber aufzeigt.

Das Projektziel ist, die Leitlinien und Kriterien für den schonenden Ausgleich der berechtigten Interessen von Arbeitgebern und Beschäftigten herauszuarbeiten und die benötigten technischen Mittel entsprechend dem gebotenen Interessenausgleich durch den Einsatz geeigneter Privacy- und Transparency-Enhancing Technologies datenschutzfördernd zu gestalten.

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

Was ist zu tun?

Der Einsatz technischer Mittel darf nicht dazu führen, dass sich im Arbeitsverhältnis das Informations- und Machtgleichgewicht zulasten der Beschäftigten verschiebt.

8.3.2 Projekt PARADISE – Selbstdatenschutz für die Dopingkontrolle im Sport

Im Jahr 1999 wurde die Welt-Anti-Doping-Agentur WADA mit dem Ziel gegründet, weltweit die Maßnahmen gegen Doping im Leistungssport zu organisieren. Viele Leistungssportlerinnen und -sportler kritisieren jedoch seit Langem die systematische Überwachung und intransparente Speicherung ihrer Lebensumstände, die mit der Einführung des Online-Meldesystems „Anti Doping Administration and Management System" (ADAMS) seit 2005 digital erfasst werden. Die sich stellenden datenschutzrechtlichen Fragen liegen im Spannungsfeld zwischen Erforderlichkeit der Datenerhebung zur Aufgabenerfüllung einschließlich einer dynamischen Standortbestimmung und dem Recht auf informationelle Selbstbestimmung. Neben Kontrollen bei Wettkämpfen gibt es für bestimmte Spitzenathletinnen und -athleten auch unangekündigte Trainingskontrollen. Es stellt dabei einen Verstoß gegen die Dopingregelungen dar, wenn solche Tests mehrfach nicht durchgeführt werden können. Damit ist es auch im Interesse der Athletinnen und Athleten, für einen Test verlässlich und zeitnah angetroffen zu werden.

Im aktuell verwendeten System ist die vorherige detaillierte Angabe der Aufenthaltsorte (Whereabouts) erforderlich. Diese Daten wurden bisher bei der WADA in Kanada verarbeitet. Unter anderem mit Blick auf Anforderungen der DSGVO zur technischen Ausgestaltung von Datenverarbeitungssystemen erscheinen Anpassungen dringend erforderlich.

Das vom BMBF geförderte Projekt „Privacy-enhancing And Reliable Anti-Doping Integrated Service Environment" (PARADISE) hatte zum Gegenstand, eine datensparsamere und transparente Alternative zu entwickeln. Die Ortsbestimmung erfolgt dabei mittels GPS-Positionierung. Positionsdaten werden den Dopingkontrolleuren auf Anforderung übermittelt. Protokolle dieser Anforderungen stehen den Betroffenen später zur Einsicht und damit zur Kontrolle der Legitimität der Abrufe zur Verfügung.

Bei der datenschutzfördernden Umsetzung waren vielfältige Designentscheidungen zu treffen. So muss die Backend-Anwendung auf sicheren IT-Systemen in Europa erfolgen. Der Kartendienst zur Darstellung der Position wird auf dem PARADISE-Server und nicht etwa durch Drittanbieter angeboten, dem auf diese Weise dann ebenfalls die Aufenthaltsdaten bekannt würden.

Whereabouts

Für unangekündigte Trainingskontrollen bedarf es detaillierter Informationen über geplante und aktuelle Orts- und Zeitangaben zu Übernachtungen, Training, Wettkämpfen und Urlauben der Athletinnen und Athleten. Diese Angaben gewähren unnötige Einblicke in das Privatleben.

Im Rahmen des Projekts befasste sich das ULD zudem eingehend mit den jüngst geänderten Datenschutzregelungen des Anti-Doping-Gesetzes.

Was ist zu tun?

Datenverarbeitung ist sicher zu gestalten – auch im Sport. Stehen datenschutzfördernde Alternativen zur Verfügung, ist deren Einsatz zu prüfen und insbesondere die Schwere der mit der Verarbeitung verbundenen Risiken angemessen zu würdigen.

8.4 Cybersicherheit und Datenschutz

Informationstechnik ist in allen Bereichen des Alltags vertreten. Sie bestimmt Berufsleben, Mobilität, Freizeit und zieht vermehrt in den Wohnbereich ein. Die verarbeiteten Informationen werden reichhaltiger, ein Verlust bzw. Missbrauch solcher Daten kann einschneidend für die Betroffenen sein. Cybersicherheit ist nicht mehr nur Expertenthema, sondern gerät vermehrt in den Fokus der Öffentlichkeit und Politik. Getroffene Maßnahmen müssen die Sicherheit der Bürgerinnen und Bürger gewährleisten, ohne dabei Bürger- und Grundrechte übermäßig einzuschränken. Das ULD beteiligt sich daher an Projekten im Bereich Cybersicherheit, um in diesem Spannungsfeld den Datenschutzaspekten das nötige Gewicht zu verleihen.

Ein besonderes Risiko für betroffene Personen besteht bei der Verwendung von Daten aus Datenlecks für Identitätsdiebstahl und Betrugsdelikte. Im Netz werden Datenbanken mit der Beute aus Angriffen gehandelt und getauscht. Eine Auswertung solcher Sammlungen kann eine Frühwarnung Betroffener ermöglichen. Wie Sammlung und Auswertung datensparsam und die Information betroffenengerecht erfolgen können, ist Gegenstand des EIDI-Projekts (Tz. 8.4.1).

Cybersicherheit steht zudem stets in einem Spannungsfeld mit Ethik und Recht, beispielsweise dem Recht auf informationelle Selbstbestimmung. In den EU-Projekten CANVAS (Tz. 8.4.2) und PANELFIT (Tz. 8.4.3) werden diese Fragen fachübergreifend erörtert und insbesondere für die Politik aufbereitet. PANELFIT zielt dabei primär auf Fragestellungen aus dem Bereich der Forschung zur Informationstechnologie ab.

Mit zunehmendem Bewusstsein der Verantwortlichen, dass IT-Systeme gesichert sein müssen, rückt der menschliche Faktor als Ansatzpunkt für Angreifer und als Risiko in den Fokus. IT-Risiken durch Beschäftigte durch Tests zu analysieren und die Belegschaft gezielt zu schulen, war Gegenstand des Projekts ITS.APT (Tz. 8.4.4).

8.4.1 Projekt EIDI – verlässliche Benachrichtigung von Betroffenen nach Cybervorfällen

In Zeiten der allgegenwärtigen Digitalisierung wird beinahe täglich über Datenschutzvorfälle berichtet, die den Verlust der Vertraulichkeit personenbezogener Daten zur Folge haben. Darauf, dass die Verantwortlichen ihren Benachrichtigungspflichten gegenüber den Behörden und Betroffenen nachkommen, ist nicht immer Verlass. Oft ist den Unternehmen selbst gar nicht bekannt, dass Daten ihrer Kundinnen und Kunden kompromittiert wurden. Es muss zudem nicht immer eine Sicherheitslücke bei einer datenverarbeitenden Stelle die Ursache sein. Phishing-Kampagnen sind nach wie vor eine beliebte Methode, um an sensible verwertbare Daten zu gelangen. Im Internet werden diese erlangten Informationen dann in Sammlungen gehandelt, in der Regel ohne dass die Betroffenen zunächst davon etwas bemerken. Erst wenn unerwartete Rechnungen eintreffen oder die Kreditwürdigkeit des Einzelnen herabgestuft wird, fällt auf, dass etwas nicht stimmt.

Ganz gleich ob die Daten aus einem Datenschutzvorfall bei einer datenverarbeitenden Stelle stammen oder ob der Betroffene Opfer einer Phishing-Attacke wurde: Frei verfügbare sensible Daten können weitreichende Schäden bei den Betroffenen verursachen. Zurzeit wird den Betroffenen ein hohes Maß an Eigeninitiative abverlangt, wenn sie die Integrität ihrer digitalen Identitäten überprüfen und wahren möchten. Das vom BMBF geförderte Projekt „Effektive Information nach digitalem Identitätsdiebstahl“ (EIDI) entwickelt daher ein Konzept, das die schnellere und proaktive Benachrichtigung der Betroffenen ermöglichen soll. Auf dieser Grundlage sollen auch Betroffene, bei denen kein Verantwortlicher für eine Warnung zustän-

dig ist, z. B. Phishing-Opfer, zukünftig informiert werden können. Die Herausforderung der proaktiven Warnung besteht darin, das Risiko eines Cybervorfalls für den Missbrauch von Daten richtig einzuschätzen. Die Betroffenen sollen einerseits nicht mit Benachrichtigungen überflutet werden. Andererseits soll eine Warnung möglichst aktuell sein und die nötige Aufmerksamkeit erzeugen. Für die Betroffenen stellt sich im Anschluss daran meist die Frage möglicher Schäden und welche Schritte erforderlich sind, um sich vor den Folgen zu schützen. Eine sorgfältige Risikobestimmung kann die Betroffenen bei der Auswahl der passenden Maßnahmen unterstützen.

Im Rahmen des EIDI-Projekts wurden bereits bestehende Identitätsschutzmodelle untersucht. Diese bieten den Nutzenden verdachtsabhängig oder auf Basis einer regelmäßigen Dienstleistung die Möglichkeit zu überprüfen, ob die eigenen Daten im Internet im Umlauf sind. Die Untersuchung zeigte jedoch, dass die Ansätze ein sehr unterschiedliches Datenschutzniveau aufweisen. Je nachdem für welches Modell man sich entscheidet, kann auch aus dem Identitätsschutz selbst ein Risiko für den Betroffenen erwachsen. Insbesondere die Verkettungsmöglichkeiten, die durch kontenbasierte Ansätze entstehen, geben Anlass zur Sorge.

Was ist zu tun?

Betroffene von Datenlecks müssen darüber vom Verantwortlichen unterrichtet werden. Ist der Verantwortliche gar nicht bekannt, ist ein zentrales Frühwarnsystem denkbar. Für die Datenverarbeitung solcher Frühwarnsysteme ist eine strikte Zweckbindung geboten.

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) zielt darauf ab, ein Expertennetzwerk für Cybersicherheit zu schaffen, um den Austausch zwischen Vertreterinnen und Vertretern von Technikentwicklung, Recht, Ethik und Sozialwissenschaft zu ermöglichen. Politische Entscheidungsträger werden über die erkannten Konfliktfelder und mögliche Lösungsansätze unterrichtet.

Der zunehmende Einsatz von Informations- und Kommunikationstechnologien in allen Bereichen der modernen Welt macht oft das Leben leichter und fördert in unterschiedlichster Weise Vielfalt, Kreativität und Interaktivität. Zugleich jedoch wächst damit die Abhängigkeit von Bürgerinnen und Bürgern sowie Organisationen von diesen Technologien. Sicherheitslücken und Missbrauchsrisiken können schwere Konsequenzen nach sich ziehen. Daher ist die Gewährleistung von Cybersicherheit zu einer Angelegenheit von nationalem und globalem Interesse geworden. Dementsprechend kann man im heutigen Cybersicherheitsdiskurs eine Betonung der ständig wachsenden und vielfältigen Bedrohungsformen beobachten, die von einfachen Computerviren über Internetkriminalität und Online-Spionageaktivitäten bis hin zu Cyberterror und Kriegsführung im digitalen Raum reichen.

Diese wachsende Komplexität des digitalen Ökosystems in Kombination mit zunehmenden globalen Risiken hat zu folgendem Dilemma geführt: Eine Überbetonung von Sicherheitsaspekten kann einerseits zulasten der Grundwerte wie Gleichheit, Fairness, Freiheit oder Privatsphäre gehen. Andererseits würde eine Vernachlässigung der Cybersicherheit ein Vertrauen der Bürgerinnen und Bürger in die digitale Infrastruktur, die Politik, in Hersteller und in Behörden untergraben und hätte gleichsam Einschnitte in Grundrechte zur Folge. Aus diesem Grund bringt das CANVAS-Projekt

Stakeholder zu drei zentralen Themenbereichen zusammen: Gesundheit, Business/Finanzen, sowie Polizei/nationale Sicherheit. In den Workshops wird nach geeigneten Lösungswegen gesucht. Die herausgearbeiteten Diskussionsergebnisse und Lösungsansätze werden der Öffentlichkeit, der Forschung sowie der Politik präsentiert und zur weiteren Verwendung aufbereitet. Beispiele hierfür sind wiederverwendbare Lehrinhalte für cybersicherheitsbezogene Fachbereiche an Universitäten oder informative Kurzdossiers für parlamentarische Entscheidungsträger, die mit der Regulierung der Cybersicherheit befasst sind.

Weitere Informationen:

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

8.4.3 Projekt PANELFIT – Cybersicherheit und Datenschutz

Die DSGVO und die noch ausstehende E-Privacy-Verordnung stellen wichtige Änderungen dar, die auch die Forschung und Innovationsvorhaben im Bereich der Informations- und Kommunikationstechnologie betreffen. Schon im Stadium der frühen Entwicklung von technischen Lösungen werden wesentliche Weichen für die Zukunft einer Technologie gestellt, sodass schon an dieser Stelle zentrale ethische, rechtliche und insbesondere datenschutzrechtliche Aspekte Berücksichtigung finden müssen. Basierend auf dieser Erkenntnis, fördert die EU-Kommission die Entwicklung von praktischen Handreichungen für die relevanten Akteure (Stakeholder) in diesem Bereich – namentlich Gesetzgeber, Fördergeber und Forschende. Das im November 2018 gestartete EU-Projekt „Participatory Approaches to a New Ethical and Legal Framework for ICT“ (PANELFIT) will dazu beitragen, Lücken im bestehenden Rahmenwerk zu erkennen und Lösungskonzepte für verschiedene Akteure vorzuschlagen. Während das Projekt auch ethische Aspekte betrachtet, konzentriert sich das ULD auf den Datenschutz.

Die Berücksichtigung und der Einbau von Datenschutz in neu entstehenden Technologien sind besonders wichtig für unsere Gesellschaft. Wir bevorzugen IT-Innovationen, die unsere Privatsphäre bewahren oder im Idealfall sogar verbessern. Um dieses Ziel zu erreichen, muss in jeder Phase der Innovation bewusst der Datenschutz in Betracht gezogen werden. Dies kann bei Ausschreibungen und der Bewertung von Projekteinreichungen anfangen, sich in Anforderungsanalysen und Design von neuen Technologien einflechten (Datenschutz „by Design“) und bis zur Festsetzung von voreingestellten Konfigurationen und Standardwerten reichen (Datenschutz „by Default“). Die Anforderungen zum Datenschutz in der DSGVO richten sich allerdings nur an Verantwortliche, nicht aber unmittelbar an die Hersteller. So könnten z. B. Fördergeber im Rahmen der Projektförderung die Erreichung der Datenschutzziele unterstützen. Dies käme zudem weiteren förderpolitischen Zielen zugute, indem gewährleistet wäre, dass die Entwicklungsergebnisse später ohne maßgebliche Änderungen oder Weiterentwicklungen ihren Einsatz bei Verantwortlichen im Geltungsbereich der DSGVO finden können.

In PANELFIT kann das ULD insbesondere die eigenen langjährigen Erfahrungen aus Forschungsprojekten einfließen lassen, um praktische Handreichungen für Forschende zu gestalten. Wichtig ist es, frühzeitig bei Forschenden ein Grundverständnis für Datenschutzbelange im konkreten Kontext des jeweiligen Forschungsvorhabens zu schaffen. Gleichsam alltäglich und unerlässlich für verteilt tätige Vorhaben ist eine IT-Infrastruktur zur gemeinsamen Arbeit, in der die Rechte und Freiheiten aller betroffenen Personen – und dazu gehören auch die Beschäftigten bei den Projektpartnern – gewährleistet sind.

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

Was ist zu tun?

Datenschutz durch Technikgestaltung sollte so früh wie möglich ansetzen – idealerweise bei der Forschung und Entwicklung neuer Technologien. Fördergeber könnten dies verstärkt anregen oder zur Bedingung bei der Vergabe von Drittmitteln machen.

8.4.4 Projekt ITS.APT – Stärken des Bewusstseins für IT-Sicherheit

Die IT-Sicherheit der eigenen Organisation selbst oder durch hierauf spezialisierte Dienstleister zu testen, ist ein sinnvoller Kontrollschritt und dient der Planung weiter gehender Maßnahmen. Oftmals ist das Testfeld einseitig auf die technische Infrastruktur beschränkt und lässt den Faktor Mensch aus der Bewertung außen vor. Angreifer machen sich jedoch menschliche Schwächen gezielt zunutze. Verschlüsselungstrojaner und Social Engineering, insbesondere Phishing, sind hierfür prominente Beispiele, bei denen unzureichendes IT-Sicherheitsbewusstsein eines Nutzenden gezielt ausgenutzt wird.

Im Forschungsvorhaben „IT-Security Awareness Penetration Testing" (ITS.APT) war die Zielsetzung, die Einhaltung datenschutzrechtlicher Anforderungen schon bei der Konzipierung einer solchen Testmethode zu gewährleisten und dies gleichsam für die Durchführung von Tests und Schulungen sicherzustellen. Die Testgestaltung wurde datenschutzrechtlich begleitet, um sicherzustellen, dass die Persönlichkeitsrechte der Beschäftigten ebenso wie die der Personen, deren Daten verarbeitet werden, geachtet werden. Neben der Gewährleistung der Rechtskonformität war es das Ziel, die Akzeptanz der Testmethode bei den betroffenen Personen zu erhöhen.

Wesentlich für solche Testverfahren mit dem Ziel, das Verhalten der Beschäftigten zu ermitteln, ist eine rechtzeitige und umfassende Einbindung der Beschäftigtenvertretung. Eine Betriebs- oder Dienstvereinbarung dient hierbei zum einen als datenschutzrechtliche Erlaubnisnorm und kann zum anderen die Akzeptanz des Verfahrens erheblich erhöhen. Hierzu sind Testmethode, Testablauf und Art und Weise der Datenverarbeitung detailliert zu beschreiben und eine Verhaltens- und Leistungskontrolle als Resultat dieser Maßnahme auszuschließen.

Die im Projekt gemeinsam mit den weiteren Projektpartnern erlangten Erkenntnisse wurden für spätere Anwender in der Praxis zusammengetragen. Die Bearbeitung aus 2017 berücksichtigt bereits die DSGVO, sodass eine Aufnahme in der Praxis erleichtert wird. Schließlich wird ein Musterverzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO sowie eine Musterdienstvereinbarung als Grundlage für eine Erörterung zwischen Leitung und dem Betriebs- oder Personalrat beigefügt.

https://www.datenschutzzentrum.de/projekte/its-apt/

8.5 Big Data, soziale Netzwerke und Datenschutz

Big Data ist aufseiten der Verarbeiter zur Realität geworden. Während sich die Technologie in diesem Bereich kontinuierlich fortentwickelt, entstehen neue Ideen für Geschäftsmodelle. Vorhandene Datenschätze sollen monetarisiert werden. Gut, wenn insoweit die Interessen und Rechte der betroffenen Personen im Blick bleiben und Maßnahmen zur Gewährleistung von

Transparenz und Betroffenenrechte ihren Niederschlag in den Prozessen finden. Die Projekte mit ULD-Beteiligung befassen sich hier mit einer effektiven Darstellung und Verwaltung von Berechtigungen, z. B. dem Einwilligungsstatus pro betroffener Person und Verarbeitungszweck im Datenpool (Projekt SPECIAL, Tz. 8.5.1). Die Erhebung und Verarbeitung von Daten auf Basis berechtigter Interessen können erheblich durch unverzügliche Anonymisierung und effektive Maßnahmen zur Risikominimierung erleichtert bzw. überhaupt erst ermöglicht werden (iTESA, Tz. 8.5.2). Schließlich sind bei Big-Data-Anwendungen im Bereich der Polizei und Strafverfolgungsbehörden besondere Anforderungen zu beachten, um die Rechtsstaatlichkeit darauf beruhender Verfahren nicht zu gefährden (VALCRI, Tz. 8.5.3).

8.5.1 Projekt SPECIAL – Transparenz- und Einwilligungsmanagement für das semantische Netz

Im Projekt „Scalable Policy-awarE linked data arChitecture for prIvacy, trAnsparency and compLiance“ (SPECIAL) werden künftige datenschutzfördernde Technologien (Privacy-Enhancing Technologies, kurz: PETs) für Big-Data-Anwender entwickelt. Mit der Datenschutz-Grundverordnung erlangen das Management von Einwilligungen, der Umgang mit deren Widerruf bzw. einem Widerspruch gegen Verarbeitungen ebenso zentrale Bedeutung wie die Herstellung hinreichender Transparenz für jegliche Verarbeitung. Dies stellt Big-Data-Anwender vor besondere Herausforderungen. SPECIAL hat daher das Ziel, verschiedene Lösungsansätze, die in Kombination zu einer Verbesserung des Datenschutzes in diesem Bereich beitragen sollen, zu erarbeiten. Diese sind:

- Eine Managementumgebung für Verarbeitungsrichtlinien (Policy Management Framework), die Kontrolle über personenbezogene Daten herstellt, Zugriffs- und Verarbeitungsrichtlinien in maschinenlesbarer Weise abbildet und eine Auditierbarkeit der Verarbeitung gewährleistet.
- Ein Transparenz- und Compliance-Framework, das die notwendigen Informationen darüber vermittelt, wie Daten verarbeitet und wem sie übermittelt werden. Dies soll so geschehen, dass betroffene Personen umfassend und in einer knappen, leicht verständlichen Weise über die beabsichtigte Datenverarbeitung informiert werden. Ferner soll es ihnen ermöglicht werden, korrigierend eingreifen zu können, z. B. durch einfache Möglichkeiten, ihr Widerspruchsrecht nach Artikel 21 DSGVO geltend zu machen.
- Eine skalierbare Architektur für Linked Data, die Verarbeitungsrichtlinien (Data Handling Policies) unterstützt. Sie soll aufbauend auf den Ergebnissen des „Big Data Europe“-Projekts fortentwickelt werden.

Diese Lösungsansätze werden sodann in verschiedenen, für das Projekt entworfenen Testanwendungsfällen ausprobiert und verbessert. Dies umfasst z. B. Anwendungsfälle, die ein Einwilligungsmanagement auf Mobilgeräten umsetzen. Mit einem solchen Einwilligungsmanagement soll gezeigt werden, dass eine Wertschöpfung aus geteilten Daten bzw. Big Data unter Einhaltung datenschutzrechtlicher Belange möglich ist und das Nutzervertrauen in digitale Dienste stärkt. Sollen gesammelte personenbezogene Informationen im Rahmen von Big Data genutzt und gegebenenfalls auch mit anderen Geschäftspartnern geteilt werden, ist insbesondere ein umfassendes Management für Einwilligungen der Nutzenden erforderlich. Damit in der gesamten Verwertungskette die Berechtigungen und Einschränkungen klar sind, sollen die von den Nutzenden erteilten Rechte und die jeweiligen Verarbeitungszwecke als Metadaten zusammen mit den personenbezogenen Daten übertragen werden. Mit einem solchen System lässt sich ebenfalls Transparenz gegenüber den Betroffenen gewährleisten und ein Widerspruchs- und Widerrufsmanagement umsetzen.

Schließlich könnten die Projektergebnisse Grundlage für eine technische Spezifikation für die Ausübung des Widerrufs im Sinne des Art. 21 Abs. 5 DSGVO werden. Das Projekt SPECIAL trägt hier zu einer Community Group unter dem Dach des World Wide Web Consortium (W3C) bei, um eine praxistaugliche Lösung zu erarbeiten.

https://datenschutzzentrum.de/projekte/special/

8.5.2 Projekt iTESA – Reisewarnungen auf Grundlage von sozialen Netzwerken

Im Projekt „intelligent Traveller Early Situation Awareness" (iTESA) ging es um die Erkennung von Reiserisiken auf Grundlage der Analyse von öffentlich zugänglichen Inhalten im Internet. Dazu wurde das Konzept eines Frühwarnsystems entwickelt, das es ermöglicht, Reisende in Echtzeit über mögliche Risiken im Verlauf ihrer Reise oder auf ihrer Reiseroute zu informieren. Durch die Analyse öffentlich zugänglicher Daten sollten so Risiken wie Epidemien, Naturkatastrophen oder ähnliche Gefährdungslagen erkannt werden und die Reisenden nicht nur informiert, sondern eine Gefährdung durch entsprechend sinnvolle Umplanung von Reiserouten auch mit größtmöglicher Chance vermieden werden. Bei den öffentlichen Informationen, die im Rahmen des iTESA-Projekts Berücksichtigung fanden, handelt es sich einerseits um amtliche Informationen (also etwa Reise- oder Wetterwarnungen) und andererseits um nicht amtliche Informationen. Besonders relevant sind in diesem Zusammenhang Nachrichten und nutzergenerierte Inhalte wie etwa Postings in sozialen Netzwerken und Microblogging-Plattformen.

Für das ULD bestand der wesentliche Teil der Projektarbeit in der Implementierung von „Privacy by Design", also der Berücksichtigung von datenschutzrechtlichen Aspekten schon zum Zeitpunkt der Entwicklung entsprechender technischer Lösungen sowie der Prüfung der Zulässigkeit einer Nutzung allgemein zugänglicher Daten im Projektkontext.

Neben datenschutzrechtlichen Aspekten und der Berücksichtigung aller an der Umsetzung eines iTESA-Systems beteiligten Akteure (Dritte, Diensteanbieter und Kunden) hat das ULD auch zivilrechtliche Fragestellungen rund um die Verwendung öffentlich zugänglicher Informationen untersucht und sich mit arbeitsrechtlichen Fragen im Zusammenhang mit der Rechtsgrundlage zur Verarbeitung personenbezogener Daten von Mitarbeitern auf Dienstreisen beschäftigt. Als Rechtsgrundlage für die Verarbeitung der öffentlich zugänglichen Daten dient Art. 6 Abs. 1 Buchst. f DSGVO nach eingehender Abwägung der Interessen der verantwortlichen Stelle mit denen der betroffenen Personen. Aus dem Projekt heraus wurde eine eingehende Darstellung für die korrekte Prüfung dieser Rechtsgrundlage entwickelt und veröffentlicht. Im iTESA-Projekt war zu Zwecken der Risikoreduzierung vorgesehen, aus den online erhobenen Daten sofort automatisiert nur die für Reiserisiken relevanten Informationen zu extrahieren und die Rohdaten zu verwerfen.

Abwägung berechtigter Interessen

Eine praxisrelevante Rechtsgrundlage ist die Datenverarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen nach Art. 6 Abs. 1 Buchst. f DSGVO. Neben dem Vorliegen des eigenen berechtigten Interesses an der Verarbeitung muss der Verantwortliche jedoch auch eingehend mögliche Einschränkungen von Interessen, Grundrechten oder Grundfreiheiten der betroffenen Personen prüfen und diese Risiken mit dem eigenen Interesse abwägen. Gegebenenfalls sind technische und organisatorische Maßnahmen zu treffen und Lösungen des Datenschutzes durch Technikgestaltung vorzunehmen, um die Risiken betroffener Personen ausreichend einzudämmen, bevor Art. 6 Abs. 1 Buchst. f DSGVO als Rechtsgrundlage herangezogen werden kann. Abwägungsvorgang und getroffene Maßnahmen sind zu dokumentieren.

https://datenschutzzentrum.de/projekte/itesa/

Was ist zu tun?

Soll eine Datenverarbeitung zu Zwecken berechtigter Interessen erfolgen, sind diese mit den Interessen der Betroffenen abzuwägen. Dabei darf die gebotene Risikoeindämmung nicht außer Acht gelassen werden.

8.5.3 Projekt VALCRI – Big Data für die Polizei

Das von der Europäischen Kommission geförderte Projekt VALCRI („Visual Analytics for Sense-Making in Criminal Intelligence Analysis") endete zum Juni 2018. VALCRI arbeitete an der Entwicklung eines Systemprototyps für visualisierte Datenanalyse im Rahmen kriminalpolizeilicher Erkenntnisgewinnung (36. TB, Tz. 8.5.3).

Soll mit IT-gestützten Lösungen Kriminalität aufgedeckt werden, geht es im Kern um das Verstehen sehr komplexer Sachzusammenhänge und Verbrechensnetzwerke. VALCRI hatte das Ziel, einen Softwareprototyp für eine solche Datenanalyse zu entwickeln, der nicht nur die polizeilichen Anforderungen erfüllt, sondern auch die datenschutzrechtlichen und ethischen Aspekte berücksichtigt. Dies ist einerseits aus Datenschutzsicht zwingend, andererseits dient es der Gewährleistung, dass der Ermittlungsvorgang im rechtsstaatlichen Rahmen erfolgt.

In Zusammenarbeit mit Universitäten, Wirtschaftsunternehmen und potenziellen Anwendern aus dem Bereich der britischen und der belgischen Polizei hat das ULD daran geforscht, wie ein solches System ausgestaltet sein muss, um die Anforderungen aus den unterschiedlichen Bereichen optimal zusammenzubringen und praktisch umzusetzen. Zu den umzusetzenden technischen und organisatorischen Maßnahmen gehörten Komponenten zur Anonymisierung und Pseudonymisierung personenbezogener Informationen, eine effiziente elektronische Zugangs- und Zugriffskontrolle sowie Konzepte zur Umsetzung von Transparenz in Bezug auf hochkomplexe Datenanalyseprozesse.

Die Anforderungen ergaben sich aus dem neuen Datenschutzrecht im Polizei- und Justizbereich, welche in der seit Mai 2018 geltenden JI-Richtlinie (EU) 2016/680 niedergelegt sind. Anhand dieser wurde das Projektkonsortium datenschutzrechtlich beraten, und Maßnahmen für eine Gestaltung nach „Privacy by Design"-Prinzipien wurden eingebracht.

Als praktische Hilfe entstanden Guidelines, welche die Anforderungen und Methoden von Datenschutz-Folgenabschätzungen im Polizei- und Justizbereich darstellen, um behördlichen Datenschutzbeauftragten eine Hilfe bei ihrer Arbeit an die Hand zu geben. Maßstab und Gliederungshilfe ist dabei der Katalog der Gewährleistungsziele des Standard-Datenschutzmodells (Tz. 6.2.2). Die rechtlichen Anforderungen der JI-Richtlinie lassen sich ebenfalls den Gewährleistungszielen zuordnen. So kann eine Vergleichbarkeit von Verfahren und getroffenen Schutzmaßnahmen ermöglicht werden, die die DSGVO und/oder die JI-Richtlinie erfüllen müssen.

https://datenschutzzentrum.de/projekte/valcri

8.6 Internet der Dinge und vernetzter Verkehr

Zunehmend durchdringt die digitale Vernetzung auch das analoge Leben. Geräte des „Internet of Things" (IoT) unterstützen die Menschen bei der Aufgabenerledigung, im Sport, Alltag und im Verkehr. Sensoren erfassen hierfür die Umwelt. Die fortschreitende Digitalisierung und Vernetzung der Lebenswelten werden an der Entwicklung des Automobils besonders deutlich. Das moderne, vernetzte und in naher Zukunft auch automatisiert fahrende Fahrzeug lässt hoffen, durch den kombinierten Einsatz von Informations- und Kommunikationstechnologie die Zahl der Unfalltoten zu senken, Ressourcen durch effizientere Einsatzmöglichkeiten zu schonen und den Nutzungskomfort spürbar zu erhöhen.

Mit den neuen Technologien gehen aber auch umfangreiche Datenverarbeitungen und sich stetig verfeinernde Möglichkeiten der Datenanalyse und -verwendung einher. Für den Betrieb benötigen die Fahrzeuge große Mengen an aussagekräftigen Informationen über den eigenen Zustand und die Umwelt, die sie auswerten, speichern und sowohl untereinander als auch mit der Infrastruktur und den Dienstanbietern zwecks Orientierung in der Umwelt austauschen. Dadurch erreichen die verarbeiteten Daten in Quantität und Qualität neue Dimensionen.

In modernen Fahrzeugen ist eine Vielzahl von Computern verbaut. Diese werden Bestandteil eines kooperativen Gesamtsystems, bei dem eine große Anzahl unterschiedlicher Akteure und Technologien zusammengeführt wird. Die zunehmende Vernetzung der Lebenswelten zeigt sich besonders im Bereich der Elektromobilität. Dabei wirken die Infrastrukturakteure der intelligenten Verkehrssysteme (Smart Traffic), der intelligenten und automatisierten Systeme eines E-Fahrzeugs (Smart Car), und der Energie-Infrastruktur (Smart Grid) zusammen. Oft ist damit die Einbindung weiterer Dienstleister, die ihrerseits personenbezogene Daten verarbeiten, verbunden, woraus wiederum Risiken resultieren.

Mit Datenschutz im vernetzten Verkehr befasste sich das ULD im Rahmen der Projekte iKoPA (Tz. 8.6.1) und SeDaFa (Tz. 8.6.2). Die Gewährleistung von Transparenz und faktische Möglichkeiten, die Betroffenenrechte wahrzunehmen, werden besonders bei kleinen Geräten des IoT herausfordernd. Hier könnte eine vereinheitlichte Darstellung zentraler Informationen unterstützen, wofür im Projekt Privacy&Us ein Transparenzlabel entwickelt wird (Tz. 8.6.3).

8.6.1 Projekt iKoPA – Datenschutz für den vernetzten Verkehr

Im Kontext des vernetzten Fahrens hat sich das ULD bis Ende 2018 im Projekt iKoPA insbesondere daran beteiligt, ein datenschutzfreundliches Architekturkonzept „by Design" am Beispiel einer pseudonymen Reservierung von Ladesäulen für Elektroautos zu entwickeln.

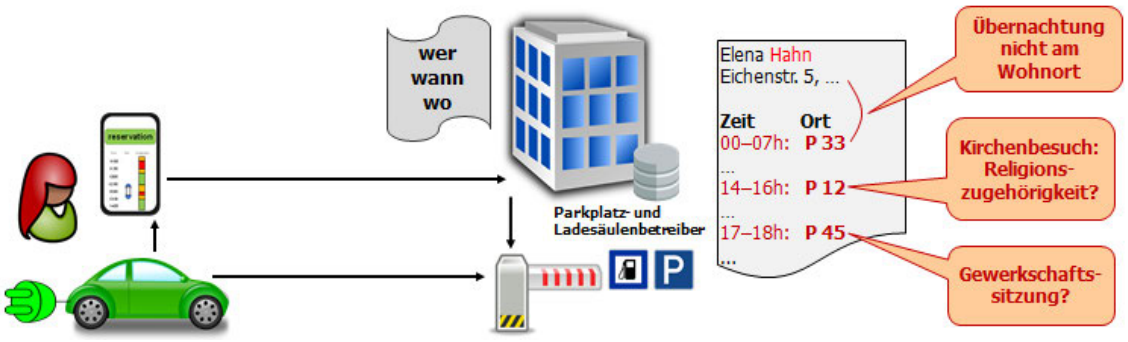


Abbildung: Reservierung von Ladesäulen: beim Betreiber anfallende Daten

Aus datenschutzrechtlicher Sicht wirft das vernetzte Fahrzeug eine Vielzahl von Fragestellungen auf, die von der Bestimmung des Personenbezugs in einem kooperativen System mit zahlreichen Technologien und Beteiligten über die transparente und eindeutige Festlegung der Verantwortlichkeiten bis hin zur Auswahl risikoadäquater bzw. risikomindernder technischer und organisatorischer Maßnahmen reichen. Die DSGVO verfolgt einen risikobasierten Ansatz, der sich am Schutzbedarf orientiert. Standort- und Bewegungsdaten sind insofern besonders schutzbedürftig. Daneben erlauben auch vermeintlich rein maschinenbezogene Fahrzeugdaten Aufschluss über Gebrauch und Nutzungsverhalten und lassen u. a. ihrerseits Rückschlüsse auf Bewegungsdaten zu.

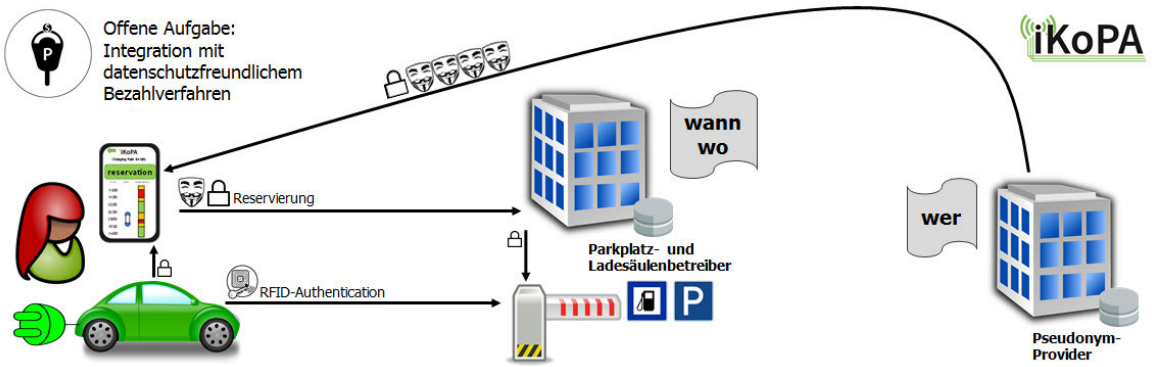


Abbildung: Reservierung von Ladesäulen unter wechselnden Pseudonymen

Die Vielzahl der eingesetzten Technologien, der beteiligten Akteure und der an den Daten Interessierten wächst durch die Vernetzung moderner Fahrzeuge ebenso rasant wie die Anzahl der möglichen betroffenen Personen. Dieser unübersichtlichen Gemengelage ist durch klare Verantwortungsfestschreibungen zu begegnen. Ferner bedarf es nicht nur der Risikobetrachtung jeder eingesetzten Technologie, sondern auch einer Gesamtbetrachtung der möglichen Risiken, die aus einer Kombination der Technologien entstehen.

Eine Reduzierung des Risikos kann durch geeignete frühzeitige Pseudonymisierung erfolgen, die fest in der Architektur vorgesehen ist. So bleibt den Betreibern einzelner Komponenten der Infrastruktur das konkrete „Wer-Wann-und-Wo" der betroffenen Personen verborgen. Die Grafiken enthalten schematische Darstellungen von einem Dienst zur Parkplatzbuchung mit und ohne konsequente Umsetzung der Pseudonymisierung.

https://datenschutzzentrum.de/projekte/ikopa/

8.6.2 Projekt SeDaFa – Selbstdatenschutz für den smarten Verkehr

Die besonderen Herausforderungen, die die Gewährleistung von Transparenz und Intervenierbarkeit für die betroffenen Personen im Kontext moderner Fahrzeuge darstellen, waren Kern des im Frühjahr 2018 beendeten Projekts „Selbstdatenschutz im vernetzten Fahrzeug" (SeDaFa).

Das ULD hat dabei die Entwicklung einer Maßnahme zum Selbstdatenschutz begleitet, mit der der jeweilige Fahrzeugnutzer Transparenz und Kontrolle über sein Fahrzeug erhalten kann. Das Infotainmentsystem bietet sich als Interface zwischen Mensch und Maschine an, um die durch die Vorgaben der DSGVO eröffneten Gestaltungsmöglichkeiten (z. B. die Kombination der Pflichtinformationen mit standardisierten Bildsymbolen und Mehrebenen-Datenschutzerklärungen (Multi-layered Policies)) umzusetzen.

Die Implementierung einer Maßnahme zum Selbstdatenschutz in die Fahrzeugsysteme, die wie eine Firewall fungiert und dem Nutzer die zentrale Kontrolle aller Datenabflüsse aus dem Fahrzeug ermöglicht, hat auch für denjenigen, der für eine Offline- oder Online-Verarbeitung verantwortlich ist, bei der Erfüllung seiner Pflichten nach der DSGVO entscheidende Vorteile. Mit ihr kann die Pflicht zur transparenten Information und Kommunikation und erleichterten Durchsetzung der Betroffenenrechte (Artikel 12 ff. DSGVO) umgesetzt werden.

Neben dem Einsatz von Privacy-Enhancing Technologies bedarf es aber auch einer lokalen Verarbeitung im Fahrzeug selbst, um betroffenen Personen die Ausübung ihrer Rechte zu erleichtern, die Gefahr von Datenschutzverletzungen wirksam zu minimieren und die Verarbeitungsgrundsätze aus Artikel 5 DSGVO wirksam umzusetzen.

Bei der Einbindung von Diensten stellt sich auch die Frage nach den Möglichkeiten zur Datenweitergabe und Verwendung der anfallenden Fahrzeugdaten. Darüber entscheidet nur derjenige, auf dessen Person sich der Informationsgehalt der Daten beziehen kann. Die Freiwilligkeit setzt das Bestehen ernsthafter Alternativen und Praktikabilität voraus. Die Ethikkommission „Automatisiertes und vernetztes Fahren" betont, dass einer normativen Kraft des Faktischen, wie sie etwa beim Datenzugriff durch die Betreiber von Suchmaschinen oder sozialen Netzwerken vorherrscht, frühzeitig begegnet werden sollte.

Die datenschutzfreundliche Gestaltung ist damit eine wesentliche Grundvoraussetzung für datengetriebene Geschäftsmodelle. Zudem müssen der betroffenen Person datenschutzfreundliche Alternativen derart zur Verfügung stehen, dass ihr Möglichkeiten zu informationellem Selbstschutz geboten werden, die sie auch ausschlagen können muss.

https://datenschutzzentrum.de/projekte/sedafa/

Was ist zu tun?

Aus datenschutzrechtlicher Sicht wirft das vernetzte Fahrzeug eine Vielzahl von Problemen auf, die vom Personenbezug über die transparente und eindeutige Klärung und Festlegung der Verantwortlichkeiten bis hin zur Auswahl risikoadäquater technischer und organisatorischer Maßnahmen reichen.

8.6.3 Projekt Privacy&Us – Usability für das Internet of Things

Seit 2017 beteiligt sich das ULD erstmals an einem Marie-Skłodowska-Curie-Projekt, bei dem die Ausbildung von Nachwuchswissenschaftlern gefördert wird. Dreizehn Doktoranden arbeiten verteilt auf Europa und Israel im Projekt „Privacy & Usability" (Privacy&Us) an der Aufgabe, wie Datenschutz verständlich und nutzergerecht gestaltet werden kann. Schwerpunkt der Forschung im ULD liegt dabei auf dem Internet der Dinge („Internet of Things" (IoT)) und den sich daraus ergebenden Fragestellungen für die Nutzungsfreundlichkeit.

Betroffene – neben dem Eigentümer und Betreiber des Gerätes sind dies auch Familienmitglieder, Gäste und sonstige Dritte, deren Daten personenbeziehbar erfasst werden – müssen dabei nachvollziehen können, was mit ihren Daten geschieht (36. TB, Tz. 8.6.2). Zentrale Problemstellungen sind dabei die Information über den gesamten Lebenszyklus des Produkts und wie die erforderlichen Informationen übersichtlich und knapp genug aufbereitet werden können, insbesondere ohne dass eine visuelle Darstellungsmöglichkeit wie ein Display für die Kommunikation mit den Betroffenen vorhanden ist.

Die Bereitstellung der Informationen muss über den gesamten Lebenszyklus des IoT-Geräts mit diesen Phasen erfolgen: Kaufentscheidung, Konfiguration und Set-up, Nutzungsphase, Wartung und Updates sowie Entsorgung bzw. weitere Nutzung durch Dritte. Betreiber von Datenverarbeitungen müssen als Verantwortliche bereits vor dem Erwerb im Rahmen der Kaufentscheidung sorgfältig auch unter Gesichtspunkten des Datenschutzes auswählen. IoT-Geräte kommunizieren vernetzt mit anderen Geräten und Servern – oftmals mit den Servern des Herstellers oder Anbieters eines Dienstes. Eine solche Einbindung von externen Diensten ist bei der Auswahl und späteren Dokumentation ebenso abzubilden wie Datenflüsse in Drittstaaten. Dies ist bei der Risikobewertung entsprechend zu würdigen. Um diese und weitere nach den Artikeln 12 ff. DSGVO erforderlichen Angaben übersichtlich darzustellen, wurde als Zwischenergebnis der Forschungen „LITE – Label for IoT Transparency Enhancement" vorgestellt und befindet sich gegenwärtig in weiterer Entwicklung (siehe Abbildung). Weitere Informationen können dann auf verlinkten Webseiten dargeboten und aktuell gehalten werden.

Usability

Der englische Begriff „Usability" setzt sich aus den Wörtern „use" und „ability" zusammen – direkt übersetzt: „Nutzungsfähigkeit". Gemeint ist die Benutzungsfreundlichkeit von Webseiten, Geräten sowie sonstigen Systemen. Gegenstand sind u. a. Aspekte des intuitiven Benutzens und des schnellen Erfassens dargebotener Informationen.

Abbildung: Entwurf eines Transparenzlabels

https://datenschutzzentrum.de/projekte/privacy-us/

Was ist zu tun?

Verantwortliche, die IoT-Geräte betreiben, müssen den Betroffenen verständlich Datenflüsse und Risiken darlegen. Hersteller und Anbieter solcher Geräte sollten diese Informationen ihren Kunden schon vor der Kaufentscheidung sinnvoll aufbereitet zur Verfügung stellen, um die Verantwortlichen bei der Wahrnehmung ihrer Pflichten zu unterstützen.

09

KERNPUNKTE

Akkreditierung und Zertifizierung nach der DSGVO

Rückblick: Audit und Gütesiegel

9 Zertifizierung: Audit und Gütesiegel

9.1 Akkreditierung und Zertifizierung in Europa

9.1.1 Zukunft von Audits und Gütesiegel nach der DSGVO

Die DSGVO ermöglicht in den Artikeln 42 und 43, dass private Stellen und Datenschutzaufsichtsbehörden Zertifizierungen durchführen dürfen. Während die Aufsichtsbehörden direkt durch das Gesetz zur Durchführung von Zertifizierungen ermächtigt sind, müssen sich private Zertifizierungsanbieter hierfür akkreditieren. Das Akkreditierungsverfahren wird durch die Deutsche Akkreditierungsstelle GmbH (DAkkS) durchgeführt. Hierin sind jedoch die zuständigen Aufsichtsbehörden maßgeblich eingebunden. So führen diese Begutachtungen der Zertifizierungsstellen durch und stimmen im Akkreditierungsausschuss mit darüber ab, ob eine Akkreditierung erfolgt, wobei hierbei das Prinzip der Einstimmigkeit gilt. Nach der Akkreditierung muss schließlich noch die Befugniserteilung durch die Aufsichtsbehörden in einem eigenen Verfahren erfolgen. Aber auch danach bestehen weiterhin Pflichten zur Überwachung der Zertifizierungsstellen und regelmäßige Überprüfungen, ob die Akkreditierungskriterien noch eingehalten werden. Hinzu kommt als Aufgabe für die Aufsichtsbehörden, dass sie den Kriterienkatalog genehmigen, mit denen Zertifizierungsstellen ihre Bewertungen vornehmen.

Für die Aufsichtsbehörden ist der hierfür erforderliche Aufwand schwer abzuschätzen und variiert wahrscheinlich stark zwischen den einzelnen Bundesländern. Daher wollen sich die deutschen Aufsichtsbehörden auf eine gegenseitige Unterstützung einigen.

Was ist zu tun?

Für die Begutachtung von Zertifizierungsstellen müssen ausreichend Kapazitäten an geschulten Mitarbeiterinnen und Mitarbeitern vorgehalten werden. Gegebenenfalls kann hierzu auch Hilfe von anderen Aufsichtsbehörden erbeten werden.

9.1.2 AK Zertifizierung

Das ULD leitet auf Wunsch der Datenschutzkonferenz seit zwei Jahren den Arbeitskreis Zertifizierung der Datenschutzaufsichtsbehörden in Deutschland. Ziel ist es, zusammen mit der Deutschen Akkreditierungsstelle GmbH (DAkkS) Kriterien und Verfahren für die gemeinsame Akkreditierung von Zertifizierungsstellen zu schaffen. Hauptaugenmerk in der Anfangszeit war jedoch die Erstellung von datenschutzspezifischen Ergänzungen zur DIN EN ISO/IEC 17065, wie es die DSGVO von den Aufsichtsbehörden fordert. Diese Norm regelt die allgemeinen Vorgaben zur Akkreditierung von Zertifizierungsstellen. Die Mitglieder des AK Zertifizierung haben hierfür ein Papier entwickelt, das nähere Vorgaben – etwa zur Fachkunde von Gutachtern

und Datenschutzmanagementaufgaben – enthält. Dieses Papier wurde 2018 von der Datenschutzkonferenz angenommen und wird nunmehr dem Europäischen Datenschutzausschuss zur Stellungnahme weitergeleitet.

Weitere Aufgaben waren und sind etwa das Erstellen einer Kooperationsvereinbarung zwischen den Aufsichtsbehörden und der DAkkS, Kriterien für die vergleichbare Bewertungen von Kriterienkatalogen zu entwickeln, Informationsmaterialen für die Verfahren zu entwerfen sowie die Klärung einer Reihe von Grundsatzfragen. Dabei sind stets die Entwicklungen des Europäischen Datenschutzausschusses in diesem Bereich zu berücksichtigen, was zu einer engen Zusammenarbeit des AK Zertifizierung mit den entsprechenden Beteiligten auf europäischer Ebene führt.

Was ist zu tun?

Die Leitung des AK Zertifizierung durch das ULD wird fortgesetzt. Aktuell sind noch zahlreiche wichtige Fragen zu klären, sodass regelmäßige Treffen erforderlich bleiben.

9.1.3 Tätigkeiten des ULD im Rahmen von Akkreditierungen

Um im Bereich des Datenschutzes zukünftig Zertifizierungen gemäß Art. 42 DSGVO durchführen zu können, benötigt die jeweilige Zertifizierungsstelle zunächst eine Akkreditierung durch die Deutsche Akkreditierungsstelle (DAkkS). Bei der Akkreditierung handelt es sich um ein mehrstufiges Verfahren (Antragsprüfung, Prüfung der Zertifizierungsprogramme, Prüfung der Fachkompetenz und des Managements der zu akkreditierenden Stelle, Akkreditierungsentscheidung, Befugniserteilung), bei dem die datenschutzrechtlichen Aufsichtsbehörden, und mithin auch das ULD, unterschiedliche Aufgaben wahrnehmen.

Zum einen prüft und genehmigt das ULD im Rahmen seiner Zuständigkeit die ihm vorgelegten Zertifizierungskriterien anhand bestimmter, im AK Zertifizierung erarbeiteter Mindestanforderungen. Diese Mindestanforderungen treffen eine Aussage zu den wesentlichen Inhalten der jeweiligen Zertifizierungskriterien und sollen eine zwischen den deutschen Aufsichtsbehörden vergleichbare Vorgehensweise bei der Prüfung und Beurteilung der eingereichten Zertifizierungskriterien sicherstellen.

Zum anderen wird gemäß § 2 Abs. 3 Satz 2 Akkreditierungsstellengesetz (AkkStelleG) die für eine Akkreditierung notwendige Fachbegutachtung der zu akkreditierenden Zertifizierungsstelle durch die Befugnis erteilende Behörde vorgenommen. Das ULD wird somit in dieser Rolle bei den zu akkreditierenden Stellen eine Vor-Ort-Prüfung der Zertifizierungstätigkeit vornehmen und dabei die Fachkompetenz und die Durchführung der Zertifizierungstätigkeit überprüfen und beurteilen.

Ferner entscheidet das ULD zusammen mit der DAkkS im Rahmen eines Akkreditierungsausschusses (AKA) über die Akkreditierung einer Zertifizierungsstelle in einem konkreten Verfahren. Darüber hinaus fungiert das ULD gemäß § 39 BDSG, im Rahmen seiner Zuständigkeit, als Befugnis erteilende Behörde für die akkreditierte Zertifizierungsstelle.

9.2 Datenschutz-Gütesiegel

9.2.1 Abgeschlossene Gütesiegelverfahren

Im Zeitraum 2017/2018 hat das ULD für fünf Produkte erstmalig ein Datenschutz-Gütesiegel verliehen. Darüber hinaus konnten im Berichtszeitraum für zwölf weitere Produkte nach Fristablauf der bestehenden Zertifizierung Rezertifizierungen erfolgreich durchgeführt werden.

Im Vergleich zum vorhergehenden Berichtszeitraum 2015/2016 sind sowohl die Zahlen der Neuvergaben von Datenschutz-Gütesiegeln als auch die der Rezertifizierungen um jeweils etwa 50 Prozent zurückgegangen. Die Anzahl der Interessenten, die das ULD bezüglich eines Datenschutz-Gütesiegels Schleswig-Holstein kontaktiert haben, war jedoch im Vergleich zu den Vorjahren in etwa konstant. Das zeigt, dass das Datenschutz-Gütesiegel Schleswig-Holstein bei Herstellern und Diensteanbietern auch im zurückliegenden Berichtszeitraum weiterhin akzeptiert und anerkannt war. Wie dem ULD in einer Vielzahl von Gesprächen mitgeteilt wurde, war die zum Zeitpunkt der Gespräche unklare Entwicklung der Rechtslage und damit der weiteren Gültigkeit einer Zertifizierung von Produkten und Dienstleistungen in den ganz überwiegenden Fällen der Grund, eine solche Zertifizierung zum entsprechenden Zeitpunkt nicht aktiv anzugehen.

Nichtsdestotrotz waren es auch im abgelaufenen Berichtszeitraum wieder Unternehmen aus einigen Branchen, in denen das Gütesiegel eine hohe Marktdurchsetzung aufweist, die sich trotz dieser Unsicherheiten für eine (Re-)Zertifizierung entschieden. Insbesondere betraf dies wieder Unternehmen aus dem Bereich der Akten- und Datenträgervernichtung.

Darüber hinaus waren neben Produkten im Bereich der Medizin- und Sozialdaten wiederum auch cloudbasierte Dienstleistungen häufig Zertifizierungsgegenstand.

Auch im abgelaufenen Berichtszeitraum zeigte sich bei den einzelnen Zertifizierungsgegenständen eine sehr unterschiedliche Ausgestaltung. Aufgrund der u. a. im Bereich der Medizin- und Sozialdaten zum Teil hochsensiblen, personenbezogenen Daten des Betroffenen war die Einbindung anderer Referate des ULD, aber auch anderer Aufsichtsbehörden in den Zertifizierungsprozess oftmals ein wichtiger Aspekt im Zertifizierungsverfahren.

Im Einzelnen wurden folgende Produkte neu zertifiziert:

- „vimacc – Video Management Software", Version 2.2: universelle Videomanagementsoftware zur Übertragung, Anzeige, Auswertung und Archivierung von Videobildern und zugehörigen Metadaten sowie zur Steuerung der Videotechnik wie z. B. von Kameras, Encodern und Schaltkontakten eines digital vernetzten CCTV-Systems,
- „healthCONNECT", Version 1: Proxy-Server zur Verschlüsselung von Daten auf Basis eines Java-Softwaremoduls,
- „Medikationsplanserver des Modellvorhabens ARMIN Stufe 3", Version 1.0.2018.2.19: IT-Service der AOK Plus zur Unterstützung des Anlegens und der Verwendung gemeinsamer Medikationspläne eines Versicherten durch den ihn betreuenden Arzt und Apotheker,
- „REISSWOLF f.i.t.", Version 1.5: webbasiertes Archivierungssystem zur Datenspeicherung und zum Datenzugriff,
- „ennit Cloud", Stand Mai 2018: Infrastructure as a Service auf performanter Hard- und Software, bei der virtuelle Maschinen betrieben werden können.

Im Rahmen eines Rezertifizierungsverfahrens wurden folgende Produkte in einem vereinfachten Verfahren erneut überprüft und zertifiziert:

- „mdex fixed.IP+ (zuvor mdex fixed.IP)", Stand Mai 2018: Ermöglichung der IP-basierten Kommunikation zwischen Mobilgeräten über Mobilfunknetze

bzw. Kommunikation von stationären Geräten mit einem Mobilgerät über ein Mobilfunknetz auf IP-Basis,

- „DC4, DCM4, DCM5“, Stand August 2017: Lesegeräte zur Altersverifikation der Firma ICT Europe GmbH,
- „e-pacs Speicherdienst “, Version 3.0: elektronische externe Archivierung von Röntgenbildern und anderen patientenbezogenen medizinischen Daten,
- „Business Keeper Monitoring System (BKMS)“, Version 3.1: Dialog zwischen Hinweisgebern und Hinweisbearbeitern, um Missstände, Gefahren und Risiken in einer Organisation melden zu können (Whistleblowing),
- „Verfahren der Akten- und Datenträgervernichtung“, Stand April 2018: Verfahren zur Vernichtung von Akten und Datenträgern durch die Ropakt GmbH,
- „Datenträgervernichtung (DV)“, Version 9: mobile und stationäre Akten- und Datenträgervernichtung im Rahmen einer Auftragsdatenverarbeitung durch die Firmen Rhenus Data Office GmbH und Datenmühle GmbH,
- „RED Medical“, Stand Mai 2018: Erhebung, Verarbeitung und Nutzung von medizinischen Patientendaten zur Unterstützung von ärztlichen Anamnesen, Diagnosen und Therapien,
- „DRACOON (ehem. Secure Data Space), Version 4.5.0“: webbasierter, virtueller Datenraum, in welchen Daten hochgeladen, gespeichert, verwaltet und ausgetauscht werden können,
- „HealthDataSpace“, Version 2, Stand Januar 2018: webbasierter, virtueller Datenraum zum Hochladen, Speichern, Verwalten und Austauschen von medizinischen Daten,
- „stepnova“, Varianten: Professional Edition, Basic Edition, Starter Edition, stepfolio, Refugee Edition, Version 4.48: webbasiertes Datenbanksystem zur Organisation im Bildungssektor,
- „ProCampaign 7.0“: multifunktionale, webbasierte Anwendung zur Unterstützung des Customer Relationship Managements bzw. Permission Marketings,
- „KOMMBOSS“, Version 2.10: Unterstützung von Kommunen und öffentlichen Stellen in den Bereichen Personalwesen, zentrale Verwaltung und Organisation.

9.2.2 Sachverständige und Prüfstellen

In den Jahren 2017 und 2018 konnten sechs neue Sachverständige für das Verfahren zur Erlangung des Datenschutz-Gütesiegels Schleswig-Holstein anerkannt werden.

Im Zuge des zweistufig aufgebauten Gütesiegelverfahrens erfolgt die Begutachtung der Zertifizierungsgegenstände durch beim ULD anerkannte Gutachter. Eine Anerkennung als Gutachter kann entweder für den Bereich Recht oder den Bereich Technik beantragt werden, bei Nachweis einer entsprechenden Qualifikation besteht auch die Möglichkeit einer Doppelzulassung. Ebenso ist die Anerkennung einer Prüfstelle möglich. Für eine Anerkennung als Gutachter sind durch den Antragsteller dessen Zuverlässigkeit und Unabhängigkeit sowie die erforderliche Fachkunde nachzuweisen. Letztere muss sich insbesondere auf den Bereich Datenschutz und die Durchführung von Prüfungen/Begutachtungen beziehen und eine mehrjährige praktische Erfahrung beinhalten.

Hinzugekommen als Sachverständige/sachverständige Prüfstellen sind 2017/2018:

- Christian Heutger, Fulda (Technik),
- Michael Pöhlsen, Hamburg (Technik),
- Dr. Thomas Schwenke, Berlin (Recht),
- ePrivacy GmbH, Hamburg (Recht/Technik),
- Stephan Dirks, Kiel (Recht),
- Dr. Volker Wodianka, LL.M., Hamburg (Recht).

Diese Möglichkeit der Anerkennung als Sachverständige bzw. sachverständige Prüfstelle ist

jedoch mit dem Wegfall der Rechtsgrundlage im LDSG am 25. Mai 2018 entfallen. Zukünftige Zertifizierungen durch das ULD auf Basis der DSGVO werden voraussichtlich in einem einstufigen Verfahren durchgeführt.

9.2.3 Die Zukunft des Gütesiegels unter der DSGVO

Mit Einführung des neuen Landesdatenschutzgesetzes Schleswig-Holstein zum 25. Mai 2018 fielen die Regelungen für das Datenschutz-Gütesiegel Schleswig-Holstein und das Behördenaudit weg. Damit endete eine 17-jährige erfolgreiche Ära der Möglichkeit, die Datenschutzkonformität von Produkten und Abläufen in einer Behörde auch vertrauensbildend nach außen tragen zu können.

Der Grund für die Abschaffung der Regelungen im LDSG liegt darin, dass die DSGVO selber die Möglichkeit für Aufsichtsbehörden schafft, Zertifizierungen vorzunehmen. Im Gegensatz zu privaten Zertifizierungsanbietern müssen sich die Aufsichtsbehörden hierfür nicht akkreditieren. Allerdings dürfen sie auch nur im Rahmen ihrer eigenen Zuständigkeit tätig werden. Das ULD kann somit nur Verantwortliche und Auftragsverarbeiter sowohl aus dem Privatbereich als auch öffentliche Stellen in Schleswig-Holstein zertifizieren. Dabei muss sich die Zertifizierung auf konkrete Datenverarbeitungsvorgänge beziehen. Zertifizierungen von reinen Produkten (etwa reine Softwarelösungen ohne einen konkreten Einsatz) sind nicht mehr möglich.

Da das ULD mit dem eigenen Angebot auch in einem Bereich tätig wird, der auch von privaten Zertifizierungsstellen bedient werden könnte, wollen wir vergleichbare Voraussetzungen, wie sie für die Privaten gelten, erfüllen. Maßgeblich sind hierfür auch Papiere zu den Themen Akkreditierung und Zertifizierungskriterien, die vom Europäischen Datenschutzausschuss erstellt werden. Diese lagen erst Ende 2018 bzw. Anfang 2019 in endgültigen Versionen vor, sodass wir hierauf auch bei der Erstellung unserer eigenen Kriterien gewartet haben. Diese werden nunmehr zusammen mit den zugehörigen Verfahren erstellt, sodass wir davon ausgehen, dass wir im Jahresverlauf 2019 auch wieder eigene Zertifikate vergeben können. Hierbei beachten wir auch die aktuell noch zu entwickelnden weiter gehenden Vorgaben aller deutschen Aufsichtsbehörden, die der AK Zertifizierung entwirft. Die bisherige Zweistufigkeit des Verfahrens, bei dem anerkannte Sachverständige die Prüfung vornehmen und das ULD dann nach einer Plausibilitätsprüfung das Siegel erteilt, wird so nicht fortgeführt werden. Vielmehr wird das ULD sowohl die Prüfung des Zertifizierungsgegenstandes als auch die Zertifizierung selbst durchführen.

Was ist zu tun?

Das ULD wird einen eigenen Kriterienkatalog für Zertifizierungen nach der DSGVO erstellen und ein Zertifizierungsverfahren entwerfen. Diese werden nach Fertigstellung auf der Webseite des ULD frei veröffentlicht.

9.2.4 Projekt PRO-OPT

2017 haben wir u. a. das Projekt PRO-OPT des Deutschen Forschungszentrums für Künstliche Intelligenz GmbH bei Datenschutzfragen unterstützt. Ein Ziel des vom Bundesministerium für Wirtschaft und Energie geförderten Projekts war die datenschutzkonforme Verarbeitung von Produktionsdaten in verteilten smarten Ökosystemen am Beispiel der Automobilindustrie.

Insbesondere sollte es ermöglicht werden, dass fahrzeugbezogene Daten von gesamten Fahrzeugflotten (etwa bei einem Autovermieter) ausgewertet werden. Hierbei bieten sich verschiedene Pseudonymisierungstechniken an, die insbesondere die sogenannte „Vehicle Identification Number" betreffen.

Zum Untersuchungsgegenstand gehörte auch das „Crowdsourcing", bei dem öffentliche Foren zu Fahrzeugen ausgewertet werden sollen.

In Form einer Studie haben wir das Projekt über die grundsätzlichen Funktionen des Datenschutzrechts auf Basis der Datenschutz-Grundverordnung informiert, aber auch Stellung zu verschiedenen Pseudonymisierungsverfahren bezogen und Grenzen der Verwendung von vermeintlich oder tatsächlich öffentlichen Daten aufgezeigt.

9.2.5 Projekt AUDITOR

Ziel des Forschungsprojekts AUDITOR ist die Konzeptionierung, exemplarische Umsetzung und Erprobung einer nachhaltig anwendbaren EU-weiten Datenschutzzertifizierung von Cloud-Diensten.

Hierfür haben die Partner des AUDITOR-Projekts bereits eine erste Version der notwendigen Kriterien für die Zertifizierung entwickelt und auf der Webseite des Projekts veröffentlicht. Momentan liegt der Fokus des Projekts auf der Entwicklung von die Zertifizierung begleitenden Prozessen, die u. a. ein gleichbleibendes datenschutzrechtliches Niveau bei der Zertifizierung sicherstellen und garantieren sollen, dass die unterschiedlichen Zertifizierungsstellen selbst nach vergleichbaren Maßstäben zertifizieren.

Im weiteren Verlauf des Jahres 2019 sind bereits die ersten Pilotzertifizierungen im Rahmen des AUDITOR-Projekts geplant.

Das ULD ist im Rahmen dieses Projekts seit Anfang 2018 Unterauftragnehmer und in dieser Rolle als beratender Partner in die Entwicklung des Zertifizierungsprogramms und der dafür erforderlichen Kriterien eingebunden.

9.3 Datenschutzaudits

9.3.1 Audit Bad Schwartau

Vor 15 Jahren, als das Datenschutzaudit vom ULD ins Leben gerufen wurde, gehörte die Stadtverwaltung Bad Schwartau zu den ersten Verwaltungen, die sich der Überprüfung in einem Datenschutzaudit stellten. Schon damals wurden vom ULD die Datenverarbeitungsprozesse bei der Stadtverwaltung begutachtet und erfolgreich zertifiziert. Nach Ablauf der dreijährigen Gültigkeit des Zertifikats hat sich die Stadtverwaltung dann kontinuierlich vom ULD reauditieren lassen und immer wieder einen guten Schutz der Daten bestätigt.

Im April 2018 hat das ULD zum fünften Mal der Stadtverwaltung Bad Schwartau ein Datenschutzauditzeichen verliehen. Damit steht die Stadtverwaltung in Schleswig-Holstein für eine vorbildliche und ordnungsgemäße Datenverarbeitung in vorderster Reihe. Die im Rahmen der Überprüfung erfassten Verarbeitungsprozesse zeichnen sich besonders durch folgende datenschutzfreundliche Aspekte aus:

- Das Datenschutz- und Informationssicherheitsmanagement führt in regelmäßigen Abständen Sitzungen durch, in denen

Datenschutz- und Informationssicherheitsaspekte bearbeitet werden.

- Es wurden organisatorische Abläufe für die Behandlung von auftretenden Datenschutz- und Sicherheitsvorfällen festgelegt.
- An den Arbeitsplätzen werden überwiegend Thin Clients eingesetzt, sodass damit eine Standardisierung der Arbeitsumgebung sichergestellt wird. Ferner lassen sich Sicherheitsfunktionen zentral und einheitlich administrieren.
- Über einen Penetrationstest wurden von einer Fachfirma die IT-Komponenten (z. B. die Firewall und die Serverbetriebssysteme) der Stadtverwaltung Bad Schwartau auf Schwachstellen überprüft. Festgestellte Sicherheitslücken wurden von der Stadtverwaltung Bad Schwartau sofort beseitigt.
- Durch die Anwendung des IT-Grundschutzstandards lassen sich Schutzmaßnahmen zu den schützenswerten Bereichen – Gebäude, Räume, Clients, Server, Router, Firewall, Fachanwendungen usw. – direkt zuordnen, sodass eine gute Transparenz und Überprüfbarkeit gewährleistet wird.
- Für den Anschluss des internen Verwaltungsnetzes an das Internet werden Sicherheitskomponenten eingesetzt, die unerwünschte Zugriffe abwehren.
- Tablets werden durch den Einsatz einer Sicherheitssoftware reglementiert und auf Systemen der Stadtverwaltung Bad Schwartau zentral verwaltet.

9.3.2 Audit Stockelsdorf

Die Gemeinde Stockelsdorf hat sich im Jahr 2017 erfolgreich einem Datenschutzaudit unterzogen, um sich einen sorgfältigen Umgang mit den Daten der Bürgerinnen und Bürger bestätigen zu lassen.

Gegenstand des Datenschutz-Behördenaudits war die Sicherheit und Ordnungsmäßigkeit der internen automatisierten Datenverarbeitung der Gemeinde Stockelsdorf. Dazu gehören

- der Betrieb der PCs, Notebooks, Tablets, Smartphones, Server und Netzkomponenten sowie
- die Anbindung des internen Netzes der Gemeinde Stockelsdorf an externe Netze.

In einer Leitlinie für Datenschutz und Informationssicherheit hat die Gemeinde Stockelsdorf Leitaussagen zu ihrer Datenschutz- und Informationssicherheitsstrategie zusammengefasst, um die festgelegten Datenschutz- und Sicherheitsziele und das angestrebte Datenschutz- und Sicherheitsniveau für alle Beschäftigten transparent zu machen.

Bei der Umsetzung von Datenschutz und Informationssicherheit orientiert sich die Gemeinde Stockelsdorf an dem Grundschutzstandard des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Darüber hinaus ist für die Bewältigung der Aufgaben ein behördlicher Datenschutzbeauftragter ernannt und ein Datenschutz- und Informationssicherheitsmanagement-Team (DISM-Team) eingerichtet worden. Das DISM-Team, bestehend aus der Bürgermeisterin, der Hauptamtsleitung, dem Datenschutzbeauftragten und der IT-Administration, steuert und kontrolliert vorbildlich den Datenschutz und den Informationssicherheitsprozess in der Verwaltung.

Die Durchführung des Datenschutz-Behördenaudits erfolgte in den folgenden Schritten:

- Analyse der Datenschutz- und Informationssicherheitsdokumentation,
- Begutachtung der Wirkungsweise des Datenschutzmanagementsystems und der Erreichung der festgelegten Datenschutzziele,
- stichprobenartige Überprüfung der Umsetzung der festgelegten Sicherheitsmaßnahmen und

- Überprüfung der Einhaltung datenschutzrechtlicher und bereichsspezifischer Vorschriften in Bezug auf den Auditgegenstand.

Die von der Gemeinde Stockelsdorf vorgelegte Dokumentation für den Auditgegenstand bildete die Grundlage für die Begutachtung vor Ort.

9.3.3 Audit Oststeinbek

Gegenstand des Datenschutz-Behördenaudits für die Gemeindeverwaltung Oststeinbek war die Sicherheit und Ordnungsmäßigkeit der internen automatisierten Datenverarbeitung. Dazu gehören

- der Betrieb der PCs, Notebooks, Server und Netzkomponenten,
- die Anbindung des internen Netzes der Gemeindeverwaltung Oststeinbek an das Internet sowie
- die netztechnische Anbindung der Außenstellen „Kindertagesstätte", „Bauhof", „Jugendzentrum" und „Jugendberatung" an das interne Netz der Gemeindeverwaltung.

Um die vielfältigen Verwaltungsaufgaben unter Berücksichtigung des Datenschutzes und der Informationssicherheit zu erbringen, hat der Bürgermeister ein Datenschutz- und Informationssicherheitsmanagement (DISM) eingerichtet, über das er von der Datenschutzbeauftragten und dem Informationssicherheitsbeauftragten über alle wesentlichen diesbezüglichen Aspekte informiert werden soll.

Zu den Aufgaben der Datenschutzbeauftragten gehört:

- Vorsitz des DISM-Teams einschließlich Managementberichte an die Dienststellenleitung,
- die Leitungsebene bei der Erstellung der Datenschutz- und Informationssicherheitsleitlinie zu unterstützen,
- die Erstellung des Sicherheitskonzepts und anderer Sicherheitsrichtlinien zu koordinieren,
- datenschutz- und sicherheitsrelevante Zwischenfälle zu untersuchen sowie
- Sensibilisierungs- und Schulungsmaßnahmen zum Datenschutz und zur Informationssicherheit zu initiieren und zu steuern.

Die Datenschutzbeauftragte wird bei allen größeren Projekten, die Auswirkungen auf die Informationsverarbeitung haben, sowie bei der Einführung neuer Anwendungen und IT-Systeme beteiligt. Sie hat während des Audits mit großem Engagement die vielfältigen Aufgaben bearbeitet.

Für die Umsetzung des Datenschutzes und der Informationssicherheit hat sich die Gemeindeverwaltung Oststeinbek folgende Anforderungen auferlegt:

- Schaffung von organisatorischen Rahmenbedingungen zur nachhaltigen Umsetzung der Datenschutzanforderungen,
- Herstellung des Bewusstseins bei den Mitarbeiterinnen und Mitarbeitern für den sicheren Umgang mit vertraulichen Daten,
- regelmäßige Durchführung von Schulungen und Unterweisungen der Mitarbeiterinnen und Mitarbeiter in den Bereichen Datenschutz und Informationssicherheit,
- Erstellung einer Sicherheitskonzeption auf der Basis des IT-Grundschutzstandards,
- Einrichtung von Kontrollmechanismen zur Überprüfung der Umsetzung der Datenschutz- und Informationssicherheitsziele bzw. der Sicherheitskonzeption.

9.4 Auditberatungen

9.4.1 Auditberatung Ärztekammer SH

Die Ärztekammer Schleswig-Holstein (ÄKSH) verarbeitet personenbezogene Daten ihrer Mitglieder und Beschäftigten sowie personenbezogene Daten im Rahmen der Patientenberatung und von Fortbildungsmaßnahmen. Darüber hinaus ist bei der ÄKSH eine Vertrauensstelle des Krebsregisters eingerichtet, die besonders sensible Daten verarbeitet.

Der Geschäftsführer der ÄKSH hat das ULD beauftragt, die ÄKSH über die grundsätzliche Beratung hinaus bei der Analyse bestehender Prozesse der Datenverarbeitung sowie bei der Festlegung und Umsetzung von geeigneten Schutzmaßnahmen zu unterstützen.

Die Datenverarbeitung der ÄKSH sollte nach Empfehlung des ULD auf Basis des IT-Grundschutzstandards in Verbindung mit den zu beachtenden Regelungen der DSGVO datenschutzkonform betrieben werden. Daraufhin hat die ÄKSH ihre Konzeption neu nach dem Grundsatz „Datenschutz auf der Basis von IT-Grundschutz“ festgelegt.

Das ULD hat danach eine Bestandsaufnahme der Datenverarbeitung der ÄKSH durchgeführt. Im Anschluss wurden in Zusammenarbeit mit der Geschäftsführung, dem Leiter der IT-Abteilung und der Datenschutzbeauftragten Schutzmaßnahmen auf der Basis des IT-Grundschutzstandards festgelegt. Ferner wurden erforderliche Datenschutzanforderungen aufgenommen und projektbezogen in die Umsetzung gebracht.

Die IT-Abteilung der ÄKSH hat den Betrieb der Datenverarbeitungssysteme einschließlich Informationssicherheits-, Softwareentwicklungs-, Netz- und Administrationsmanagement professionell umgesetzt. Auch die in der Verantwortung der IT-Abteilung betriebenen Server- und Technikräume werden mit hoher Sorgfalt fachkundig geführt. Geringfügig festgestellte Schwachstellen wurden mit der Implementierung der neuen Konzeption abgestellt.

Die Datenschutzanforderungen wurden gemeinsam mit der Datenschutzbeauftragten erörtert. Eine Bestandsaufnahme der Verarbeitungstätigkeiten und der damit verbundenen noch zu ergreifenden Schutzmaßnahmen wurden im Rahmen von umsetzenden Aufgaben beschrieben. Diese wurden von ihr in angemessener Zeit bearbeitet.

Insgesamt hat die Geschäftsführung die vom ULD festgestellten Sachverhalte konstruktiv aufgenommen und mit allen beteiligten Mitarbeiterinnen und Mitarbeitern besprochen. Daraufhin wurden von ihr die Empfehlungen des ULD zur Verbesserung des Datenschutzes und der Informationssicherheit zeitnah umgesetzt.

Was ist zu tun?

Für ein gutes Niveau an Informationssicherheit können sich Verantwortliche und Auftragsverarbeiter an dem aktualisierten IT-Grundschutzstandard des Bundesamts für Sicherheit in der Informationstechnik (BSI) orientieren und geeignete Sicherheitsmaßnahmen für die Daten der Betroffenen umsetzen.

10

KERNPUNKTE

Verschlüsselung mit TLS 1.3

Tracking mit Ultraschall

Gelbe Punkte vom Farbdrucker: Zwangscodierung

10 Aus dem IT-Labor

10.1 TLS 1.3 ist da – jetzt aktualisieren!

In den letzten Jahren hat sich die Situation verschlüsselter Kommunikation im Internet erfreulich verbessert. So hat sich im Bereich der Webseiten das verschlüsselnde HTTPS als Standardprotokoll etabliert. Einige Browser warnen schon, wenn noch das unsichere HTTP (ohne „S“) zum Einsatz kommt. Auch Suchmaschinen strafen Webseiten ab, die in puncto Sicherheit hier der Zeit noch hinterherhängen.

Im März 2018 wurde von der Internet Engineering Task Force (IETF) nach langer Diskussion endlich der aktuelle Versionsstand 1.3 des Protokolls TLS („Transport Layer Security“) zur verschlüsselten Übertragung von Daten verabschiedet. Wie der Vorgänger SSL wird TLS eingesetzt, um eine Transportverschlüsselung beim Aufruf von Webseiten, bei der Übertragung von E-Mails, bei der Kommunikation per Instant Messaging sowie bei vielen weiteren Anwendungsfällen zu etablieren.

TLS 1.3 bietet dabei weitgehende Vorteile gegenüber den vorherigen Versionen. So wird insbesondere das im schon zehn Jahre alten Vorgänger TLS 1.2 noch optionale „Forward Secrecy“-Prinzip jetzt durch TLS 1.3 durchgehend umgesetzt. „Forward Secrecy“ gewährleistet, dass ausgespähte und aufgezeichnete Verbindungen auch dann nicht nachträglich entschlüsselt werden können, wenn das Kryptozertifikat in falsche Hände gerät. Dabei wird für jede Verbindung ein eigener Schlüssel generiert, der mithilfe des Zertifikats lediglich ausgetauscht und danach verworfen wird.

Das neue TLS v1.3 bietet zudem auch einen besseren Schutz vor Schad-Proxies, die die Verbindungen aufbrechen und Inhalte ausspähen, unterdrücken oder verändern wollen. Dafür wurden u. a. veraltete und inzwischen als nicht hinreichend sicher erkannte Algorithmen und Verfahren entfernt, andere Bereiche des Standards wurden neu gefasst und gestrafft, um auch das Ausspähen von Kommunikationsbeziehungen besser zu verhindern.

Vorsicht bei der Einführung von TLS 1.3 ist allerdings angesagt, denn mit TLS 1.3e bzw. eTLS oder (nach Intervention der IETF ob des Namens) nun ETS wurde an der IETF vorbei unter einer sehr ähnlichen Bezeichnung eine künstlich kompromittierte Variante von TLS 1.3 publiziert, die einige der neuen Sicherheitsfeatures wieder untergräbt und damit deutlich hinter den Stand der Technik zurückfällt: Unter anderem kommen statische Schlüssel zum Einsatz, sodass das Konzept von „Forward Secrecy“ nicht wirkt. Vorgeblich dient diese Schwächung des Standards dem Zweck, innerhalb von Rechenzentren auch verschlüsselten Datenverkehr überwachen zu können; in der Außenkommunikation soll TLS 1.3 verwendet werden. Aber ob ETS an Rechenzentrumsgrenzen haltmacht, oder auch bei Providern zum Einsatz kommt, bleibt unklar. Im Ergebnis bedeutet dies, dass sich Clients nicht auf eine ununterbrochene Verschlüsselungskette zwischen Client und Server verlassen können. Für die Absicherung personenbezogener Daten ist ein Einsatz von ETS daher nicht geeignet.

Trotz der grundsätzlich erfreulichen Entwicklung, dass immer mehr Kommunikation nach dem neuesten Stand der Technik verschlüsselt wird, verbleiben aber auch noch einige Herausforderungen: Große Schwachstellen bei der Sicherheit der Kommunikation gibt es nach wie vor bei E-Mail und Telefonie. Während bei E-Mails mit dem Update auf TLS 1.3 zumindest die Transportsicherung auf den aktuellen Stand gebracht werden kann, bietet diese allein jedoch nicht immer das erforderliche Schutzniveau für die Übermittlung sensibler Kommunikationsinhalte. Ein handhabbares Verfahren für eine Ende-zu-Ende-Verschlüsselung der Kommunikationsinhalte, wie Messenger sie zunehmend bieten, ist bei E-Mails nicht in Sicht. Dies ist auch ein Grund, warum Messenger in der Alltagskommunikation der Menschen inzwischen einen höheren Anteil als E-Mails verzeichnen.

Bei der Telefonie ist darüber hinaus oft noch nicht einmal eine Transportverschlüsselung gegeben, sondern es wird allein auf die Abschottung der Netze gesetzt. Wie spätestens aus den Snowden-Enthüllungen bekannt ist, ist dies ein unzureichender Ansatz. Hier besteht daher noch großer Entwicklungs- und Handlungsbedarf, um auch für Sprachtelefonie endlich sichere Ende-zu-Ende-Verschlüsselung allgemein zu etablieren. Derzeit ist man dafür zumeist noch auf Softwarelösungen wie die Sprachfunktionalitäten von Messengern angewiesen.

Was ist zu tun?

Servicebetreiber sollten ihre Technik spätestens bis Ende 2019 auf TLS 1.3 aktualisieren. TLS ohne Forward Secrecy sollte gar nicht mehr eingesetzt und die Unterstützung von TLS 1.2 bis Ende 2020 eingestellt werden. ETS (TLS 1.3e/eTLS) sollte nicht eingesetzt werden.

10.2 Messenger

WhatsApp als Platzhirsch der Instant Messenger bekommt 2019 eine aus Sicht der Facebook-Betreiber lang ersehnte Funktion: Mit Werbung soll der Dienst nun monetarisiert werden. Neben den bisherigen Kritikpunkten Adressbuchabgleich und Metadatenanalyse (siehe 36. TB, Tz. 7.3) kommt nun der Aspekt der zugeschnittenen Werbung hinzu. Vorausgesetzt, Facebook möchte in seiner teuer erkauften Messaging-App nicht nur generische Banner anbieten, muss das Verhalten der Nutzenden analysiert werden, um auf sie angepasste Anzeigen auszuspielen. Bei Redaktionsschluss war noch nicht bekannt, wie genau die Werbung beschaffen sein wird – lediglich die Darstellung im Statusbereich der App ist bislang bestätigt. Sicher ist hingegen, dass ein solches Angebot die App nicht datenschutzfreundlicher machen wird. Immerhin bewahrt uns momentan die Ende-zu-Ende-Verschlüsselung vor der Auswertung der Chatverläufe. Was die Medieninhalte angeht, existiert allerdings nach wie vor ein fragwürdiger Passus in der Datenschutzerklärung von WhatsApp: „Um die Leistung zu verbessern und Mediennachrichten effizienter zuzustellen, beispielsweise wenn viele Personen ein beliebtes Foto oder Video teilen, können wir solche Inhalte länger auf unseren Servern behalten. Wir bieten außerdem eine Ende-zu-Ende-Verschlüsselung für unsere Dienste an, die standardmäßig aktiviert ist [...]“

https://www.whatsapp.com/legal/?lang=de
(Abruf 01.02.2019)

Man könnte aus dieser Passage herauslesen, dass die Verschlüsselung nicht für Medieninhalte gilt. Das widerspricht allerdings den Aussagen des Entwicklers der Verschlüsselung, Moxie Marlinspike, dessen für den Messenger „Signal“ entwickeltes Verfahren auch bei WhatsApp zum Einsatz kommt: „[...] Signal Protocol support for all WhatsApp communication across all WhatsApp clients [...] includes chats, group chats, attachments, voice notes, and voice calls.“

https://signal.org/blog/whatsapp-complete/
(Abruf 04.02.2019)

Auch die für 2020 geplante Zusammenlegung von Facebook Messenger, Instagram und WhatsApp dürfte den Datenschutz nicht weiter nach vorn bringen: Zum einen könnte dies die Bereitschaft von Nutzenden weiter senken, datenschutzgerechtere Messenger zu verwenden, zum anderen steigt die Menge der für Facebook auswertbaren Metainformationen nochmals an. Daneben wird zunehmend deutlich, welche Macht von Facebook ausgeht, das schon jetzt den weitaus größten Teil der Kurznachrichtenkommunikation weltweit kontrolliert. Durch die Gestaltung der Dienste als Silo, in dem Kommunikation nur mit Nutzenden des

eigenen Dienstes möglich ist, werden alternative Anbieter zunehmend unattraktiv, je mehr Nutzende Facebook für die eigenen Kundinnen und Kunden erreichbar macht. Bei Telefon, Briefpost oder E-Mail gilt es als selbstverständlich, mit Menschen unabhängig von ihrem Diensteanbieter zu kommunizieren. Auf dem Markt der Instant Messenger hingegen ist jeder Anbieter sein eigener Monopolist, der keine Konkurrenz im eigenen Netz fürchten muss. Alternative Messenger, die auf einen föderierten Ansatz ähnlich der Struktur von E-Mail setzen, existieren zwar, sind allerdings in Sachen Nutzerzahl den als Silo konzipierten Diensten weit unterlegen.

Dass die Suche nach Alternativen zu WhatsApp mitunter Fallstricke bergen kann, zeigt der Messenger Telegram. Er bietet zwar ebenfalls eine Ende-zu-Ende-Verschlüsselung, diese muss aber manuell und für jeden Chat einzeln aktiviert werden. Wer die Aktivierung dieser Funktion vergisst, chattet lediglich transportverschlüsselt. Die Unterhaltung ist dann sogar weniger sicher, als dies bei WhatsApp der Fall gewesen wäre: Telegram speichert diese unverschlüsselten Chats auf seinen Servern und ist damit in etwa so sicher wie ein herkömmlicher Webmailer: Wer Zugriff auf das Konto erlangt, kann die Nachrichten auch aus der Ferne einsehen. Gruppenchats lassen sich in Telegram generell nicht verschlüsseln, hier werden stets alle Mitteilungen zentral gespeichert. Auf der Suche nach einem Messenger, der auch vor dem Diensteanbieter selbst schützt, ist Telegram also keine gute Wahl.

Gestaltung als Silo

In IT-Anwendungen, die als Silo gestaltet werden, werden die Daten in der Regel zentral von Anbietern verwaltet. Es handelt sich um eine Insellösung, abgeschottet von anderen Anwendungen. Bei Messengern bedeutet dies, dass die Nutzenden bei einem Anbieter nicht mit den Personen bei anderen Anbietern kommunizieren können – anders, als dies im Telefonnetz der Fall ist.

Was ist zu tun?

Nach wie vor lohnt sich ein Blick in die Messenger-Übersicht bei Wikipedia: Viele Mitteilungsdienste unterstützen standardmäßige Ende-zu-Ende-Verschlüsselung und verwenden etablierte Algorithmen zur Verschlüsselung, einige sind sogar unter einer freien Softwarelizenz erhältlich.

https://de.wikipedia.org/wiki/Liste_von_mobilen_Instant-Messengern

10.3 Nutzerverfolgung durch Ultraschall

Nutzerverfolgung ist im Internet allgegenwärtig. Durch die Möglichkeiten, die Smartphones bieten, gewinnt das Thema allerdings erheblich an Brisanz.

Das liegt vor allem an der enormen Informationsdichte, die auf einem Smartphone vorliegt: Personenbezogene Daten werden hier nicht nur in Form von Fotos oder Kontakten gespeichert, sondern vor allem in Echtzeit erzeugt, wie z. B. Nutzungsverhalten oder die Daten der diversen Sensoren der Geräte. So kann ein Smartphone nicht nur seine GPS-Position bestimmen, sondern auch den Luftdruck, Beschleunigung, Erschütterungen oder Geräteausrichtung messen – man denke an „Wasserwaagen-Apps".

Durch sogenannte Seitenkanalattacken lassen sich auf dem Smartphone vorliegende Informationen zweckentfremdet nutzen. So ist es

beispielsweise gelungen, durch das Messen der Erschütterungen des Gerätes die auf dem Touchdisplay eingegebenen Kennworte zu rekonstruieren.

Durch Aussenden und Empfangen von Ultraschallsignalen können Geräte in räumlicher Nähe Informationen austauschen, ohne dass eine Datenverbindung im klassischen Sinn bestehen muss. Nutzen lässt sich so ein Verfahren z. B. in Schulungen, um den Austausch von Zugangsdaten zu erleichtern, indem Teilnehmende eine gemeinsame App starten, die dann alle umliegenden Geräte miteinander bekannt macht. Aber auch zum unbemerkten Verfolgen und Überwachen ist die Technik nutzbar. So gibt es Anwendungen, bei denen Ultraschallsignale in Fernsehsendungen eingebunden sind. Smartphone-Apps der Zuschauenden empfangen diese Signale und melden den Empfang weiter. Auf diese Weise kann der Medienkonsum der Nutzenden analysiert werden. Auch Kundenbewegungen in Supermärkten sind auf diese Weise erfassbar, wenn das Geschäft mit entsprechenden Ultraschallsendern ausgestattet ist und Apps der Nutzenden den Empfang melden. Dies wurde unter dem Stichwort „Ultrasound Cross-Device Tracking“ (uXDT, geräteübergreifende Nachverfolgung per Ultraschall) bekannt. Problematisch an solchen Varianten des Ausspähens ist vor allem, dass die zugrunde liegenden Aufzeichnungsverfahren vom Berechtigungskonzept der Smartphone-Betriebssysteme nur unzureichend erfasst werden. So brauchen Apps im Allgemeinen keine (technische) Berechtigung, um Erschütterungen, Kompassdaten oder den Lautsprecher zu verwenden. Die Verwendung des Mikrofons muss zwar genehmigt werden, wird aber von Nutzenden für gewöhnlich nicht mit der Verfolgung ihrer Position und Gewohnheiten assoziiert.

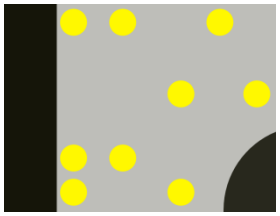
Nutzung von Ultraschall auf Mobilgeräten

Unter Ultraschall versteht man Frequenzen jenseits des menschlichen Hörvermögens, also höher als 20 kHz. Die bekannteste Anwendung dieser Frequenzen ist die Sonografie in der Medizin. Ultraschallsignale können von gewöhnlichen Lautsprechern erzeugt und von ebenso gewöhnlichen Mikrofonen aufgezeichnet werden. Für das menschliche Ohr sind sie nicht wahrnehmbar, können also auch unbemerkbar eingesetzt werden. Auf Mobilgeräten lassen sich so kleinste Datenpakete per Tonübermittlung übertragen – ähnlich dem Akustikkoppler aus den Anfangstagen der Vernetzung.

Was ist zu tun?

Smartphone-Nutzende sollten einmal mehr auf Berechtigungen der installierten Apps achten. Insbesondere der Zugriff auf das Mikrofon muss skeptisch betrachtet werden. Entwickler sollten möglichst umfassende Transparenz in Bezug auf die Hardwarezugriffe ihrer Apps herstellen.

10.4 Gelbe Punkte im Farbdruck



Multifunktionsgeräte (Netzgeräte mit Druck-, Kopier-, Scan-, Mail- und Fax-Funktionalitäten) sind heutzutage nahezu in jedem Behörden- oder Unternehmensnetz vertreten. Auch in Privathaushalten werden immer mehr dieser multifunktionalen Geräte eingesetzt. Damit diese Geräte unterschiedlichen Systemumgebungen und Anforderungen gerecht werden, sind sie mit umfangreichen Diensten ausgestattet, die einen angepassten Einsatz erlauben. Schon 2009 hat das ULD an seinem eigenen Multifunktionsgerät einen professionellen Penetrationstest vornehmen lassen. Die Ergebnisse wurden im 31. Tätigkeitsbericht des ULD (2009) sowie in einer technischen Handreichung (Beschreibung von Sicherheitsmaßnahmen beim Einsatz von Multifunktionsgeräten) dargestellt, die die Wichtigkeit der „Härtung" von Multifunktionsgeräten unterstreicht.

https://www.datenschutzzentrum.de/tb/tb31/kap10.html#103

Doch Verantwortliche müssen nicht nur die Risiken aus netztechnischer Sicht beim Einsatz von Multifunktionsgeräten berücksichtigen. Auch die Kopien und Ausdrucke von Multifunktionsgeräten und Farblaserdruckern selbst können ein Risiko darstellen. Der Grund dafür liegt im üblicherweise nicht sichtbaren Bereich, bei den Yellow Dots.

Yellow Dots

„Yellow Dots", „Tracking Dots" oder „Machine Identification Code": Diese Begriffe bezeichnen mikroskopisch kleine, für das bloße Auge nicht sichtbare und in einem Raster angeordnete gelbe Punkte, die einen Ausdruck so eindeutig kennzeichnen, dass er bis zum Drucker zurückverfolgbar ist.

Das Problem ist nicht neu, schon 2004 hat die Firma Canon für die Einbettung einer unsichtbaren eindeutigen Gerätekennung den Big Brother Award in der Kategorie Technik erhalten. Bis zum Jahr 2017 hat die Electronic Frontier Foundation (EFF – *https://www.eff.org/*) eine Liste der Farblaserdrucker geführt und regelmäßig aktualisiert, die Yellow Dots in ihre Farbdrucke integriert haben. Danach wurde diese Liste nicht weiter aktualisiert, da davon ausgegangen wird, dass heute jeder Farblaserdrucker einen individuellen Machine Identification Code in Form von Yellow Dots auf Farbausdrucke integriert.

Das ULD hat im Rahmen einer Neubeschaffung eines Multifunktionsgeräts den Planungs- und Beschaffungsprozess sowie den praktischen Einsatz des neuen Multifunktionsgerätes unter die Lupe genommen. Dabei standen besonders die Fragen zur Verwendung von Yellow Dots im Vordergrund, u. a.:

- Werden bei dem Multifunktionsgerät Yellow Dots verwendet?
- Wenn ja, ist die Verwendung von Yellow Dots dokumentiert?
- Wenn ja, welche Informationen sind in den Machine Identification Code hineincodiert?
- Wenn ja, gibt es eine Möglichkeit, das Aufdrucken der Yellow Dots zu unterbinden?

Im Ergebnis lässt sich festhalten, dass sich während der Entscheidungsfindung für ein entsprechendes Multifunktionsgerät weder vom Lieferanten noch vom Hersteller ausreichende Informationen darüber einholen ließen, ob die Funktionalität der Yellow Dots bei ihrem Gerät eingesetzt wird. Somit konnte die Geräteauswahl nur anhand der technischen Systemspezifikationen vorgenommen werden.

Während der Einführungsphase des neuen Multifunktionsgeräts in den Räumen des ULD wurden sowohl die definierten Funktionalitäten und Sicherheitsfunktionen implementiert und getestet als auch zusätzlich intensiv überprüft, ob Yellow Dots auf Farbkopien ausgebracht werden bzw. ein Machine Identification Code verwendet wird.

Die Grundlage der Untersuchungen zum Machine Identification Code ist eine farbige Vorlage, die mit den standardmäßig vorgegebenen Farbprofilen kopiert wurde. Technisch gesehen besteht „Kopieren" aus dem Einscannen der Vorlage und dem anschließenden Ausdruck. Daher ist jede Kopie auch ein Ausdruck. Auf allen Kopien, die mit einem Farbprofil erstellt wurden, konnten die Yellow Dots mit einem Mikroskop (siehe Abbildung) eindeutig nachgewiesen werden. Auf Ausdrucken, die mit dem Druckprofil „Schwarz" erstellt wurden, konnten keine Yellow Dots nachgewiesen werden.

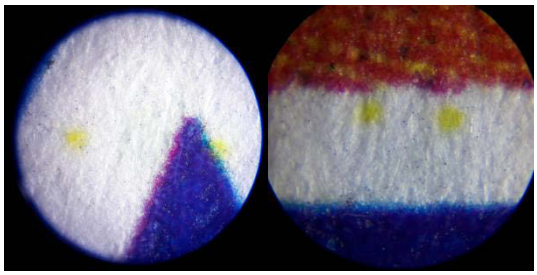


Abbildung: Vergrößerte Darstellung der Yellow Dots

Eine zusätzliche Untersuchung der Kopien mit Schwarzlicht zeigte neben dem Nachweis, dass Yellow Dots vorhanden sind, auch eine systematische Anordnung der Punkte. Dazu wurde ein Bereich der Farbkopie vergrößert und mit Schwarzlicht angestrahlt (siehe Abbildung). Das Ergebnis zeigt, dass der komplette Ausdruck mit einem punktförmig angeordneten Code überzogen ist.

Abbildung: Sichtbare Yellow Dots unter Schwarzlicht

Mithilfe von Kontrast, Farb- und Stilisierungsfiltern wurde das Bild so bearbeitet, dass es für die Augen einfacher ist, ein eventuelles Muster zu identifizieren. In der folgenden Abbildung sind zur besseren Erkennbarkeit einige markante Punkte zusätzlich rot eingefärbt. Es ist deutlich nachweisbar, dass es sich hier um ein wiederkehrendes Muster handelt.

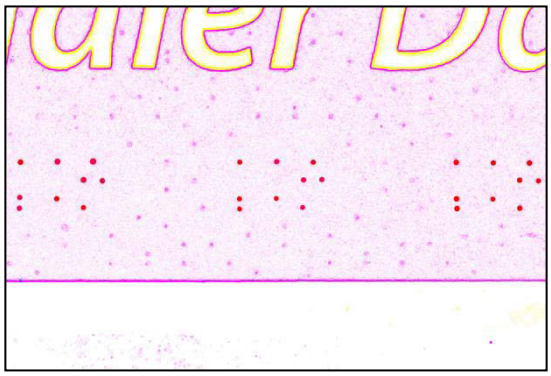


Abbildung: Wiederkehrendes Muster (zur besseren Erkennbarkeit nachträglich rot eingefärbt)

In Anlehnung an die Entschlüsselung des Machine Identification Code des Multifunktionsgeräts Xerox DocuColor 12 durch die EFF (2005), die im Code eines 8 x 15-Punktrasters die Seriennummer und den Zeitstempel des Drucks decodieren konnte, ist davon auszugehen, dass in der Anordnung der Punkte die Seriennummer des Gerätes sowie Datum und Uhrzeit des Druckes codiert sind.

Über die Verwendung der Yellow Dots, die sich auf den Farbkopien des Multifunktionsgeräts befinden, wird weder auf der Webseite des Herstellers, in der Systemspezifikation noch in der Bedienungsanleitung des Gerätes hingewiesen. Der Hersteller reagierte auf Anfrage zur Yellow-Dot-Problematik mit einem allgemeinen Hinweis auf das Kennzeichnungs- und Banknotenerkennungssystem und einen Verweis auf die Webseite Banknotes & Counterfeit Deterrence der Central Bank Counterfeit Deterrence Group.

Eine ausführliche Handreichung über diese Untersuchung zu den Yellow Dots kann auf der ULD-Webseite heruntergeladen werden:

https://www.datenschutzzentrum.de/artikel/1274-Yellow-Dots.html

Was bedeutet das Ergebnis für die praktische Arbeit mit diesen Geräten in Behörden und

Unternehmen? Jede Farbkopie, die mit einem Multifunktionsgerät erzeugt wird, enthält eine zurückverfolgbare Spur zu diesem Gerät. Der Code kann auf den Farbkopien eindeutig nachwiesen werden; unklar ist allerdings, welche Informationen in dem Code gespeichert sind. Die notwendige Transparenz liefern weder die Handbücher, Dokumentationen und Systemspezifikationen noch eine Anfrage beim Hersteller. Somit ist eine Farbkopie nicht mehr für eine (vermeintliche) vertrauliche Kommunikation zu verwenden, denn es werden auf einer zusätzlichen (nicht mit dem bloßen Auge sichtbaren) Ebene zusätzliche Daten auf der Farbkopie gespeichert, die nicht den Transparenzanforderungen entsprechen.

Setzt das ULD das Multifunktionsgerät ein? Ja, aber mit stark eingeschränkten Funktionalitäten, einer restriktiven Konfiguration und einer starken Sensibilisierung und organisatorischen Anweisungen an die Mitarbeitenden. Alle Nutzerinnen und Nutzer sind darüber informiert, dass jede Farbkopie so gekennzeichnet ist, dass sie bis zum erzeugenden Gerät zurückverfolgbar ist. Somit muss jede Mitarbeiterin und jeder Mitarbeiter bei der Nutzung des Gerätes entscheiden, inwieweit eine Zurückverfolgbarkeit des Dokuments oder der Datei in ihrem oder in seinem Verantwortungsbereich vertretbar ist. Im Zweifelsfalle ist es besser, auf eine Farbkopie zu verzichten und auf eine Schwarz-Weiß-Kopie auszuweichen.

Was ist zu tun?

Dieses Beispiel zeigt eindrucksvoll auf, dass beim Einsatz technischer Geräte zur Datenverarbeitung das Risiko von Datenspuren besteht. Das Wissen um diese Tatsache sollte bei allen Mitarbeitenden in die Arbeitsabläufe und Prozesse mit einfließen, um eine Weitergabe von personenbezogenen oder anderweitig vertraulichen Daten zu verhindern und um eine unbeabsichtigte Nachverfolgbarkeit von selbst erzeugten Dateien (auf Papier oder elektronisch) zu unterbinden oder zumindest zu erschweren.

10.5 Test mit Echtdaten

Das LDSG-neu enthält zum Thema Testen eine Regelung in § 7 Abs. 1 (und parallel in § 40 Abs. 4 zur Umsetzung der EU-Richtlinie 2016/680) sowie Verweise auf die Datenschutzverordnung (§ 7 Abs. 2 und § 40 Abs. 5 LDSG-neu), die aber nach dem Außerkrafttreten der Datenschutzverordnung am 31.12.2018 leerlaufen. Dennoch ist es hilfreich, sich an diesen Regelungen zu orientieren.

Die dort genannten Regelungen beziehen sich auf den Test von technisch-organisatorischen Datensicherheitsmaßnahmen, die vor der Freigabe zu erfolgen haben. Hintergrund ist, dass vor der Aufnahme der Produktion Gewissheit über die Zuverlässigkeit und Wirksamkeit der Datensicherheitsmaßnahmen herrschen soll.

Werden Echtdaten für Entwicklungszwecke verarbeitet, besteht die Gefahr, dass solche Daten unbefugt verbreitet werden. Sie werden dann in einer Weise verarbeitet, bei der die Wirksamkeit der Datensicherheitsmaßnahmen (noch) unklar ist. Ebenso wäre dies eine Zweckdurchbrechung, denn die Daten sind üblicherweise nicht für Entwicklungszwecke erhoben worden. Eine Nutzung durch Dritte (Entwickler) wäre zudem als Auftragsverarbeitung abzubilden und dürfte durch den Entwickler nicht für eigene Zwecke verwendet werden – kein realistisches Szenario. Daher dürfen Echtdaten nicht für Entwicklungszwecke eingesetzt werden; eine Nutzung könnte aber mit anonymisierten Daten erfolgen.

Davon unabhängig sind fachliche Tests in der Bereitstellungsphase der Software, insbesondere bei Softwareupdates. Zwar ist die Integrität der Datenverarbeitung eines der laut Art. 5 Abs. 1 Buchst. f DSGVO zu erreichenden Ziele, doch erstrecken sich diese Regelungen der DSGVO nicht primär auf die fachliche Korrektheit von Entscheidungen oder Berechnungen, sondern auf den Schutz von Daten vor unbefugter Manipulation und Schädigung. Allerdings kann man in Art. 5 Abs. 1 Buchst. e DSGVO im Begriff „Richtigkeit der Daten" durchaus den Anspruch der DSGVO sehen, dass eine Datenverarbeitung korrekte Ergebnisse zu liefern hat.

Eine solche Sicht gebieten die fachlichen Tests in der Bereitstellungsphase mit Systemen, die möglichst nahe an die Echtsysteme herankommen (sowohl im Hinblick auf die Daten als auch die Software). Sofern es sich bei dem „Test" um Abnahmetests handelt, kann man dies unter „Wartung" subsumieren; insofern präzisiert hier § 3 LDSG-neu die Regelungen von Art. 5 Abs. 1 Buchst. e DSGVO durch eine Präzisierung der Zwecke, die mit dem ursprünglichen Zweck der Datenverarbeitung vereinbar sind. Dies steht aber unter dem Vorbehalt, dass schutzwürdige Interessen der betroffenen Personen nicht entgegenstehen.

Für Abnahmetests im Rahmen einer Wartung bedeutet dies, dass unter Umständen Kopien eines Echtdatenbestandes eingesetzt werden können. Voraussetzungen sind:

- Eine Durchsicht der Dokumentation, insbesondere des „Changelogs", zeigt keine Gefährdungen der Datensicherheit und des Datenschutzes durch neue Funktionalitäten oder Schnittstellen („jetzt mit Cloud-Anbindung"). Sollte dies allerdings der Fall sein, müssen eventuell notwendige Sicherungsmaßnahmen vor dem Test implementiert werden.
- Die Verwendung anonymisierter Daten ist unverhältnismäßig.
- Die Verarbeitung (hier: fachliche Tests) erfolgt durch Personen, die zur Nutzung der Daten im Echtbetrieb befugt sind (d. h. keine Durchbrechung von Zugriffsbefugnissen).
- Die Tests erfolgen in einer isolierten Umgebung, die den gleichen Datenschutz- und Sicherheitsmaßnahmen unterliegen wie die Echtsysteme.
- Die Tests haben keinen Einfluss/keine Rückkopplung auf die Echtdaten (isolierte Umgebung); es darf auch keine Verwechslungsgefahr bestehen oder Bescheide/Ausgaben aus Testsystemen als Echtbescheide versandt werden. Daher ist hier eine besondere Aufmerksamkeit geboten.
- Die Datenkopien auf den Testsystemen werden nach den Tests umgehend gelöscht.

Wenn stattdessen anonymisierte Daten zum Einsatz kommen, können sie auf den Testsystemen verbleiben – dies spricht ebenfalls für den Einsatz anonymisierter Testdaten. Ebenso lassen sich die Testergebnisse mit anonymisierten Daten besser dokumentieren, denn ein Test darf nicht dazu führen, dass personenbezogene Daten über die fachliche Erforderlichkeit hinaus gespeichert werden, nur weil sie als Testfall verwendet und daher in die Dokumentation aufgenommen wurden.

Details sind in Abschnitt 2.2 der Orientierungshilfe „Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb" zu finden:

https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_Projekt-Produktivbetrieb.pdf

Was ist zu tun?

Der Einsatz von Echtdaten zu Testzwecken ist nur unter engen Voraussetzungen und unter Wahrung der Zugriffsberechtigungen und Sicherheitsanforderungen im Rahmen einer Wartung zulässig.

11

KERNPUNKTE

Kernbegriffe des Datenschutzes europäisch abgestimmt

E-Privacy-Verordnung

11 Europa und Internationales

Europäische Vorgaben sind mittlerweile Bestandteil der täglichen Arbeit und werden daher auch nicht mehr in diesem Berichtskapitel erörtert, sondern gehören zu den jeweiligen Themen. Die Zusammenarbeit und notwendige Abstimmung der Datenschutzaufsichtsbehörden der europäischen Mitgliedstaaten findet in verschiedenen Gremien statt (Tz. 2.1.2). Für Deutschland sind stets Vertreter des Bundesbeauftragten für den Datenschutz beteiligt; daneben entsenden die Landesbeauftragten für Datenschutz eigene Vertreter. Das ULD hat für die Landesbeauftragten für Datenschutz in Deutschland die Vertretung in der Key Provisions Expert Subgroup, in der Technology Expert Subgroup und zeitweise in der Enforcement Expert Subgroup übernommen. Außerdem werden Expertinnen und Experten aus dem ULD zu Spezialthemen wie z. B. Diskussionen zu sozialen Medien in verschiedene europäische Gremien eingeladen.

11.1 Key Provisions Expert Subgroup – Abstimmungen zur Einwilligung, zur Transparenz und zu Datenschutzbeauftragten

Die Key Provisions Expert Subgroup des Europäischen Datenschutzausschusses befasst sich regelmäßig mit Kernbegriffen des Datenschutzrechts. Im Berichtszeitraum wurden unter Mitwirkung des ULD u. a. Stellungnahmen zur Transparenz, zur Einwilligung und zu den Datenschutzbeauftragten überarbeitet und vom Europäischen Datenschutzausschuss angenommen.

Die Stellungnahme zur Einwilligung (WP 259 rev. 01) befasst sich mit den Elementen einer gültigen Einwilligung, ihrer Einholung, den zusätzlichen Bedingungen, spezifischen Formen – wie beispielsweise der Einwilligung von Kindern oder zu wissenschaftlichen Forschungszwecken – sowie mit Wechselwirkungen zwischen der Einwilligung und anderen Rechtsgrundlagen des Artikels 6 DSGVO.

Die Leitlinien für Transparenz (WP 260 rev. 01) befassen sich mit den maßgeblichen Faktoren zur Herstellung von Transparenz und insbesondere mit den Informationspflichten gegenüber der betroffenen Person aus Artikel 13 und Artikel 14 DSGVO sowie der Wahrnehmung und Beschränkung von Rechten der Betroffenen.

Die Leitlinien zu den Datenschutzbeauftragten (WP 243 rev. 01) führen Grundvoraussetzungen für die Benennung, die Stellung und die Aufgaben aus. In einem Anhang werden die wichtigsten Fragen zu diesem Bereich in leicht verständlicher Form beantwortet.

Die Stellungnahmen sind unter den folgenden Links abrufbar:

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

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

11.2 Stellungnahme zur E-Privacy-Verordnung

Obwohl es vonseiten des europäischen Gesetzgebers ursprünglich beabsichtigt war, die Richtlinie 2002/58/EG (E-Privacy-Richtlinie) parallel zur DSGVO zu überarbeiten und diese in Form einer Verordnung neu zu erschaffen, fand dies bis heute noch nicht statt. Die bisherigen Vorschläge, insbesondere des Parlaments, sind umstritten, die Diskussionen werden äußerst kontrovers geführt. Aufgrund der Entwicklungen bei den Beratungen über den Vorschlag

und als Hilfestellung für die beiden gesetzgebenden Organe hat sich der Europäische Datenschutzausschuss auf Vorschlag der Technology Subgroup (unter Beteiligung des ULD als Co-Rapporteur) im Frühjahr 2018 entschieden, weitere Beratungen und Klärungen zu spezifischen Fragen anzubieten, die durch die vorgeschlagenen Änderungen der gesetzgebenden Organe aufgeworfen wurden. Der Europäische Datenschutzausschuss veröffentlichte in diesem Zusammenhang eine Stellungnahme, die auf einige wichtige Punkte hinweist, die bei einer Neuregelung seiner Ansicht nach zu berücksichtigen sind.

Die bisherigen Entwürfe bringen eine Erweiterung des örtlichen Anwendungsbereichs mit sich, der sich entsprechend den Vorgaben der DSGVO u. a. am Marktortprinzip orientiert. Auch hinsichtlich des sachlichen Anwendungsbereichs zeichnet sich eine Erweiterung im Vergleich zur jetzigen Rechtslage ab. Zum einen sollen nämlich sogenannte Over-the-Top-(OTT-)Dienste in den Anwendungsbereich aufgenommen werden. Dies sind solche Dienste, die funktionsäquivalent zu klassischen Telekommunikationsdiensten (wie z. B. SMS) erbracht werden, ohne im klassischen Sinne Telekommunikationsdienste zu sein, da sie nur mittels bzw. auf der Internetinfrastruktur erbracht werden (beispielsweise Messenger-Dienste wie WhatsApp). Für die Nutzerinnen und Nutzer ergibt sich jedoch hinsichtlich der Funktion (interpersonelle Kommunikation) kein Unterschied, weshalb sie rechtlich gleich behandelt werden sollen wie klassische Telekommunikationsdienste. Das heißt, dass die Verarbeitung personenbezogener Daten durch diese Dienste u. a. dem Telekommunikationsgeheimnis unterworfen würden.

Außerdem enthalten die bisherigen Entwürfe Vorgaben für Software (beispielsweise klassische Browser, aber auch Apps für mobile Betriebssysteme), mittels derer ein Zugang zum Internet erlangt werden kann. So soll es verpflichtend Einstellungsmöglichkeiten für die Nutzer und Nutzerinnen geben. Da das aus dem allgemeinen Datenschutzrecht geltende Prinzip des Verbots mit Erlaubnisvorbehalt auch den Entwürfen der E-Privacy-Verordnung zugrunde liegt, ist von besonderer Bedeutung, welche Ausnahmen vom grundsätzlichen Verbot der Verarbeitung von elektronischen Kommunikationsdaten durch die Verordnung gemacht werden. Zu befürworten wären klare Erlaubnistatbestände, die hinreichend präzise Vorgaben für die Verarbeitung personenbezogener Daten in bestimmten Verarbeitungssituationen machen. Auch die Verarbeitung von Daten, die z. B. von Smartphones ausgesendet werden (z. B. sogenannte „Probe Requests“) oder von den Endgeräten ausgelesen werden können, sollte nur zu bestimmten festgelegten Zwecken zugelassen sein.

Die Verarbeitung personenbezogener Daten von einer vorherigen Einwilligung der betroffenen Personen abhängig zu machen, stellt zwar betroffene Personen in den Fokus einer Entscheidung, bringt jedoch die Gefahr mit sich, dass die Verantwortung für das „Ob“ der Datenverarbeitung auf die betroffenen Personen abgewälzt wird, ohne dass diese tatsächlich überblicken können, ob bestimmte Verarbeitungstätigkeiten der Verantwortlichen risikoreich sein werden oder nicht. Ebenso begegnet es Bedenken, wenn durch die E-Privacy-Verordnung Rechtsgrundlagen eingeführt würden, die eine Verarbeitung personenbezogener Daten auf Grundlage eines berechtigten Interesses erlauben. Denn gerade Datenverarbeitungen in einem derart spezifischen Umfeld sollten nicht auf eine unspezifische Interessenabwägung gestützt werden, die allen an der Datenverarbeitung Beteiligten viel zu wenig Rechtsklarheit und Rechtssicherheit gibt. Vielmehr wäre es angebracht, wenn der Gesetzgeber sich für einen abschließenden Numerus clausus der zulässigen Verarbeitungstätigkeiten entscheiden würde.

Derzeit – Anfang 2019 – wird der Text des Verordnungsentwurfs in der Arbeitsgruppe „Telekommunikation und Informationsgesellschaft“ des Europäischen Rats verhandelt. Die Diskussionen werden kontrovers geführt. Obwohl es ursprünglich das Ziel war, dass die E-Privacy-Verordnung das Schutzniveau der DSGVO nicht unterschreiten und die DSGVO lediglich bereichsspezifisch ergänzen und präzisieren soll, gibt es Stimmen, die beispielsweise eine weitreichendere Verarbeitung von Meta- und Standortdaten erlauben wollen. Metadaten sind die Daten, die anfallen, um Kommunikationsinhalte übertragen zu können, wie z. B. die ange-

rufenen Nummern, besuchte Websites, der geografische Standort, Uhrzeit, Datum und Dauer von getätigten Anrufen. Aus ihnen lassen sich präzise Schlussfolgerungen über das Privatleben der an der elektronischen Kommunikation beteiligten Personen ziehen. Schon das Parlament hat darauf hingewiesen, dass Metadaten – da sie bereits in ein strukturiertes und standardisiertes Format überführt wurden – viel einfacher zu verarbeiten und zu analysieren sind als Inhalte. Ihre Verarbeitung sollte daher nur zulässig sein, wenn und solange sie zur Kommunikation notwendig sind. Darüber hinaus gibt es Bestrebungen, eine Regelung aufzunehmen, die sicherstellt, dass die Nutzung werbefinanzierter Online-Dienste davon abhängig gemacht werden kann, dass Nutzer in das Setzen von Cookies für Werbezwecke einwilligen. Die DSGVO enthält in Art. 7 Abs. 4 eine Regelung, die weithin als „Kopplungsverbot" verstanden wird und wonach eine Einwilligung zu einer Verarbeitung von personenbezogenen Daten als unfreiwillig angesehen werden kann, wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von einer solchen Einwilligung abhängig gemacht wird. Würden sich die Positionen durchsetzen, wonach eine solche Kopplung im Online-Bereich zulässig sein soll, hätte dies weitreichende Folgen und das Schutzniveau der DSGVO würde massiv unterschritten.

Die Stellungnahme des Europäischen Datenschutzausschusses, die einen Teil der hier dargestellten Problemkreise und noch weitere behandelt, ist hier abrufbar:

https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-statement-eprivacy-25052018_en

12

KERNPUNKTE

Änderung des IZG-SH nötig

Informationszugang und Ausschlussgründe

Weit gefasste Informationen über Emissionen

12 Informationsfreiheit

12.1 Änderung des IZG-SH nötig – nicht haltbarer Verweis vom IZG-SH ins LDSG-neu

Zur Anpassung an die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) und zur Umsetzung der Richtlinie (EU) 2016/680 ist im Mai 2018 das neue Landesdatenschutzgesetz (LDSG) in Kraft getreten (Tz. 4.1.1). Damit verbunden ist eine gesetzliche Konkretisierung der Aufgaben und Befugnisse der oder des Landesbeauftragten für Datenschutz Schleswig-Holstein für den Bereich der Datenschutzaufsicht über öffentliche Stellen. Dadurch erhält die aufsichtsbehördliche Tätigkeit im Verhältnis zu der beratenden Tätigkeit deutlich mehr Gewicht. Im Gegensatz dazu weist die Tätigkeit der oder des Landesbeauftragten für Datenschutz im Bereich der Informationsfreiheit maßgeblich beratenden Charakter auf.

Der im IZG-SH enthaltene Verweis auf die im LDSG geregelten Aufgaben und Befugnisse der oder des Landesbeauftragten für Datenschutz Schleswig-Holstein ist wegen der unterschiedlichen Ausrichtung beider Gesetze nicht haltbar. So kann beispielsweise die nach dem LDSG (in Verbindung mit der DSGVO) bestehende Anweisungs- und Anordnungsbefugnis der oder des Landesbeauftragten für Datenschutz Schleswig-Holstein nicht auf den IZG-SH-Bereich übertragen werden.

Diese Situation erfordert eine Änderung des IZG-SH, und zwar dahin gehend, dass in das IZG-SH eine eigene und abschließende Regelung für die Aufgaben und Befugnisse der oder des Landesbeauftragten für den Bereich der Informationsfreiheit aufgenommen wird, wie dies auch in Nordrhein-Westfalen (§ 13 IFG NRW), Thüringen (§ 12 ThürIFG) oder Brandenburg (§ 11 AIG Brandenburg) der Fall ist.

Das ULD hat die bestehende unsichere Rechtslage gegenüber dem Ministerium für Inneres, ländliche Räume und Integration des Landes Schleswig-Holstein aufgezeigt.

Was ist zu tun?

Dem Landesgesetzgeber wird empfohlen, in das IZG-SH eine eigenständige Bestimmung aufzunehmen, welche die Aufgaben und Befugnisse der oder des Landesbeauftragten für Datenschutz für den Bereich der Informationsfreiheit regelt.

12.2 Der Begriff der Emissionen aus informationsfreiheitsrechtlicher Sicht

Viele Anträge nach dem IZG-SH beziehen sich auf Informationen über Emissionen. Nach den gesetzlichen Vorgaben kann sich die informationspflichtige Stelle in diesen Fällen auf einige Ausschlussgründe nicht berufen, wie z. B. auf den Schutz der Vertraulichkeit von Beratungen von informationspflichtigen Stellen, auf den Schutz personenbezogener Daten sowie auf Betriebs- und Geschäftsgeheimnisse.

Vor diesem Hintergrund ist von hoher Bedeutung, welche Angaben zu den „Informationen über Emissionen“ zählen. Das IZG-SH enthält dazu keine Begriffsbestimmung. Ein Rückgriff

auf die Definition zu Emissionen im Bundesimmissionsschutzgesetz kommt nicht in Betracht, da der Europäische Gerichtshof (EuGH) für den Bereich der Informationsfreiheit den Begriff bestimmt und dessen Reichweite definiert hat (EuGH, Urteile vom 23.11.2016, C-442/14; C-673/13). Danach sind unter den Begriff „Informationen über Emissionen in die Umwelt" nicht nur die Angaben über Emissionen als solche erfasst (wie etwa Angaben über Art, Zusammensetzung, Menge, Zeitpunkt und Ort dieser Emissionen), sondern auch die Daten über die Auswirkungen auf die Umwelt. Nach Auffassung des EuGH bedeutet dies für Umweltauswirkungen bei Anwendung eines Produkts, dass zu den Emissionsdaten z. B. Informationen über die Rückstände in der Umwelt nach der Anwendung des Produkts und Studien zur Messung der Stoffdrift bei dieser Anwendung gehören, unabhängig davon, ob diese Daten aus Feldstudien, aus Laboruntersuchungen oder aus Translokationsstudien stammen. Weitere Informationen gibt der Leitfaden des ULD „Bauakten und Informationszugangsgesetz Schleswig-Holstein", Ziffer II.3:

https://www.datenschutzzentrum.de/uploads/informationsfreiheit/ULD-Leitfaden-Bauakten-IZG_SH.pdf

Was ist zu tun?

Bei Anträgen nach dem IZG-SH ist zu prüfen, ob der Zugang zu Informationen über Emissionen begehrt wird. Dabei kann sich die informationspflichtige Stelle nicht auf jedweden gesetzlichen Ausschlussgrund berufen.

12.3 IZG-SH und Urhebergesetz

Im IZG-SH wurden Ausschlussgründe normiert, die dem Schutz privater Interessen dienen. Einer dieser Ausschlussgründe bezieht sich auf den Schutz der Rechte am geistigen Eigentum, insbesondere auf das Urheberrecht (§ 10 Satz 1 Nr. 3 IZG-SH). Soweit durch die Bekanntgabe von Informationen Urheberrechte verletzt würden und schutzwürdige private Interessen an der Geheimhaltung gegenüber dem öffentlichen Bekanntgabeinteresse überwiegen, ist der Antrag auf Zugang zu Informationen abzulehnen, es sei denn, die jeweils Betroffenen haben zugestimmt.

Urheberrechte stehen einem Informationszugang folglich dann entgegen, wenn es sich bei den begehrten Informationen

- um ein urheberrechtlich geschütztes Werk im Sinne von § 2 Abs. 2 Urhebergesetz handelt,
- kein Nutzungsrecht eingeräumt worden ist, das die behördliche Genehmigung des Informationszugangs einschließt, und
- der Urheber in die Gewährung des Informationszugangs nicht eingewilligt hat bzw. das Geheimhaltungsinteresse gegenüber dem öffentlichen Bekanntgabeinteresse überwiegt.

Für den Schutz von Urheberrechten ist es unerheblich, ob es sich um Informationen zu Emissionen, sonstige Umweltinformationen oder andere Informationen handelt. Liegen die Voraussetzungen des Ausschlusses nach § 10 Satz 1 Nr. 2 IZG-SH vor, kommt ein Informationszugang, gleich um welche Art der Informationen es sich handelt, nicht in Betracht. Das ULD hat einen ausführlichen Beitrag zu diesem Thema veröffentlicht. Dieser ist abrufbar unter:

https://www.datenschutzzentrum.de/artikel/1250-.html

Was ist zu tun?

Die informationspflichtige Stelle muss in jedem Einzelfall prüfen, ob dem beantragten Informationszugang Urheberrechte Dritter entgegenstehen. Vor der Entscheidung über die Offenbarung der urheberrechtlich geschützten Informationen sind die betroffenen Dritten anzuhören, wobei ermittelt werden kann, ob eine Einwilligung in die Weitergabe der Information an den Antragsteller erteilt wird.

12.4 Keine Herausgabe von Informationen, die laufende Gerichtsverfahren betreffen

Mitunter kommt es vor, dass IZG-SH-Anfragen an Verwaltungseinrichtungen als informationspflichtige Stellen gerichtet sind und Informationen betreffen, die dort zwar vorhanden sind, jedoch laufende Verfahren bei Gericht betreffen. In diesen Fällen stellt sich die Frage, ob und wenn ja, in welchem Umfang diese Informationen herausgegeben werden dürfen.

Dies richtet sich nach § 9 Abs. 1 Nr. 4 IZG-SH. Danach dürfen die Informationen von der informationspflichtigen Stelle nicht herausgegeben werden, soweit dies nachteilige Auswirkungen u. a. auf die Durchführung eines laufenden Gerichtsverfahrens hätte und das öffentliche Interesse an der Geheimhaltung gegenüber dem öffentlichen Bekanntgabeinteresse überwiegt. Das bedeutet: Dieser Ausschlussgrund gilt nur für die Dauer des laufenden Gerichtsverfahrens.

Mit der Regelung des § 9 Abs. 1 Nr. 4 IZG-SH soll die Funktionsfähigkeit der Rechtspflege gewährleistet werden. Dieser Ausnahmegrund greift immer dann ein, wenn entsprechend dem Zweck des Schutzes der Rechtspflege und der Rechtsdurchsetzung eine Verfahrensbeeinträchtigung zumindest möglich erscheint. Diese Möglichkeit kann beispielsweise dann gegeben sein, wenn durch das Bekanntwerden der betreffenden Informationen möglicherweise der Druck der öffentlichen Meinung auf den entscheidungsbefugten Spruchkörper einwirken könnte, wodurch letztendlich die Richtigkeit des Verfahrensergebnisses nicht mehr gewährleistet sein könnte. Um beurteilen zu können, ob eine solche Gefährdungslage möglich erscheint, bietet es sich an, dass die informationspflichtige Stelle beispielsweise das Gericht um eine entsprechende Stellungnahme bittet.

Hervorzuheben ist, dass sich der Ausschlussgrund nach § 9 Abs. 1 Nr. 4 IZG-SH nicht auf Gerichte bezieht. Gerichte sind vielmehr, sofern sie als Organe der Rechtspflege tätig sind, vom Anwendungsbereich des IZG-SH nicht erfasst (§ 2 Abs. 4 Nr. 3 IZG-SH).

Was ist zu tun?

Beziehen sich die bei den informationspflichtigen Stellen vorhandenen begehrten Informationen auf ein laufendes Gerichtsverfahren, haben die informationspflichtigen Stellen insbesondere den Ausschlussgrund nach § 9 Abs. 1 Nr. 4 IZG-SH zu prüfen.

12.5 Informationspflicht öffentlicher Schulen

Im Rahmen einer Eingabe war zu klären, ob öffentliche Schulen in Schleswig-Holstein als informationspflichtige Stellen zu erachten sind. Maßgebend für die Beurteilung war der Umstand, dass nach dem IZG-SH insbesondere Behörden des Landes, der Gemeinden, Kreise und Ämter sowie die sonstigen juristischen Personen des öffentlichen Rechts zu den informationspflichtigen Stellen zählen. Nach den schulrechtlichen Vorgaben sind öffentliche Schulen solche Schulen, deren Träger das Land, die Kreise, die Gemeinden oder die gesetzlich bestimmten Körperschaften des öffentlichen Rechts ohne Gebietshoheit sind. Die öffentlichen Schulen sind nicht rechtsfähige Anstalten des öffentlichen Rechts des Schulträgers. Soweit die Schulen als nicht rechtsfähige Anstalten aufgrund des Schulgesetzes Verwaltungsakte an Schülerinnen und Schüler oder Eltern richten, gelten sie als untere Landesbehörden (§ 2 Abs. 2 des Schulgesetzes Schleswig-Holstein).

In Abstimmung mit dem Ministerium für Bildung, Wissenschaft und Kultur Schleswig-Holstein vertritt das ULD die Auffassung, dass es sich bei öffentlichen Schulen um informationspflichtige Stellen nach § 2 Abs. 3 Nr. 1 IZG-SH handelt. Das bedeutet, dass öffentliche Schulen bei Anträgen nach dem IZG-SH zunächst zu prüfen haben, ob spezialgesetzliche Regelungen (z. B. § 89 Abs. 4 Landesbeamtengesetz SH für den Bereich der Personalaktendaten) der Anwendung des IZG-SH entgegenstehen könnten (36. TB, Tz. 12.8). Ist dies nicht der Fall, ist zu prüfen, ob Ausschlussgründe nach §§ 9, 10 IZG-SH dem beantragten Informationszugang entgegenstehen könnten.

Was ist zu tun?

Öffentliche Schulen in Schleswig-Holstein sind informationspflichtige Stellen, müssen aber im Falle eines Zugangsantrags zunächst etwaige spezialgesetzliche Regelungen prüfen, die einer Anwendung des IZG-SH generell entgegenstehen können. Ist dies nicht der Fall, wird das IZG-SH angewendet.

13

KERNPUNKTE

Datenschutzbildung und -fortbildung

DATENSCHUTZAKADEMIE

Sommerakademie

13 DATENSCHUTZAKADEMIE Schleswig-Holstein

Das Landesdatenschutzgesetz Schleswig-Holstein formulierte in seiner Fassung vor dem 25.05.2018 in § 43 Abs. 3 als Auftrag, dass „das Unabhängige Landeszentrum für Datenschutz Fortbildungsveranstaltungen zu den Themen Datenschutz und Datensicherheit durchführt". Auch die Datenschutz-Grundverordnung betont die Wichtigkeit des Fachwissens bei den behördlichen und betrieblichen Datenschutzbeauftragten. 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) und „die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten sensibilisieren (Art. 57 Abs. 1 Buchst. e) – auch dafür werden Veranstaltungen angeboten. Für die Konzeption und Organisation dieser Veranstaltungen ist seit 1993 die DATENSCHUTZAKADEMIE Schleswig-Holstein verantwortlich.

13.1 Fortbildungsveranstaltungen im Programm der DATENSCHUTZAKADEMIE

Im Schulungsjahr 2017 hat die DATENSCHUTZAKADEMIE mehr als 55 Schulungsveranstaltungen durchgeführt. Dabei ließen sich über 750 Teilnehmende von den Dozentinnen und Dozenten der DATENSCHUTZAKADEMIE zu dem vielfältigen Themenbereich von Datenschutz, Datensicherheit und Informationsfreiheit fortbilden. Im Schulungsjahr 2018 waren mehr als 80 Veranstaltungen und 1.200 Teilnehmende zu verzeichnen. Die Steigerung der Nachfrage ist sicherlich auf die Einführung der DSGVO zurückzuführen.

Die seit Jahren durchgeführten behördlichen Grundlagenkurse der DATENSCHUTZAKADEMIE werden kontinuierlich gut angenommen und bilden damit eine solide Grundlage für datenschutzkonformes Handeln in schleswig-holsteinischen Landesbehörden und kommunalen Verwaltungen. Diese sind:

- Datenschutzrecht für behördliche Datenschutzbeauftragte
- Datensicherheit in der Verwaltung
- Informationszugangsgesetz SH
- Datenschutz im E-Government
- Grundlagen der Dokumentation

Der dreitägige Lehrgang „Betrieblicher Datenschutz Kompakt" bietet in handlungsoptimierter und praxisbezogener Form betrieblichen Datenschutzbeauftragten eine gute Grundlage für ihre Tätigkeit.

Zum Angebot für Wirtschaft, Vereine und Verbände gehörten im Berichtszeitraum ebenso:

- Beschäftigtendatenschutz
- Das Standard-Datenschutzmodell
- Datenschutz-Folgenabschätzung

Im Themenschwerpunkt „Technischer Datenschutz und Datensicherheit" werden die folgenden Kurse veranstaltet:

- Datenschutzmanagement
- IT-Grundschutz nach BSI
- Datenschutzkontrolle, Sicherheitschecks und Datenschutzaudits
- Datenschutzlecks in Behörden und Unternehmen
- Mit dem Grundschutztool „Verinice" zum IT-Sicherheitskonzept

Diese Kurse befähigen die Absolventen, die Sicherheit von Verfahren oder Geschäftsprozessen und die Verwaltung von IT-Verbünden von Organisationen mithilfe der IT-Grundschutzmethode umzusetzen.

Fortbildungsangebote im Bereich Medizin erfuhren durch die DSGVO eine stark gestiegene Nachfrage. In Zusammenarbeit mit der Zahnärztekammer Schleswig-Holstein hat die DATENSCHUTZAKADEMIE im Jahr 2018 insgesamt fünf Sonderkurse durchgeführt.

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 2011 eingeführten Schülerkurse „Entscheide DU – sonst tun es andere für dich!“ erfreuen sich im Berichtszeitraum weiterhin großer Beliebtheit. Mehr als 2.000 Schülerinnen und Schüler im Jahr 2017 und mehr als 2.600 Schülerinnen und Schülern im Jahr 2018 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 aktuelle Jahresprogramm der DATENSCHUTZAKADEMIE finden Sie unter:

https://datenschutzzentrum.de/akademie/programm/

13.2 Sommerakademie – jährliche Datenschutzkonferenz in Kiel

Die alljährlich an einem Montag im Spätsommer stattfindende Sommerakademie der DATENSCHUTZAKADEMIE zog in den Jahren 2017 und 2018 wieder knapp 400 bzw. 500 Datenschutzexperten und Interessierte aus dem gesamten Bundesgebiet und darüber hinaus nach Kiel.

Mit dem Thema „Herausforderung ‚Informationelle Nichtbestimmung‘“ im Jahr 2017 wurden gesellschaftspolitische Fragen zur informationellen Selbstbestimmung, Fremdbestimmung und Nichtbestimmung diskutiert (Tz. 2.2.1).

Die Sommerakademie im Jahr 2018 widmete sich dem Thema des Beschäftigtendatenschutzes. Unter der Überschrift „Update nötig: Beschäftigtendatenschutz im digitalen Zeitalter 4.0“ stellten die Vortragenden vor, welche Veränderungen sich durch die Digitalisierung im Arbeitsleben ergeben, welche Gestaltungsoptionen es gibt und welcher Regelungsbedarf in Deutschland und auf europäischer Ebene besteht (Tz. 2.2.2).

Index

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Y

Z

ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

Schleswig-Holsteins
Zentrum für Datenschutz
und Informationszugang

https://www.datenschutzzentrum.de/tb/